

Enigma bez tajemnic

85. rocznica sukcesu polskich kryptologów

redakcja naukowa

Marek Grajek

RECENZENT
prof. dr hab. Lech Wyszczelski

REDAKTOR PROWADZĄCY
Paweł Jaroniak

REDAKTOR TECHNICZNY
Miroslaw Głodkowski

KOREKTA
Zespół

PROJEKT OKŁADKI
Aleksandra Bednarczyk

© Copyright by Wydawnictwo Adam Marszałek
© Copyright by Agencja Bezpieczeństwa Wewnętrznego

Wszystkie prawa zastrzeżone. Książka, którą nabyłeś, jest dziełem twórcy i wydawcy.
Żadna jej część nie może być reprodukowana jakimkolwiek sposobem – mechanicznie, elektronicznie,
drogą fotokopii itp. – bez pisemnego zezwolenia wydawcy. Jeśli cytujesz fragmenty tej książki,
nie zmieniaj ich treści i koniecznie zaznacz, czyje to dzieło

Toruń 2020

ISBN 978-83-8180-382-3

Projekt realizowany w ramach obchodów stulecia odzyskania niepodległości
oraz odbudowy polskiej państwowości

Wydawnictwo Adam Marszałek
ul. Lubicka 44, 87-100 Toruń, tel. 56 664 22 35
e-mail: info@marszalek.com.pl, www.marszalek.com.pl
Drukarnia, ul. Warszawska 54, 87-148 Łysomice, tel. 56 678 34 78

Spis treści

Zamiast wstępu	5
Marek Grajek Enigma po Enigmie – przyczynek do dziejów pewnej dezinformacji	11
Marek Grajek, Jan Stanisław Ciechanowski Płk Gwido Karol Langer i mjr Maksymilian Ciężki – architekci sukcesu polskich kryptologów	29
Marek Grajek Odnaleziony raport – czego nowego dowiedzieliśmy się o historii złamania Enigmy?	41
Kamil Kulesza Łamanie Enigmy jako przykład rozwiązywania praktycznych problemów za pomocą matematyki – wnioski na dziś	59
Krzysztof Osiński Marian Rejewski – pogromca niemieckiej maszyny szyfrującej Enigma	77
Elżbieta Szczuka O Jerzym Różyckim i jego rodzinie	113
Patryk Piłasiewicz Henryk Zygański i muzyka szyfrów	123

Zamiast wstępu

W ostatnich trzech dekadach wiele się zmieniło w narracji poświęconej historii złamania szyfrów Enigmy. Przez 30 powojennych lat był to jeden z najpilniej strzeżonych sekretów trwającej zimnej wojny. Po obu stronach żelaznej kurtyny korzystano bowiem wtedy z wirnikowych maszyn szyfrujących, których konstrukcja stanowiła udoskonalenie rozwiązań zastosowanych w Enigmie. To wykluczało publiczną dyskusję na temat sukcesów kryptologów, które znacząco wpłynęły na losy drugiej wojny światowej. Taki stan rzeczy utrzymał się nawet po ujawnieniu w 1973 r. sukcesu polskich matematyków i dalszych, już wojennych, losów dokonanego przez nich kryptologicznego przełomu. Wirnikowe maszyny szyfrujące były wykorzystywane operacyjnie do połowy lat 80. XX w., toteż służby specjalne państw anglosaskich zgodnie uznały, że sekret złamania Enigmy został ujawniony zdecydowanie przedwcześnie. W związku z tym podjęły stanowcze działania, aby ukryć prawdę na ten temat za pomocą dezinformacji. Zmianę polityki przyniósł dopiero postęp w dziedzinie elektroniki, który pozwolił w połowie lat 80. zastąpić wirnikowe maszyny szyfrujące nową generacją urządzeń, już w pełni elektronicznych. Mimo to jeszcze opublikowanie w latach 1982–1983 wspomnień Gordona Welchmana z jego wojennej pracy w ośrodku kryptologicznym w Bletchley Park przysporzyło mu ze strony byłych kolegów z brytyjskiego i amerykańskiego wywiadu dużych przykrości, które przyczyniły się do jego przedwczesnej śmierci. Wkrótce potem rozpoczął się jednak proces stopniowego odtajniania przez amerykańskie i brytyjskie archiwa dokumentów źródłowych dotyczących kryptologicznego wysiłku aliantów w czasie wojny. Proces ujawniania tych materiałów trwa, w zmiennym rytmie, do dziś.

Upublicznienie tego rodzaju dokumentów sprawiło, że wielu bezpośrednich uczestników wydarzeń poczuło się zwolnionych z obowiązku

respektowania tajemnicy, do czego zostało zobligowanych z chwilą zakończenia swojego udziału w pracach dekrytażowych podczas wojny. Ich wspomnienia uzupełniły suchą, oficjalną narrację raportów złożonych w archiwach i pozwoliły historykom oraz kryptologom zrekonstruować poprawny i – jak się wydaje – wierny historycznej prawdzie obraz wydarzeń związanych z Enigmą. Ten obraz okazał się fascynujący dla odbiorców zainteresowanych drugą wojną światową, kryptologią i matematyką. Historycy odkryli, że kilkadziesiąt lat po zakończeniu wojny należałoby zrewidować liczne dogmaty dotyczące dziejów tego konfliktu, przejrzeć poświęconą mu literaturę i wprowadzić w niej wiele poprawek. Kryptolodzy i matematycy stwierdzili, że korzenie współczesnej kryptologii matematycznej sięgają zdecydowanie głębiej, niż byli skłonni sądzić do tej pory. Atrakcyjność tematu i jego znaczenie dla wielu obszarów badań sprawiły, że w minionych 20–30 latach nastąpił ogromny wzrost liczby poświęconych mu prac naukowych. Dzięki temu środowisko historyków wypracowało konsensus co do rzeczywistego przebiegu wydarzeń związanych ze złamaniem szyfrów Enigmy oraz znaczenia, jakie miały poszczególne wątki tej historii. Pojawiające się nowe dokumenty źródłowe oraz nowe interpretacje nie przyczyniają się już do jego znaczącej modyfikacji, gdyż z reguły dotyczą kwestii o niewielkim znaczeniu dla głównego nurtu wydarzeń.

Na tym tle pomysł zorganizowania kolejnej konferencji, której przewodnim motywem miała być historia z Enigmą w tle, wydawał się kontrowersyjny. Z uwagi na wyczerpanie tematu w dostępnej literaturze próba nowego spojrzenia na powszechnie znane fakty wymagała zdefiniowania odmiennego od dotychczasowych punktu odniesienia oraz zaproszenia do udziału w konferencji uczestników zdolnych wypełnić tak wyznaczone ramy interesującą i nowatorską treścią. Takim nowym punktem odniesienia stał się zamiar spojrzenia na polskich uczestników kryptologicznego przełomu z czysto ludzkiej, a nie – jak dotąd – głównie historycznej perspektywy. Pytanie o ich zawodowe dokonania zostało zastąpione pytaniem o to, jakie cechy charakteru złożyły się na ich

indywidualny oraz kolektywny, tj. Biura Szyfrów, sukces. Czy wpływ na to miały ich wcześniejsze doświadczenia życiowe? Czy, a jeśli tak, to w jakim stopniu do sukcesu przyczyniły się różnice osobowościowe i odmienne postawy członków zespołu? Wreszcie – jaką rolę odegrała intelektualna atmosfera panująca w środowisku międzywojennego polskiego wywiadu?

Tak zdefiniowane ujęcie tematu okazało się interesujące poznawczo. Już we wcześniejszych dyskusjach w gronie badaczy zajmujących się historią złamania Enigmy pojawiał się wątek niepowtarzalnego splotu talentów i zainteresowań członków zespołu jako kluczowego warunku sukcesu. Było to połączenie wiedzy i kompetencji w zakresie matematyki abstrakcyjnej, teorii grup oraz inżynierii elektromechanicznej. Należy w tym miejscu podkreślić, że żadna z wymienionych dyscyplin nie należała ani do klasycznego instrumentarium działania służb specjalnych, ani do głównego nurtu kryptologii okresu międzywojennego. Sięgnięcie w 1928 r. po pomoc matematyków stanowiło rozwiązanie pionierskie, które inne państwa świata zaczęły naśladować dopiero, gdy poznały efekty jego zastosowania przez Polaków. Nawet wtedy jednak proces wdrażania matematyki i matematyków w praktykę dekryptażu nie był łatwy i natychmiastowy. Szef ówczesnej brytyjskiej służby kryptologicznej Alastair Denniston już po powrocie z konferencji w Pyrach w lipcu 1939 r. nalegał, aby w jego służbie zatrudniać raczej fizyków niż matematyków, ponieważ ci pierwsi dysponowali – jego zdaniem – przynajmniej elementarnym kontaktem z rzeczywistością. Nieco wcześniej Niemcy przeorientowali nielicznych matematyków zatrudnionych w ich komórkach kryptologicznych na próby zastosowania matematyki do badania bezpieczeństwa własnych szyfrów. Z fatalnym rezultatem. Ich matematycy sumiennie obliczyli liczbę kombinacji elementów szyfru, po czym orzekli, że jej wielkość stanowi gwarancję jego bezpieczeństwa. Trzeba zatem podkreślić, że przed Polakami nikt nie wykorzystał, pomijając elementarne zastosowania statystyki do łamania szyfrów historycznych (analiza częstości występowania znaków tekstu jawnego),

zaawansowanych metod matematycznych do łamania szyfru. Posługiwano się nimi jedynie w analizie jego teoretycznego bezpieczeństwa.

Wszelkie dane wskazują, że inicjatorem rewolucyjnego podejścia do dekryptażu był Maksymilian Ciężki. Ciężki nie ukończył szkoły rolniczej w rodzinnych Szamotułach z powodu powołania do wojska w czasie pierwszej wojny światowej, egzamin maturalny zdał eksternistycznie w trakcie służby w Wilnie, a mundur założony w wieku 17 lat zdjął dopiero po zakończeniu drugiej wojny światowej. Chyba żadne z doświadczeń życiowych nie wpoilo mu przesadnego szacunku dla matematyki. Od Jana Kowalewskiego znał jednak historię udziału matematyków w łamaniu sowieckich szyfrów w 1920 r. i potrafił wyciągnąć z niej właściwe wnioski. Można jednak wątpić, czy przedstawiona przez niego długofalowa strategia łamania szyfrów Enigmy znalazłaby uznanie wyższych przełożonych, gdyby nie wsparcie ze strony Franciszka Pokornego, oficera dowodzącego Biurem Szyfrów. Pokorny w trakcie służby w armii austriackiej, a później także w szeregach polskiej Dywizji Syberyjskiej był instruktorem topografii wojskowej. U topografa, dla którego matematyka stanowi jedno z naturalnych narzędzi opisu rzeczywistości, propozycja Ciężkiego miała szansę spotkać się nie tylko ze zrozumieniem, lecz także z poparciem.

Przewrotność historii oraz, mimo wszystko, wysokie kompetencje kryptologicznego adwersarza sprawiły jednak, że polski sukces nie zapisały się w historii, gdyby nie drugi konieczny składnik – talenty inżynierskie pozostałych członków zespołu. Zmiany w sposobie użycia Enigmy wprowadzone przez Niemców we wrześniu 1938 r. spowodowały, że czysta matematyka przestała wystarczać do złamania szyfru. W krytycznym momencie okazało się jednak, że zespół Biura Szyfrów dysponuje także innymi umiejętnościami, pozwalającymi zapewnić kontynuację dekryptażu. Charakterystyczne przemilczenia zawarte w powojennych wspomnieniach Mariana Rejewskiego pozwalają sądzić, że nie cenił on zbyt wysoko własnej koncepcji bomby kryptoanalitycznej – elektromechanicznego urządzenia umożliwiającego potwierdzenie lub zanegowanie

w rozsądnym czasie określonej hipotezy dotyczącej aktualnych ustawień maszyny szyfrującej. Wydaje się, że jako rasowy matematyk uznawał konieczność sięgnięcia po jej pomoc za porażkę własnej dyscypliny naukowej. Miał prawo do pewnego dystansu – ani w czasie wojny, ani po jej zakończeniu Rejewski nie poznał dalszego ciągu technologicznej przygody, którą zainicjował, prezentując koncepcję bomby. Nie wiedział zatem, że w rękach jego brytyjskich i amerykańskich naśladowców i kontynuatorów rozwinęła się ona w rodzinę urządzeń, które w okresie drugiej wojny światowej stanowiły główne narzędzie łamania niemieckich szyfrów, a po jej zakończeniu okazały się bodźcem do powstania pierwszych elektronicznych komputerów.

Można spekulować, czy historia złamania szyfru i zapewne dzieje drugiej wojny światowej potoczyłyby się w znany nam sposób, gdyby w przedwojennym Biurze Szyfrów i w jego otoczeniu zabrakło ludzi zdolnych do przekształcenia teoretycznej koncepcji Rejewskiego w funkcjonalną konstrukcję oraz udowodnienia jej skuteczności w łamaniu szyfru. Dostępne informacje na temat obu oficerów dowodzących Biurem Szyfrów, Gwidona Langera i Maksymiliana Ciężkiego, potwierdzają ich techniczne zainteresowania i talenty. Swego czasu odpowiedzieli oni na zastosowanie przez Niemców Enigmy skonstruowaniem polskiej maszyny szyfrującej LCD. W zachowanych w archiwach rocznych ocenach obu oficerów ich kompetencje techniczne zostały wysoko oszacowane. Ze wspomnień członków ich rodzin wiadomo, że obaj zgromadzili obszerne biblioteki literatury technicznej i nie unikali weryfikacji swej wiedzy w praktyce, często stając przy desce kreślarskiej lub stole warsztatowym. Ich mentorem mógł być podwładny i jednocześnie bliski przyjaciel Antoni Palluth, jeden z pionierów polskiego ruchu krótkofalarskiego, utalentowany konstruktor sprzętu radiowego i jednocześnie sprawny menedżer zarządzający firmą AVA, będącą głównym dostawcą specjalistycznego sprzętu dla polskiego radiowywiadu. Wspólnie byli w stanie realizować projekty techniczne wyprzedzające ich czasy. Gdy Rejewski zaproponował pokonanie chwilowego kryzysu w dekrypcji

dzięki wykorzystaniu dedykowanego urządzenia elektromechanicznego, zdołali w rekordowym czasie (w ciągu miesiąca) zorganizować dostawę sześciu egzemplarzy. Matematycy z Biura Szyfrów dokonali rewolucji w kryptoanalizie, stosując po raz pierwszy zaawansowane metody matematyczne. Związani z nim oficerowie i inżynierowie udowodnili, że najskuteczniejszym przeciwnikiem maszyny szyfrującej jest maszyna ułatwiająca proces dekryptażu. Gdyby nie efekty ich pracy, prezentacja polskich osiągnięć podczas spotkania w Pyrach byłaby zdecydowanie mniej spektakularna i przekonująca dla odbiorców. Jego brytyjscy uczestnicy niezwłocznie po powrocie z Polski przystąpili do projektowania własnych odpowiedników bomby Rejewskiego, a efekt ich pracy, bomba Turinga, stanowił klucz do zwycięstwa w kryptologicznym pojedynku trwającym do końca drugiej wojny światowej.

To tylko nieliczne przykłady ilustrujące, w jaki sposób osobiste cechy oraz doświadczenia ludzi związanych z Biurem Szyfrów przyczyniły się do jego przedwojennych i wojennych sukcesów. Materialiści są skłonni twierdzić, że historia jest procesem obiektywnym, niezależnym od działań jednostek. Przyjmując ten punkt widzenia, można skonstatować, że szyfry Enigmy zostałyby złamane niezależnie od pracy Polaków, wymagała tego bowiem wojenna konieczność. Historię tworzą jednak działania jednostek, w których uzewnętrzniają się ich indywidualne predyspozycje i umiejętności. Na polskich twórców sukcesu złamania szyfrów Enigmy warto zatem spojrzeć jako na tych, którzy do zespołowego wysiłku wnieśli własny, znaczący wkład.

W imieniu uczestników konferencji dziękuję kierownictwu Agencji Bezpieczeństwa Wewnętrznego oraz Centralnego Ośrodka Szkolenia i Edukacji ABW za możliwość spojrzenia na dobrze znaną historię z perspektywy nieco odmiennej od tradycyjnych ujęć. Wszystkim autorom dziękuję z kolei za wysiłek włożony w zaprezentowanie bohaterów tej historii w nowy sposób, wydobywający na światło dzienne nieznane wcześniej aspekty ich życia i pracy.

Marek Grajek

Marek Grajek

Enigma po Enigmie – przyczynek do dziejów pewnej dezinformacji

Historia ujawnienia światu dziejów złamania szyfru Enigmy jest równie zagmatwana i fascynująca jak dzieje samego sukcesu polskich kryptologów. Gdy spoglądamy na nią z perspektywy drugiego dziesięciolecia XXI w., okazuje się, że na kanwę wytyczoną przez fakty nałożyło się z czasem kilka dodatkowych warstw narracji, które łącznie sprawiły, że rekonstrukcja prawdziwego przebiegu wydarzeń stała się wyzwaniem dla historyków i kryptologów. A gdy specjaliści obu dyscyplin zakończyli pracę, uznając, że prawda o złamaniu Enigmy jest powszechnie znana i dostępna zainteresowanym, okazało się, że nie jest ona wystarczająco atrakcyjna dla dostawców kultury masowej. Autorzy sensacyjnych książek i filmowi scenarzyści przetworzyli fakty w historie atrakcyjne dla czytelnika i widza, choć jedynie symbolicznie nawiązujące do prawdziwych wydarzeń.

W rezultacie w potocznej świadomości funkcjonuje wiele wersji historii złamania szyfrów Enigmy. Wzmianka o niej w rozmowie tocznej w Polsce spowoduje z reguły pełne zrozumienie skinieniem głowy rozmówcy: dla Polaków jest oczywiste, że autorami sukcesu byli ich rodacy. Jednak identyczna wzmianka w trakcie podróży po świecie może przynieść zaskakujący wynik. W rozmowie z Niemcem możemy się dowiedzieć, że szyfru Enigmy nigdy nie złamano; z Brytyjczykiem – że złamał ją genialny matematyk Alan Turing; z Amerykaninem – że sekret szyfrów gdzieś na Atlantyku zdobyli dzielni amerykańscy marynarze. Na dobrą sprawę rezultat zależy głównie od tego, który z sensacyjnych

filmów z historią złamania szyfru Enigmy w tle obejrzał ostatnio rozmówca. Zniekształcenia historycznej prawdy o Enigmie miały swoje źródła w kilku mechanizmach, które w różnych okresach działały z różną intensywnością. Wszystko zaczęło się od urażonej dumy, do której z czasem dołączyła niewiedza z domieszką spekulacji, dużo później w ślad za nimi podążyła świadoma dezinformacja, a najpóźniej dołączyły potrzeba konsekwencji oraz zwykła fantazja. Spróbujmy wspólnie prześledzić, w jaki sposób wpływały one kolejno na pamięć o prawdziwej historii złamania szyfru.

Wszystko rozpoczęło się w lipcu 1939 r. Polski wywiad, przekonany o nadchodzącym wybuchu wojny, uzyskał zgodę szefa Sztabu Głównego na ujawnienie polskiego sukcesu w zmaganiach z Enigmą przyszłym aliantom. Przez cały pierwszy dzień zwołanej w podwarszawskich Pyrach konferencji brytyjscy i francuscy kryptolodzy przysłuchiwali się prezentacjom polskich kolegów o historii zmagania z szyframi Enigmy. Kiedy czytamy ich relacje ze spotkania, nietrudno wychwycić emocje, które stały się udziałem jego uczestników. Francuz kapitan Gustave Bertrand miał pretensje do gospodarzy ogniskujące się wokół dwóch kwestii. Pierwszą była swego rodzaju maskarada, którą Polacy uprawiali wobec Francuzów w ciągu ostatnich lat. Bertrand od 1931 r. dostarczał polskiemu wywiadowi dokumenty dotyczące Enigmy, które sam kupował od sprzedajnego urzędnika niemieckiej służby kryptograficznej. Udostępniał Polakom informacje przy założeniu wzajemności wymiany; oczekiwał, że Polacy podzielą się jakimikolwiek wynikami, które osiągną, wykorzystując przekazane dane. Gdy w przeddzień konferencji dowiedział się o polskim sukcesie w zmaganiach z szyfrem Enigmy, uznał za pewnik Polaków o oparciu przełomu na podstawach zupełnie odmiennych od dostarczonych dokumentów za uprzejme kłamstwo. Nie dał poznać po sobie zawodu, jednak z wydanych w wiele lat po opisywanych wydarzeniach wspomnień wygląda oblicze człowieka, który nie zwykł zapominać urazy. Bertrand był poirytowany także zaproszeniem do Warszawy Brytyjczyków. Uważał, że trwająca od kilku lat współpraca

kryptologiczna Francji i Polski upoważnia go do zajęcia uprzywilejowanej pozycji, czego nie można powiedzieć o Brytyjczykach, którzy włączyli się do wspólnych prac dopiero w styczniu 1939 r.

Obecni przy stole Brytyjczycy, a co najmniej jeden z nich, Dillwyn Knox, mieli odmienne powody do irytacji. Uważali kryptologię za własne boisko. Government Codes and Ciphers School (G.C.&C.S.), ich służba kryptologiczna, wyrosła z sukcesów brytyjskich kryptologów w okresie pierwszej wojny światowej. Prawda, Francuzi mieli równie piękną tradycję sukcesów w łamaniu szyfrów przeciwnika w czasie Wielkiej Wojny, w odróżnieniu jednak od Brytyjczyków zaprzepaścili ją w powojennym okresie. Polaków Knox znał słabo. Swoją opinię o nich opierał na wynikach poprzedniego, jedyne do tej pory spotkania kryptologów trzech państw w Paryżu w styczniu 1939 r. Prezentacje przedstawicieli polskiego Biura Szyfrów nie zrobiły na nim wtedy wrażenia. W raporcie ze spotkania spisany po powrocie do Londynu określił Polaków mianem „głupców i ignorantów”. Jednak w trakcie bieżącego spotkania owi „głupcy i ignoranci” usiłowali udzielać mu lekcji rozwiązywania problemów, na których załamały się jego własne ataki na szyfr Enigmy.

Przy stole zgromadzili się profesjonaliści tajnych służb, więc w trakcie obrad nie dawali poznać po sobie emocji. Ujawniły się one dopiero, gdy wieczorem uczestnicy spotkania wsiedli do samochodów, które miały odwieźć ich do hoteli w stolicy. Ówczesny szef brytyjskich kryptologów Alastair Denniston zapisał po powrocie z Warszawy, że Knox siedział przez cały dzień naburmuszony, nie odzywając się ani słowem. Dopiero w samochodzie „nagle otworzył się i zakładając, że żadna z osób towarzyszących nie zna angielskiego, pieniał się i pieklił, że [Polacy] kłamią tak samo, jak robili to w Paryżu. [Cały ich sukces] był oparty na kradzieży. Nigdy tego nie rozpracowali, musieli to ukraść przed laty, a następnie obserwowali rozwój, jak każdy by potrafił, jednak na początku musieli to ukraść lub kupić”. Denniston zrezygnował z komentowania pozostałych wypowiedzi i zachowań Knoxa, z innych źródeł wiemy jednak, że z ich powodu wieczorem pierwszego dnia konferencji rozważał rezygnację

z dalszego udziału i natychmiastowy wyjazd do Londynu, by uniknąć dyplomatycznego skandalu w kolejnych dniach.

Sam Knox po powrocie do Londynu, 30 lipca 1939 r., opracował raport, w którym zapisał: „Spójrzmy na sprawę wprost. Polacy czytali maszynę do 15 września 1938 r. dzięki szczęściu. (...) Jeśli chcemy tego [dekryptażu Enigmy] spróbować, musimy przeanalizować ich system i statystyki (jeśli je mamy) ze znacznym sceptycyzmem. (...) Jestem przekonany, że Schessky [Ciężki] niewiele wie o maszynie i zapewne próbuje ukrywać przed nami fakty. Młodzi ludzie [trójka kryptologów] wydają się zdolni i uczciwi”. Kilka bezcennych zdań zachowanych w archiwum obrazuje najwcześniejszą i najbardziej autentyczną brytyjską reakcję na polskie rewelacje. Można zrozumieć rozczarowanie Knoxa. Został zaskoczony przez sukces zawodowych kolegów odniesiony na boisku, które do tej pory zwykł traktować jako własne. Co gorsza, wobec braku przygotowania matematycznego nie był w stanie nadażyć za ich wyjaśnieniami. Niezwłocznie po powrocie do Wielkiej Brytanii zaprosił na weekend do swego wiejskiego domu Alana Turinga i przedstawił mu przywiezione z Warszawy informacje. Dopiero gdy Turing potwierdził ich prawdziwość, Knox złagodził swój osąd. Nie zmienia to jednak faktu, że jego najwcześniejsza hipoteza, zakładająca oparcie sukcesu Polaków na kradzieży lub przekupstwie, miała w przyszłości zrobić prawdziwą karierę.

Losy samego sekretu Enigmy, kilkunastu związanych z nim ludzi, a także losy przyszłej recepcji tej historii ułożyłyby się zapewne inaczej, gdyby polskim kryptologom dane było pracować przez większą część wojny ramię w ramię z brytyjskimi kolegami. Polacy, którzy położyli teoretyczne i praktyczne fundamenty pod ataki na szyfr Enigmy, nie wzięli istotnego udziału w ich wykorzystaniu do zwycięstwa alianców w drugiej wojnie światowej. Oznaczało to także, że nie znaleźli się wśród kronikarzy spisujących po zakończeniu drugiej wojny światowej dzieje zwycięstwa. Historię ich sukcesu spisywali przedstawiciele innych nacji, dla których obiektywne przedstawienie historii nie było głównym priorytetem. Gdy tylko w Europie zamilkły działa, historia Enigmy

została skazana na zapomnienie. Ośrodek kryptologiczny w Bletchley Park, gdzie w trakcie drugiej wojny światowej rozgrywała się jej kluczowa część, jeszcze w ostatnich tygodniach wojny rozbrzmiewał głosem ponad 10 tysięcy pracowników. Prawie wszyscy zostali zdemobilizowani w ciągu pierwszych tygodni pokoju, a na pożegnanie każdy musiał ponownie podpisać zobowiązanie do bezterminowego utrzymania w tajemnicy wszystkiego, co czynił, widział lub słyszał w ośrodku w czasie wojny. Nieco dłużej w Bletchley Park pozostali wyłącznie szefowie sekcji, którym powierzono zadanie spisania raportów z wojennej działalności ich zespołów. Kiedy ukończyli pracę, większość powróciła do przedwojennych zajęć, a spisane przez nich raporty trafiły do archiwum, gdzie opatrzone je adnotacjami zakazującymi ujawniania zawartości.

Tajemnica, którą otoczono wojenny dekryptaż niemieckich depesz, wynikała z czysto praktycznych względów. Koniec drugiej wojny światowej oznaczał kres konfrontacji z jednym totalitaryzmem i początek zmagania z innym, sowieckim. Jeszcze w czasie wojny zachodni alianci zauważyli, że nowy potencjalny przeciwnik posługuje się urządzeniami szyfrującymi, których zasada działania nawiązuje wprost do konstrukcji Enigmy. Ujawnienie sukcesów w zmaganiach z niemieckimi szyframi byłoby równoznaczne z ostrzeżeniem nowego adwersarza, że jego szyfry, oparte na identycznej zasadzie działania, nie są bezpieczne. Dzisiaj wiadomo, że ostatnie urządzenia służące do łamania szyfrów Enigmy zostały wycofane z użytku w USA dopiero w 1956 r.; co najmniej do tego czasu Enigma była używana do szyfrowania depesz przekazywanych przez wschodnioniemiecką milicję. Inne typy wirnikowych maszyn szyfrujących pozostawały w użyciu jeszcze w pierwszej połowie lat 80. Gdy szefowie komórek ośrodka w Bletchley Park przystępowali do redakcji raportów z wojennej działalności ich zespołów, było dla nich rzeczą oczywistą, że ich treść nie stanie się wiedzą publiczną przez wiele lat, lub wręcz nigdy.

Z polskiego punktu widzenia było rzeczą niezwykle niefortunną, że wśród kronikarzy dziejów złamania Enigmy nie znaleźli się uczestnicy jej

najwcześniejszego etapu. Szef brytyjskiej delegacji na konferencję w Pyrach Alastair Denniston padł w początku 1942 r. ofiarą czegoś w rodzaju przewrotu pałacowego; utracił stanowisko szefa ośrodka w Bletchley Park i został przesunięty do sekcji, która w Londynie zajmowała się łamaniem mniej istotnych kodów dyplomatycznych. Dillwyn Knox zimą 1943 r. przegrał długotrwałą walkę z chorobą; odszedł 27 lutego. Trzeci uczestnik brytyjskiej delegacji komandor porucznik Humphrey Sandwith nie był kryptologiem, toteż jego incydentalny kontakt z Enigmą nie pozostawił żadnych śladów. W rezultacie większość informacji o wkładzie Polaków w kryptologiczny sukces brytyjscy kronikarze uzyskali za pośrednictwem Alana Turinga, który nie uczestniczył wprawdzie w przedwojennym spotkaniu, był jednak pierwszą osobą, której Knox przedstawił przywiezione z Polski rewelacje po powrocie do Londynu. Był też jedynym poza Knoxem i Dennistonem członkiem brytyjskiego zespołu, który spotkał Polaków, gdy w połowie stycznia 1940 r. dostarczył do Paryża wykonane w Bletchley Park kopie płacht Zygalskiego.

Ślad roli Turinga można odnaleźć w oficjalnej kronice Baraku 8 (Hut 8) w Bletchley Park, spisanej przez jego ostatniego szefa A.P. Mahona: „Sam dołączyłem do zespołu w październiku 1941 roku i dobrze pamiętam wydarzenia od tej chwili. Co do wcześniejszych zdarzeń mam osobisty dług wdzięczności wobec Turinga, pierwszego szefa zespołu; większość informacji dotyczących wczesnej historii opiera się na informacjach uzyskanych w trakcie rozmów z nim”¹. I dalej: „Prawie cała wczesna praca nad Enigmą Kriegsmarine została wykonana przez Polaków, którzy przekazali szczegóły swych znaczących osiągnięć tuż przed wybuchem wojny. Większość informacji, którą zebrałem na temat okresu przedwojennego, pochodzi od nich i dotarła do mnie za pośrednictwem Turinga”². Nieco dalej Mahon zauważa jednak, że „zdolności komunikacyjne Turinga były fatalne i – jak słusznie zauważył Pan Birch – nie był

¹ A.P. Mahon, *The History of Hut Eight*, United Kingdom 2010, s. 1.

² *Ibidem*, s. 12.

on praktycznym człowiekiem: właśnie z tego powodu opuścił Barak 8, gdy ukończono pionierską część prac”³.

Jeśli ocena Mahona jest trafna, głównym źródłem, z którego kronikarze ośrodka w Bletchley Park mogli poznać wczesny wkład Polaków we własne sukcesy, nie były ustne relacje Turinga, lecz dokument przekazany Brytyjczykom w trakcie przedwojennego spotkania w Pyrach. Bezpośredni następca Turinga w roli szefa Baraku 8 Conel H.O’D. Alexander zapisał w raporcie, że: „(...) prawie wszystkie wczesne prace nad Enigmą zostały wykonane przez polskich kryptologów, którzy tuż przed rozpoczęciem wojny przekazali szczegółowy opis swych bardzo wartościowych wyników”⁴. Ślad raportu przekazanego przez Polaków odnajdujemy także u Mahona: „Polacy opracowali nową metodę, która zasługuje na znaczące zainteresowanie. Ich opis tej metody, sporządzony w nieco koturnowym języku niemieckim, istnieje do dzisiaj i stanowi interesującą lekturę dla wszystkich, którzy mieli styczność z maszyną”⁵. Niestety, wzmianka Mahona dotycząca polskiego raportu jest ostatnim jego śladem w alianckich archiwach. Wieloletnie poszukiwania samego raportu do tej pory nie przyniosły sukcesu.

Wydaje się, że memorandum polskich kryptologów było niedostępne już w latach 1945–1946, kiedy zespół pod kierownictwem Stuarta Milner-Barry’ego pracował nad trzytomową historią Baraku 6. Jego autorzy zanotowali silnie zniekształconą wersję wczesnej historii Enigmy: „Nie jest historycznie pewne, w jaki sposób Polacy otrzymali połączenia wirników, i nie jest to kwestia, co do której byli oni szczególnie komunikatywni. Z pewnością w znacznym stopniu wykorzystywali pracę tajnych agentów i jest najbardziej prawdopodobne, że otrzymali fotografie kluczy i depesz z odpowiadającym tekstem jawnym. Przyznali,

³ Ibidem, s. 24.

⁴ C.H.O’D. Alexander, *Cryptographic History of Work on the German Naval Enigma*, HW 25/1, s. 17.

⁵ A.P. Mahon, *The History...*, s. 13.

że kluczowy element, połączenia walca wejściowego, otrzymali od agenta, choć utrzymywali, bez wątplenia słusznie, że mogli byli zrekonstruować je także matematycznie⁶. Żadne ze stwierdzeń w powyższym zdaniu nie odpowiada prawdzie. Nawet jeśli nie udało się odnaleźć raportu z Pyr, dysponujemy kilkoma dokumentami z epoki, które można uznać za jego streszczenia lub omówienia. Matematyczna metoda określenia połączeń wirników została w nich zaprezentowana szczegółowo i z pełną otwartością. Inny z cytowanych dokumentów potwierdza to zresztą jednoznacznie: „Polacy zdołali zrekonstruować połączenia wszystkich trzech wirników metodami kryptograficznymi”⁷. Z dokumentów jasno wynika, że Polacy nie wykorzystywali efektów pracy tajnych agentów i nie uzyskali tekstów depeš z odpowiadającym tekstem jawnym. Polscy kryptolodzy nie mogli także przyznać, że połączenia walca wejściowego otrzymali od agenta, w przekazanym aliantom materiale zamieścili bowiem zarówno informację o odgadnięciu połączeń walca, jak i o opracowanej następnie czysto matematycznej metodzie ich rekonstrukcji.

Ujęcie roli Polaków w najwcześniejszych brytyjskich relacjach dotyczących złamania szyfru Enigmy zawiera w sobie osobliwy dysonans. Z jednej strony głosy uznania i podziwu: „Spoglądając wstecz na pracę Polaków i uwzględniając, jak niewiele wiedziano wtedy na temat szyfrów maszynowych oraz jak skromnym wyposażeniem mechanicznym dysponowali, przepełnia nas poczucie podziwu dla osiągniętych przez nich rezultatów. (...) Nasze późniejsze sukcesy zawdzięczały wiele ich wczesnym wysiłkom”⁸. Z drugiej jednak strony zupełnie chybotne spekulacje na temat sposobów pokonania różnych aspektów maszyny i szyfru nawiązujące do najwcześniejszej tezy Knoxa – kradzieży lub przekupstwa. Wątek kradzieży i tajnych agentów miał z czasem zrobić

⁶ S. Milner-Barry, *The History of Hut Six*, t. 1, PRO HW 43/70, September 1945, s. 44.

⁷ C.H.O'D. Alexander, *Cryptographic History...*, s. 17.

⁸ *Ibidem*, s. 19.

prawdziwą karierę, jednak na razie raporty spisane przez wojennych szefów komórek ośrodka w Bletchley Park trafiły do archiwum, a nad historią złamania szyfru na długie 30 powojennych lat rozciągnęła się zasłona milczenia.

Nie oznacza to jednak, że dzieje złamania Enigmy były całkowicie nieznane wśród historyków wojskowości, szczególnie brytyjskich. Co więcej, wydaje się, że fakt złamania szyfru był jednoznacznie kojarzony z kluczową rolą polskich kryptologów. Kilka niepublikowanych wypowiedzi oraz szczątkowych wzmianek we wczesnych publikacjach świadczy o tym, że w środowisku brytyjskich historyków zarys prawdy był znany co najmniej w połowie lat 60. Znał go z pewnością kontrowersyjny brytyjski historyk David Irving. Zapewne świadomy własnej, nie najlepszej reputacji w środowisku historyków uznał, że bezpiecznie będzie włożyć najbardziej zapalne kwestie w cudze usta. Wybrał do tego renomowanego historyka z London School of Economics Donalda Camerona Watta. Ten w przedmowie do opublikowanej w 1968 r. książki Irvinga *Breach of Security* stwierdził, że: „Wielka Brytania otrzymała od polskiego wywiadu klucze oraz wyposażenie umożliwiające odczytywanie niemieckich depesz wojskowych i dyplomatycznych”. Ani niedyskrecja Watta, ani o rok wcześniejszy sygnał z Polski (jednozdaniowa wzmianka o łamaniu niemieckich szyfrów przez przedwojenny polski wywiad zawarta w książce Władysława Kozaczuka *Bitwa o tajemnice*) nie zwróciły jednak uwagi historyków ani weteranów kryptologii.

Burzę rozpętała dopiero opublikowana w 1973 r. książka francuskiego emerytowanego generała Gustave’a Bertranda pt. *Enigma ou la plus grande énigme de la guerre 1939–1945*. Stało się tak zresztą nie tyle ze względu na sensacyjne ujawnienie złamania szyfru Enigmy, ile na skutek zawartego w pracy ładunku historycznych przeinaczeń oraz tradycyjnych francuskich uszczypliwości pod adresem perfidnych Anglików. Sprawily one, że publikacji francuskiego generała nie można było po prostu przemilczeć, a jednocześnie w żadnym wypadku nie wolno było

potwierdzić prezentowanej przezeń wersji historii nawet w tych przypadkach, w których Bertrand uczciwie relacjonował wydarzenia, i to nie tylko z uwagi na wrażliwość brytyjskiego sumienia. Była pierwsza połowa lat 70. XX w., Europa była podzielona żelazną kurtyną, w najlepsze trwała cicha konfrontacja Zachodu ze światem komunizmu. Kryptolodzy obu obozów nadal wykorzystywali maszyny szyfrujące, których konstrukcja wywodziła się od Enigmy. Przyznanie, że Enigma była łamana już w czasie drugiej wojny światowej, stanowiłoby oczywiste skierowane do przeciwnika ostrzeżenie dotyczące bezpieczeństwa jego obecnych szyfrów.

Służby specjalne Wielkiej Brytanii i USA najwyraźniej uznały, że rewelacje Bertranda są dalece przedwcześnie. Ponieważ sam dekryptaż Enigmy został ujawniony i nie można było sprawy zamieść z powrotem pod dywan, trzeba było posłużyć się starym jak świat trickiem tajnych służb – dezinformacją. Do jej rozpowszechniania Brytyjczycy przekonali m.in. weterana wywiadu z okresu drugiej wojny światowej Frederica Winterbothama. Był on swego czasu jednym z twórców systemu dystrybucji informacji pochodzących z dekryptażu do najważniejszych agend rządowych i sztabów, w tej roli nie miał jednak żadnego kontaktu z kryptologicznym warsztatem. W opublikowanej w 1974 r. książce *The Ultra Secret* zawarł wiele ciekawostek dotyczących m.in. tzw. brązowej bogini – maszyny służącej do łamania szyfru. Z punktu widzenia jego mocodawców najważniejszy okazał się zapewne fragment relacjonujący historię udziału Polaków w zwycięstwie nad Enigmą: „W 1938 roku w fabryce we wschodnich [sic!] Niemczech, która (...) produkowała pewien rodzaj sprzętu łącznościowego, był zatrudniony polski mechanik. (...) We właściwym czasie młody Polak został (...) sekretnie przeszmuglowany pod fałszywym paszportem (...), zainstalowany w Paryżu, gdzie dostał do swej dyspozycji warsztat. Tam pod opieką przydzielonego stolarza zaczął pracować nad drewnianą makietą urządzenia, w którego produkcji uczestniczył w Niemczech”.

Rok później inny Brytyjczyk, Anthony Cave Brown, opublikował książkę *Bodyguard of Lies*, w której zawarł podobną historię: „Gibson [szef stacji MI6 w Pradze] (...) spotkał polskiego Żyda [zatrudnionego wcześniej przy produkcji maszyny], który zaoferował MI6 sprzedaż za 10 000 funtów swej wiedzy na temat Enigmy. (...) Po sprawdzeniu jego wiarygodności, jak głosi historia, MI6 zainstalowało go w apartamencie w Paryżu, gdzie Lewiński odtwarzał z pamięci dane Enigmy”.

Wreszcie w 1976 r. William Stevenson opublikował biografię sir Williama Stephensona, w czasie wojny szefa komórki brytyjskiego wywiadu w USA, pt. *A Man Called Intrepid*, w której przedstawił jeszcze inną wersję zdobycia przez Polaków sekretu Enigmy: „Polska zdobyła Enigmę w początku 1939 roku, gdy jej agenci uprowadzili wojskową ciężarówkę dostarczającą maszyny Enigma w rejon przygraniczny”. Wersje przedstawiane kolejno przez brytyjskich pisarzy różniły się wzajemnie. Zawierały jednak punkt wspólny, który stanowił ich kluczowy, a zarazem zgodny ze spekulacjami Knoxa i jego następców z Bletchley Park element: sukces Polaków w zmaganiach z Enigmą był oparty na kradzieży lub zdobyciu w inny sposób egzemplarza maszyny. Zawarty był w nim czytelny komunikat dla kryptologicznego adwersarza: tak długo, jak długo jesteście w stanie chronić fizyczne bezpieczeństwo waszych maszyn szyfrujących, wasze szyfry są także bezpieczne.

Jeżeli rewelacje brytyjskich historyków były, jak zakładam, świadomą dezinformacją, jej poziom budził zakłopotanie i zapewne nie był w stanie wprowadzić w błąd funkcjonariuszy żadnej z tajnych służb. Ale przyniósł nieoczekiwany efekt uboczny, którego skutki do dziś stawiają barierę na drodze poznania historycznej prawdy o złamaniu Enigmy. W połowie lat 80. XX w. Brytyjczycy musieli uznać, że maszyny bazujące na Enigmie powoli wychodzą z użycia, a zatem prawda o niej nikomu już nie może zaszkodzić. Rozpoczęli więc stopniowe ujawnianie dokumentów źródłowych dotyczących jej historii. Od końca lat 80. każdy, kto pragnie poznać dzieje złamania Enigmy, bez większych trudności może zapoznać się z podstawowymi dokumentami źródłowymi

i podsumowaniami opracowanymi z udziałem weteranów alianckich ośrodków kryptologicznych.

Problem w tym, że znaczna część materiałów źródłowych z brytyjskich archiwów odwołuje się wprost do spekulacji i stereotypów wywodzących się wprost z najwcześniejszej, historycznej reakcji Knoxa: Polacy łamali szyfr, bo zdołali ukraść lub kupić egzemplarz Enigmy. W tej sytuacji nie można się dziwić, że także współcześni historycy mają tendencję do powtarzania z upodobaniem dawnych dezinformacji. Norman Davies w opublikowanej w 2006 r. książce *Europa walczy 1939–1945. Nie takie proste zwycięstwo* rolę Polaków w złamaniu Enigmy opisał następująco: „Przedwojenny polski wywiad dowiedział się, że niemiecka armia rozwija (...) kod bazujący na komercyjnej maszynie zwanej »Enigma«. Polscy agenci przedostali się do fabryki, w której była produkowana zaawansowana wersja maszyny i zdobyli jej projekty”. W 2010 r. Richard Aldrich przedstawił w swej książce *GCHQ. The Uncensored Story of Britain's Most Secret Intelligence Agency* jeszcze jedną wersję polskiej zdobyczy: „Zanim polski wywiad musiał uciekać z Warszawy, jego agenci osiągnęli znakomity sukces, kradnąc kilka egzemplarzy wojskowej Enigmy z niemieckiej fabryki, w której maszyna była produkowana”.

W tym kontekście zrozumiałe stają się wieloletnie starania polskich historyków o odnalezienie w alianckich archiwach oraz ujawnienie kopii memorandum przekazanego przez Polaków w Pyrach. To memorandum, jeżeli się zachowało, stanowi najbardziej autorytatywne potwierdzenie i podsumowanie wkładu Polaków w złamanie szyfru Enigmy. Można argumentować, że tę rolę mogą odegrać także inne dokumenty opracowane przez polskich kryptologów w różnych okresach ich działalności. Mowa tu przede wszystkim o tzw. *Dokumencie L*, stanowiącym załącznik do raportu ppłk. Gwidona Langerera dotyczącego przedwojennej działalności polskiego Biura Szyfrów. Dokument, opracowany zapewne w pierwszej połowie 1940 r., znajduje się w zbiorach Instytutu Polskiego i Muzeum im. gen. Sikorskiego w Londynie. Jego skrótowy charakter pozwala się domyślać, że stanowi próbę rekonstrukcji z pamięci źródeł

utraconych w trakcie ewakuacji z Polski i w konsekwencji nie oddaje w pełni zakresu informacji przekazanych aliantom w lipcu 1939 r. Dwie części powojennych wspomnień Mariana Rejewskiego zostały utrwalone odpowiednio w latach 1967 i 1974; dystans czasowy wobec opisywanych wydarzeń oraz brak dostępu do choćby szczątkowych dokumentów źródłowych także ograniczają ich użyteczność jako punktów odniesienia do analizy polskiego wkładu w złamanie szyfru. Co więcej, oba dokumenty zachowały się wyłącznie w polskich archiwach, co w pewnej mierze ogranicza potencjał ich wykorzystania w dyskusji nad rolą kryptologów kilku państw w triumfie nad Enigmą.

Dotychczasowe starania o odnalezienie w wojennych archiwach aliantów Polski kopii raportu z Pyr pozostają bezskuteczne. Jednak w 2016 r. autor odnalazł w archiwum francuskich sił zbrojnych dokument będący zapewne skróconą wersją poszukiwanego raportu, bazującą na pełnym tekście, do którego autorzy musieli mieć dostęp i który uzupełnili opisem wydarzeń pomiędzy lipcem 1939 a czerwcem 1940 r. W konsekwencji dokument stanowi najpełniejsze znane obecnie podsumowanie wkładu Polaków w złamanie Enigmy pochodzące z zasobów archiwalnych aliantów. Jest on częścią zespołu akt odtajnionych 2 grudnia 2015 r. decyzją Direction Générale de la Sécurité Extérieure i przeniesionych do archiwum Service Historique de la Defense w Vincennes⁹. Skład zespołu akt jednoznacznie wskazuje na to, że stanowią one część prywatnego archiwum emerytowanego generała armii francuskiej Gustave'a Bertranda, wojennego zwierzchnika polskich kryptologów. Skądinąd wiadomo, że w ramach likwidacji półkondspiracyjnego ośrodka kryptologicznego, który działał od listopada 1940 do listopada 1942 r. w pobliżu Uzès w nieokupowanej części Francji, Bertrand ukrył archiwum, zamurując je w domu swojej matki w Grasse. Po wyzwoleniu południa Francji w 1944 r. dokumenty odzyskał, jednak bezpośrednio po jego śmierci 23 maja 1976 r. posiadłość w Théoule-sur-Mer (w którym pełnił funkcję

⁹ Service Historique de la Defense, SHD DE2016 ZB25.

mera) została przeszukana przez przedstawicieli armii, którzy skonfiskowali znaczną ich część. Sądząc z przekazanych przez wdowę po generale informacji dotyczących objętości zajętych akt, zespół ujawniony w 2015 r. stanowi skromną część archiwum Bertranda.

Niedatowany i niepodpisany maszynopis został oznaczony w wykazie akt jako notatka techniczna w języku niemieckim (*Notice technique en allemande*); towarzyszy mu rękopiśmienne tłumaczenie na język francuski. Zbieg zdarzeń sprawił, że znamy okoliczności i powody powstania dokumentu. Powojenny raport płk. Langerera z działalności Ekspozytury 300 oraz ewakuacji ośrodka z Francji¹⁰ zawiera informację, że: „(...) w Fuzach (nasze m.p.) prosił Bolek o napisanie elaboratu, w którym w sposób obiektywny przedstawiono, w jakiej mierze każdy z trzech partnerów przyczynił się do rozwiązania zagadnienia maszyny Enigmy. Elaborat opracowali por. Rejewski i Zygałski. Gdy Bolek go przestudował powiedział on, że całą pracę musi przerobić, bo czytając go w obecnej formie odnosi się wrażenie, jakoby Francuzi prawie nic nie zrobili”.

Kwestia autorstwa memorandum jest nieco złożona. Langer wskazuje, że opracowali je Marian Rejewski i Henryk Zygałski, co może dowodzić jego powstania w okresie po śmierci Jerzego Różyckiego lub co najmniej w czasie jego pobytu w Afryce Północnej w 1941 r. Z drugiej strony chronologia wydarzeń opisanych w dokumencie obejmuje okres do drugiej połowy czerwca 1940 r. Ze wspomnień Bertranda oraz raportów Langerera wiadomo, że kryptolodzy kontynuowali dekryptaż Enigmy co najmniej w ciągu 1941 r. Można przypuszczać, że memorandum opracowane w tymże roku albo później zawierałoby choć szczątkowe odniesienia do tych prac. Ich brak wskazuje na drugą połowę 1940 r. jako najbardziej prawdopodobny okres powstania dokumentu. We wspomnieniach Mariana Rejewskiego widnieje informacja, że we wczesnej fazie pracy w ośrodku P.C. Cadix Francuzi mieli problemy z dostarczeniem kryptologom szyfrogramów. Aby czymkolwiek zająć zespół, którego morale

¹⁰ IJP 709/133/5, s. 39.

szwankowało w wyniku narzuconej przeprowadzki do Francji, Bertrand dostarczył kryptologom pakiet szwajcarskich depesz szyfrowanych za pomocą komercyjnej Enigmy, które Polacy szybko złamali. Opracowanie podsumowań i sprawozdań należy do klasyki działania każdej biurokracji, jest więc prawdopodobne, że analizowany dokument powstał w drugiej połowie 1940 r., gdy francuscy zwierzchnicy usiłowali zająć kryptologów jakąkolwiek pracą. Jeśli jednak domysł ten jest poprawny, memorandum jest zapewne zbiorowym dziełem całej trójki: Rejewskiego, Różyckiego i Zygalskiego. Pominięcie Różyckiego przez Langera w raporcie składanym już po zakończeniu wojny może być podyktowane psychologicznym wyparciem postaci Różyckiego po jego przedwczesnej śmierci. Skądinąd wiadomo, że w trakcie przesłuchania na zamku Eisenberg w marcu 1944 r. Langer powoływał się na prace dwóch matematyków, najwyraźniej dostosowując swoje wspomnienia (lub co najmniej zeznania) do rzeczywistości po śmierci Różyckiego. W powojennym raporcie mógł zadziałać identyczny mechanizm.

Dokument nosi tytuł *ENIGMA. Kurzgefasste Darstellung der Auf Lösungsmethoden* (pol. *Enigma. Skrócona prezentacja metod rozwiązania*). Odwołanie do skrótu użyte w tytule sugeruje istnienie pełnej wersji tego samego tekstu. Jedyne dokument, który mógł pełnić taką rolę, to raport przygotowany dla uczestników spotkania w Pyrach. Wskazuje na to kilka elementów. Po pierwsze wiadomo, że raport z Pyr został opracowany w języku niemieckim, jedynym, w jakim mogli się porozumieć wszyscy uczestnicy spotkania. Zważywszy na okoliczności powstania analizowanego tekstu, nie istniały żadne powody, aby w dalszym ciągu sięgać po pomoc języka przeciwnika. Opracowanie dokumentu w języku niemieckim wskazuje na to, że stanowił on, zgodnie z tytułem, skrót tekstu źródłowego przygotowanego właśnie w tym języku. Drugą okolicznością wskazującą na to, że autorzy mieli dostęp do swojego pierwotnego raportu, jest jego szczegółowość, zwłaszcza w zestawieniu z wcześniejszym o co najmniej pół roku *Dokumentem L*. Ten ostatni ma objętość odpowiadającą około połowie analizowanego tekstu i pomija

kilka interesujących zawartych w nim wątków. Dotyczy to szczególnie kilku sekcji poświęconych analizie szyfrów Kriegsmarine. Powojenne komentarze brytyjskich kryptologów jednoznacznie potwierdzają, że Polacy podzielili się z nimi wynikami swoich prac dotyczących wykorzystania Enigmy przez niemiecką marynarkę. Brytyjczycy nigdy nie zdołali wyjść poza i ponad rezultaty osiągnięte przez Polaków wyłącznie na gruncie kryptologicznej teorii. Rozpoznanie brakujących elementów szyfru Enigmy Kriegsmarine oraz jego finalne złamanie zawdzięczali dokumentom znalezionym na pokładzie zdobytych okrętów przeciwnika. Tymczasem w znanych dotąd polskich źródłach (*Dokument L* oraz *Wspomnienia* Mariana Rejewskiego) dekryptaż Enigmy Kriegsmarine został jedynie zasygnalizowany, bez podawania szczegółów. Zestawienie brytyjskich raportów z treścią polskich dokumentów jednoznacznie wskazuje, że Brytyjczycy odwoływali się do innego dostarczonego przez Polaków dokumentu niż teksty znane do tej pory. Obszerne informacje na temat historii dekryptażu szyfrów Kriegsmarine przez polskie Biuro Szyfrów pojawiają się po raz pierwszy właśnie w analizowanym dokumencie.

Różnice pomiędzy domniemanym oryginałem a ujawnionym dokumentem nie ograniczają się do skrótów. Raport przygotowany w związku z konferencją w Pyrach siłą rzeczy nie mógł objąć jej samej ani wydarzeń, które nastąpiły po niej. Omawiany dokument doprowadza narrację do punktu bezpośrednio poprzedzającego domniemany czas jego redakcji. Dzięki temu mamy możliwość poznania wydarzeń obserwowanych z polskiego punktu widzenia aż do kapitulacji Francji. Raport obejmuje konferencję w Pyrach oraz wczesny okres alianckiej, trójstronnej współpracy kryptologicznej. Autorzy dostarczają informacje o najwcześniejszych sukcesach brytyjskich kryptologów: od metody ataku opracowanej przez Knoxa aż po zmianę procedury szyfrowania poprzedzającą kampanię francuską i jej pokonanie dzięki zastosowaniu metody Herivela. Ostatni rozdział potwierdza okoliczności powstania raportu przekazane przez Gwidona Langera: zawiera wyliczenie elementów

wkładu uczestników kryptologicznego aliansu w złamanie szyfrów Enigmy. Można zrozumieć podenerwowanie Gustave'a Bertranda po lekturze dokumentu – na tle dorobku polskich i brytyjskich kryptologów wkład Francuzów w postaci dwóch dokumentów rysuje się nader skromnie.

Znacząca część informacji prezentowanych w raporcie powiela zagadnienia znane z innych, wcześniej dostępnych dokumentów. Jego wyjątkowy charakter sprowadza się do dwóch wartości. Jest on jedynym znanym obecnie dokumentem podsumowującym wkład Polaków w złamanie Enigmy oraz wczesny etap alianckiej współpracy kryptologicznej pochodzącym z archiwów alianckich. Jednocześnie stanowi najszersze ujawnione do tej pory sprawozdanie z tego okresu zawarte w źródłach innych niż brytyjskie. Zgodnie z literą rozkazu Bertranda, za którego przyczyną opracowanie powstało, choć zapewne niezupełnie zgodnie z jego intencjami, zakres memorandum pozwala poszerzyć analizę wkładu kryptologów trzech państw w złamanie Enigmy w stosunku do dotychczasowego stanu wiedzy.

Marek Grajek
Jan Stanisław Ciechanowski

Płk Gwido Karol Langer i mjr Maksymilian Ciężki – architekci sukcesu polskich kryptologów

Uwaga większości komentatorów sukcesu polskich kryptologów, czyli złamania szyfrów maszyny Enigma, skupia się w naturalny sposób na głównych jego aktorach – trójce matematyków. Ktokolwiek jednak jest świadom skomplikowania struktury i funkcjonowania współczesnego radiowywiadu, musi zadawać sobie pytania o głębsze źródła tego osiągnięcia. Kto i w jaki sposób zapewnił złożoną infrastrukturę techniczną i organizacyjną niezbędną do funkcjonowania radionasłuchu i dekryptażu? Kto wypracował i kto zatwierdził długoterminową strategię ataku na szyfry potencjalnych przeciwników? Kto stał za decyzją o powołaniu zintegrowanej organizacji radiowywiadowczej? Kto podjął decyzję o rekrutacji matematyków? Wreszcie – kto zapewnił ciągłość wysiłku w okresie kilkunastu międzywojennych lat? Jeżeli powiążemy odpowiedzi na te i kilka innych pytań z decyzjami i działaniami podejmowanymi przez konkretne osoby, staną one w jednym szeregu z głównymi bohaterami kryptologicznego przełomu. Spróbujmy więc ocenić, czy znajomość historii polskiego Biura Szyfrów pozwala wskazać nie tylko pierwszo-, lecz także drugoplanowych bohaterów zwycięstwa nad szyframi niemieckiej Enigmy.

Współcześni kryptolodzy są zgodni co do tego, że w realiach międzywojennych centralizacja służby radiowywiadowczej stanowiła jeden z kluczowych czynników sukcesu w zabezpieczeniu własnej łączności oraz atakach na szyfry i kody przeciwnika. Po okresie gwałtownego,

lecz nieco spontanicznego rozwoju w latach pierwszej wojny światowej kryptologia weszła w okres nacechowany wewnętrznymi sprzecznościami. Z jednej strony rozwój jej metod i zastosowań w okresie globalnego konfliktu wymuszał profesjonalizację służby – bardziej systematyczne szkolenie personelu i doskonalenie struktur organizacyjnych. Z drugiej w stosunku do okresu wojennego czasy pokoju drastycznie zredukowały zapotrzebowanie na kryptologów i ich usługi. Grupowanie tych nielicznych adeptów dyscypliny, których państwa decydowały się zachować także w pokojowych realiach w ramach zcentralizowanej służby kryptologicznej, było rozwiązaniem nie tylko ekonomicznym, lecz także skutecznym. W większości państw świata przeważyły jednak różnego rodzaju animozje i współzawodnictwa – każda służba korzystająca z szyfrów lub kodów tworzyła własną komórkę kryptologiczną. Jednym ze skrajnych przykładów takiej polityki były służby kryptologiczne Trzeciej Rzeszy, w której doliczono się prawie dziesięciu agencji zajmujących się projektowaniem szyfrów własnych i odczytywaniem łączności przeciwnika (i przy okazji także konkurencyjnych służb)¹. W Stanach Zjednoczonych Ameryki już po zaangażowaniu kraju w czynne działania wojenne rywalizacja pomiędzy kryptologami armii lądowej i marynarki była tak zacięta, że jeden z weteranów floty wyznał po latach, że „z kryptologami armii lądowej nie współpracowało się nawet pod karą śmierci”².

Na tym tle wyróżniały się służby kryptologiczne dwóch państw: Wielkiej Brytanii i Polski, które z różnych przyczyn wybrały zcentralizowany model działania. Znamy powody takiego wyboru w Wielkiej Brytanii; gdy reorganizowano kryptologię po zakończeniu pierwszej wojny światowej, wśród zainteresowanych wybuchł konflikt o pieniądze. Drastycznie zredukowane budżety armii lądowej i marynarki nie pozwalały utrzymać służb o standardzie z okresu Wielkiej Wojny. Wojskowi

¹ J. Jackson, *Hitler's Codebreakers. German Signals Intelligence in World War 2*, Redditch 2012.

² P.H. Currier, NSA-OH-38-80, s. 34.

i marynarze zwracali także uwagę, że w pokojowych realiach głównym konsumentem informacji przekazywanych przez radiowywiad jest dyplomacja, to ona więc winna finansować funkcjonowanie kryptologów. Foreign Office nie uchylało się przed takim obowiązkiem, jednak argumentowało, że pieniądзом towarzyszy władza; finansując projektowaną służbę, musiało mieć decydujący wpływ na kierunki jej działania. W rezultacie ukształtowano typowo brytyjski kompromis – nowa organizacja, która została zakamuflowana pod nazwą Rządowej Szkoły Kodów i Szyfrów (Government Code and Cypher School, GC&CS), będzie działać formalnie w ramach struktur resortu odpowiedzialnego za politykę zagraniczną, który swe uprawnienia decyzyjne będzie wykonywać za pośrednictwem szefa wywiadu, a w strukturze Szkoły zostaną powołane w znacznym stopniu autonomiczne sekcje wojsk lądowych i marynarki³.

Nie znamy powodów, dla których także kierownictwo polskiego wywiadu zdecydowało się sięgnąć po zcentralizowany model funkcjonowania służb radiowywiadowczych. Była to decyzja nieco zaskakująca, zważywszy, że w okresie kształtowania struktury Wojska Polskiego pozostawało ono pod znacznym wpływem wzorców francuskich. Liczni oficerowie sztabowi WP studiowali na francuskich uczelniach wojskowych oraz odbywali praktyki w sztabach i jednostkach francuskiej armii. Funkcję dyrektora nauk Wyższej Szkoły Wojennej w Warszawie pełnił francuski generał Louis Faury. Można się było spodziewać, że organizując radiowywiad, Polacy podążą drogą wytyczoną przez armię francuską, która równolegle rozpraszała swych kryptologów pomiędzy niezależnie funkcjonujące służby kryptologiczne rodzajów wojsk, organizując dodatkowo komórki specjalistyczne, jak np. dowodzoną przez kpt. Gustave'a Bertranda służbę specjalizującą się w międzynarodowym handlu kryptologicznymi sekretami licznych państw świata. Stało się jednak inaczej: Polacy wykazali pełną niezależność od francuskich

³ Zob. szerzej: J. Ferris, *Whitehall's Black Chamber. British Cryptology and the Government Code and Cypher School, 1919–29*, London 1987.

doktryn, organizując jednolitą służbę kryptologiczną, służącą wszystkim rodzajom sił zbrojnych. Proces centralizacji dobiegł końca z chwilą powołania płk. Gwidona Langera na szefa Biura Szyfrów; do jego struktury włączono komórkę odpowiedzialną za opracowanie szyfrów własnych Wojska Polskiego⁴.

Można jedynie spekulować na temat powodów, dla których Polacy sięgnęli po rozwiązania organizacyjne odmienne od wzorców stosowanych ówczesnie przez większość państw świata. Zapewne ważnym argumentem był sukces złamania szyfrów sowieckich i jego konsekwencja – zwycięstwo w wojnie z bolszewikami w latach 1919–1920⁵. W warunkach wojennej improwizacji nikt nie zastanawiał się nad modelem organizacyjnym radiowywiadu; utworzono jednolitą strukturę organizacyjną, a kiedy dowiodła ona swej skuteczności w najtrudniejszych, wojennych warunkach, zachowano ją bez istotnych zmian także w czasach powojennych. Z pewnością znaczącą rolę odegrał deficyt przeszkolonych kryptologów w kraju, który dopiero co odzyskał niepodległość. Z pewnością centralizacja polskiego radiowywiadu i kryptologii była w równej mierze efektem specyficznych warunków, w jakich tworzone odpowiednie służby, oraz świadomego zamiaru ich twórców. Istotne jest to, że Langer i jego zastępca Maksymilian Ciężki zdołali nie tylko doprowadzić do finału proces centralizacji, lecz także utrzymać jego efekty w burzliwym, przedwojennym czasie. Niemniej jednak uczciwość nakazuje przyznać, że nawet im nie udało się go w pełni zakończyć – Ministerstwo Spraw Zagranicznych zachowało własną komórkę szyfrową. Z dokumentów odnalezionych przez aliantów po drugiej wojnie światowej wiadomo, że przyniosło to fatalne rezultaty. Niedbałość

⁴ M. Grajek, *Enigma. Bliżej prawdy*, Poznań 2007, s. 38–43.

⁵ G. Nowik, *Zanim złamano „Enigmę”... Polski radiowywiad podczas wojny z bolszewicką Rosją 1918–1920*, Warszawa 2004; idem, *Zanim złamano „Enigmę”... rozszyfrowano rewolucję. Polski radiowywiad podczas wojny z bolszewicką Rosją 1918–1920*, Warszawa 2010; M. Grajek, *Enigma...*, s. 34–39.

w projektowaniu i użyciu kodów stosowanych przez komórki podległe MSZ sprawiła, że Niemcy czytali polską korespondencję dyplomatyczną w okresie kilku przedwojennych lat⁶.

Bezdiskusyjna jest rola Maksymiliana Ciężkiego w decyzjach, które legły u podstaw zwycięstwa nad szyframi Enigmy – koncepcji pozyskania dla Biura Szyfrów matematyków przeszkolonych w zakresie kryptologii. Międzywojenna kryptologia bez istotnych wyjątków kontynuowała tradycje ukształtowane przed pierwszą wojną światową i w jej trakcie, zakładające wykorzystanie w atakach na szyfry i kody przeciwnika przede wszystkim metod lingwistycznych. Autorami najważniejszego sukcesu brytyjskich kryptologów w okresie Wielkiej Wojny, czyli złamania tzw. telegramu Zimmermana, byli wielbny William Montgomery oraz Nigel de Grey. Pierwszy był duchownym Kościoła prezbiteriańskiego, który specjalizował się w przekładach niemieckojęzycznych dzieł teologicznych na język angielski. De Grey przed podjęciem pracy w komórce kryptologicznej floty pracował w koncernie wydawniczym Williama Heinemanna, zyskując sporą biegłość w posługiwaniu się językiem niemieckim⁷. W latach 20. i 30. XX w. komórki kryptologiczne kilku państw świata zaczęły, co prawda, zatrudniać matematyków, jednak czyniły to w większej mierze ze względu na ich ogólną dyscyplinę intelektualną niż możliwość wykorzystania warsztatu matematycznego w atakach na szyfry i kody. Dr Werner Kunze rozpoczął pracę w komórce kryptologicznej niemieckiego Ministerstwa Spraw Wewnętrznych wkrótce po zakończeniu pierwszej wojny światowej. Musiało jednak minąć prawie dwadzieścia lat, zanim w 1936 r. stanął na czele nowo powołanej sekcji matematycznej służby⁸. Ojciec nowoczesnej kryptologii matematycznej

⁶ TICOM DF-187G, *Replies by Ministerrat Fenner to Questions Regarding Cryptologic Matters*, s. 11–19.

⁷ P. Gannon, *Inside Room 40. The Codebreakers of World War 1*, London 2010.

⁸ M. Grajek, *The Vanguard of Mathematicians in Cryptology*, „Wiadomości Matematyczne” 2012, z. 2 (48), s. 99–100.

William Friedman dopiero w 1930 r. umieścił w prasie ogłoszenie o zamiarze zatrudnienia w anonimowej agencji federalnej trzech matematyków. W konkursie na stanowisko „rządowego matematyka” zwyciężyli: Solomon Kullback, Frank Rowlett i Abraham Sinkov, którzy z czasem mieli stworzyć fundamenty amerykańskiej kryptologii matematycznej. Z ich wspomnień wynika jednak, że początkowo ich praca miała niewiele wspólnego z matematyką. Sinkov np. wspominał, jak wraz z kolegami pracowali nad nową księgą kodową armii USA. By zapewnić losową kolejność poszczególnych pozycji w księdze, zapisywali słowa kodu na kartkach papieru, które następnie rzucali w strumień powietrza z silnego wentylatora. Cała trójka musiała poczekać jeszcze kilka lat, zanim zaczęła wykorzystywać swój matematyczny warsztat w kryptologicznej praktyce⁹.

W tak zarysowanym kontekście podjęta w końcu 1928 r. decyzja polskiego Biura Szyfrów o organizacji kursu kryptologii dla grupy studentów matematyki nosiła jednoznacznie pionierski charakter. W naturalny sposób pojawia się pytanie o źródła tej decyzji. Ani Franciszek Pokorny, ówczesny szef Biura Szyfrów, ani Maksymilian Ciężki, jego zastępca i szef niemieckiej sekcji biura, nie mieli w dotychczasowej karierze znaczących kontaktów z matematyką i matematykami. Ciężki przerwał naukę w szamotulskiej szkole rolniczej w wieku siedemnastu lat, by założyć mundur niemieckiej armii i trafić na front we Francji. Po zakończeniu wojny, w trakcie służby w sztabie wojsk Litwy Środkowej, zdołał ukończyć szkołę średnią i zdać maturę, na tym jednak jego formalna edukacja dobiegła końca¹⁰. W dostępnych danych na temat biografii Pokornego także brak informacji o przygotowaniu

⁹ A. Sinkov, *Elementary Cryptanalysis. A Mathematical Approach*, Washington, D.C., [b.r.].

¹⁰ B. Ciężka, M. Grajek, *Maksymilian Ciężki 1898–1951*, Szamotuły 2008, s. 10–16.

matematycznym wykraczającym poza średnie wykształcenie. Skąd więc decyzja, której natura wyprzedzała resztę świata o kilka lat?

Wydaje się, że jej korzeni także należy szukać w wydarzeniach wojny polsko-sowieckiej z lat 1919–1920. Kiedy armia nieprzyjaciela zbliżała się do brzegów Wisły, szeregi Wojska Polskiego zasiliły dziesiątki tysięcy ochotników. Wśród nich znalazła się liczna reprezentacja środowisk akademickich, którą zorganizowano zresztą w znacznej części w odrębne jednostki Legii Akademickiej. Na szczęście uczyniono wyjątek od tej reguły dla trójki profesorów matematyki Uniwersytetu Warszawskiego: Stanisława Leśniewskiego, Stefana Mazurkiewicza i Wacława Sierpińskiego, których w lipcu 1920 r. przydzielono do komórki kryptologicznej Sztabu Generalnego WP. Szybko okazało się, że matematyczna dyscyplina umysłu stanowi skuteczne narzędzie w zmaganiach z szyframi przeciwnika, chociaż żaden z matematyków nie wykorzystywał ówczesnie w dekrypcji narzędzi swej dyscypliny naukowej. Począwszy od lipca 1920 r. nazwiska całej trójki regularnie pojawiają się w raportach jako autorów kolejnych dekrypcji. Ich skuteczność musiała zapaść w pamięć właściwemu twórcy i pierwszemu dowódcy komórki sztabu, która z czasem miała przyjąć nazwę Biura Szyfrów, por. Janowi Kowalewskiemu. Ten ostatni pożegnał się z Biurem Szyfrów wkrótce po zwycięstwie 1920 r.; pośrednie świadectwa potwierdzają jednak, że utrzymał ściśle kontakty ze swymi następcami. Dotyczyło to w szczególności młodego podporucznika, który właśnie zaczął służbę w niemieckiej sekcji Biura, Maksymiliana Ciężkiego. W oficjalnych archiwach nie zachowały się żadne dokumenty, które wskazywałyby na ich wzajemne relacje służbowe. W prywatnym archiwum Ciężkiego jednak znajdujemy wiele zdjęć, na których Jan Kowalewski i Maks Ciężki występują razem, a język ciała obu oficerów wyraźnie wskazuje na funkcjonowanie między nimi silnej relacji mistrz–uczeń¹¹. W trakcie rozmów z Kowalewskim Ciężki musiał

¹¹ Zdjęcia w posiadaniu Barbary Ciężkiej.

wielokrotnie słyseć o kluczowej roli matematyków w zmaganiach z sowieckimi szyframi. Gdy w 1928 r. polski wywiad stanął przed zupełnie nowym wyzwaniem niemieckiego szyfru maszynowego, Ciężki nie musiał zbyt długo poszukiwać rozwiązania – postanowił postawić na ten sam los na loterii, który już raz zagwarantował Polakom zwycięstwo.

Ograniczając się do takiego stwierdzenia, zdeprecjonowalibyśmy jednak poważnie skalę rzeczywistych zasług Ciężkiego. W rzeczywistości młody podporucznik wykazał się zadziwiająco wyobraźnią i siłą przekonania. Planując zaangażowanie matematyków w atak na szyfr Enigmy, musiał naszkicować długoterminową strategię działania. Pragnął przekonać swych przełożonych do akceptacji rozwiązania wymagającego kilkuletniej inwestycji w ludzi, zanim podejmą oni wysiłek, do którego zamierzał ich przygotować. Ciężki zakładał organizację kilkumiesięcznego kursu kryptologii dla grupy studentów matematyki. Kurs miał wyłonić kandydatów do roli terminatorów w profesji kryptologa, którzy w okresie kilku lat mieli doskonalić swój warsztat w specjalnie w tym celu zorganizowanej filii Biura Szyfrów w Poznaniu. Dopiero po upływie kilku lat można było planować przedstawienie finalnego wyzwania tym, którzy doczekają tej chwili. Prezentując swą strategię ataku na szyfry Enigmy, Ciężki nie mógł pominąć zastrzeżenia, że nie może zagwarantować jej skuteczności; należało liczyć się z możliwością, że wysiłek włożony w wyszkolenie nowej generacji kryptologów nie przyniesie oczekiwanego skutku. Oficer zaprezentował podejście, które na tle historii polskiej wojskowości nosi unikatowy charakter. Zdecydowana większość polskich triumfów militarnych nawiązuje do najbardziej chlubnych tradycji polskiego oręża; ich charakter jest zbliżony do szarży kawaleryjskiej – gwałtownej, niepowstrzymanej, jednak krótkotrwałej, po której nadchodzi nieuniknione odprężenie. Ciężki był architektem bodaj jedynego w dziejach polskiej wojskowości zwycięstwa, które wymagało długotrwałego, skoncentrowanego i całkowicie zakulisowego wysiłku. Taki charakter triumfu nad szyframi Enigmy wiele mówi o jego autorze, ale przynosi także zaszczyt tym oficerom polskiego wywiadu,

którzy wykazali się wystarczającą wyobraźnią, by zatwierdzić plan bez precedensu w dziejach Wojska Polskiego.

Ani Ciężki, szkicując swój plan ataku na szyfr, ani jego przełożeni, akceptując zamiar młodego podporucznika, ani nawet trzej kryptolodzy, wypracowując matematyczne fundamenty łamania szyfru, nie byli świadomi, że uczestniczą w przedsięwzięciu o skutkach dalece wykraczających poza doraźny efekt odczytania niemieckich depeesz. W ciągu dziesięciu lat od pierwszego przełomu ich sukces zmienił na zawsze oblicze kryptologii. Jeszcze latem 1939 r., gdy po powrocie z Warszawy szef brytyjskich kryptologów Alastair Denniston z rezygnacją godził się na zatrudnianie w swej służbie akademików, podkreślał konieczność preferencji fizyków, którzy w jego opinii i w odróżnieniu od matematyków cechowali się przynajmniej elementarnym kontaktem z rzeczywistym światem. W archiwach nie zachowały się ślady reakcji Dennistona na rzeczywistość kierowanej przezeń jednostki niespełna w rok później, gdy w Bletchley Park stopniowo zameldowała się elita młodych matematyków reprezentujących czołowe brytyjskie uniwersytety. I to właśnie oni zapewnili sukces aliantów w zmaganiach z niemieckimi szyframi w czasie drugiej wojny światowej. Pracownicy polskiego Biura Szyfrów tym bardziej nie mogli przewidzieć powojennej ewolucji kryptologii, która w ciągu około trzydziestu powojennych lat stała się jedną z dziedzin matematyki stosowanej. Ta ewolucja kryptologii dokonałaby się zapewne także niezależnie od decyzji Ciężkiego o sięgnięciu po pomoc matematyków, jednak nikt i nic nie może współcześnie kwestionować jego pierwszeństwa w wytyczeniu drogi, którą kryptologia i kryptolodzy kroczą do dziś.

Niemniej zaangażowanie matematyków nie stanowiło jedynej zasługi kierownictwa Biura Szyfrów. Matematyka umożliwiła dokonanie teoretycznego przełomu, jednak organizacja wywiadowcza, której część stanowiło Biuro, zainteresowana była przede wszystkim praktycznym uzyskaniem informacji, i to w czasie, który czynił tę informację użyteczną. Dekryptaże Enigmy dokonane w kilka miesięcy po przejściu depeesz nie

miałyby dla służby istotnego znaczenia. Należało wypracować metody i środki gwarantujące możliwie szybkie łamanie szyfru. Dzięki sukcesowi matematyków Polacy jako pierwsi stanęli przed tym problemem i jako pierwsi zaproponowali rozwiązanie: w ich opinii naturalnym adwersarzem maszyny szyfrującej była maszyna wspierająca i przyspieszająca łamanie szyfru. Począwszy od 1935 r. zaprojektowali, zbudowali i zastosowali w praktyce dekryptażu kilka pomysłowych urządzeń wspierających proces dekryptażu. Zapewne polskie Biuro Szyfrów nie stałoby się pionierem automatyzacji dekryptażu, gdyby nie inżynierskie talenty i pasje obu oficerów dowodzących – Langerera i Ciężkiego. Ten ostatni już we wczesnym okresie pracy w Biurze Szyfrów musiał zauważyć, że radiowywiad stanowi złożoną strukturę, w której technologia odgrywa kluczową rolę. Proces rozpoczyna się od samego przejęcia depeszy nadawanej przez przeciwnika, a to wymaga posiadania odbiorników radiowych o parametrach technicznych niedostępnych na otwartym rynku. Równoległe z przechwytem wiadomości należy możliwie precyzyjnie określić lokalizację nadajnika. Przechwyconą depeszę należy przekazać do centrali służby możliwie szybko i w bezpieczny sposób. Jeżeli centrala odniesie sukces w dekryptażu depeszy, należy dokonać dodatkowej obróbki wywiadowczej jej tekstu jawnego, po czym możliwie szybkim i bezwarunkowo bezpiecznym kanałem przekazać efekt do nadrzędnego sztabu. Funkcjonowanie opisanej struktury wymagało dysponowania sprzętem łączności całkowicie niedostępnym na otwartym rynku. Jego zamówienie w zwykłych firmach było dyskusyjne; wymagane parametry zdradzałyby natychmiast przeznaczenie urządzenia i zwracały uwagę adwersarza na kierunki działania radiowywiadu.

Chronologia i kwestie personalne dowodzą, że Maksymilian Ciężki musiał być co najmniej jednym z inicjatorów stworzenia firmy, która funkcjonując w sposób otwarty, jednak z dyskretnym udziałem wywiadu i pod jego nadzorem, byłaby zdolna do realizacji poufnych zamówień wywiadu, a w szczególności Biura Szyfrów. Dyrektorem technicznym utworzonej w tym celu firmy Wytwórnia Radiotechniczna „AVA”

został inż. Antoni Palluth, jeden z najbliższych przyjaciół Ciężkiego jeszcze z czasów powstania wielkopolskiego i zarazem pracownik Biura Szyfrów. Początkowo „AVA” specjalizowała się w projektowaniu i produkcji sprzętu radiowego. Zaprojektowała dla Wojska Polskiego m.in. wiele radiostacji lotniczych i okrętowych, jak również specjalistyczne odbiorniki szerokopasmowe oraz sprzęt goniometryczny. Osiągnięte dzięki temu doświadczenie pozwalało inżynierom i pracownikom firmy realizować także mniej typowe zamówienia Biura Szyfrów. Kiedy w 1933 r. Marian Rejewski dokonał pełnej rekonstrukcji Enigmy wyłącznie na podstawie wniosku matematycznego, „AVA” w krótkim terminie wyprodukowała kilkadziesiąt egzemplarzy polskiego odpowiednika maszyny, identycznej funkcjonalnie, choć nie konstrukcyjnie, z oryginałem. Później, w latach 1935–1938, firma uczestniczyła w projektowaniu i konstrukcji innych urządzeń wspierających dekryptaż Enigmy, cyklometrów i tzw. bomb Rejewskiego.

W archiwach zachowały się nieliczne potwierdzenia udziału Gwidona Langer i Maksymiliana Ciężkiego w pracach o technicznym charakterze. Zapewne najbardziej dobitnym potwierdzeniem ich pasji i talentów inżynierskich było zaangażowanie obu oficerów w konstrukcję polskiej maszyny szyfrującej znanej pod akronimem utworzonym z pierwszych liter nazwisk jej konstruktorów – LCP lub LCD. Do dziś nie udało się rozstrzygnąć kwestii trzeciego nazwiska; nie wiemy, czy współkonstruktorem maszyny był Antoni Palluth, czy któryś z braci Danilewiczów, Ludomir albo Leonard. Jest jednak bezsporne, że pierwsze dwie litery w nazwie odnoszą się do Langer i Ciężkiego. Wspomnienia przechowane w tradycji rodzin Gwidona Langer, Maksymiliana Ciężkiego i Antoniego Pallutha potwierdzają, że cała trójka współdzieliła techniczne zainteresowania i nadawała im jednoznacznie praktyczny wymiar. Palluth po dniu pracy spędzonym w biurach „AVA” często udawał się do siedziby Biura Szyfrów, gdzie pracował nad konstrukcją urządzeń służących do dekryptażu. Analogicznie Langer i Ciężki po dniu służby w siedzibie sztabu nierzadko pojawiali się w biurze konstrukcyjnym lub warsztatach

firmy, gdzie zawijali rękawy i stawali za deską kreślarską lub przy stole warsztatowym, pracując nad prototypami urządzeń. Zachowane w archiwum wojskowym okresowe opinie wystawiane oficerom przez ich przełożonych szczególnie podkreślają ich zainteresowania i kompetencje techniczne¹². Opinie te znajdują potwierdzenie we wspomnieniach rodzin obu oficerów; obaj zgromadzili obszerne i stale aktualizowane biblioteki literatury fachowej w kilku językach dotyczącej dyscyplin kluczowych dla ich profesji.

Współcześnie wśród kryptologów i historyków funkcjonuje konsensus, że aliancki sukces w atakach na niemieckie szyfry w okresie drugiej wojny światowej stanowił wypadkową dwóch całkowicie nowatorskich koncepcji: zastosowania w atakach na szyfry metod matematycznych oraz wsparcia procesu dekryptażu przez specjalistyczne urządzenia elektromechaniczne. Jest kwestią całkowicie bezdyskusyjną, że pionierami zastosowania obu koncepcji byli oficerowie dowodzący polskim Biurem Szyfrów – Gwido Karol Langer i Maksymilian Ciężki. W tym sensie musimy postrzegać ich nie tylko jako właściwych architektów triumfu nad szyframi Enigmy, ale przede wszystkim jako innowatorów, których poszukiwania i decyzje otworzyły drogę do wojennych sukcesów alianckich kryptologów.

¹² Centralne Archiwum Wojskowe Wojskowego Biura Historycznego im. gen. broni Kazimierza Sosnkowskiego, Warszawa-Rembertów, Kolekcja Akt Personalnych 1918–1939, Spis zdawczo-odbiorczy nr 1769/89, akta przekazane z MSW, sygn. AP 1769/89/2897 oraz \$.

Marek Grajek

Odnaleziony raport – czego nowego dowiedzieliśmy się o historii złamania Enigmy?

Raport polskich kryptologów odnaleziony we francuskich archiwach nie wzbudzi zapewne w środowisku historyków zajmujących się dziejami złamania szyfru Enigmy istotnej sensacji. Wręcz przeciwnie – umacnia on tę wersję historii, która nie sięga po elementy sensacyjne, eksponując raczej systematyczną pracę i wysiłek intelektualny autorów kryptologicznego przełomu. Kiedy jednak zaakceptujemy tak zdefiniowaną płaszczyznę dyskusji i przyjrzymy się szczegółom, okaże się, że zawarte w raporcie informacje rzucają sporo światła na tezy przyjmowane dotąd przez historyków Enigmy bez istotnej dyskusji i krytyki. Taka analiza jest o tyle ciekawa dla rodzimych komentatorów, że pozwala poszerzyć skalę sukcesu kryptologów polskiego Biura Szyfrów poza te elementy, które międzynarodowa społeczność historyków była gotowa przyznać im do tej pory.

W literaturze trwa spór o znaczenie dokumentów dostarczonych Polakom przez francuski wywiad. Francuzi, a w ślad za nimi historycy innych państw utrzymują, że dopiero dostarczona przez Bertranda instrukcja użycia maszyny pozwoliła Marianowi Rejewskiemu sformułować matematyczny model maszyny zawarty w jego znanym układzie równań. W rozdziale 2 raportu, poświęconym początkom zmagania Biura Szyfrów z Enigmą, Rejewski potwierdza jednak, że polski wywiad zdobył istotne informacje na temat maszyny na długo przed tym, jak Gustave Bertrand jesienią 1931 r. przekazał Polakom dwa dokumenty pochodzące od Hansa-Thilo Schmidta. Można się było tego domyślać

na podstawie znanych wcześniej wspomnień Rejewskiego; opisując najwcześniejszy etap ataku na szyfr Enigmy, posługiwał się on nomenklaturą odnoszącą się raczej do Enigmy G niż modelu I, którego dotyczyły rewelacje Bertranda. Opisany przez Rejewskiego zakres wiedzy Polaków na temat Enigmy oraz posługiwanie się terminologią odnoszącą się do Enigmy G wskazują, że rozpoczął on prace nad matematycznym modelem maszyny na podstawie danych zdobytych samodzielnie przez polski wywiad. Dokumenty dostarczone przez Bertranda jedynie potwierdziły i uszczegółowiły przyjęte założenia.

Rozdział 4 stanowi kompromis pomiędzy zobowiązaniami wobec zleceniodawcy prac a własną dumą zawodową. Z informacji pochodzących z raportu Langera wiadomo, że raport powstał na zlecenie Bertranda i miał zaprezentować wkład trzech państw w złamanie Enigmy. Znając charakter Bertranda z innych źródeł, możemy założyć, że oczekiwał on potwierdzenia znaczącej, jeśli nie kluczowej, roli Francji oraz własnej w tym sukcesie. Jego przekonanie o decydującej roli w przedsięwzięciu umacniały chociażby pochlebstwa zawarte w korespondencji z brytyjskim partnerem. 3 sierpnia, wkrótce po powrocie z Polski, szef brytyjskich kryptologów Alastair Denniston pisał do Bertranda: „(...) pragnę podkreślić, że zawdzięczamy wszystko wyłącznie Panu, liczę na przyszłą współpracę naszego trio, w której Pan musi zająć wiodącą pozycję”. W tych okolicznościach kryptolodzy musieli wskazać na jakąkolwiek okoliczność pozwalającą docenić rolę Francji i Francuzów. Znaleźli ją w dokumentach dostarczonych Polakom w latach 1931–1932. Odnotowali, że: „(...) posiadanie dokumentów, a w szczególności klucza dziennego, w rozstrzygający sposób wpłynęło na postęp prac. Bez nich rozwiązanie szyfru Enigmy opóźniłoby się co najmniej o lata”. Pierwsze zdanie stanowi dodatkowe potwierdzenie wniosku sformułowanego powyżej. Autorzy raportu podnoszą znaczenie wyłącznie znajomości klucza dziennego, dając tym samym do zrozumienia, że dostarczona instrukcja obsługi Enigmy nie była dokumentem istotnym. Oznacza to zapewne, że Rejewski był w stanie zbudować matematyczny model

maszyny na podstawie informacji zdobytych przez polski wywiad wcześniej i samodzielnie. Polacy podkreślają rozstrzygające znaczenie znajomości kluczy dziennych wyłącznie po to, żeby natychmiast zrelatywizować to twierdzenie; bez niego rozwiązanie szyfru Enigmy zapewne także okazałoby się możliwe, choć „(...) opóźniłoby się co najmniej o lata”. Temat rozwiązania Enigmy bez dokumentów dostarczonych przez Francuzów powraca nieco dalej, gdy w rozdziale 7 autorzy raportu szkicują zarys metody, która zapewne pozwoliłaby złamać szyfr także bez pomocy z zewnątrz. Współcześni kryptolodzy potwierdzili, że zarysowana metoda rzeczywiście prowadzi do złamania szyfru, ale pod warunkiem zrealizowania pewnych założeń dotyczących materiału szyfrowego. Brak depesz archiwalnych z tego okresu nie pozwala potwierdzić, czy założenia te rzeczywiście zostały spełnione. Musimy zatem przyjąć zapewnienie autorów, że wkład Francuzów okazał się decydujący dla praktycznego sukcesu w zmaganiach z Enigmą. Jednak po potwierdzeniu tego faktu Rejewski i jego koledzy natychmiast osłabili siłę własnego argumentu i wykazali, że na gruncie teorii kryptologicznej poradziliby sobie także bez dostarczonych kluczy, łamiąc Enigmę metodami czysto matematycznymi.

Zapewne redagując rozdział 6, autorzy nie zdawali sobie sprawy, że toczą w nim zdalną polemikę z kryptologami brytyjskimi. W rozdziale 5 kryptolodzy opisali, w jaki sposób odtworzyli połączenia walca wejściowego: „(...) problem sprowadzał się do niezajomości podstawienia E. Wydaje się, że właśnie na nim załamały się wysiłki kryptologów brytyjskich. Późniejsze badania polskiego Biura Szyfrów dowiodły, że podstawienie E może zostać wyznaczone analitycznie (pod warunkiem znajomości podstawienia S), w rzeczywistości jednak znaleziono je metodą prób i błędów”.

Takie określenie niezupełnie oddaje istotę sukcesu Mariana Rejewskiego. Dla rekonstrukcji podstawienia E posłużył się on nie tyle metodą prób i błędów, ile intuicją i znajomością niemieckiej mentalności. Wiedząc, że w handlowym modelu maszyny połączenia walca wejściowego

odpowiadają układowi klawiszy maszyny, założył, że w modelu wojskowym systematyczni Niemcy także sięgnęli po jakąś formę porządku. Najprostszą możliwością był układ alfabetyczny i to właśnie on okazał się poprawnym rozwiązaniem. Sukces osiągnięty na skrót nie usatysfakcjonował jednak Rejewskiego i z czasem opracował on również czysto analityczną metodę rekonstrukcji połączeń walca, którą opisano w rozdziale 6 raportu. Autorzy z pewnością nie byli świadomi, że w raportach z Warszawy i w późniejszych opracowaniach brytyjskich kryptologów rekonstrukcja walca wejściowego stała się jednym z kluczowych zagadnień. Dillwyn Knox już w pierwszym raporcie z Warszawy zauważył, że: „(...) Polacy czytali maszynę do 15 września 1938 r. dzięki szczęściu”. Odnosił się do odnalezienia przez Rejewskiego połączeń walca wejściowego, przypisując większą rolę szczęściu niż psychologicznej intuicji kryptologa. W trakcie spotkania w Pyrach Rejewski najwyraźniej usiłował przekonać rozmówcę, że niezależnie od rozwiązania opartego na intuicji opracował także matematyczną metodę rekonstrukcji połączeń walca. Ten fragment rozmowy musiał toczyć się w języku francuskim, Brytyjczyk zanotował bowiem deklarację Polaków w wersji: „(...) nous l'aurion pu trouver aussi par mathematique”¹, po czym udał słabą znajomość tego języka i dodał, że deklaracja zapewne odnosiła się do... daty znalezienia rozwiązania. Opinia Knoxa rzucała długi cień na późniejszą percepcję zagadnienia w gronie brytyjskich kryptologów. W jednym z powojennych raportów, sporządzonym w 1945 r., Stuart Milner-Barry zapisał, że: „(...) kluczowy element, połączenia walca wejściowego, otrzymali od agenta, choć utrzymywali, bez wątpienia słusznie, że mogli byli zrekonstruować je także matematycznie”. Zainicjowana przez Knoxa narracja, zgodnie z którą łut szczęścia miał być decydującym czynnikiem sukcesu Polaków, wkrótce po zakończeniu wojny rozwinęła się w wersję pokutującą przez dziesięciolecia: w złamaniu Enigmy kryptologów wyręczyli agenci. Taka narracja utrzymywała się

¹ (...) mogliśmy [je] znaleźć także [metodami] matematycznymi.

mimo tego, że w alianckich archiwach były dostępne dokumenty jednoznacznie potwierdzające intelektualną uczciwość Polaków.

Treść rozdziału 13 jest znana z innych dokumentów, w których opisano polskie metody łamania szyfru, mimo to zasługuje na krótki komentarz. Opisano w niej metodę identyfikacji prawego wirnika z wykorzystaniem metody zaproponowanej przez Jerzego Różyckiego, znanej w gronie polskich kryptologów jako „metoda zegara”. Wykorzystuje ona właściwość szyfru opisaną pierwotnie w 1922 r. przez ojca współczesnej kryptologii amerykańskiej Williama Friedmana i określaną współcześnie mianem indeksu koincydencji. Od dawna zainteresowanie badaczy budziło to, że opis metody stosowanej przez Polaków w żadnym stopniu nie odwoływał się do terminologii zaproponowanej przez jej pierwotnego odkrywcę. Oryginalna praca Williama Friedmana zawierająca opis indeksu koincydencji została utajniona niezwłocznie po publikacji i doczekała się odtajnienia dopiero w latach 70. XX w. Krótki okres jej dostępności sprawił, że jej zasada działania była znana w wybranych kręgach kryptologów, zwłaszcza w USA i we Francji, w której wydano reprint pracy Friedmana. Narzuca się pytanie, czy Jerzy Różycki lub którykolwiek z jego kolegów poznał koncepcję indeksu koincydencji w trakcie szkolenia, czy też opracował ją samodzielnie, odkrywając jedno z najważniejszych narzędzi współczesnej kryptologii niezależnie od Friedmana. Marian Rejewski zapisał, że w trakcie pobytu we Francji stwierdził, iż program kursu kryptologicznego realizowanego w Poznaniu w 1929 r. był ściśle oparty na książce jednego z najlepszych kryptologów francuskich Marcela Givierge'a zatytułowanej *Cours de cryptographie*. W dostępnym współcześnie angielskim tłumaczeniu tej książki nazwisko Friedmana i wzmianka o indeksie koincydencji występują wyłącznie w jednozdaniowym przypisie odsyłającym do publikacji niedostępnej w trakcie poznańskiego kursu oraz pracy Polaków nad szyfrem. W tej sytuacji znaczenia nabiera treść oryginalnego, francuskojęzycznego wydania książki. Być może indeks koincydencji został w nim omówiony szerzej? Poszukiwania autora prowadzone wspólnie z Philippem

Guillotem pozwoliły dotrzeć do oryginalnego wydania publikacji. Wzmianka o indeksie koincydencji ma w nim strukturę identyczną jak w tłumaczeniu angielskim; jednozdaniowa nota nie pozwalała poznać natury narzędzia. Spostrzeżenie to nie rozstrzyga samo przez się o możliwości niezależnego odkrycia indeksu koincydencji przez Jerzego Różyckiego, choć zwiększa prawdopodobieństwo takiego biegu wydarzeń.

W literaturze zwykło się przyjmować, że zmiany sposobu użycia Enigmy wprowadzone 15 września i 15 grudnia 1938 r. pokonały metody dekryptażu wykorzystywane przez Polaków, uzależniając dalsze czytanie szyfrogramów sporządzanych przy użyciu tej maszyny od dwóch nowych metod – bomby oraz płacht Zygalskiego. Dillwyn Knox podkreślił w raporcie z warszawskiej konferencji, że polski dekryptaż Enigmy dobiegł kresu po zmianie procedury szyfrowania wprowadzonej 15 września 1938 r.: „Polacy czytali maszynę do 15 września 1938 r. dzięki szczęściu”. Treść rozdziału 21 potwierdza nieskuteczność większości opracowanych wcześniej metod ataku, przeczy jednak twierdzeniu o oparciu dekryptażu wyłącznie na bombach i płachtach. W tym okresie polscy kryptolodzy posiadli już tak głęboką znajomość subtelności szyfru Enigmy, że w wielu wypadkach potrafili sobie radzić, wychytując zależności znaków klucza depeszy całkowicie nieczytelne dla innych osób. Być może właśnie metody opisane w rozdziale tłumaczą, w jaki sposób Polacy byli zdolni czytać szyfr w pierwszej połowie 1939 r., gdy bomby utraciły skuteczność, a płachty Zygalskiego nie były jeszcze gotowe. Wbrew twierdzeniom kryptologów brytyjskich Biuro Szyfrów czytało co najmniej wybrane niemieckie depesze do ostatnich dni przed wybuchem wojny. W rozdziale 27 autorzy raportu podkreślają, że: „(...) [m]iesiąc później wybuchła wojna niemiecko-polska. Udało się jeszcze złamać depesze z 25 sierpnia 1939, dnia powszechnej mobilizacji w Niemczech”. W tym czasie bomby były już bezużyteczne, a Polacy posiadali komplety płacht Zygalskiego wyłącznie dla dwóch spośród sześćdziesięciu możliwych kolejności wirników. Skądinąd wiadomo, że w tym okresie klucze do szyfru używane przez niemieckie siły zbrojne

obligatoryjnie wykorzystywały co najmniej jeden z nowych wirników wprowadzonych do użytku w grudniu 1938 r., toteż płachty w dyspozycji Biura Szyfrów nie gwarantowały rozwiązania. Polscy kryptolodzy musieli łamać szyfr innymi metodami, zapewne zbliżonymi do zarysowanych w rozdziale 21.

W standardowej historii złamania szyfru Enigmy istotny wkład Polaków dobiega końca z chwilą zakończenia konferencji w Pyrach. W jej trakcie Polacy przekazują całość swej wiedzy brytyjskim i francuskim kolegom, po czym ciężar wydarzeń przesuwają się do Londynu. Ślad takiej percepcji także pojawia się w raporcie, w rozdziałach opisujących wydarzenia po wybuchu wojny (tj. począwszy od rozdziału 27). W wyniku godnych pożałowania machinacji wojskowego kierownictwa na emigracji polscy kryptolodzy zostają pozbawieni przywileju służby w szeregach własnej armii i przekazani pod dowództwo francuskie. Okazuje się przy tym, że na polską ekipę nie czekają przedstawiciele gospodarzy zdolni przyjąć i wykorzystać jej wiedzę – Polacy (wraz z grupką republikańskich rozbitek hiszpańskich) stanowią główną, jeśli nie jedyną, kompetentną ekipę kryptologów we Francji. Francuzi nie zdołali nawet skopiować sprzętu, którego dokumentację i egzemplarz otrzymali w trakcie konferencji w Pyrach. W rezultacie Polacy odnosili się do własnej pracy z dozą cichej rezygnacji: „(...) polscy kryptolodzy siedzieli bez przerwy nad Enigmami stukając depesze i manipulując płachtami, by nie pozwolić się całkowicie zdystansować Anglikom. Była to całkowicie mechaniczna praca, którą mógł wykonać personel pomocniczy. W tej sytuacji było zrozumiałe, że polscy kryptolodzy nie osiągnęli już istotnych rezultatów kryptologicznych, a punkt ciężkości prac teoretycznych przesunął się do Londynu”.

W raporcie zaczynają się przewijać odniesienia do sukcesów brytyjskich kolegów. Okazuje się przy tym, że niektóre z nich miały swe źródło w pracach polskiego Biura Szyfrów: „(...) brytyjscy kryptolodzy urzeczywistnili jeszcze jedną metodę zaproponowaną wcześniej przez Polaków”. Pomysł sprowadzał się do sporządzenia katalogu określającego

nie tylko lokalizację przypadków żeńskich, lecz także określenie znaków, których dany przypadek dotyczył. Posiadanie takiego katalogu ułatwiało weryfikację możliwych rozwiązań zidentyfikowanych z wykorzystaniem płacht Zygalskiego. Polacy nie zdołali zrealizować pomysłu samodzielnie, ponieważ ogrom pracy niezbędnej do wykonania katalogu wymagał jej automatyzacji. Brytyjczycy, którzy skonstruowali niezbędne urządzenie do wykonania płacht, wykorzystali je obecnie także do realizacji polskiego pomysłu towarzyszącego płachtom katalogu: „(...) [d]zięki swoim możliwościom finansowym i organizacyjnym [Brytyjczycy] wprowadzili w życie nasze plany, które w innym przypadku nie ujrzałyby światła dziennego”. Opisywana metoda ataku jest znana także ze źródłowych dokumentów brytyjskich, w których jednak brak odniesień do jej polskich korzeni.

W rozdziale 31 opisano zmiany wprowadzone przez przeciwnika w przededniu kampanii francuskiej. Rezygnacja z dwukrotnego szyfrowania klucza depeszy stanowiła ciężki cios dla Polaków, którzy opierali na nim większość, jeśli nie wszystkie, używanych metod dekryptażu. Ale to właśnie Polacy wykryli przygotowywaną zmianę i rozpracowali strukturę nowego systemu. Niektórzy niemieccy szyfranci zastosowali ją przedwcześnie, w przeddzień oficjalnego wprowadzenia. Polacy w tym okresie dysponowali już wyprodukowanymi przez Brytyjczyków kompletami płacht Zygalskiego i regularnie łamali klucze niemieckich depesz. Dysponując kluczami do szyfru na dzień 30 kwietnia, zidentyfikowali depesze oparte na procedurze, która miała wejść do powszechnego użytku w dniu następnym. Bez trudu rozpracowali naturę nowego systemu i jego charakterystykę przekazali do Londynu.

Wdrożenie nowego szyfru lub nowej procedury szyfrowania stanowi rutynowe działanie poprzedzające ważne operacje wojskowe. W dziesięć dni po wdrożeniu przez Wehrmacht i Luftwaffe zmian w sposobie użycia Enigmy ruszyło niemieckie natarcie na państwa Beneluxu i Francję. W ciągu kluczowych dni kampanii alianccy kryptolodzy nie byli w stanie wspierać swych wojsk – nie zdołali dotąd opracować metody łamania

nowego klucza do szyfru. Dopiero 22 maja, gdy kampania francuska była rozstrzygnięta, przełom przyniosło zastosowanie przez Brytyjczyków nowej metody łamania szyfru opracowanej przez Johna Herivela i opisaney w rozdziale 30 raportu. Na kanwie brytyjskiego sukcesu pewna satysfakcja przypadła także Polakom. Herivel opracował swą metodę jeszcze w lutym 1940 r., jednak do tej pory nie pozwalała ona złamać szyfru. Przyczyną była błędna identyfikacja punktów przeskoku dwóch wirników Enigmy dodanych w grudniu 1938 r. Kiedy jednak kampania w Norwegii przyniosła obfitość materiału szyfrowego, Polacy zdołali skorygować wcześniejsze hipotezy: „(...) korekty zostały znalezione i natychmiast zakomunikowane Anglikom. Dopiero po nich metoda Herivela mogła zostać efektywnie zastosowana”. Nie znalazło to jednak odzwierciedlenia w źródłach brytyjskich.

Aż do rozdziału 31 raport ma strukturę chronologiczną. Począwszy od rozdziału 32, poświęconego łamaniu szyfrów SD, chronologia ulega jednak załamaniu – ostatnie rozdziały raportu zostały najwyraźniej dodane jako odrębne bloki o tematycznym charakterze. Najbardziej interesujący, jeśli nie fascynujący, jest blok poświęcony łamaniu szyfrów Kriegsmarine, rozpoczynający się od rozdziału 33. Sam fakt łamania przez Polaków depesz Kriegsmarine był znany z wcześniej dostępnych materiałów, ale jego szczegóły, a przede wszystkim zakres, pozostawały niedostępne. Wskutek braku danych na temat osiągnięć Polaków ugruntowało się przekonanie, że główny ciężar zmagania z Enigmą Kriegsmarine wzięli na swe barki kryptolodzy brytyjscy, a największy wkład w późniejszy sukces wniósł Alan Turing. Informacje zawarte w rozdziałach 33–35 zmuszają do ponownej analizy przyjętej wersji historii.

Kilka komentarzy rozproszonych w raporcie potwierdza, że z przyczyn czysto praktycznych łączność niemieckiej marynarki nie mieściła się w centrum zainteresowań polskiego Biura Szyfrów. W rozdziale 2 znajdujemy informację, że: „(...) [j]eszcze w wiele lat po utworzeniu polskiego Biura Szyfrów brak kadr nie pozwalał poświęcać uwagi materiałowi szyfrowemu napływającemu z niemieckiej marynarki”. Także

w rozdziale 34 kryptolodzy uskarżają się na trudności w atakach na Enigmę Kriegsmarine wynikające z „(...) niewystarczającego materiału szyfrowego”. Uwzględniając, że Polska nie była morską potęgą, drugoplanowy charakter prac nad szyframi niemieckiej marynarki jest całkowicie zrozumiały. Mimo to Biuro Szyfrów osiągnęło w tej dziedzinie bardzo znaczące rezultaty.

Opis kodów wykorzystywanych przez Kriegsmarine przed wdrożeniem Enigmy (rozdział 33) nie mieści się w zakresie niniejszej analizy. Przygoda Polaków z Enigmą Kriegsmarine rozpoczęła się formalnie z początkiem 1926 r., po wdrożeniu w marynarce modelu Enigma C, a w sensie praktycznym w 1933 r., gdy kryptolodzy postanowili zastosować wobec archiwalnych depeesz metody, które wypracowali i skutecznie zastosowali w ataku na szyfry Enigmy wojsk lądowych. Ten atak przyniósł natychmiastowy sukces, ułatwiony dzięki brakowi w Enigmie C łącznicy. Polacy trafnie zidentyfikowali cechy modelu maszyny (29 klawiszy, ruchomy reflektor, specyficzna rola litery X itd.). Zauważyli też najważniejszą cechę szyfrów Kriegsmarine – odmienność wykorzystywanych procedur od tych używanych w innych rodzajach sił zbrojnych. Od najwcześniejszego okresu trójliterowe klucze depeesz nie były wybierane samodzielnie przez szyfrantów, lecz pobierane z listy kluczy. Ponadto były one losowo uzupełniane do czterech znaków, co sygnalizowało zamiar wdrożenia w późniejszym okresie maszyny czterowirnikowej.

Powszechnie przyjmuje się, że 1 października 1934 r. Enigma C została zastąpiona w Kriegsmarine przez model Enigma M1, tożsamy co do zasady z wykorzystywanym w armii lądowej modelem Enigma I (różnice dotyczyły m.in. opisu pierścieni maszyny: liczbowych w przypadku maszyny Wehrmachtu, literowych w Kriegsmarine). Autorzy raportu opisują jednak sposób wykorzystania Enigmy C jeszcze w 1936 r. – tekst jawny był przed zaszyfrowaniem kodowany znanym z wcześniejszej praktyki kodem czteroznakowym. Wynika stąd wniosek, że Enigma M1 nie tyle zastąpiła Enigmę C, ile została wprowadzona równoległe do niej, a z czasem wyparła starszy model z użytku. Niemieccy kryptolodzy, świadomi

słabości związanej z brakiem łącznicy, usiłowali podnieść bezpieczeństwo szyfru tworzonego przez maszynę typu C i wymagali kodowania tekstu jawnego przed jego szyfrowaniem Enigmą. Środki ostrożności, które podejmowali, okazały się jednak bezskuteczne: Polacy rozpracowali zarówno konstrukcję maszyny, jak i nietypowe procedury szyfrowania wiążące się z jej użyciem.

Najbardziej interesujące są zawarte w raporcie informacje dotyczące użycia w Kriegsmarine Enigmy M1, wykorzystywanej w marynarce (z pewnymi zmianami) od 1 października 1934 r. do końca drugiej wojny światowej. Raport zawiera informację o ciekawej i wcześniej nieznannej niekonsekwencji kryptologów Kriegsmarine. W wersji wprowadzonej do użytku 1 października 1934 r. Enigma M1 była wyposażona w pięć wirników, spośród których w maszynie montowano trzy (podobnie jak w maszynach Wehrmachtu i Luftwaffe począwszy od grudnia 1938 r.). Pozwalało to na łamanie kluczy depesz w dniach, w których obejmowały one jedynie wirniki znane z Enigmy wojsk lądowych. Stanowiły one około dziesięć procent wszystkich depesz. Ta liczba umożliwiała potwierdzenie praktyki znanej z okresu użycia Enigmy C, tj. czerpanie kluczy depesz wyłącznie z listy przygotowanej wcześniej, ale była niewystarczająca do rekonstrukcji kompletnej listy kluczy. Z raportu wynika, że 16 listopada 1936 r. nieoczekiwanie wycofano z użytku dwa dodatkowe wirniki; pozostawiono wyłącznie wirniki znane z Enigmy Wehrmachtu. Pozwoliło to na łamanie bieżących depesz za pomocą tych samych metod, którymi łamano depesze wojsk lądowych i lotnictwa. Złamane depesze umożliwiły pełną rekonstrukcję listy kluczy, której znajomość stanowiła przepustkę do depesz archiwalnych sprzed zmiany – wystarczyło skorzystać ze starej metody rusztu, aby określić połączenia dodatkowych wirników używanych przed listopadem 1936 r. Polacy nazwali je wirnikami IVM i VM, od M jak *Marine* (marynarka), żeby uniknąć konfuzji ze standardowymi wirnikami IV i V. Odczytanie depesz archiwalnych pozwoliło na zidentyfikowanie (oprócz bazowego) także dwóch specjalnych wariantów szyfru: oficerskiego i sztabowego (admiralskiego). Biuro

Szyfrów rozpracowało całkowicie wariant oficerski, dla sztabowego natomiast zabrakło czasu i zapewne materiału szyfrowego.

1 maja 1937 r. nastąpiła kolejna zmiana procedury szyfrowania. Od-tąd indywidualny klucz depeszy nie był szyfrowany z wykorzystaniem maszyny, ale za pomocą zewnętrznego podstawienia, niezależnego od Enigmy. Podobnie jak przy innych zmianach, także i tu Niemcy popełnili błąd, który mógł ich kosztować sekret szyfru. Torpedowiec o sygnale wywoławczym AFA nie otrzymał w porę informacji o nowej procedurze szyfrowania (lub tabel pozwalających na szyfrowanie klucza depeszy) i w ciągu kilku pierwszych dni maja wykorzystywał starą procedurę, rozpracowaną przez polskie Biuro Szyfrów. W rezultacie Polacy odczytali wiele depesz Kriegsmarine z okresu 1–8 maja 1937 r. Okazało się, że ustawienia maszyny nie uległy zmianie od 27 kwietnia do 8 maja, co dało kryptologom obszerny materiał do analiz. Pozwolił on w znacznej mierze określić sposób szyfrowania klucza depeszy. Okoliczności złamania szyfru Kriegsmarine po zmianie w maju 1937 r. są epizodem, który w analizowanym dokumencie jest opisany nieco mniej szczegółowo niż w raportach z Bletchley Park, zwłaszcza w oficjalnej *Historii Baraku 8* pod redakcją Mahona (szczegóły dotyczące sygnału wywoławczego okrętu, którego depesze umożliwiły Polakom włamanie do szyfru, pochodzą właśnie z tego raportu). W konkluzji epizodu Mahon zapisał, że: „(...) [Polacy] stosując opisaną metodę łamali około 16 depesz dziennie dochodząc do wniosku, że szyfrowanie klucza depeszy stanowi jakąś formę podstawienia bigraficznego, jednak nie posunęli się znacznie poza ten punkt. (...) Polacy zwrócili uwagę na jeszcze jedną możliwość, tzn. że trygramy nie były wybierane przypadkowo”. Opis Mahona potwierdza, że Polacy trafnie zidentyfikowali kluczowe cechy procedury szyfrowania klucza depeszy, a pójście dalej wymagało rekonstrukcji lub zdobycia tabel używanego w niej podstawienia bigraficznego.

Do tej pory materiał zawarty w polskim raporcie uzupełniał lub korygował informacje zamieszczone w powojennych raportach z Bletchley Park. Dotarliśmy do miejsca, w którym polskie i brytyjskie raporty nieco

się rozchodzą. Zgodnie z raportami brytyjskimi Alan Turing poszerzył szczelinę otwartą przez Polaków: „Turing w istocie rozwiązał najważniejszą część problemu klucza depezy”². W rzeczywistości brytyjski matematyk nie wyszedł poza punkt osiągnięty w 1937 r. przez zespół Biura Szyfrów i nie mógł przekroczyć tego punktu tak długo, jak długo tablice bigramów pozostawały nieznane. Zgodnie z oficjalną *Historią Baraku 8* przełom nadszedł dopiero 19 kwietnia 1940 r. W trakcie kampanii norweskiej Brytyjczycy zdobyli i przeszukali uzbrojony niemiecki trawler „Polares”. W ich ręce wpadły dokumenty, które „(...) dostarczyły precyzyjnych informacji na temat sposobu szyfrowania klucza depezy, ustawienia łącznicy i pozycję bazową 23 i 24 kwietnia”³. Zdobyte dokumenty ostatecznie potwierdziły trafność wcześniejszych ustaleń Polaków oraz zgodnych z nimi domysłów Alana Turinga. Przełom był jednak połowiczny: dzięki „fantowi z Narwiku” Brytyjczycy zdołali odczytać depeze z sześciu dni, od 22 do 27 kwietnia, po czym (poza incydentalnymi sukcesami) Enigma Kriegsmarine ponownie zamilkła na rok; nadal brakowało tablic bigramów. Dopiero 9 maja 1941 r. na pokładzie opuszczonego przez załogę okrętu podwodnego U-110 znaleziono nie tylko instrukcje obsługi, lecz także tabele bigramów, które umożliwiły efektywny start dekryptażu szyfrów niemieckiej marynarki.

Na gruncie teorii łamania szyfrów Kriegsmarine Brytyjczycy nie wyszli poza punkt osiągnięty przez polskich kryptologów jeszcze w 1937 r. Przełom stał się możliwy dopiero po zdobyciu dokumentów na pokładzie U-Boota, dzięki czemu brytyjscy kryptolodzy zdołali utrzymać kontrolę nad szyfrem mimo późniejszych zmian. Nieco przewrotnie można w tym miejscu przypomnieć przedwojenną opinię Knoxa na temat sukcesu polskich kryptologów: „(...) [n]igdy tego nie rozpracowali, musieli to ukraść przed laty, a następnie obserwowali rozwój, jak każdy by potrafił, jednak na początku musieli to ukraść lub kupić”. Okazuje się

² A.P. Mahon, *The History of Hut Eight*, United Kingdom 2010, s. 14.

³ *Ibidem*, s. 22.

jednak, że to właśnie powodzenie brytyjskiego ataku na szyfry Kriegsmarine opierało się na dokumentach zdobytych na pokładzie niemieckiego okrętu.

Ostatni rozdział raportu potwierdza, że przytoczone przez pułkownika Langerę okoliczności jego powstania odpowiadają faktom. Zadaniem autorów było sporządzenie swego rodzaju inwentaryzacji wkładu trzech krajów w triumf nad Enigmą. Jego autorzy poszli po linii najmniejszego oporu. W zasadniczej części raportu podkreślali raczej korzyści ze współpracy kryptologów trzech państw, niż rozbierali na części składowe zasługi wniesione przez każdą nację z osobna. Dopiero w zakończeniu raportu dodali tabelaryczne podsumowanie, w którym sumiennie wyliczyli elementy sukcesu, dzieląc je pomiędzy współpracujące państwa. Taka forma wzbudziła irytację inicjatora raportu. Zlecając jego wykonanie, musiał być on przekonany, że wydzwitek całości będzie jednoznaczny i przypisze Francji oraz jemu samemu przewodnią rolę w kryptologicznym triumfie. Tymczasem w tabeli pracowicie wyliczono ponad dwadzieścia elementów wniesionych przez Polaków, sześć elementów wkładu Brytyjczyków i zaledwie jeden istotny element wkładu Francuzów – dostarczenie dwóch ważnych dokumentów. Bertrand musiał czuć się rozczarowany. Przez kilka lat sumiennie dostarczał Polakom klucze do szyfru przekazywane przez niemieckiego zdrajcę i miał nadzieję, że tak istotny z jego punktu widzenia wkład znajdzie odzwierciedlenie w bilansie.

Nie wiedział, że decyzją szefów polskiego Biura Szyfrów klucze trafiają prosto do sejfu Maksymiliana Ciężkiego i nie docierają na biurka kryptologów. Ciężki wychodził z rozsądnego założenia, że w przypadku wzrostu napięcia międzynarodowego komunikacja z francuskim szpiegiem zostanie przerwana, a Polacy zostaną pozbawieni najważniejszych informacji właśnie w chwili, gdy ich znaczenie dramatycznie wzrośnie. Ufał swoim kryptologom i zakładał, że pozbawieni prostego dostępu do kluczy opracują własne metody ich rekonstrukcji. Matematycy nie zawiedli jego zaufania – Ciężki nigdy nie musiał sięgać do sejfu po materiały

od Bertranda. Zapewne jednak nikt nie poinformował o tym Francuza, który poczuł się urażony czymś, co uznał za minimalizowanie jego wkładu w dekryptaż Enigmy.

Dwa aspekty analizowanego dokumentu wymagają dodatkowego komentarza. Pierwszy dotyczy jego początkowych rozdziałów. Po zarysowaniu tematu w dwóch wstępnych sekcjach autorzy wrzucają czytelnika na głęboką wodę, prezentując matematyczne podstawy swoich sukcesów. Podczas pracy nad tekstem znali jego domyślnych adresatów i mieli pełną świadomość, że matematyka zdecydowanie nie jest ich żywiołem. Gdyby zależało im jedynie na ukazaniu tła swojej pracy, zapewne wystarczyłoby rozbudowany przypis lub matematyczny załącznik dyskretnie dodany w końcowej części dokumentu. Lokując sekcje poświęcone teoretycznym podstawom sukcesu na początku tekstu, jego autorzy pragnęli zwrócić uwagę na to, co uważali za najważniejszy aspekt swojej pracy – na rolę matematyki w sukcesie.

Musieli rozumieć, a co najmniej przeczuwać charakter rewolucji w kryptologii, jaka była skutkiem ich triumfu. Przed Rejewskim, Różyckim i Zygalskim nikt nie podejmował poważnych prób zaprzęgnięcia zaawansowanej matematyki do służby w kryptologii. Użycie najprostszych metod statystycznych w celu zliczenia częstotliwości występowania pojedynczych znaków, bigramów lub trygramów w tekstach jawnych nie zasługuje na uwagę. Nawet gdy służby kryptologiczne kilku państw świata zdecydowały się zatrudniać matematyków, sięgały bardziej po ludzi niż po metody reprezentowanej przez nich dyscypliny naukowej.

Rozpoczęcie raportu poświęconego złamaniu Enigmy właśnie od podstaw teoretycznych wskazuje na to, że jego autorzy byli świadomi znaczenia matematycznej rewolucji w kryptologii, którą zainicjowali. Kiedy oddali swoje dzieło w ręce Brytyjczyków, ci w znaczeniu czysto praktycznym rozwinęli ich dokonania na wielką skalę, jednak w innym sensie ich zaangażowanie przyniosło regres. Algebraiczne metody stosowane przez Polaków miały olbrzymią zaletę: gwarantowały możliwość złamania szyfru. Brytyjczycy od pierwszych chwil traktowali je nieco

nieufnie, zauważając, że warunkiem zastosowania polskich metod jest występowanie dwukrotnie szyfrowanego klucza depeszy. Od pierwszych dni po spotkaniu w Pyrach przygotowywali się do nieuniknionego, ich zdaniem, momentu, w którym ten warunek nie będzie spełniony. Jako remedium proponowali metody łamania szyfru oparte na jego własnościach statystycznych (sito E, banbaryzm, później zautomatyzowane metody łamania szyfrów dalekopisowych z wykorzystaniem urządzenia Colossus itp.). Doraźnie mieli rację – przed rozpoczęciem kampanii francuskiej Niemcy usunęli dotychczasową słabość w procedurze użycia Enigmy. Algebraiczne podejście Polaków stało się chwilowo bezużyteczne. Brytyjski sukces dotyczący nowego wariantu szyfru miał jednak swoją cenę: Brytyjczycy czytali szyfr Enigmy tylko wtedy, gdy dysponowali wiarygodnym i stabilnym fragmentem prawdopodobnego tekstu depesz. Bardziej długofalowym efektem ich podejścia był wieloletni, ścisły mariaż kryptologii ze statystyką i teorią prawdopodobieństwa. Trzeba było wielu lat, aby kryptolodzy powrócili do algebraicznego podejścia Mariana Rejewskiego i jego kolegów, przywracając równowagę w zastosowaniach matematyki w kryptologii.

Drugim wątkiem zasługującym na uwagę jest przedstawiona przez autorów ocena wartości międzyalianckiej współpracy kryptologicznej. Pisali swój tekst najwcześniej w drugiej połowie 1940 r. W tym czasie zainicjowana rok wcześniej współpraca należała w zasadzie do przeszłości. Kryptolodzy przedwojennego Biura Szyfrów doznali zawodu ze wszystkich stron. Po ewakuacji z Polski spotkali się z despektem ze strony własnych rodaków, którzy nie dopuścili ich do służby w odradzającej się we Francji armii polskiej, kierując zespół pod rozkazy Francuzów. Jak wynika ze wspomnień matematyków, Francuzi nie potrafili zorganizować pracy w sposób, który pozwoliłby na wykorzystanie doświadczenia i wiedzy kryptologów Biura Szyfrów. Brytyjczycy, na których lojalną współpracę Polacy mogli liczyć w ciągu minionego roku, przerwali w zasadzie kontakt z chwilą upadku Francji. Autorzy raportu musieli odczuwać wielkie osamotnienie. Mimo to konsekwentnie podnosili znaczenie współpracy

trzech państw przy łamaniu Enigmy i wynikające z niej wymierne korzyści. Można jedynie spekulować, jak wielkie sukcesy odnieśliby kryptolodzy Francji, Wielkiej Brytanii i Polski, gdyby ich dowódcy dostroili się do sposobu myślenia podwładnych i nie tylko zezwolili na kontynuację współpracy, lecz także na nadanie jej takich form, jakie w późniejszym okresie przybrała (nie bez początkowych zgrzytów) współpraca kryptologów Wielkiej Brytanii i USA.

Kamil Kulesza

Łamanie Enigmy jako przykład rozwiązywania praktycznych problemów za pomocą matematyki – wnioski na dziś

Polski wkład w złamanie szyfru Enigmy oraz późniejsze prace prowadzone w Bletchley Park, w tym te dotyczące również innych maszyn wirnikowych i szyfrów, są już całkiem niezłe opisane w literaturze przedmiotu. I choć niewątpliwie występują nadal obszary wymagające dalszych badań, w tym artykule autor skupia się przede wszystkim na innych, długofalowych skutkach działań zainicjowanych sukcesem Polaków, zwłaszcza że część z nich zaczęła być dobrze widoczna dopiero ostatnio, już w XXI w. Z kolei ich waga wydaje się pozwalać na postawienie tych prac i stymulacji intelektualnej, jaką zapewniły one w kolejnych dziesięcioleciach po drugiej wojnie światowej, na równi z projektem Manhattan.

W artykule została też przedstawiona matematyka użytkowa (ang. *industrial mathematics*). Jest to nowatorska metoda uprawiania nauk matematycznych, w której matematyczny sposób myślenia stosuje się do rozwiązywania rzeczywistych problemów. Zaprezentowano również, jak prace nad złamaniem szyfru Enigmy, a zwłaszcza ich polska część, wpisują się w ten sposób działania.

Ostatni rozdział artykułu, przedstawiający wnioski na dziś, zaczyna się od opisanego smutnego stanu dzisiejszej, zinstytucjonalizowanej nauki polskiej. W jego dalszej części pokazano, jak możemy skorzystać z doświadczeń z czasów II Rzeczypospolitej, gdy potrafiliśmy skutecznie

mierzyć się z najtrudniejszymi wyzwaniami, a takim było niewątpliwie złamanie szyfru Enigmy.

Niniejszy artykuł w założeniu ma mieć postać przystępnego eseju, dlatego też zrezygnowano z formalnej bibliografii, zwłaszcza że zdecydowana większość okoliczności, o których w nim mowa, jest znana i dość dobrze udokumentowana. W kilku niezbędnych, zdaniem autora, przypadkach informacje uzupełniające zostały podane w przypisach.

Łamanie Enigmy – długofalowy wpływ na zmiany cywilizacyjne

Złamanie szyfru Enigmy, czy też – mówiąc bardziej dokładnie – całego systemu komunikacji opartego na maszynie szyfrującej Enigma, było niekwestionowanym osiągnięciem o bardzo daleko idących konsekwencjach. Dopiero z perspektywy czasu widać, jak bardzo wykraczały one poza pierwotnie postawione zadanie polegające na złamaniu szyfru. Zagadnienia jego wpływu na historię, zwłaszcza drugiej wojny światowej, zostały już dość dobrze przebadane i opisane.

Wydaje się jednak, że jeśli spojrzymy na ten problem szerzej, nie będzie przesadą stwierdzenie, iż długofalowy wpływ na zmiany cywilizacyjne będący pochodną działań prowadzonych w Bletchley Park¹ może być porównywalny z tymi, które są efektem badań prowadzonych w ramach projektu Manhattan. I to mimo krańcowo odmiennych sposobów komunikowania uzyskanych wyników, a więc ich upowszechnienia w obiegu naukowym i publicznej percepcji.

¹ Dla porządku zaznaczyć należy, że zaowocowały one całym pakietem technik, które wykorzystywano również do łamania szyfru innych maszyn wirnikowych, jak np. maszyny Lorentz. Część z nich skutkowało dalszymi rozwiązaniami, tak jak choćby powstaniem optoelektronicznej maszyny Colossus w przypadku ostatniego przykładu.

Nie bez znaczenia były zupełnie odmienne sposoby wykorzystania wyników uzyskanych w obszarze fizyki jądrowej oraz tych z zakresu kryptografii i technik obliczeniowych. Z jednej strony trudno o coś bardziej spektakularnego i trudnego do przeoczenia niż wybuch nuklearny. Nie bez powodu nawet kostium kąpielowy bikini został nazwany od miejsca próby nuklearnej, aby podkreślić „bombowy efekt”. Z drugiej strony jest codzienna praca matematyka kryptografa, mało widowiskowa i z pozoru nudna niczym robota księgowego². Z kolei jej końcowe efekty – tak jak było to w przypadku Enigmy – często nie manifestują się w spektakularnych fajerwerkach, raczej subtelnie korygują przebieg wydarzeń, w dodatku często nie w jednym miejscu i czasie. Takie działanie nie musi być łatwo zauważalne nawet dla dość wnikliwego obserwatora, zwłaszcza jeśli dodatkowo podejmowane są celowe działania, aby źródło informacji, a często też wynikające z nich wnioski dodatkowo zamaskować i zniekształcić – w przypadku Enigmy tę rolę pełniła ULTRA. Dziś już wiadomo, że utajnianie, choć nie pod wspomnianą nazwą, nie ustało jeszcze przez dziesięciolecia po zakończeniu drugiej wojny światowej. Głównym uzasadnieniem wydaje się wykorzystanie wiedzy nabytej przy łamaniu Enigmy i jej pochodnych w zmaganiach prowadzonych w ramach zimnej wojny.

Warto podkreślić, że oba wielkie wyzwania intelektualne przyciągały, zwłaszcza w latach drugiej wojny światowej, najlepsze umysły swojej epoki. Dobrym przykładem jest fakt, że spora część wybitnych brytyjskich matematyków tego okresu wzięła udział w działaniach prowadzonych w Bletchley Park, zaś po zakończeniu wojny, często już w cywilnym życiu, tworzyła nową, oryginalną naukę, niekoniecznie bezpośrednio

² Przemysł filmowy stara się, zwłaszcza w ostatnich hollywoodzkich produkcjach, przekonać nas, że może być inaczej. Jednak głównym celem tych zabiegów wydaje się przede wszystkim uniknięcie znudzenia widowni. Cóż, za klasykiem można powiedzieć: „Jest prawda czasów, o których mówimy, i prawda ekranu”.

związaną z pracami prowadzonymi w ramach tzw. *war research*. Tak było np. w wypadku samego Alana Turinga³. Jest ciągle przedmiotem dyskusji, na ile jego powojenne osiągnięcia w tworzeniu zarówno podstaw biologii matematycznej (m.in. prace w zakresie morfogenezy i tzw. *pattern formation*), jak i fundamentów informatyki mają swoje początki i inspiracje w Bletchley Park. Takich przykładów jest zdecydowanie więcej i choć niniejsza praca nie jest poświęcona tzw. wpływowologii w nauce, to dla porządku należy zauważyć, iż zagadnienie jest dość złożone. Jak powiedział bowiem chyba najbardziej znany przedstawiciel lwowskiej szkoły matematycznej Stefan Banach, „dobrzy matematycy widzą analogie między twierdzeniami, najlepsi zaś analogie między analogiami”. Wydaje się, że czas, który upłynął od chwili złamania szyfrów Enigmy, coraz lepiej pokazuje, jak zrodzone wtedy idee zmieniły i ciągle jeszcze zmieniają świat.

Aby usytuować powyższe stwierdzenie w odpowiedniej perspektywie, warto zapoznać się z podstawowymi informacjami o tzw. matematyce użytkowej. Jest to podejście do uprawiania matematyki powstałe wiele lat po drugiej wojnie światowej, jednak bardzo istotne z punktu widzenia długofalowego wpływu cywilizacyjnego prac związanych z łamaniem Enigmy.

Matematyka użytkowa, czyli o wykorzystaniu matematycznego myślenia do rozwiązywania praktycznych problemów

Matematyka użytkowa to jedno z możliwych polskich tłumaczeń angielskiego terminu *industrial mathematics*, które zdaniem autora chyba najlepiej oddaje istotę tego sposobu uprawiania matematyki.

³ Inni to np. W.T. Tutte – jeden z głównych twórców współczesnej teorii grafów oraz J.H.C. Whitehead – jeden z głównych twórców teorii homotopii, gałęzi topologii algebraicznej. Lista jest znacznie dłuższa.

Wielka Brytania to państwo, w którym rozpoczęła się rewolucja przemysłowa. Jednym z jej skutków była duża estyma, jaką cieszył się zawsze zawód inżyniera, rozumiany jednak inaczej niż np. w powojennej Polsce. Inżynier bowiem to przede wszystkim osoba, która podejmuje wyzwania i rozwiązuje problemy (ang. *problem solver*), a czyni to, wykorzystując podejście naukowe, w tym metody matematyczne. Wielka Brytania ma też długą tradycję rozwoju matematyki stosowanej (ang. *applied mathematics*). Studiowanie matematyki było w dobrym tonie i często stanowiło wstęp do dalszych zaawansowanych studiów i kariery w różnych obszarach. Dobrym przykładem są tzw. *Wranglers*⁴ z University of Cambridge – wielu z nich w tamtych czasach zostało wybitnymi prawnikami, duchownymi etc., a tylko nieliczni zdecydowali się kontynuować akademicką karierę w dzisiejszym rozumieniu. Studiowanie matematyki traktowano jako jeden z etapów czy elementów edukacji uniwersyteckiej, mającej na celu rozwój umysłowy, a przy okazji jako swego rodzaju test potencjału intelektualnego. Dla porządku należy też zauważyć, że sporą część ówczesnego nauczania matematyki dzisiaj klasyfikowalibyśmy raczej jako matematykę stosowaną, tj. głównie budowanie modeli matematycznych, często dla zjawisk występujących w naturze.

Współczesna matematyka użytkowa powstała na przełomie lat 60. i 70. XX w. w Oxfordzie. Już wcześniej zauważono, że wbrew opisanym powyżej tradycjom matematyka, nawet ta stosowana, staje się coraz bardziej oderwana od rzeczywistości, karmiąc się głównie problemami stawianymi w ramach własnego środowiska. Jak ładnie to wówczas

⁴ Wrangler to student, który uzyskał w danym roku najlepszy wynik na egzaminie kończącym nauczanie matematyki na University of Cambridge. Było to bardzo prestiżowe wyróżnienie – merytokracja w najczystszej postaci. Osoby takie cieszyły się sławą i prestiżem w takim stopniu, że nawet wiele lat później i po wielu istotnych dokonaniach w życiu fakt bycia wranglerem był podkreślany z dumą. Lista wranglerów jest zresztą do dziś dostępna.

podsumowano, „w środowisku akademickim jest coraz więcej profesorów matematyki stosowanej, którzy nigdy nie zastosowali jej poza murami uczelni”. Zdaniem wielu powodowało to naturalne skostnienie dziedziny i prowadziło do jej uwiędnięcia, o spadku użyteczności, np. dla gospodarki, a więc i społecznego prestiżu nie wspominając.

I wtedy, pod koniec lat 60. XX w., w Oxfordzie pojawiła się propozycja, aby wrócić do korzeni matematyki, w tym tych najdawniejszych, sięgających starożytności, gdy rozwój matematyki był stymulowany poprzez rozwiązywanie praktycznych problemów, jak np. konieczność mierzenia kanałów, przewidywania wylewów Nilu, zjawisk astronomicznych lub prowadzenia kalendarza. Innym argumentem były brytyjskie sukcesy badawcze w czasach drugiej wojny światowej, gdy pracowano nad konkretnymi problemami, stosując naukowy sposób myślenia.

Bazując na tym rozumowaniu, niektórzy matematycy postanowili zwrócić się do sfery gospodarki⁵ po praktyczne problemy i inspiracje. Poza stymulacją intelektualną i niejako „odświeżeniem dziedziny” liczone też na inne cele, m.in. zdobycie finansowania na badania. Podstawą było założenie, że jeśli za pomocą matematyki rozwiązany zostanie praktyczny problem, powstanie tym samym wartość dodana. Ta zaś może zostać zmonetyzowana w sferze gospodarki, a część wyniku tej operacji powinna przyspaść tym, którzy rozwiązanie stworzyli, czyli matematykom.

Przy całej swojej atrakcyjności i innowacyjności opisany program spotkał się w środowisku nie tylko z pozytywnym przyjęciem, miał także wielu przeciwników. Byli wśród nich ci, którzy dobrze odnajdywali się

⁵ Angielski termin *industry* ma znacznie szersze pole znaczeniowe niż słowo „przemysł” w języku polskim. I tak można mówić np. o *financial industry* (po polsku „sektor finansowy”) czy *entertainment industry* (po polsku „biznes rozrywkowy” czy „show-biznes” od amerykańskiego określenia tej dziedziny). Z tego powodu *industrial mathematics* nie powinno być raczej tłumaczone na język polski jako „matematyka przemysłowa”.

w dotychczasowym sposobie prowadzenia badań, ale również ci, którzy uważali, że uzyskiwanie korzyści finansowych z wyników prowadzonych badań prowadzi do swoistego zbrukania moralnego naukowców.

Ostatecznie debata w Oxfordzie zakończyła się swego rodzaju kompromisem. Uznano, że osoby zainteresowane nowym podejściem mogą go spróbować – zwyciężyło brytyjskie podejście pragmatyczne, szczególnie że z założenia rozwój matematyki użytkowej miał się samofinansować.

Brytyjska matematyka użytkowa okazała się wielkim sukcesem⁶. Dziś mówi się, że to jeden z najlepszych brytyjskich akademickich produktów eksportowych (ang. *one of the best academic export products*). Dzieje się tak ze względu na jej dynamiczny europejski, a następnie globalny rozwój w ostatnich dziesięcioleciach. *Know-how* zapoczątkowane w Oxfordzie i potem rozwinięte w brytyjskim środowisku matematyków jest wdrażane w rosnącej liczbie państw jako jeden z nowoczesnych sposobów uprawiania matematyki.

Innym przejawem tego sukcesu jest praktyczna weryfikacja przedstawionego powyżej nowatorskiego mechanizmu finansowania badań naukowych. Pozwoliło to matematykom, którzy chcieli podjąć wyzwanie, choć częściowo uniezależnić się od standardowych akademickich kanałów finansowania i oceny pracy. W przypadku matematyki użytkowej weryfikacja jakości pracy jest z reguły szybka i pragmatyczna, co mocno kontrastuje z wysokim stopniem uznaniowości w ramach tradycyjnego podejścia. Skutkuje to dużą swobodą badawczą, uniezależnieniem się od aktualnych mód naukowych i możliwością badania oryginalnych tematów.

⁶ Do dziś zdarzają się osoby krytycznie nastawione do matematyki użytkowej, zwłaszcza w obszarze tzw. matematyki czystej. Niestety, ludzi z talentem na miarę Johna von Neumanna, którzy potrafią łączyć wybitne wyniki w obszarze matematyki czystej z sukcesami w praktycznych zastosowaniach, jest mało.

W efekcie obszar tematów podejmowanych w ramach matematyki użytkowej jest bardzo szeroki⁷. Badaczy zajmujących się tą dziedziną zachęca się do przekraczania kolejnych barier, argumentując, że o ile opis problemu pochodzi ze sfery gospodarki, o tyle ich zadaniem jest jego ustrukturyzowanie z wykorzystaniem matematycznego sposobu myślenia i potwierdzenie, czy i jak można do rozwiązania wykorzystać matematykę. Często jest to mierzenie się z nieznanym, wkraczanie na obszary, z którymi matematycy niekoniecznie mieli wcześniej do czynienia.

I choć prawdą jest, że matematyka użytkowa działa w odpowiedzi na zadania pochodzące ze sfery gospodarki (ang. *industry driven*), osoby się nią zajmujące mają możliwość wyboru tematów. Dodatkowo rosnące znaczenie nauk matematycznych we współczesnym świecie powoduje, że nie tylko warto oczekiwać na wyzwania pochodzące ze sfery gospodarki, ale również proponować instytucjom własne tematy badawcze. Akceptacja praktycznej korzyści, np. w postaci zbudowania przewagi konkurencyjnej w jakimś obszarze poprzez opracowanie i wdrożenie innowacyjnych modeli matematycznych, powoduje pojawienie się zainteresowania i finansowania, i to na warunkach⁸ z reguły zdecydowanie korzystniejszych niż tradycyjne kanały finansowania nauki.

Należy wspomnieć też o czysto akademickiej dywidendzie z takiego sposobu uprawiania nauk matematycznych – możliwości uzyskania wyników dalece wykraczających poza bezpośrednio rozwiązanie problemu. Sprzyja ją temu zarówno stymulacja intelektualna, jak i zdobycie

⁷ John Ockendon, jeden z pionierów brytyjskiej matematyki użytkowej, zwykł mawiać, że zakres tematyczny rozciąga się co najmniej od „modelowania problemów społecznych do obliczeń kwantowych”.

⁸ Należy zwrócić uwagę, że nie odnosimy się tu jedynie do wysokości finansowania. Ważnymi elementami są też często odbiurokratyzowanie całego procesu i jego szybkość, ale również elastyczność i swoboda w zakresie finansowania prac i realizacji celów badawczych. Głównym wyznacznikiem jest z reguły stwierdzenie: „ma działać i mieścić się w budżecie”, a nie spełnianie abstrakcyjnych biurokratycznych reguł sprawozdawczości finansowej i merytorycznej.

finansowania na własne badania prowadzone w „wieży z kości słoniowej”. Ta niezależność badawcza skutkowałą już nieraz wynikami o charakterze teoretycznym. Dobrym przykładem jest słynne równanie pantografu, którego źródłem było zlecenie dotyczące usprawnienia sposobu dostarczania energii elektrycznej do pojazdów szynowych. Prąd elektryczny był doprowadzany do pojazdu za pomocą napowietrznej sieci elektrycznej łączącej się z nim właśnie za pośrednictwem pantografu. Przy okazji rozwiązywania tego problemu stworzono nieznanne dotąd równanie różniczkowe. Obecnie znajduje ono zastosowanie w modelowaniu innych zjawisk niepowiązanych z pantografem czy – szerzej – ze swoim pierwotnym przeznaczeniem.

I właśnie takie osiągnięcie stanowi dobry łącznik z historią łamania Enigmy i udziałem w niej Polaków.

„Matematyk zrobi to lepiej”⁹

Wszystko zaczęło się w latach 20. XX w., kiedy Niemcy zaczęli stosować maszynę wirnikową Enigma do utajniania łączności w ramach sił zbrojnych. Ich oponenti dość szybko zorientowali się, że mają do czynienia z szyfrem maszynowym, w przypadku którego stare metody kryptoanalizy zawodzą. W efekcie większość kryptologów, którzy próbowali łamać szyfr Enigmy, nie odnotowała większych sukcesów aż do początku drugiej wojny światowej.

W tym czasie w Polsce Biuro Szyfrów działające w ramach Oddziału II Sztabu Głównego WP zdecydowało się na innowacyjne podejście i postanowiło zaangażować w prace nad złamaniem szyfru Enigmy matematyków. Dziś podejście takie wydaje się oczywiste – w końcu

⁹ To hasło, którym prof. Hugo Steinhaus promował rozwój zastosowań matematyki po drugiej wojnie światowej; w ten sposób próbował kontynuować tradycje lwowskiej szkoły matematycznej, której był jednym z założycieli. I choć miał liczne osiągnięcia matematyczne, to jako swoje największe odkrycie matematyczne zwykł wymieniać Stefana Banacha.

kryptologia bazuje na matematyce, ale wtedy było ono nowatorskie i innowacyjne. W tamtych czasach ciągle jeszcze dominowało przekonanie, że do łamania szyfrów najlepiej nadają się lingwiści i „rozwiązywacze” krzyżówek. Dopiero m.in. sukces w łamaniu szyfru Enigmy sprawił, że od przełomu lat 30. i 40. XX w. matematycy i ich teorie zaczęli być niezbędni w kryptologii.

Jak się wydaje, inspiracją dla polskich wojskowych mogły być sukcesy w łamaniu szyfrów sowieckich w czasie wojny polsko-bolszewickiej w 1920 r. Bo choć bazowały one, jak byśmy dziś powiedzieli, na *know-how* wyniesionym przez ówczesnych polskich oficerów z wcześniejszej służby w tzw. radiowywiadzie armii austro-węgierskiej, to swój udział w nich mieli też polscy matematycy¹⁰.

Niezależnie od powyższego „postawienie na matematyków” oraz zaangażowanie znacznych środków w ich pozyskanie i wyszkolenie (m.in. specjalny kurs na uniwersytecie w Poznaniu) były z pewnością aktem sporej odwagi, i to zarówno intelektualnej, jak i administracyjno-zarządczej, zwłaszcza że w grę wchodziły publiczne pieniądze.

Również dla matematyków ta dziedzina była zupełnie nowa, nie istniały żadna teoria ani wzorce, a kryptologia nie była uznawana za naukę matematyczną. Nie byłoby więc trudno stwierdzić, iż „to nie jest zadanie dla nas” i szkoda czasu, aby się tym zajmować, zwłaszcza że były też inne lukratywne możliwości¹¹.

Mimo wszystkich opisanych czynników wyzwanie zostało podjęte – wkroczone na wcześniej nieznanym terenie – i jak wiemy z historii, w praktyce sprawdziła się maksyma Hugona Steinhausa stanowiąca tytuł tego rozdziału. Z punktu widzenia też prezentowanych w ramach niniejszego

¹⁰ Nazwiska niektórych z nich widzimy potem wśród osób zaangażowanych w działalność lwowskiej szkoły matematycznej.

¹¹ Jak wiadomo, po ukończeniu studiów Marian Rejewski zaczął bliżej interesować się matematyką aktuarialną – jest to do dziś jeden z lepiej opłacanych zawodów matematycznych.

artykułu ważne są też jednak jeszcze inne elementy historii. Choć są znane, spróbujemy pokazać je z nieco odmiennej perspektywy.

Po odtworzeniu schematu połączeń w ramach Enigmy i sposobu działania¹² maszyny kolejnym krokiem było stworzenie modelu matematycznego, czyli w tym przypadku opisanie jej funkcjonowania za pomocą równań. Zadanie to zostało wykonane, a równania zdawały się podobne do tych, z którymi stykamy się w czasie szkolnej edukacji, z tą różnicą, że obiektami występującymi w równaniach – zarówno stałymi, jak i zmiennymi – były permutacje, a nie liczby naturalne lub rzeczywiste. W tamtych czasach nie tylko nie istniała teoria pozwalająca na rozwiązywanie takich równań, ale nie było nawet cząstkowych metod rozwiązywania dla przypadków szczególnych. To wszystko należało wymyślić od podstaw. W efekcie stworzone zostały m.in. podstawy teorii permutacji, a jedno z jej twierdzeń bywa nazywane twierdzeniem Rejewskiego. Poza wartością praktyczną było to osiągnięcie w obrębie matematyki czystej.

Równie pionierski charakter miały kolejne działania – prace mające na celu uproszczenie i przyśpieszenie procesu łamania szyfru poprzez jego automatyzację. Przykładami mogą być zarówno płachty Zygal-skiego, jak i urządzenie nazwane bombą Rejewskiego. W obu wypadkach możemy mówić o próbach zautomatyzowania obliczeń za pomocą specjalnie przeznaczonych do tego urządzeń. Mówimy o czasach, kiedy nie istniały elektroniczne komputery, a nawet nie stworzono ich podstawowych założeń w dzisiejszym rozumieniu¹³. W obu urządzeniach można dostrzec przodków komputerów. I niech nie zwiedzie nas ich mechaniczny/elektromechaniczny charakter. Maszyny tworzone

¹² Było to działanie pionierskie. Dziś prace tego typu noszą nazwę tzw. inżynierii odwrotnej (ang. *reverse engineering*), a sposób ich realizacji stanowi cały osobny dział wiedzy. W ich ramach stosowane bywają też matematyczne techniki z obszaru tzw. problemów odwrotnych (ang. *inverse problems*).

¹³ Co najmniej jeszcze kilkanaście lat dzieliło świat od przedstawienia zarówno architektury von Neumanna, jak i maszyny Turinga – w obu wypadkach nastąpiło to kilka lat po drugiej wojnie światowej.

bezpośrednio po drugiej wojnie światowej były wykonywane w podobnych technologiach. Bomba Rejewskiego może być postrzegana jako pierwsze elektromechaniczne urządzenie wyspecjalizowane – dedykowany komputer przeznaczony do łamania szyfrów. W tym rozumieniu jest przodkiem wszystkim sprzętowych urządzeń używanych do kryptoanalizy (ang. *hardware based cryptoanalysis*). I choć rewolucja informatyczna w ostatnich dziesięcioleciach dokonała się w większej części w oparciu o programowalne komputery uniwersalne, w zakresie zastosowań kryptograficznych dominowało podejście tworzenia wyspecjalizowanych urządzeń sprzętowych. Przez całe dziesięciolecie była to jednak dziedzina spowita tajemnicą, a wiedza jej dotycząca zastrzeżona była dla sił zbrojnych, agend rządowych i służb specjalnych. Nie bez znaczenia były wysokie koszty związane z produkcją i wykorzystaniem takich urządzeń¹⁴. Cywilni badacze zaczęli intensywniej zgłębiać ten obszar dopiero na przełomie XX i XXI w., gdy z jednej strony odtajniona została część wcześniejszych rozwiązań, z drugiej kilka dziesięcioleci obowiązywania prawa Moore’a istotnie obniżyło ich ceny.

W efekcie w ostatnich latach analogiczne rozwiązania praktycznie „trafiły pod strzechy”. Najbardziej znanym przykładem są tzw. koparki kryptowalut, które są niczym innym jak dedykowanymi kryptograficznymi urządzeniami sprzętowymi – dalekimi potomkami bomby Rejewskiego.

Choć inicjatorem prac nad złamaniem szyfru Enigmy był Oddział II Sztabu Głównego WP, nie sposób pominąć jego współpracy z firmą Wytwórnia Radiotechniczna AVA. Była ona m.in. wykonawcą bomb Rejewskiego. W ramach współpracy dokonywał się trudny proces, w trakcie którego matematycy, pracując wraz z inżynierami,

¹⁴ Jak pewnie pamiętają czytelnicy, z problemem tym zetknęli się już polscy kryptolodzy pracujący nad łamaniem szyfru Enigmy – koszt produkcji pierwszych sześciu bomb Rejewskiego był porównywalny z rocznym budżetem Biura Szyfrów.

musieli znaleźć drogę do praktycznej realizacji swoich idei. Było to w czasach, w których nie znano wielu rezultatów ułatwiających taką współpracę, które, jak np. teoria komunikacji Shannona, powstały dopiero po drugiej wojnie światowej.

Podsumowując, na powyższą historię można spojrzeć jak na modelowy przykład tego, że „matematyk robi to lepiej”. W obliczu rzeczywistego problemu wynikającego z wprowadzenia szyfrów maszynowych decydenci odważyli się zaangażować matematyków do zmierzania się z nieznanym. W efekcie zostały znalezione praktyczne rozwiązania problemu, a przy okazji stworzono też interesującą matematyczną teorię. Elementem tej historii jest też owocna współpraca ze sferą gospodarki w zakresie wdrażania wyników pracy matematyków, a nawet w pewnym zakresie komercjalizacji tych wyników. Są działania prowadzone w pionierskich warunkach, które następnie stały się częstą i standardową praktyką, jak np. inżynieria odwrotna. Są podstawy i dalekosiężne inspiracje do tworzenia technologii komputerowej.

Znaczenia tych osiągnięć nie umniejsza wcale fakt, że w czasie drugiej wojny światowej i po jej zakończeniu idee te rozwijali już inni badacze. W nauce i technologii najważniejsze jest bowiem to, kto po raz pierwszy sformułował daną ideę, zwłaszcza jeśli potrafił pokazać jej działanie (ang. *proof-of-concept*).

Patrząc z długofalowej perspektywy, niezależnie od wpływu na historię drugiej wojny światowej właśnie w tym obszarze należy doszukiwać się głównych efektów polskiego wysiłku w zakresie łamania szyfru Enigmy. Poza osiągnięciem głównego celu stworzono nową matematyczną teorię oraz wskazano podstawy nowych technologii, które współcześnie kształtują naszą rzeczywistość.

Warto zauważyć, że wszystko to stało się w ramach działań mających wszelkie cechy projektu z zakresu matematyki użytkowej, z tym że był on prowadzony jednak kilkadziesiąt lat przed powstaniem tego pojęcia i akceptacją takiego sposobu uprawiania nauk matematycznych. Także w tym kontekście można mówić o działaniach pionierskich.

Wnioski na dziś

Polscy naukowcy, a zwłaszcza matematycy, mieli okazję wnieść wkład zarówno w projekt Manhattan¹⁵, jak i złamanie szyfru Enigmy – dwa naukowo-technologiczne projekty z czasów drugiej wojny światowej, które istotnie zmieniły otaczający nas świat i wpłynęły na kierunek zmian cywilizacyjnych. W dodatku w obu przypadkach wkład ten miał charakter przede wszystkim intelektualny i w części dotyczącej Polaków nie wymagał wielkich nakładów finansowych¹⁶.

W II Rzeczypospolitej potrafiliśmy stworzyć warunki do tego, aby Polacy mogli podejmować wyzwania na poziomie światowym. Niestety obecnie wygląda na to, że jesteśmy od tego daleko. Przyczyn tej smutnej sytuacji jest oczywiście wiele, ale w najmniejszym stopniu upatrywałbym ich w problemach natury finansowej. Zresztą II Rzeczpospolita środków finansowych też w nadmiarze nie miała, a nasza dzisiejsza pozycja gospodarcza, jeśli ocenimy ją globalnie, jest znacznie lepsza, niż była wtedy.

Ze splotu wielu czynników chciałbym wskazać grupę tych związanych z odwagą w myśleniu i realizacji zamierzeń, zarówno po stronie decydentów, jak i administracji, które bezspornie dowodzą, że zatrudnienie

¹⁵ Wśród nich m.in. Stanisław Ulam, jeden z najbliższych współpracowników Johna von Neumanna, ale też inni, zwłaszcza matematycy wywodzący się z lwowskiej szkoły matematycznej.

¹⁶ Uważny czytelnik mógłby stwierdzić, że swoistym kontrprzykładem jest wysoki koszt bomb Rejewskiego. Zdaniem autora argumentacja jest o tyle chybiłona, że głównym osiągnięciem było stworzenie swoistego *proof-of-concept*. Zmiany wprowadzone przez Niemców niedługo przed drugą wojną światową skutkowały koniecznością znacznego zwiększenia liczby używanych bomb Rejewskiego, czego Polacy nie byli w stanie udźwignąć finansowo. W pewnym stopniu podobne zjawisko wystąpiło w połowie drugiej wojny światowej w Bletchley Park, kiedy Brytyjczycy musieli zwrócić się o pomoc do Amerykanów, aby móc nadążyć ze zwiększaniem liczby urządzeń, co wymusiły kolejne modyfikacje wprowadzane przez Niemców.

matematyków do łamania szyfru Enigmy zostało zorganizowane i sfinansowane przez Sztab Główny WP, a więc organ polskiego państwa.

Na ile odważne było to przedsięwzięcie, możemy uświadomić sobie, gdy wyobrazimy sobie jego organizację w dzisiejszych realiach. Samo uwzględnienie regulacji typu ustawa o zamówieniach publicznych lub konstrukcja systemu grantów finansujących badania naukowe (m.in. ścieżka obronna w NCBiR¹⁷) powodują, że w dzisiejszych czasach przedsięwzięcie należałoby uznać za praktycznie niewykonalne.

Jeszcze gorzej jest z odwagą i możliwością zmierzenia się z wyzwaniami po stronie współczesnego polskiego establishmentu naukowego. Widać to zresztą dobrze np. w przypadku projektów dotyczących sektora obronnego, ale też innych dziedzin nauki i technologii. Nieefektywny system organizacji nauki i spetryfikowany model awansu naukowego doprowadził do tego, że jak stwierdził prof. Jerzy Marcinkowski, „prawdopodobnie większość publikacji dotyczących nowoczesnych dziedzin wiedzy nie może w Polsce liczyć na choćby jednego rozumiejącego o co chodzi czytelnika”¹⁸. Jak czytamy w tym samym artykule, ma to związek z tym, że: „codziennosc polskiej nauki to trzeciorzędni liderzy, którzy niejednokrotnie przez całe naukowe życie nie wytknęli nosa poza mury jednej uczelni, a nawet jeśli gdzieś wyjechali, to rzadko coś przywieźli z powrotem. Ludzie, których jedynym marzeniem jest dotrzeć do emerytury, niczego nie zmieniając i nie ucząc się już nigdy niczego nowego. I ich czwartorzędni uczniowie, kontynuujący anachroniczną tematykę badawczą i feudalny sposób myślenia swoich mistrzów”. Wszystko to jest z kolei obudowane skomplikowanym systemem biurokratycznym,

¹⁷ Jak podsumowują niektórzy, wydatki są duże, ale rzeczywistych rezultatów brak, i to od lat. Potwierdziły to wyniki kontroli przeprowadzonej przez NIK, które zostały upublicznione w maju 2020 r. (<https://www.nik.gov.pl/aktualnosci/daleko-od-oczekiwan-sil-zbrojnych-rp.html>) [dostęp: 10.06.2020].

¹⁸ J. Marcinkowski, K. Kulesza, *Uniwersytet potiomkinowski obiecuje innowacje*, „Rzeczpospolita”, 18.04.2008 (<https://www.rp.pl/artypk/122336-Uniwersytet-Potiomkinowski-obejuje-innowacje-.html>).

który rzekomo ma dbać o jakość prowadzonych badań i poziom reprezentowany przez polskich uczonych. W systemie tym swobodę badawczą zyskuje się najwcześniej po habilitacji¹⁹.

Wśród naukowców, którzy złamali szyfr Enigmy, nie było żadnego profesora, ani nawet doktora habilitowanego²⁰. Matematycy, którzy tego dokonali, a przy okazji w ciągu zaledwie kilku lat przeprowadzili pionierskie przedsięwzięcia opisane w poprzedniej części, byli jedynie absolwentami ówczesnych dobrych polskich uczelni²¹. Przyznać też trzeba, że zostali poddani starannej selekcji i kwalifikacji do projektu, a ich poziom wykształcenia był wystarczający, by mogli podejmować, i to z sukcesem, najtrudniejsze wyzwania tamtych czasów, mimo że nikt nie wiedział, czy zagadnienie w ogóle ma rozwiązanie²². Na marginesie warto zaznaczyć, że podobna odwaga w działaniu cechowała w II Rzeczpospolitej wielu ludzi – w obszarze nauki przykładem jest słynna sprawa

¹⁹ Obecna sytuacja jest prawie dokładnym zaprzeczeniem zasad zawartych w tzw. dekalogu lwowskiej szkoły matematycznej, może zresztą dlatego tak opłakane są efekty systemu funkcjonującego w ten sposób. Dla porządku należy jednak zaznaczyć, że choć operujemy głównie przykładami z obszaru nauk matematycznych, to nasze zastrzeżenia w najmniejszym akuracie stopniu tyczą się polskiego środowiska matematycznego. Polscy matematycy, podobnie jak przedstawiciele śladowej ilości innych dyscyplin, wydają się w swojej większości jednak pozostawać w kontakcie intelektualnym z resztą świata. A środowisko matematyczne, przy wszystkich swoich słabościach, jest zdecydowanie bardziej „cywilizowane”, niż ma to miejsce standardowo w zinstytucjonalizowanej nauce polskiej.

²⁰ W dodatku przed drugą wojną światową habilitacja miała zupełnie inne znaczenie niż obecnie – przede wszystkim dawała prawo do prowadzenia wykładów na uczelni.

²¹ *De facto* współpracę z Biurem Szyfrów nawiązali pod koniec studiów.

²² Przekonanie o braku efektywnej możliwości znalezienia takiego rozwiązania było powodem zarzucenia prac nad kryptoanalizą Enigmy zarówno przez Francuzów, jak i niezależnie Brytyjczyków, i to mimo doskonałych tradycji obu tych narodów w zakresie kryptologii i wielu sukcesów odniesionych przez nie na podobnym polu w czasie pierwszej wojny światowej.

doktoratu Stefana Banacha, który otrzymał go mimo braku ukończenia studiów wyższych. Dziś podobna sytuacja nie byłaby możliwa, zarówno w świetle obowiązujących przepisów, jak i ze względu na sposób działania zinstytucjonalizowanej nauki.

Po powyższych pesymistycznych obserwacjach warto zapytać: czy można coś z tym zrobić?

Doświadczenia ostatnich trzydziestu lat pokazują, że skuteczne zreformowanie zinstytucjonalizowanej nauki polskiej jest mało prawdopodobne. Nie dlatego, że jest to przesadnie trudne zadanie czy tytaniczna praca. Wymaga ono jednak determinacji, podjęcia i wdrożenia niepopularnych decyzji. Niestety nauka polska zdążyła sama siebie skutecznie zmarginalizować, więc decydenci nie widzą potrzeby podejmowania niepopularnych działań wobec nieznaczącego celu.

Aby nie kończyć tekstu pesymistyczną konkluzją, trzeba zwrócić uwagę, że może jednak nie wszystko jest stracone.

Polskie działania związane z łamaniem szyfru Enigmy spełniają wszystkie wymogi, by zostały potraktowane jako projekt z obszaru matematyki użytkowej, w dodatku realizowany kilkadziesiąt lat przed powstaniem tego pojęcia. Rozsądne wydaje się zatem założenie, że mimo licznych zmian będących wynikiem drugiej wojny światowej i lat powojennych polski potencjał intelektualny, który znalazł swoje odzwierciedlenie choćby we lwowskiej szkole matematycznej, nadal jest dostępny.

W połowie pierwszej dekady XXI w. spróbowano wdrożyć w Polsce brytyjskie *know-how* w zakresie matematyki użytkowej. W ramach przedsięwzięcia postawiono na rekrutację młodych ludzi – studentów i doktorantów z polskich uczelni.

Okazało się, że te same mechanizmy, które sprawdzały się kiedyś, działają także dzisiaj. W oparciu o młody zespół, wzmocniony kilkoma osobami o większym doświadczeniu, w ciągu ponad dziesięciu lat przeprowadzono kilkadziesiąt projektów naukowo-badawczych z obszaru matematyki użytkowej. Ich znakomita większość została opłacona przez firmy i instytucje, zgodnie z brytyjskim mechanizmem finansowania

matematyki użytkowej. Jak się okazało, całe przedsięwzięcie samo się sfinansowało. Zakres projektów był bardzo szeroki: od mediów i gier komputerowych, poprzez finanse i projekty z obszaru przemysłu ciężkiego, po sektor energetyczny i obronny. Pokazano w praktyce, że możliwe jest działanie w ramach innego modelu niż system zinstytucjonalizowanej nauki. Wykorzystywane zasady wpisują się doskonale w polskie tradycje z czasów największych osiągnięć, w tym łamania szyfru Enigmy. Jeśli zdołamy skutecznie nawiązać do nich w skali kraju, mamy szansę powtórzyć intelektualne sukcesy z przeszłości oraz podjąć aktualne wyzwania cywilizacyjne i technologiczne.

Matematycy na końcu twierdzeń piszą często łacińską sentencję *quod erat demonstrandum* (w skrócie Q.E.D.), co oznacza: „co było do wykazania”. Mam nadzieję, że w powyższym artykule udało mi się zawrzeć główne idee dotyczące długofalowego wpływu łamania szyfru Enigmy na zmiany cywilizacyjne oraz praktyczne wnioski na dziś, jakie można wyprowadzić z tej historii.

Krzysztof Osiński

Marian Rejewski – pogromca niemieckiej maszyny szyfrującej Enigma

W grudniu 1932 r. Marian Rejewski samotnie złamał szyfr niemieckiej maszyny Enigma. Miał wówczas tylko 27 lat. Młody wiek nie był jednak w tym przypadku przeszkodą, ale – jak się okazało – stanowił dodatkowy atut dla kryptologa, ponieważ pełen entuzjazmu, zapału i nowatorskich pomysłów młody człowiek nie poszedł śladem starszych kolegów, a tym samym nie powielił ich wcześniejszych błędów. Po prostu podszedł do rozwiązania problemu Enigmy w zupełnie inny niż jego poprzednicy sposób. Dzięki temu wszedł na stałe do historii nie tylko Polski, ale również całego świata.

Przed złamaniem szyfru Enigmy Marian Rejewski był stosunkowo krótko związany z Biurem Szyfrów Oddziału II Sztabu Głównego Wojska Polskiego, czyli wywiadem wojskowym. W 1929 r., a więc jeszcze w czasie studiów, uczestniczył w Poznaniu w ponad dwumiesięcznym kursie kryptologicznym (15 stycznia–22 marca 1929 r.)¹. Następnie, po rocznej przerwie na studia specjalistyczne z matematyki ubezpieczeniowej na uniwersytecie w niemieckiej Getyndze, pracował przez dwa lata (w latach 1930–1932) na posterunku oficerskim wywiadu w Poznaniu. Co jednak ciekawe, zarówno podczas kursu kryptologicznego, jak i późniejszej dwuletniej pracy w poznańskiej placówce „dwójki” nie został wtajemniczony w sprawę Enigmy. Zajmował się tam zupełnie innymi szyframi. „Praca nasza – pisał we wspomnieniach Rejewski – polegała [wówczas] wyłącznie na rozwiązywaniu w dalszym ciągu przedstawienia

¹ Z.J. Kapera, *Poznański kurs szyfrów obcych w 1929 roku*, [w:] *Wywiad wojskowy II Rzeczypospolitej*, red. P. Kołakowski, A. Pepłoński, Kraków 2011, s. 97–113.

podwójnego, bo klucze szyfru zmieniały się co 24 godziny i trud rozwiązywania trzeba było podejmować codziennie na nowo”².

W sprawę Enigmy wtajemniczony został dopiero po przeniesieniu do Warszawy, co nastąpiło 1 września 1932 r.³ Początki pracy w centrali Biura Szyfrów Rejewski wspominał w następujący sposób: „Pierwszą całkowicie samodzielną pracą, którą w Biurze Szyfrów wykonaliśmy było rozwiązanie czteroliterowego kodu używanego przez niemiecką marynarkę wojenną. (...) Zanim jeszcze ukończyliśmy pracę nad rozwiązaniem kodu morskiego, zlecono mi nową pracę, początkowo dodatkowo w godzinach wieczornych, później – gdy otrzymałem pierwsze pozytywne wyniki – w normalnych godzinach urzędowania. Dostarczono mi dość obfity materiał zaszyfrowany nowym rodzajem szyfru używanym przez niemieckie wojsko lądowe. (...) Czy to z odczytanych depeš zaszyfrowanych szyfrem przedstawienia podwójnego, czy też z innych źródeł, dość, że wiedziano, że jest to szyfr maszynowy. Wiedziano nawet, że maszyna, którą szyfrowano nazywa się »Enigma«”⁴.

W odróżnieniu od swoich poprzedników Rejewski nie pracował nad Enigmą latami, ale zaledwie po kilku tygodniach od wtajemniczenia go w sprawę, już w grudniu 1932 r., udało mu się znaleźć rozwiązanie⁵. Trudność złamania szyfru Enigmy bardzo plastycznie przedstawił amerykański historyk David Kahn: „Jeśli 1000 kryptoanalityków, każdy dysponujący zdobytą Enigmą, sprawdzałoby po cztery klucze na

² Rejewski przekazał kopię maszynopisu swoich wspomnień do zasobu Wojskowego Instytutu Historycznego. Obecnie znajduje się on w zasobie CAW (zob. CAW, Polska w latach 1918–1939, IX.1.2.48, M. Rejewski, *Wspomnienia*). Pamiętać jednak musimy, że wspomnienia te były już kilkakrotnie wydane drukiem.

³ R. Woytak, *Werble historii*, Bydgoszcz 1999, s. 129–131.

⁴ M. Rejewski, *Wspomnienia z mej pracy w Biurze Szyfrów Oddziału II Sztabu Głównego w latach 1930–1945*, Poznań 2011, s. 25–26.

⁵ J. Garliński, *Enigma. Tajemnica drugiej wojny światowej*, Lublin 1999, s. 47; Z.J. Kapera, *Łamanie szyfrów Enigmy przez Polaków. Mity i prawda*, „Przegląd Historyczno-Wojskowy” 2005, nr 5 (210), s. 26–27.

minutę, pracując każdego dnia przez okrągłą dobę, a chciałoby sprawdzić wszystkie klucze, to ich praca trwałaby 1,8 miliarda lat⁶. Ponadto pamiętać musimy, że maszyna była cały czas udoskonalana.

W uznaniu zasług w 1938 r. Rejewski odznaczony został Złotym Krzyżem Zasługi (Jerzy Różycki i Henryk Zygalski za to samo osiągnięcie otrzymali Srebrne Krzyże⁷). Nadał go prezydent RP Ignacy Mościcki na wniosek premiera Felicjana Sławoja Składkowskiego. Szef Wydziału Wywiadowczego Oddziału II płk Stefan Mayer w następujący sposób uzasadniał w 1938 r. propozycję przyznania swojemu podwładnemu tego odznaczenia: „Wybitna i nieprzeciętna siła w dziedzinie szyfrów obcych. Wyjątkowo uzdolniony. Bardzo sumienny, pracowity i pełen inicjatywy. Oddaje dla dobra sprawy nieocenione usługi. Zasługuje w pełni na proponowane odznaczenie”⁸.

Wspomniane przez płk. Mayera zasługi Rejewskiego rzeczywiście były nieocenione. Nie tylko opracował on sposób łamania kodu Enigmy, który później udoskonalął wraz z Różyckim i Zygalskim, ale również opracowywał różne urządzenia, które były pomocne w pracy z niemiecką maszyną szyfrującą. Wymyślił m.in. cyklometr (urządzenie pomagające obliczać cykliczne permutacje Enigmy) oraz tzw. bombę, czyli urządzenie przyspieszające proces odnajdywania kluczy dziennych, według których nastawiono maszynę szyfrującą. Od stycznia 1933 r. Rejewskiego wydatnie wspomagali koledzy, którzy również wykazali się pomysłowością. Zygalski wymyślił system płacht perforowanych, za pomocą których można było ustalać kolejność wirników w Enigmie, z kolei

⁶ D. Kahn, *Łamacze kodów. Historia kryptologii*, Warszawa 2004, s. 1150.

⁷ Zob. CAW, Oddział II SG WP, I.303.4.558, Wniosek o odznaczenie Srebrnym Krzyżem Zasługi dla Jerzego Różyckiego, bp; ibidem, Wniosek o odznaczenie Srebrnym Krzyżem Zasługi dla Henryka Zygalskiego, bp.

⁸ CAW, AP.1769/89/4265, Wniosek o odznaczenie Złotym Krzyżem Zasługi, [1938], bp.

Różycki opracował „metodę zegara”, która służyła do identyfikacji prawego, szybkiego wirnika maszyny⁹.

Co godne podkreślenia, Marian Rejewski był osobą niezwykle skromną, nieszukającą poklasku czy rozgłosu, ale również człowiekiem, który w pełni doceniał pomoc i wkład w sukces kolegów, którzy od początku 1933 r. pracowali wraz z nim nad łamaniem szyfrów Enigmy. W liście z końca lat 70. XX w. do Stanisława Portalskiego z Londynu Marian Rejewski pisał: „Byliśmy przez cały czas równorzędnymi i równoprawnymi kolegami, z wyjątkiem krótkiego czasu w r. 1932, kiedy nad »Enigmą« pracowałem sam. Pomijając więc ten krótki okres, należy nasze sukcesy uznać jako sukcesy wspólne i nie podobna, zwłaszcza po tylu latach, określić, kto co robił, z jednym atoli wyjątkiem: pomysł z roku 1938 płacht perforowanych jest pomysłem Heńka [Zygalskiego]”¹⁰.

W literaturze wymienia się Rejewskiego, Różyckiego i Zygalskiego jako jedyne osoby pracujące nad sprawą Enigmy. Tymczasem chociażby we wspomnieniach tego pierwszego można przeczytać, że zespół był większy i w jego skład wchodziło jeszcze kilka innych osób, które prawdopodobnie dlatego nie weszły do szerszej świadomości, gdyż nie miały takiego wpływu na postęp prac jak wymienieni wcześniej matematycy. Mimo wszystko były częścią zespołu i chociażby z tego względu należy o nich wspomnieć. Rejewski pisał o tym następująco: „Przez krótki okres czasu, na przełomie lat 1932 i 1933, czyniłem to sam, wraz ze swymi dwoma kolegami, których mi w międzyczasie przydzielono do

⁹ J. Garliński, *Enigma. Tajemnica...*, s. 58–60; M. Grajek, *Enigma. Bliżej prawdy*, Poznań 2007, s. 103–116; J.S. Ciechanowski, J. Tebinka, *Współpraca kryptologiczna. Enigma*, [w:] *Polsko-brytyjska współpraca wywiadowcza podczas II wojny światowej*, t. 1: *Ustalenia Polsko-Brytyjskiej Komisji Historycznej*, red. T. Dubicki, D. Nałęcz, T. Sterling, Warszawa 2004, s. 446–447; Z.J. Kapera, *The triumph of Zygal'ski's sheets. The Polish Enigma in the early 1940*, Kraków–Mogilany 2015, s. 28–29.

¹⁰ Cyt. za: S. Portalski, *Tajemnice „Enigmy”*, „Notatki Płockie” 2011, nr 2, s. 38–42.

pomocy [chodzi o Różyckiego i Zygalskiego], ale wkrótce już uruchomiono do tego celu biuro z pięcioma czy sześcioma pracownikami, których wyłącznym zadaniem było odczytywanie wszystkich niemieckich depesz przy pomocy klucza przez nas codziennie dostarczanego. (...) Na kilka lat przed wojną, prawdopodobnie w roku 1937, przeniesiono całą naszą komórkę z gmachu Sztabu Głównego przy Placu Saskim do nowo wybudowanego pomieszczenia w lesie pyrkim. W tym też okresie lub może nieco później odkomenderowano do naszego pokoju czterech oficerów (rtm. [Stefan] Żukotyński, kpt. [Jan] Tuszyński, kpt. [Kazimierz] Hellebrand, kpt. [Aleksander] Czwartacki) dla zapoznania się z naszymi metodami pracy”¹¹.

* * *

W literaturze podkreśla się często, że źródłem sukcesu Rejewskiego była jego doskonała znajomość matematyki, ale również języka i mentalności Niemców. Ta ostatnia okoliczność była pochodną czasu i miejsca urodzenia. Kryptolog urodził się bowiem w 1905 r. w Bydgoszczy, która w tym czasie wchodziła w obręb ziem objętych zaborem pruskim. Od dziecka miał możliwość „nasiąkania” niemiecką kulturą, językiem i obyczajami, a tym samym później mógł lepiej „wnikać” w to, jak rozumują przedstawiciele narodu niemieckiego.

Zobaczmy, kim był Marian Adam Rejewski i jak wyglądała jego droga życiowa. Urodził się 16 sierpnia 1905 r. w Bydgoszczy jako syn Józefa i Matyldy z domu Thoms. Jego matka pochodziła z rodziny właścicieli browaru w Podgórzu pod Toruniem. Z przekazów rodzinnych wynika, że była kobietą energiczną i zaradną, która w doskonały sposób zarządzała domem. Jego ojciec pochodził natomiast ze zubożałej rodziny ziemiaństwa wielkopolskiego, która w XIX w. zarządzała majątkami Braciszewo, Strzyżewo i Żmijewo pod Gnieznem. Po usamodzielnieniu się Józef zamieszkał w Bydgoszczy, gdzie został dobrze prosperującym kupcem w branży tytoniowej (prowadził m.in. sklep przy ul. Dworcowej 17). Był

¹¹ M. Rejewski, *Wspomnienia z mej pracy w Biurze Szyfrów...*, s. 64.

również działaczem społecznym. Popierał inicjatywy polskich mieszkańców Bydgoszczy, angażując się w walkę z germanizacyjną polityką zaborcy. Był jednym z założycieli utworzonego w 1909 r. Towarzystwa Kupców, które propagowało patriotyzm ekonomiczny wyrażony w hasle: „swój do swego po swoje”. Wspomagało również rozwój ekonomiczny polskich kupców, powołując Bank Bydgoski oraz podnosząc jakość usług świadczonych przez kupców, kształcąc młodzież i przygotowując ją do pracy¹².

Marian Rejewski był najmłodszym dzieckiem w rodzinie. Miał sześcioro rodzeństwa, trzy siostry i trzech braci. Najstarszy był Tadeusz, który urodził się w 1892 r. Rok później urodził się Waław, w 1894 r. na świat przyszła Łucja, w 1897 r. Zofia, w 1899 r. Aniela, a w 1900 r. urodził się Jan. Chłopcy w rodzinie Rejewskich byli słabego zdrowia i większość z nich zmarła przedwcześnie. Waław zmarł jako niemowlę w pierwszym roku życia, natomiast Jan i Tadeusz zapadali na choroby płuc, obaj zmarli dożywszy 25. roku życia. Tadeusz zmarł w 1917 r., z kolei Jan w osiem lat później. Ten ostatni studiował na politechnice w Gdańsku, gdzie nabawił się szybko postępującej gruźlicy. Matka, próbując ratować Jana, wysłała go na kurację do sanatorium w Oberstdorfie w Bawarii. Choroba była jednak zbyt zaawansowana, nie można już było nic zrobić¹³.

¹² Informacje od Janiny Sylwestrzak, córki Mariana Rejewskiego; *Historia Bydgoszczy*, t. 1: *Do roku 1920*, red. M. Biskup, Warszawa–Poznań 1991, s. 565; *Rozmowa z Janiną Sylwestrzak, córką Mariana Rejewskiego*, [w:] *Rejewski 1905–1980. Życie Enigmą pisane*, red. J.S. Ciechanowski et al., Bydgoszcz 2005, s. 26–29.

¹³ J. Lubiawski, *Rejewski Marian Adam*, [w:] *Polski słownik biograficzny*, t. 31, red. E. Rostworowski, Wrocław–Warszawa–Kraków–Gdańsk–Łódź 1988–1989, s. 54–55; G. Nowik, *Rejewski Marian Adam*, [w:] *Polski wkład w przyrodoznawstwo i technikę. Słownik polskich i związanych z Polską odkrywców, wynalazców oraz pionierów nauk matematyczno-przyrodniczych i techniki*, t. 3, red. B. Orłowski, Warszawa 2015, s. 412–413; J. Kutta, *Rejewski Marian Adam*, [w:] *Bydgoski słownik biograficzny*, t. 1, red. J. Kutta, Bydgoszcz 1998, s. 90–92; K. Osiński, *Marian Rejewski 1905–1980*, Warszawa 2015, s. 3; Z.J. Kapera, *Marian Rejewski. Pogromca Enigmy*, Kraków–Mogilany 2005, s. 43; M. Grajek, *Enigma...*, s. 46–47; H. Sowińska, *Życie Enigmą znaczone. Rozmowa z Janiną*

Rejewscy mieszkali w Bydgoszczy w kamienicy przy ul. Wileńskiej 6. Jako niezależni finansowo zadbali o wykształcenie swoich dzieci, posyłając je do najlepszych szkół. Marian nie był w tym zakresie wyjątkiem. W latach 1912–1915 uczył się w szkole elementarnej przy Miejskiej Szkole Realnej w Bydgoszczy. Naukę w niej traktowano jako okres przygotowawczy do dalszej edukacji. Szkoła była elitarna, uczęszczali do niej chłopcy z zamożnych rodzin, ponieważ chesne było dość wysokie. W kolejnych latach uczył się w Königliches Friedrich-Wilhelm Gymnasium in Bromberg (Królewskie Gimnazjum Fryderyka Wilhelma w Bydgoszczy), którego ceglany gmach wznosił się u zbiegu ulic Weltzienplatz i Gymnasiastrasse (dzisiaj w tym samym budynku u zbiegu pl. Wolności i ul. Gimnazjalnej znajduje się siedziba I LO im. Cypriana Kamila Norwida¹⁴). Szkoła powstała w 1817 r. na podwalinach istniejącego wcześniej Kolegium Jezuickiego. Charakteryzowała się wysokim poziomem nauczania, wszystkie przedmioty wykładane były w języku niemieckim. Pod koniec pierwszej wojny światowej wśród uczniów Gimnazjum było tylko około 17 proc. Polaków. Większość uczniów stanowili Niemcy, których odsetek sięgał 77 proc., natomiast resztę stanowili zgermanizowani Żydzi. Jak podaje jeden z badaczy dziejów I LO w Bydgoszczy na przełomie XIX i XX w., „wśród uczniów Polaków dominowali synowie okolicznej szlachty. Wysokie chesne pobierane za naukę w szkole ograniczało dostęp do gimnazjum grupie uboższych obywateli miasta, zwłaszcza Polaków. W niewielkim tylko stopniu pomocne były specjalnie fundowane stypendia”¹⁵. Rodzice Mariana byli na tyle majątni, że mogli opłacić edukację syna.

Sylwestrzak, córką Mariana Rejewskiego, [w:] *Rejewski 1905–1980. Życie Enigmą pisane*, red. J.S. Ciechanowski et al., Bydgoszcz 2005, s. 26–29.

¹⁴ Więcej na temat szkoły zob. też: *Z dziejów I Liceum Ogólnokształcącego. IV wieku kształcenia w Bydgoszczy*, red. M. Pawlak, Bydgoszcz 2007.

¹⁵ M. Romaniuk, *Bydgoskie gimnazjum w latach 1817–1919*, [w:] *Z dziejów I Liceum Ogólnokształcącego. IV wieku kształcenia w Bydgoszczy*, red. M. Pawlak, Bydgoszcz 2007, s. 58.

Bydgoszcz powróciła w granice odrodzonego państwa polskiego 19 stycznia 1920 r. w następstwie postanowień traktatu wersalskiego. W kolejnych dniach Polacy podporządkowali sobie wszystkie urzędy i instytucje, w tym również szkołę, do której uczęszczał Rejewski. Jej nazwę zmieniono na Państwowe Gimnazjum Klasyczne w Bydgoszczy i zaczęto polonizować system edukacji. Był to proces długotrwały i trudny, ponieważ brakowało wykwalifikowanej polskiej kadry nauczycielskiej, która byłaby w stanie prowadzić zajęcia na dotychczasowym wysokim poziomie. W czerwcu 1921 r., a więc jeszcze w trakcie nauki Mariana w Gimnazjum, zmarł jego ojciec¹⁶. Od tej pory utrzymanie domu spoczywało na Matyldzie Rejewskiej, którą wspomagać musiały dzieci, w tym Marian. Źródłem utrzymania rodziny były w tym czasie prowadzony przez matkę przy ul. Dworcowej punkt loterii państwowej oraz odziedziczony po mężu sklep tytoniowy. W okresie nauki w Gimnazjum Marian był solidnym, ale raczej przeciętnym uczniem. Co jednak charakterystyczne, już w tym czasie można było zauważyć u niego zamiłowanie do przedmiotów ścisłych, w tym zwłaszcza matematyki. Dobitnie pokazują to oceny na świadectwie maturalnym z 1923 r. Z przedmiotów humanistycznych otrzymał wówczas oceny dobre i dostateczne, ale z przedmiotów ścisłych, w tym z matematyki, bardzo dobre. Jego zainteresowania wpłynęły zapewne na wybór kierunku studiów, które rozpoczął w tym samym roku¹⁷.

Marian Rejewski studiował matematykę na Wydziale Matematyczno-Przyrodniczym (do reorganizacji w 1925 r. na Wydziale Filozoficznym) Uniwersytetu Poznańskiego. Niestety nie mamy zbyt wielu informacji o studenckim okresie jego życia. Wiemy jedynie, że w czasie pierwszego roku studiów w Poznaniu mieszkał przy ul. Wierzbicice 31a, a w czasie kolejnych lat odpowiednio przy ulicach: Patrona Jackowskiego 25,

¹⁶ *Kronika*, „Dziennik Bydgoski”, 7.04.1921, s. 4.

¹⁷ Świadectwa szkolne Mariana Rejewskiego znajdują się w archiwum prywatnym Janiny Sylwestrzak.

Ogrodowej 11, Wały Zygmunta Starego 6 oraz Ratajczaka 33. W 1927 r. stanął przed komisją poborową w Poznaniu, która ze względów zdrowotnych przyznała mu kategorię C, co oznaczało zdolność do służby wojskowej z ograniczeniami. Jego opiekunem naukowym był znany matematyk prof. Zdzisław Krygowski¹⁸, który szybko dostrzegł talent drzeмиący w studencie. Pod jego kierunkiem Rejewski napisał pracę magisterską, której tytuł brzmiał: „Opracować teorię funkcji podwójnie okresowych drugiego i trzeciego rodzaju oraz wykazać jej zastosowanie”. 1 marca 1929 r. Marian Rejewski obronił ją z wynikiem bardzo dobrym i uzyskał w ten sposób tytuł magistra filozofii w zakresie matematyki. Otrzymane w trakcie studiów oceny dobitnie potwierdzają trafność wyboru kierunku kształcenia. Z egzaminów dyplomowych otrzymał prawie same najwyższe noty¹⁹.

Pod koniec studiów rozpoczęła się również współpraca Mariana Rejewskiego z Oddziałem II Sztabu Głównego Wojska Polskiego, czyli wywiadem wojskowym, potocznie nazywanym „dwójką”. Na początku 1929 r. młody matematyk uczestniczył bowiem w zorganizowanym przez Oddział II kursie kryptologicznym skierowanym do studentów matematyki Uniwersytetu Poznańskiego. Kurs ten był ewenementem, ponieważ do tej pory wywiad nie zatrudniał cywilów, zwłaszcza w tak młodym wieku. Po czasie okazało się jednak, że nowatorska i zaskakująca decyzja o wyborze młodych matematyków była przysłowiowym „strzałem w dziesiątkę”. W gronie kursantów znalazły się bowiem osoby, które w istotny sposób przyczyniły się do późniejszych sukcesów Biura Szyfrów.

¹⁸ D. Pędziński, *Zdzisław Jan Antoni Krygowski*, [w:] *Wielkopolski słownik biograficzny*, red. A. Gąsiorowski et al., Warszawa–Poznań 1981, s. 385.

¹⁹ Archiwum UAM, 103c/1907, Teczka personalna studenta Mariana Rejewskiego. Zob. też: *Kronika Uniwersytetu Poznańskiego za rok szkolny 1928/1929*, Poznań 1930, s. 150.

Oficjalnym organizatorem kursu było Dowództwo Okręgu Korpusu VII w Poznaniu, zaś faktycznym „dwójka”. Szkolenie zorganizowano w oparciu o wydany 9 października 1928 r. rozkaz szefa Oddziału II płk. Tadeusza Schaetzla. Miało ono wyłonić utalentowanych młodych matematyków z doskonałą znajomością języka niemieckiego, którzy po ukończeniu studiów zajęliby się łamaniem szyfrów niemieckiej armii. Zorganizowanie kursu w Poznaniu wynikało zarówno z pogranicznego położenia tego miasta, jak i ulokowania w nim nakierowanej na Niemcy ekspozytury polskiego wywiadu (była to Ekspozytura nr 3, którą w 1930 r. zlikwidowano, tak samo jak placówkę w Gdańsku, a na ich miejsce utworzono nową ekspozyturę w Bydgoszczy, która również nosiła numer 3. W kolejnych latach w Poznaniu funkcjonował posterunek oficerski wywiadu) oraz ośrodka nasłuchowego, który przechwytywał niemieckie depesze. Nie bez znaczenia był też fakt, że mieszkający tam młodzi ludzie doskonale znali język i mentalność Niemców. W czasie zaborów przymusowo uczyli się języka niemieckiego w szkołach, ale również posługiwali się nim w codziennych relacjach z kolegami z sąsiedztwa²⁰.

Kurs kryptologiczny trwał od 15 stycznia do 22 marca 1929 r. Spotykano się wieczorami dwa razy w tygodniu, każdorazowo na kilka godzin. Zajęcia miały miejsce na terenie poznańskiej Cytadeli i uczestniczyły w nich 23 osoby. Prowadzili je zarówno prof. Krygowski, jak i przybyli z Warszawy przedstawiciele Oddziału II: mjr Franciszek Pokorny, kpt. Maksymilian Ciężki i inż. Antoni Palluth. Kurs oparto w głównej mierze na treści wydanej w 1925 r. we Francji książki pt. *Cours de cryptographie* autorstwa gen. Marcela Givierge’a. Obejmował on podstawy kryptologii²¹. Rejewski wspominał: „zapoznano uczestników

²⁰ CAW, Oddział II SG WP, I.303.4.2416, Utworzenie Ekspozytury Ref. RW, 2 V 1929, bp.

²¹ J. Kaperka, *Poznański kurs szyfrów obcych...*, s. 97–113; D. Turing, *XYZ. Prawdziwa historia złamania szyfru Enigmy*, Poznań 2019, s. 56–57.

z podstawowymi pojęciami z dziedziny szyfrów, z klasyfikacją szyfrów i z niektórymi elementarnymi metodami rozwiązywania szyfrów. Stosunkowo dużo czasu poświęcono na zapoznanie nas z teorią i praktyką rozwiązywania szyfru zwanego przestawieniem podwójnym. Szyfr ten był wówczas w ogólnym użyciu przez niemieckie wojska lądowe i istnienie komórki szyfrów niemieckich opierało się w pewnym stopniu na tym, że umiano rozwiązywać telegramy radiowe zaszyfrowane przy pomocy wspomnianego szyfru²². Trzy osoby nie podołały wymaganiom organizatorów kursu i odpadły jeszcze w jego trakcie. Szkolenie zakończył egzamin pisemny i ustny, który okazał się stosunkowo trudny, ponieważ nie zdało go czterech studentów. Oceny osób, które go zaliczyły, wyglądały następująco: 1 osoba uzyskała ocenę celującą, 4 osoby ocenę bardzo dobrą, 4 dobrą i 7 dostateczną²³.

Niestety nie wiemy, jakie oceny otrzymali poszczególni kursanci, w tym Marian Rejewski. Biorąc pod uwagę jego dalszą karierę, przypuszczając jednak możemy, że jego wynik był bardzo wysoki. On sam w swoich wspomnieniach sugeruje jednak, że kursu nie ukończył, ponieważ wyjechał na studia do Getyngi²⁴. Twierdzenie to jest zaskakujące, ponieważ studia rozpoczął kilka miesięcy po zakończeniu kursu.

Wyniki kursu były zadowalające również dla jego organizatorów, o czym może świadczyć fakt, że prawie od razu po jego zakończeniu zaczęto przygotowywać się do zatrudnienia w Poznaniu młodych matematyków, którzy pracowaliby dla Biura Szyfrów, czyli komórki zajmującej się łamaniem, badaniem i tworzeniem własnych szyfrów. Wniosek o powołanie takiej grupy złożono 2 maja 1929 r., jednak z jej formalnym utworzeniem zaczękano do jesieni, czyli do czasu, gdy studenci wrócą z wakacji. Z tego też względu grupa rozpoczęła swoje prace dopiero 1 października 1929 r. w podziemiach Komendy Miasta przy

²² M. Rejewski, *Wspomnienia z mej pracy w Biurze Szyfrów...*, s. 16.

²³ J. Kapera, *Poznański kurs szyfrów obcych...*, s. 106.

²⁴ R. Woytak, *Werble...*, s. 127.

ul. Święty Marcin, nieopodal siedziby Instytutu Matematyki Uniwersytetu Poznańskiego. Na początek zatrudnienie w niej znalazło prawdopodobnie sześciu absolwentów wcześniejszego kursu kryptologicznego. Wśród nich na pewno nie było Mariana Rejewskiego, który w tym czasie ukończył studia i wyjechał do Niemiec, aby podjąć dwuletnie studia podyplomowe w zakresie matematyki ubezpieczeniowej na Uniwersytecie w Getyndze²⁵.

Po rocznym pobycie w Niemczech Marian powrócił na wakacje do Bydgoszczy. Rozczarowany poziomem nauki oraz atmosferą polityczną panującą u zachodniego sąsiada postanowił przerwać studia. Wpływ na podjęcie takiej decyzji miał również prof. Zdzisław Krygowski, który zaproponował mu w tym czasie pracę na Uniwersytecie Poznańskim. W efekcie od 1 września 1930 r. został zatrudniony w Instytucie Matematyki na stanowisku młodszego asystenta. Poza pracą dla prof. Krygowskiego ściśle współpracował również z prof. Mieczysławem Biernackim. Prowadził ćwiczenia oraz wygłaszał zlecone przez profesorów wykłady z matematyki wyższej dla studentów przedmiotów przyrodniczych²⁶.

Równoległe otrzymał od wywiadu propozycję dołączenia do zespołu matematyków utworzonego przy posterunku oficerskim Oddziału II w Poznaniu. Zespół ten stawał się coraz mniejszy, ponieważ nie wszyscy potrafili łączyć studia z pracą dla „dwójki”. Zatrudnienie Rejewskiego stanowiło więc jego istotne wzmocnienie. Poza małymi wyjątkami nie znamy personaliów studentów pracujących w tej placówce, nie wiemy nawet, jak długo byli w niej zatrudnieni. Wiemy, że w całym okresie funkcjonowania grupy pracowało w niej łącznie osiem osób, w tym siedmiu mężczyzn i jedna kobieta. Wiemy również, że obecność

²⁵ M. Rejewski, *Wspomnienia z mej pracy w Biurze Szyfrów...*, s. 16–17; R. Woytak, *Werble...*, s. 127; Z.J. Kapera, *Poznański kurs szyfrów obcych...*, s. 108–110.

²⁶ Archiwum UAM, Teczka personalna Mariana Rejewskiego, 696/82; M. Rejewski, *Wspomnienia z mej pracy w Biurze Szyfrów...*, s. 17.

Rejewskiego znacząco ją wzmocniła, a jego zaangażowanie i pomysłowość zostały docenione, ponieważ prawie natychmiast został on kierownikiem grupy poznańskich kryptologów, zastępując w tej roli Henryka Zygalskiego, który wcześniej kierował jej pracami²⁷.

Praca w poznańskiej placówce była monotonna i trudna, jednak osobom w niej zatrudnionym zapewniono dogodne warunki pracy. Po latach Rejewski wspominał: „W pracy naszej w ekspozyturze [w rzeczywistości w posterunku oficerskim – przyp. K.O.] nie byliśmy krępowani żadnymi godzinami, każdy mógł pracować, kiedy mu było najdogodniej, z tym tylko, że każdy winien był przepracować 12 godzin tygodniowo. Praca nasza polegała wyłącznie na rozwiązywaniu w dalszym ciągu przedstawienia podwójnego, bo klucze szyfru zmieniały się co 24 godziny i trud rozwiązywania trzeba było podejmować codziennie na nowo. Treść depech była, o ile pamiętam, nieciekawa, w przeważającej mierze były to depeche ćwiczebne. Tyle w każdym razie można powiedzieć o tych kilku, przeważnie krótkich depechach, które służyły do odtworzenia klucza. Treść pozostałych, nieraz bardzo długich, wieloczęściowych depech była nam nieznana, więc bardzo jest możliwym, że z punktu widzenia wywiadu wojskowego były interesujące. Nie trudziliśmy się by je odczytać, nie było to zresztą naszym zadaniem, lecz cały materiał szyfrowy z danego dnia, po odtworzeniu klucza, odsyłaliśmy dla dalszej eksploatacji do Centrali do Warszawy”²⁸. Jak więc widzimy, młodzi matematycy zajmowali się wówczas głównie łamaniem kluczy do szyfrów ręcznych używanych przez niemiecką armię.

Jesienią 1932 r. matematyków zatrudnionych na posterunku oficerskim w Poznaniu przeniesiono do centrali w Warszawie. Wszystko wskazuje na to, że pod koniec działania tej grupy należały do niej tylko trzy osoby – poza Rejewskim byli to Jerzy Różycki i Henryk Zygalski. Obydwaj uczestniczyli w kursie kryptologicznym z 1929 r., pracowali

²⁷ Z.J. Kapera, *Poznański kurs szyfrów obcych...*, s. 109–110.

²⁸ M. Rejewski, *Wspomnienia z mej pracy w Biurze Szyfrów...*, s. 17.

dla „dwójki” w posterunku oficerskim po jego ukończeniu i studiowali matematykę, którą ukończyli w 1932 r. Byli młodsi od Rejewskiego (Różycki urodził się w 1909 r., a Zygalski w 1907 r.), ale równie innowacyjni i zaangażowani.

Pracę w Warszawie rozpoczął Rejewski 1 września 1932 r. jako urzędnik cywilny referatu niemieckiego Biura Szyfrów (BS4)²⁹. Przeprowadzka do stolicy oznaczała dla niego rezygnację z równoległej pracy na uniwersytecie. Nowa posada była jednak na tyle atrakcyjna, że bez wahania się na to zdecydował. W Warszawie młodzi matematycy niezwłocznie przystąpili do pracy. Referat niemiecki Biura Szyfrów, w którym byli zatrudnieni, ulokowany był w siedzibie Sztabu Głównego Wojska Polskiego, w północnym skrzydle Pałacu Saskiego w Warszawie. Rejewski pracował w niewielkim pokoju na drugim piętrze, z oknem wychodzącym na wewnętrzny dziedziniec. W jego wspomnieniach czytamy: „Pierwszą całkowicie samodzielną pracą, którą w Biurze Szyfrów wykonaliśmy, było rozwiązanie czteroliterowego kodu używanego przez Niemców marynarkę wojenną. Początek pracy był trudny. Zapoznaliśmy się przede wszystkim bardzo dokładnie z materiałem szyfrowym, sporządziliśmy frekwencję wszystkich grup kilkakrotnie etc. Ale nie mieliśmy żadnego punktu zaczepienia. Spodziewaliśmy się jedynie, że kod będzie ułożony alfabetycznie”³⁰. Do łamania otrzymanych kodów wykorzystywano zarówno znajomość języka niemieckiego, jak i zasady matematyki. Rejewski podkreślał, że „jest wielką zasługą (...) mjr. Pokornego, jak i jego zastępcy, ppłk. Karola G[wido] Langerera i jego zastępcy, kpt. Maksymiliana Ciężkiego, że znacznie wcześniej niż w innych biurach szyfrów zorientowali się w celowości wymagania od kryptologów obok znajomości języków jeszcze studiów matematycznych”.

²⁹ CAW, Oddział II SG WP, I.303.4.485, Umowa o pracę Mariana Rejewskiego; ibidem, I.303.4.558, Dodatkowa umowa o pracę Mariana Rejewskiego, 3 IV 1936, k. 79; ibidem, I.303.4.2415, Pismo o zatrudnieniu Mariana Rejewskiego.

³⁰ M. Rejewski, *Wspomnienia z mej pracy w Biurze Szyfrów...*, s. 25.

Po kilku tygodniach z zespołu wyłączono Mariana Rejewskiego, który otrzymał specjalne zadanie. Miał zająć się złamaniem szyfru niemieckich depeš, które szyfrowane były maszynowo, urządzeniem o nazwie Enigma. Polscy kryptolodzy z „dwójki” od dłuższego czasu próbowali złamać ten szyfr, ale nikomu się nie udało. Postanowiono spróbować czegoś nowego, stąd pomysł na powierzenie sprawy młodemu matematykowi. W celu zapewnienia pełnej konspiracji, ale również komfortowych warunków pracy Rejewskiemu przydzielono w gmachu Sztabu Głównego osobny pokój. Materiału pomocniczego było niewiele. Otrzymał notatki oficerów „dwójki”, którzy wcześniej pracowali nad złamaniem szyfru Enigmy, egzemplarz zakupionej przez polski wywiad handlowej wersji maszyny, a także porcję kilkudziesięciu zaszyfrowanych niemieckich depeš przechwytywanych codziennie przez polskie stacje nasłuchowe. Prace były prowadzone z dużym zaangażowaniem, ale początkowo nie dawały pozytywnych rezultatów. Przełom nastąpił 8 grudnia 1932 r., kiedy to Rejewski otrzymał od swoich zwierzchników kopie tabeli kluczy Enigmy za wrzesień i październik 1932 r. Klucze te zostały przekazane „dwójce” przez kpt. Gustave’a Bertranda z francuskiego wywiadu, który zdobył je z kolei od francuskiego szpiega ulokowanego w niemieckim biurze szyfrów³¹.

Powiązanie ze sobą wszystkich otrzymanych informacji oraz zastosowanie nowatorskich metod matematycznych pozwoliło Rejewskiemu odnieść sukces. Pod koniec grudnia 1932 r. odtworzył wewnętrzną konstrukcję maszyny szyfrującej, a następnie opracował skuteczny sposób

³¹ Ibidem, s. 48–49; R. Woytak, *Werble...*, s. 131–132; M. Grajek, *Enigma...*, s. 64–66, 84–86; W. Kozaczuk, *W kręgu Enigmy*, Warszawa 1986, s. 58–60; D. Kahn, *Łamacze kodów...*, s. 1151–1152; J. Garliński, *Enigma. Tajemnica...*, s. 43; H. Sebag-Montefiore, *Enigma*, Warszawa 2010, s. 29–34, 47–52; J. Tebinka, *Wkład Polski i Polaków w dzieło złamania szyfrów niemieckiej Enigmy (1932–1942)*, [w:] *Bydgoszcz jako ośrodek działań wywiadowczych w przededniu i w trakcie II wojny światowej*, red. S. Pastuszewski, Bydgoszcz 2015, s. 13–14.

odszyfrowywania utajnianych przez nią depeš. Do dziś wyczyn Rejewskiego okreśłany jest jako największe osiągnięcie kryptologiczne pojedynczego człowieka. Dokonał tego w wieku zaledwie 27 lat. W styczniu 1933 r. na polecenie swoich zwierzchników Rejewski wtajemniczył w sprawę Enigmy Różyckiego i Zygalskiego. Od tej pory trójka ta stanowiła zespół pracujący wyłącznie nad dalszym udoskonalaniem sposobów łamania kodu niemieckiej maszyny szyfrującej. Grupa otrzymała kryptonim „E” (od Enigma), a jej kierownikiem został Rejewski³².

Rozpracowanie sposobu działania niemieckiej maszyny szyfrującej pozwoliło również polskim inżynierom ze współpracującej z „dwójką” warszawskiej fabryki AVA na wykonanie duplikatów wojskowej Enigmy, które znacząco ułatwiały dekryptaż³³. Rejewski wspominał, że skuteczność odczytywania szyfrów Enigmy była wysoka, szczególnie na początku działalności grupy „E”. W kolejnych latach również taka była, pomimo wprowadzania usprawnień i zmian w konstrukcji maszyny. Przykładowo, na początku 1938 r. odczytywano zawartość 75 proc. przechwyconych niemieckich meldunków. Płk Stefan Mayer wspominał, że „pod koniec roku 1937 nasi kryptolodzy całkowicie opanowali metodę przechwytywania i odczytywania niemieckich radiogramów szyfrowanych przez Enigmę. W styczniu 1938 r. wykonano badania nad rozszyfrowywaniem przechwyconych materiałów Enigmy. Wówczas rozszyfrowano ok. 75 proc. tych materiałów. Pewnego dnia, dla sprawdzenia, sam wybrałem materiały z przechwyconych radiogramów i nakazałem zespołowi rozszyfrować je przy mojej obecności. Wynik był bezbłędny”³⁴. Rejewski podkreślał jednak, że odsetek ten mógłby sięgać

³² K. Osiński, *Marian Rejewski...*, s. 8.

³³ Nieco informacji na temat fabryki AVA odnaleźć można w broszurze poświęconej jednemu z jej założycieli, czyli Ludomirowi Danilewiczowi. Należy jednak podchodzić z dużą ostrożnością do danych zawartych w tej publikacji. Zob. W. Nosowski, *Ludomir, Maria i inni...*, Warszawa 2003, s. 14–26.

³⁴ S. Mayer, *Łamanie niemieckiej maszyny szyfrującej Enigma przez Biuro Szyfrów Oddziału II Sztabu Głównego Wojska Polskiego*, [w:] *Rejewski 1905–1980*.

nawet 90 proc., gdyby Biuro Szyfrów miało więcej pieniędzy na zatrudnienie nowych osób.

Szczęście dopisywało Rejewskiemu nie tylko w pracy, ale również w życiu osobistym. W lutym 1934 r. ożenił się z długoletnią przyjaciółką Ireną Lewandowską, córką znanego bydgoskiego dentysty Stanisława Lewandowskiego oraz Jadwigi Lewandowskiej z domu Bornej. Młoda para znała się od dawna, ponieważ w Bydgoszczy mieszkała niedaleko siebie. Rodziny nowożeńców przyjaźniły się, czego dowodem są przechowywane w zbiorach rodzinnych zdjęcia ze wspólnych wycieczek i spotkań, na których widnieją zarówno rodzice nowożeńców, jak i Marian z Ireną jako małe dzieci. Często bawili się razem, ponieważ byli w tym samym wieku (Irena urodziła się 30 marca 1905 r.). W kolejnych latach wielokrotnie się spotykali, ale także wyjeżdżali wraz z przyjaciółmi na wyprawy górskie do Zakopanego. Co ciekawe, znajomość pary rozciągała się również na pracę w „dwójce”, ponieważ Irena Rejewska przez pewien czas pracowała w strukturach Oddziału II Sztabu Głównego Wojska Polskiego. Niestety nie zachowała się jejteczka personalna, nie wiemy więc, w jakim okresie tam pracowała, a tym bardziej na jakim stanowisku³⁵.

Ślub i wesele Rejewskich odbyły się w Bydgoszczy. W podróż poślubną młoda para pojechała do Juraty na Półwyspie Helskim. Po powrocie zamieszkali w Warszawie, w wynajmowanym przez Mariana pokoju przy ul. Sułkowskiego. Zarobki Mariana były dość wysokie, pozwalały rodzinie na wygodne życie. Wakacje spędzali najczęściej w Zakopanem, czasami również za granicą. W 1935 r. kupili mieszkanie spółdzielcze

Życie Enigmą pisane, red. J.S. Ciechanowski et al., Bydgoszcz 2005, s. 209. Więcej na temat łamania szyfrów Enigmy zob. też: *Enigma. Zarys metod rozwiązania*, [w:] *Sztafeta Enigmy. Odnaleziony raport polskich kryptologów*, red. M. Grajek, Warszawa–Emów 2017, s. 155–184.

³⁵ *Fototeka Oddziału II Sztabu Głównego Wojska Polskiego w dokumentacji Ministerstwa Bezpieczeństwa Publicznego*, wstęp i oprac. M. Sobieraj, Lublin 2013, s. 108, 229; AIPN By, 069/137, t. 6, Album zdjęć pracowników Oddziału II do sprawy krypt. „Targowica” (zdjęcia Mariana i Ireny Rejewskich), k. 111, 122.

przy ul. Mickiewicza 12³⁶. Z czasem doczekali się dwojga dzieci. Syn Andrzej Zygmunt urodził się 26 czerwca 1936 r., a córka Janina Maria przyszła na świat 16 lutego 1939 r.

Marian nie był w stanie w pełni wspomagać swojej żony, zmuszony spędzać wiele godzin w pracy. Coraz więcej czasu poświęcał również na dotarcie do pracy, bowiem od 1937 r. siedziba referatu niemieckiego Biura Szyfrów (BS4) została przeniesiona do znajdującego się w miejscowości Pyry w Lasach Kabackich k. Warszawy nowo wybudowanego tajnego ośrodka o kryptonimie „Wicher”³⁷. Żona miała jednak zrozumienie dla sytuacji, w jakiej się znalazł. Za każdym razem, gdy była w ciąży, udawała się do Bydgoszczy pod opiekę swoich rodziców. Wracała do stolicy, gdy dziecko miało już kilka miesięcy. Rejewscy zatrudnili do pomocy opiekunkę do dzieci, która związała się z nimi na kilka kolejnych lat.

Rejewski miał bardzo dużo pracy, Niemcy nieustannie udoskonalali bowiem wykorzystywaną przez siebie maszynę szyfrującą oraz procedurę jej użycia. Polscy kryptolodzy starali się nadążyć za wprowadzanymi zmianami, ale około 1938 r. zaczęli natrafiać na coraz większe trudności. Aby je przezwyciężyć, potrzebowali znacznie więcej pieniędzy, a tych niestety brakowało. Tym samym nie można było w pełni wykorzystać potencjału młodych matematyków ani wdrażać w życie ich pomysłów. Coraz poważniej zaczęto zastanawiać się nad wtajemniczeniem

³⁶ Adres ten widnieje chociażby w dokumentacji archiwalnej związanej z przyznaniem Rejewskiemu odznaczenia (CAW, AP.1769/89/4265, Wniosek o odznaczenie Złotym Krzyżem Zasługi, [1938], bp.). Z dostępnej dokumentacji wynika, że zarówno dom przy ul. Mickiewicza, jak i wiele innych budynków w tej dzielnicy zagospodarowane były na potrzeby osób związanych z wojskiem, ponieważ spółdzielnia budująca te domy i zarządzająca nimi była instytucją powołaną przez wojsko. Zob. W. Klepacz, *W sercu Żoliborza. Historia Spółdzielni Budowlano-Mieszkaniowej Żoliborz*, t. 1, Warszawa 2011; idem, *W sercu Żoliborza. Suplement do tomu pierwszego. Historia Spółdzielni Budowlano-Mieszkaniowej Żoliborz*, Warszawa 2017.

³⁷ M. Grajek, *Enigma...*, s. 97–98; J. Garliński, *Enigma. Tajemnica...*, s. 64.

w sprawę Enigmy sojuszników Polski. Do takiego rozwiązania skłaniała coraz bardziej napięta sytuacja polityczna w Europie, a zwłaszcza agresywne zachowanie rządzonych przez Adolfa Hitlera Niemiec. Dla wszystkich było oczywiste, że wybuch wojny jest tylko kwestią czasu.

Od 7 do 9 stycznia 1939 r. w Paryżu przedstawiciele Biura Szyfrów brali udział w konferencji kryptologów z Francji, Polski i Wielkiej Brytanii. Płk Mayer podkreślał w swoim raporcie, że „zadaniem konferencji było lepsze zintegrowanie współpracy, a szczególnie zaplanowanie działań prowadzących do rozwiązania zagadnienia Enigmy”³⁸. Słowa te można uznać za kurtuazję, bowiem Polacy od kilku lat znali sekret Enigmy i z powodzeniem odczytywali depesze szyfrowane tym urządzeniem. W trakcie spotkania zorientowano się, że zarówno Anglicy, jak i Francuzi nie zdołali dorównać naszym dokonaniom. Co więcej, nie byli w stanie dostarczyć nam nic w zamian za informację o niemieckiej maszynie szyfrującej. Wobec powyższego Polacy zdecydowali się zachować wiedzę o Enigmie wyłącznie dla siebie³⁹.

Wydarzenia polityczne w Europie dość szybko zmusiły polskie władze do zmiany stanowiska. Kilka miesięcy później doszło do kolejnego spotkania. Miało ono miejsce w Warszawie w dniach 25–26 lipca 1939 r. Podczas konferencji stroną francuską reprezentowali kpt. Gustave Bertrand i kpt. Henri Bracqueniet, z kolei brytyjską: kmdr Alastair Denniston, kryptolog Dilwyn Knox oraz specjalista radionasłuchu Humphrey Sandwith. 25 lipca w ośrodku „Wicher” przedstawiciele polskiego wywiadu przekazali Francuzom i Brytyjczykom całą swoją wiedzę na temat Enigmy. Podzielili się z nimi nie tylko informacjami o tym, jak łamać kod maszyny szyfrującej, ale również przekazali po jednym egzemplarzu sporządzonej przez siebie repliki wojskowej wersji urządzenia. W trakcie

³⁸ S. Mayer, *Łamanie niemieckiej maszyny szyfrującej Enigma...*, s. 210.

³⁹ J.S. Ciechanowski, J. Tebinka, *Współpraca kryptologiczna...*, s. 447–448; M. Grajek, *Maksymilian Ciężki. Architekt triumfu nad Enigmą*, Szamotuły 2016, s. 41.

spotkania Rejewski, Różycki i Zygałski omawiali zasadę działania Enigmy oraz tłumaczyli, w jaki sposób złamali jej szyfr⁴⁰.

Pomimo złamania szyfru Enigmy i uzyskania w ten sposób dostępu do najbardziej tajnych planów niemieckich nie dało się uniknąć wojny, która wybuchła 1 września 1939 r.⁴¹ W następstwie powszechnej mobilizacji pierwszego dnia wojny Rejewski został powołany do wojska i oddelegowany do Wyższej Szkoły Wojennej. Służby nie zdążył rozpocząć, bowiem tego samego dnia został wyreklamowany przez „dwójkę” i jako cywil wrócił do pracy w Biurze Szyfrów. Prowadzono tam prace na trzy zmiany bez przerwy, dniem i nocą. Sytuacja na froncie okazała się niekorzystna, więc władze podjęły decyzję o ewakuacji. Biuro Szyfrów i fabrykę AVA ewakuowano 6 września specjalnym pociągiem (eszelon F), który wyruszył z Dworca Wileńskiego. Wywieziono nie tylko personel, ale również dokumentację i sprzęt, które w trakcie podróży systematycznie niszczone, aby nie wpadły w ręce wroga⁴².

Pracownicy Biura Szyfrów mogli ewakuować się wraz z rodzinami. Rejewski nie zdecydował się na to, nie chcąc narażać żony i małych dzieci na niebezpieczeństwo. Wiedział, że na wschodzie kraju, dokąd się

⁴⁰ *Przekazanie Enigmy aliantom, Pyry, lipiec 1939 r. Nowe dokumenty z archiwów brytyjskich*, oprac. J.S. Ciechanowski, E. Maresch, [w:] *Rejewski 1905–1980. Życie Enigmą pisane*, red. J.S. Ciechanowski et al., Bydgoszcz 2005, s. 215–240; Z.J. Kapera, *Polski radiowywiad w sierpniu i wrześniu 1939 r.*, [w:] *Studia nad wywiadem i kontrwywiadem Polski w XX wieku*, t. 1, red. W. Skóra, P. Skubisz, Szczecin 2012, s. 275–276; idem, *Marian Rejewski...*, s. 26–28; S. McKay, *Tajemnice Bletchley Park. Kulisy łamania szyfrów Enigmy*, Warszawa 2013, s. 56–59; D. Turing, *XYZ. Prawdziwa historia...*, s. 120–136; *Sztafeta Enigmy. Odnaleziony raport polskich kryptologów*, red. M. Grajek, Warszawa–Emów 2017.

⁴¹ Więcej na temat działań wywiadu związanych z przygotowaniem do wojny zob. m.in.: P. Kołakowski, *Czas próby. Polski wywiad wojskowy wobec groźby wybuchu wojny w 1939 roku*, Warszawa 2012; Ł. Ulatowski, *Polski wywiad wojskowy w 1939 roku. Struktura organizacyjna, składy osobowe, personel, budżet, mob.*, Warszawa 2013.

⁴² R. Woytak, *Werble...*, s. 138.

ewakuowano, nie mają żadnych krewnych, więc rodzina nie będzie mogła czuć się bezpiecznie. Odmiennie postąpił Różycki, który miał rodzinę na Rzeszowszczyźnie. Zabrał ze sobą żonę i czteromiesięczne dziecko, aby wydostali się ze stolicy i wraz z nim przedostali na wschód, do krewnych. Żona Różyckiego w następujący sposób wspomina chwile związane z wyjazdem z miasta: „Zaledwie znaleźliśmy się w wagonie, zaczęło się bombardowanie dworca i pociągów tam stojących. Kryjemy się wszyscy pod wagony. Na razie o wyjeździe nie może być mowy. Tory są uszkodzone i niektóre wagony [również]. Skład pociągu musi być uzupełniony. Jurek poszedł szukać mleka [dla dziecka]. Jego kolega, M. Rejewski, pobiegł jeszcze do domu do żony i dzieci. Przy nas został Zyga (przyjaciel Jurka, Henryk Zygalski), który tu nikogo nie miał z rodziny – był z Poznania. Wieczorem byliśmy w komplecie. Pociąg ruszył. Z ulgą wyjeżdżamy z dworca w stronę Siedlec”⁴³.

Droga była dramatyczna. Pociąg był wielokrotnie ostrzeliwany i bombardowany przez niemieckie samoloty. Kilka razy zatrzymywano się, aby pasażerowie mogli ukryć się w pobliskich lasach. Ze względu na zniszczone bombami tory trzeba było przerywać podróż i dokonywać niezbędnych napraw. Barbara Różycka wspominała: „Zdawałoby się, że dokąd się zbliżamy, tam rozpoczynają się pierwsze naloty, spadają pierwsze bomby. Coraz częściej prześladuje mnie myśl, że to my przywozimy ze sobą same nieszczęścia do tych do niedawna spokojnych stron Polski”⁴⁴. Droga wiodła przez Siedlce, Łuków, Białą Podlaską do Brześcia n. Bugiem, do którego dotarli 9 września około południa. Dalszą podróż uniemożliwiło zbombardowanie dworca kolejowego i zniszczenie części pociągu, którym jechali. Następnego dnia Rejewski, Różycki i Zygalski zostali odkomenderowani do Oddziału II Kwatery

⁴³ *Wspomnienia żony kryptologa mgr. Jerzego Różyckiego z dni od 1 do 9 września 1939 roku na podstawie notatek z zachowanego kalendarzyka z 1939 roku (kopia w zbiorach autora).*

⁴⁴ *Ibidem.*

Główniej Naczelnego Wodza. 11 września zapadła decyzja o dalszej ewakuacji na wschód. W związku ze zbombardowaniem torów odbywała się ona samochodami. Podróż przebiegała przez miasta: Kowel, Krzemieniec, Łuck, Dubno i Husiatyn. Na wieść o ataku sowieckiej Rosji na Polskę trzej kryptolodzy otrzymali rozkaz dalszej ewakuacji do Rumunii.

Po przekroczeniu granicy w Kutach 17 września⁴⁵ jako cywile zostali przez Rumunów oddzieleni od przedstawicieli wojska i skierowani w inne miejsce. Zarekwirowano im samochód i nakazano stawić się w obozie dla internowanych. Zignorowali to polecenie i na własną rękę przedostali się do Bukaresztu. Dotarli do polskiej ambasady, gdzie od attaché wojskowego płk. Tadeusza Zakrzewskiego uzyskali zgodę na skontaktowanie się z ambasadą francuską lub brytyjską w celu kontynuowania prac kryptologicznych. Początkowo udali się do Anglików, ale nie zdołali uzyskać od nich wsparcia (gospodarze byli w tym czasie zajęci rozlokowaniem personelu brytyjskiej ambasady w Warszawie). Więcej szczęścia mieli w ambasadzie francuskiej, która prawdopodobnie została powiadomiona o możliwości ich pojawienia się w Bukareszcie. Otrzymali nowe paszporty, wizy i bilety na pociąg do Francji.

Rejewski wraz z kolegami wyruszył w podróż do stolicy Francji 22 września 1939 r. Droga wiodła przez Rumunię, Jugosławię i Włochy. Po trzech dniach w miejscowości Modane przekroczyli granicę z Francją i prawdopodobnie jeszcze tego samego dnia dotarli do Paryża. Z ustnego polecenia gen. Stanisława Burhardt-Bukackiego kryptolodzy zostali oddelegowani do Oddziału V francuskiego Sztabu Głównego, gdzie otrzymali stanowisko i wyposażenie kapitana wojsk francuskich. Co jednak ważniejsze, dostali też możliwość prowadzenia prac dekryptażowych, ponieważ Francuzi – dzięki otrzymanym kilka miesięcy wcześniej od Polaków materiałom polskich kryptologów – mogli rozpocząć prace nad łamaniem szyfru Enigmy. Dołączenie Rejewskiego, Różyckiego i Zygal-skiego do francuskiego zespołu wydatnie go wzmocniło.

⁴⁵ M. Rejewski, *Wspomnienia z mej pracy w Biurze Szyfrów...*, s. 113–114.

20 października 1939 r. kryptolodzy zostali przewiezieni do leżącego około 40 km od Paryża tajnego ośrodka kryptologicznego „Bruno”. Pracowało tam łącznie 15 Polaków (poza Rejewskim byli to: mjr Ciężki, Edward Fokczyński, Kazimierz Gaca, Jan Graliński, Bronisław Krajewski, ppłk Langer, mjr Michałowski, por. Antoni Palluth, Sylwester Palluth, por. Henryk Paszkowski, Różycki, Stanisław Sachno, Piotr Smoleński i Zygałski) oraz 7 Francuzów i 7 Hiszpanów. Początkowo mieli do dyspozycji trzy egzemplarze Enigmy, spośród których dwa wykorzystywano do prac dekrytażowych, a jeden zdemontowano, aby inż. Palluth mógł na jego podstawie wykonać rysunki techniczne potrzebne do wyprodukowania duplikatów maszyny.

Rejewski wspominał okres pobytu w ośrodku „Bruno” następująco: „Praca nasza, gdy wreszcie się zaczęła, była bardzo gorączkowa. Pracowaliśmy na zmianę dniem i nocą, zwłaszcza jednak nocą. Telegrafści francuscy przekazywali nam niemieckie depeze za pośrednictwem dalekopisu natychmiast, bieżąc tak jak je odbierali”⁴⁶. Intensywność pracy wynikała z trwającej wojny. Polska ekipa odczytała w tym czasie łącznie 8440 depesz niemieckich, z czego większość szyfrowanych Enigmą. Były one niezmiernie istotne dla przebiegu wojny, bowiem 1151 spośród nich dotyczyło kampanii norweskiej, a 5084 – kampanii francuskiej. Ponadto rozszyfrowano 287 depesz nadanych przez radiostacje dywersantów niemieckich oraz 833 przechwycone meldunki z innych źródeł. Tylko 1085 spośród odczytanych depesz pochodziło z sektora sowieckiego, ale one z oczywistych powodów nie były szyfrowane Enigmą. W tym okresie pozostawano w ścisłym kontakcie z działającym w Bletchley Park brytyjskim Biurem Szyfrów. Współpraca ta polegała m.in. na wymianie informacji oraz wzajemnym przekazywaniu złamanych kluczy do deszyfrowania Enigmy, aby uniknąć dublowania pracy. Poza normalnymi obowiązkami Rejewski szkolił również kolegów. Na początku 1940 r.

⁴⁶ Ibidem, s. 68.

przygotował dokument pt. *Metodyka rozwiązywania szyfrów*, który był podstawą szkolenia pracowników ośrodka „Bruno”⁴⁷.

W tym czasie Rejewski nawiązał również korespondencyjny kontakt z pozostawioną w okupowanym kraju rodziną. Za pośrednictwem Francuzów wysyłał żonie listy oraz niewielkie przesyłki z żywnością. Córka Rejewskiego wspominała po latach: „Ojciec rzeczywiście pisał, ale nie pod swoim nazwiskiem. Nadchodziły też paczki, w zasadzie paczuszki. Były to bowiem niewielkich rozmiarów kartoniki, zawierające np. parę czekolad, puszkę sardynek, trochę fig i migdałów. To były prawdziwe święta w domu!”⁴⁸. Przesyłki były nie tyle wsparciem dla rodziny, ile rodzajem sygnału, że Rejewski żyje, tęskni i pamięta o swoich najbliższych. Korespondencja była jednostronna, ponieważ kryptolog z oczywistych względów nie mógł się podpisać prawdziwym nazwiskiem, ani tym bardziej podać adresu. Dla zmylenia Niemców listy były zresztą wysyłane z anonimowych lokalizacji, m.in. ze Szwajcarii. Przez całą wojnę Rejewski nie wiedział nic na temat losów żony i dzieci. Jego nastrój poprawiała świadomość, że rodzina nie musi się zamartwiać o niego i żyć w niepewności, czy nie spotkała go jakaś tragedia.

W trakcie kampanii francuskiej ośrodek został ewakuowany na południe kraju, stamtąd samolotem do Oranu w Afryce Północnej, a następnie pociągiem do Algieru, gdzie znajdowała się ekspozytura francuskiego wywiadu. Polacy nie zajmowali się w tym okresie łamaniem niemieckich szyfrów, lecz wypoczywali i uczyli się języka francuskiego. Rejewskiemu nauka szła stosunkowo łatwo, ponieważ języka tego uczył się wcześniej, w trakcie studiów. W wyniku machinacji Gustave’a Bertranda grupa polskich kryptologów przeniosła się do nieokupowanej części Francji, aby wznowić działalność na terenach należących do państwa Vichy.

⁴⁷ Z. Kapera, *Efekty pracy polskich kryptologów w P.C. Bruno: styczeń–czerwiec 1940*, „Prace Komisji Historii Wojen i Wojskowości” 2016, t. 10, s. 99–116; J. Garliński, *Enigma. Tajemnica...*, s. 81–82.

⁴⁸ H. Sowińska, *Życie Enigmą znaczone...*, s. 36.

Przybyli do Uzés niedaleko Nimes i Awinionu, gdzie w murach lokalnej willi utworzono kolejny tajny ośrodek wywiadowczy, tym razem o kryptonimie „Cadix”. Dla zmylenia Niemców jego lokatorzy udawali pracowników Przedsiębiorstwa Budownictwa Wiejskiego⁴⁹.

Przez Polaków ośrodek „Cadix” nazywany był Ekspozyturą „300”. Obok Polaków w ośrodku pracowali również Francuzi i Hiszpanie, nie odgrywając jednak znaczącej roli. W związku z konspiracyjnymi warunkami pobytu w ośrodku wszyscy jego pracownicy otrzymali nową tożsamość. Rejewski otrzymał dokumenty, w których występował jako Pierre Ranaud, nauczyciel matematyki z liceum w Nantes. Ponadto każdej osobie przebywającej w ośrodku „Cadix” polski wywiad nadał dodatkowy pseudonim. Rejewski został w ten sposób „Okszą”, Różycki „Rola”, a Zygałski „Bemolem”.

Efekty pracy ośrodka „Cadix” nie były już tak istotne jak ośrodka „Bruno”, ponieważ ekipa miała bardzo ograniczone możliwości odbierania zaszyfrowanych depeš niemieckich. Dysponowano zaledwie czterema radiostacjami, z których dwie wykorzystywane były do kontaktów z Londynem, pozostałe dwie do nasłuchu. Do szyfrowania własnych depeš posługiwano się polską, opracowaną jeszcze przed wojną maszyną szyfrującą Lacida⁵⁰. W lipcu 1942 r. Rejewski z Zygałskim, nie mając innego zajęcia, poprosili o udostępnienie depeš zaszyfrowanych Lacidą. Ku własnemu zaskoczeniu złamali jej szyfr w ciągu zaledwie dwóch godzin. Wiedząc o ograniczeniach maszyny, Polacy wykorzystywali ją nadal, stosując jednak podwójne szyfrowanie. Wszystko wskazuje na to, że Niemcom do końca wojny nie udało się powtórzyć wyczynu Rejewskiego i Zygałskiego – nie złamali szyfru Lacidy⁵¹.

⁴⁹ Z.J. Kapera, *Powołanie „Ekspozytury 300” i jej losy w okresie czerwiec 1940–listopad 1942*, [w:] *Okupowana Europa. Podobieństwa i różnice*, red. W. Grabowski, Warszawa 2014, s. 175–192.

⁵⁰ W. Nosowski, *Ludomir, Maria...*, s. 18.

⁵¹ M. Rejewski, *Wspomnienia z mej pracy w Biurze Szyfrów...*, s. 72–73.

Na początku 1942 r. ekipa ośrodka „Cadix” została dotknięta tragedią. 9 stycznia 1942 r. w pobliżu Balearów na Morzu Śródziemnym zatonął statek „Lamoricière”, na którego pokładzie znajdowała się grupa pracowników Biura Szyfrów powracająca z Algieru, gdzie przez trzy miesiące pracowała w lokalnej ekspozyturze ośrodka „Cadix”. Wśród osób, które zginęły w katastrofie, byli: Jerzy Różycki, Jan Graliński i Piotr Smoleński⁵².

Jesienią 1942 r. pracownicy ośrodka „Cadix” zdali sobie sprawę, że Niemcy są coraz bliżej zlokalizowania ich placówki. 6 listopada zapadła decyzja o jej likwidacji. Pracownicy ośrodka usiłowali przedostać się w małych grupach do Hiszpanii, skąd mieli być ewakuowani do Wielkiej Brytanii. Rejewski i Zygalski przekroczyli granicę francusko-hiszpańską 29 stycznia 1943 r. Przeprawa miała nieco dramatyczny przebieg, ponieważ kryptolodzy zostali obrabowani przez przemytnika wynajętego do przeprowadzenia ich przez granicę. Błąkając się, wpadli w ręce hiszpańskich żandarmów, zostali aresztowani i osadzeni w areszcie w miejscowości Puigcerdá. W kolejnych tygodniach przenoszono ich do innych więzień, m.in. w miejscowościach: Belver, Seo de Urgel i Lerida. Wolność odzyskali w wyniku zabiegów brytyjskiego wywiadu, który został poinformowany o ich losie przez więziennego kapelana. Brytyjczycy wynegocjowali uwolnienie więźniów za pośrednictwem Czerwonego Krzyża. Rejewski z Zygalskim opuścili areszt 4 maja, pozostali jednak pod nadzorem policji w Madrycie⁵³.

W trakcie pobytu polskich kryptologów w Hiszpanii Brytyjczycy przygotowywali ich przerzut do Anglii. Ewakuacja rozpoczęła się pod koniec lipca 1943 r. Najpierw przerzucono ich do Portugalii, stamtąd łodzią rybacką wywieziono na pełne morze, gdzie przesiedli się na pokład brytyjskiego okrętu wojennego. Ten przewiózł ich bezpiecznie do bazy w Gibraltarze, skąd 30 lipca samolotem dostali się do Kinghorn

⁵² Ibidem, s. 71–72, 118; M. Grajek, *Enigma...*, s. 539–540.

⁵³ J.S. Ciechanowski, J. Tebinka, *Współpraca kryptologiczna...*, s. 459.

w Szkocji. Stamtąd odesłano ich do polskiej kompanii radiowywiadu stacjonującej w Boxmoor koło Londynu. Rejewski został mianowany kierownikiem kilkusobowej sekcji niemieckiej („N”) w Plutonie Eksploatacyjnym Kompanii Radiowywiadowczej. W związku z tym, że zarówno Rejewski, jak i Zygałski nadal zachowywali cywilny status, wcielono ich do wojska w stopniu szeregowca z cenzusem. Już w październiku 1943 r. obydwaj awansowali na stopień podporucznika. W Wielkiej Brytanii nie dane im jednak było zajmować się łamaniem szyfrów Enigmy⁵⁴.

1 stycznia 1945 r. był dla Rejewskiego wyjątkowym dniem. Otrzymał awans na porucznika czasu wojny, został odznaczony Krzyżem Zasługi z Mieczami, a dodatkowo mianowano go zastępcą kierownika referatu Kompanii Radiowywiadowczej Batalionu Łączności Sztabu Naczelnego Wodza. Wszystkie te splendory w żaden sposób nie zrekompensowały irytacji spowodowanej odsunięciem na boczny tor. Rejewski i jego koledzy byli rozżaleni, że nie mogą zajmować się sprawą Enigmy i zmuszeni są wykonywać drugoplanowe prace kryptologiczne, które w znikomym stopniu wykorzystywały ich wiedzę i umiejętności. W okresie tym ich głównym zajęciem było łamanie szyfrów ręcznych, którymi posługiwały się oddziały Waffen SS. Od maja 1944 r. Rejewski i Zygałski byli przydzieleni do pracy w sekcji „R”, która zajmowała się szyframi sowieckimi. Wyrazem nastrojów w ekipie polskich kryptologów był memoriał napisany przez Rejewskiego w październiku 1944 r. W piśmie domagał się on od Anglików zwrotu przekazanego przed wojną egzemplarza Enigmy. Uzasadniał, że „maszyna ta jest polskim kryptologom potrzebna, jeżeli nie do innych celów, to choćby do celów archiwalnych. Wypada, aby ci, którzy maszynę tę zrekonstruowali, byli w posiadaniu choć jednego jej egzemplarza”⁵⁵. Ponadto żądał od Anglików, „by zechcieli podzielić

⁵⁴ D. Turing, *XYZ. Prawdziwa historia...*, s. 281–294.

⁵⁵ Polish Institute and Sikorski Museum, A.XII.24/63, M. Rejewski, Kilka uwag na temat trudności w jakich znajduje się w chwili obecnej Dział szyfrów niemieck[ich], 1 X 1944, s. 3 [kopia w zbiorach autora za pośrednictwem Janiny Sylwestrzak].

się doświadczeniami poczynionymi przez nich w ciągu ostatnich pięciu lat w dziedzinie szyfrów niemieckich najlepiej przez bezpośrednie skontaktowanie zainteresowanych kryptologów polskich i angielskich”⁵⁶. Apele nie zdały się na nic, Polacy nie zostali dopuszczeni do dekryptażu Enigmy.

W obliczu kończącej się wojny na początku maja 1945 r. Rejewski i Zygalski udali się do Francji, aby odebrać rzeczy pozostawione tam po ewakuacji ośrodka „Cadix” i zdeponowane w Cannes. Z Londynu polecili do Paryża. W stolicy Francji spotykali się z płk. Bertrandem, kpt. Honoré Louistem i kpt. Henri Bracqueniem. Podczas pobytu w Paryżu stołowali się w amerykańskiej kantynie wojskowej, ponieważ we Francji występowały wówczas duże problemy aprowizacyjne. Amerykanie zapewnili Polakom zapasy żywności na drogę do Cannes i użyczyli samochodu. Na miejscu okazało się, że część pozostawionych bagaży została okradziona przez opiekuna depozytu. Matematycy zapakowali resztki dobytku i udali się do Paryża, gdzie dotarli 9 maja 1945 r., a więc w dniu, gdy miasto świętowało koniec wojny. Dalszą podróż zorganizowali Anglicy; podstawili ciężarówkę, która dowiozła kryptologów do portu w Calais, a po przeprawie promem przez kanał – do bazy w Boxmoor.

W grudniu 1945 r. Rejewski i Zygalski zostali skierowani do Szkocji na Oficerski Kurs Doskonalący Administracji Wojskowej, który stanowił w istocie zakamuflowane szkolenie wywiadowcze. Nie wiemy, jakie były powody uczestnictwa Rejewskiego w szkoleniu. Po demobilizacji jesienią 1946 r. odmówił wstąpienia do Polskiego Korpusu Rozmieszczenia i Przystosobienia i postanowił powrócić do kraju (Zygalski zdecydował się pozostać na stałe w Anglii). Już wcześniej udało mu się ustalić miejsce pobytu rodziny i nawiązać kontakt z żoną. Niektóre dokumenty sugerują, że Rejewski zamierzał powrócić do opanowanej przez komunistów Polski tylko na chwilę, aby wywieźć z niej rodzinę. W wypełnionej

⁵⁶ Ibidem, s. 3–4.

6 września 1946 r. ankiecie personalnej Rejewski napisał, że chciałby osiedlić się z rodziną we Francji i zajmować się tam matematyką ubezpieczeniową. Plany te okazały się niewykonalne ze względu na politykę komunistycznych władz w Polsce. Rejewski mógł próbować nielegalnego przekroczenia granicy, ale w towarzystwie żony i małych dzieci była to opcja trudna do realizacji (choć taką właśnie drogę wybrała rodzina jednego z jego kolegów z Biura Szyfrów Stanisława Szachno).

21 listopada 1946 r. Rejewski powrócił do kraju. Wysiadł w porcie w Gdyni i pociągiem udał się do Bydgoszczy, gdzie przebywała jego żona z dziećmi. Trafiła tam po wysiedleniu z Warszawy, gdzie mieszkała do upadku powstania warszawskiego. Przez kilka miesięcy zamieszkiwała u krewnej pod Skierniewicami, aby ostatecznie w czerwcu 1945 r. powrócić do Bydgoszczy i zamieszkać u rodziców przy ul. Dworcowej 10. Córka Rejewskiego wspomina powrót ojca do domu w następujący sposób: „Mieszkałam wtedy z mamą, bratem Andrzejem i dziadkami przy ul. Dworcowej 10 w Bydgoszczy. Rozległ się dzwonek. W mieszkaniu pod numerem 2. był długi korytarz. Pamiętam, że Andrzej pobiegł otworzyć drzwi. Wrócił, podskakując: »Tata przyjechał, tata przyjechał!« – wołał. Zabrzmiało to dziwnie, ale ten pan, który pojawił się nagle, był dla mnie obcą osobą”⁵⁷. Kiedy Marian Rejewski wyjechał z kraju, jego dzieci były małe – Andrzej skończył dopiero trzy lata, a Janina miała zaledwie kilka miesięcy.

W wieku 41 lat Rejewski zmuszony był zaczynać życie od nowa. Sprawy rodzinne udało się szybko poskładać. Trzeba było jednak zadbać także o uporządkowanie spraw zawodowych, aby zdobyć środki na utrzymanie rodziny. Rejewski skontaktował się z prof. Krygowskim i poprosił o pomoc w znalezieniu pracy. Pomimo przychylności profesora nie udało mu się zatrudnić na Uniwersytecie Poznańskim, ponieważ nie dysponował ani stopniem naukowym, ani mieszkaniem w Poznaniu. Z podobnych

⁵⁷ H. Sowińska, *Życie Enigmą znaczone...*, s. 23.

względów nie zdołał uzyskać zatrudnienia na powstającej Politechnice Szczecińskiej⁵⁸. Zmuszony do poszukiwania pracy w Bydgoszczy 1 lutego 1947 r. zatrudnił się w fabryce Kabel Polski na stanowisku kierownika sekcji fakturowej (w grudniu 1948 r. fabryka została upaństwowiona i zmieniła nazwę na Pomorskie Zakłady Wytwórcze Materiałów Elektrotechnicznych w Bydgoszczy)⁵⁹. Gdy wydawało się, że życie Rejewskich zaczęło się stabilizować, rodzina doświadczyła tragedii. 9 lipca 1947 r., w wyniku powikłań związanych z chorobą Heinego-Medina, zmarł ich jedenastoletni syn Andrzej. Według relacji udzielonej autorowi przez córkę Mariana Rejewskiego, a zarazem siostrę zmarłego Andrzeja choroba była zaskoczeniem dla wszystkich, a śmierć nastąpiła bardzo szybko, zaledwie po kilku dniach od wystąpienia pierwszych objawów. Janina Sylwestrzak wspomina, że jeszcze na początku lipca zaczęła uczęszczać z bratem na półkolonie, które odbywały się w podbydgoskiej Smukale. Wraz z bratem byli na nich przez dwa lub trzy dni, po czym Andrzej zaczął chorować. Początkowo przebywał w domu, ale choroba postępowała tak szybko, że już po kilku dniach trafił do szpitala. Lekarze podejrzewali zapalenie opon mózgowych, z czasem okazało się jednak, że diagnoza ta była błędna. W związku z nieudzieleniem odpowiedniej pomocy zaledwie po trzech dniach pobytu w szpitalu mały pacjent zmarł. Dopiero po czasie okazało się, że objawy były efektem powikłań po chorobie Heinego-Medina⁶⁰.

W niedługim czasie na Rejewskiego spadły kolejne nieszczęścia. 28 stycznia 1950 r. został zwolniony z pracy. Otrzymał trzymiesięczne wypowiedzenie, w czasie którego musiał znaleźć nowe źródło utrzymania. Zwolnienie było efektem prowadzonej przez Urząd Bezpieczeństwa

⁵⁸ Ibidem, s. 38; R. Woytak, *Werble...*, s. 137–138.

⁵⁹ Archiwum Muzeum Wojsk Lądowych, Teczka personalna Mariana Rejewskiego.

⁶⁰ Rozmowa telefoniczna z Janiną Sylwestrzak, 4 grudnia 2015 r.

sprawy operacyjnej o kryptonimie „Sztab”, w ramach której inwigilowano grupę pracujących w bydgoskich zakładach przemysłowych osób związanych przed wojną z wojskiem lub „dwójką”. Na liście znalazł się również Rejewski. Z braku dowodów szkodliwej działalności grupy postanowiono ją rozbić, zmuszając jej członków do zmiany miejsca pracy. Nastąpiły zwolnienia i dalsza inwigilacja, a osoby szczególnie niewygodne dla władz stawiano przed sądem pod fikcyjnymi zarzutami. Rejewski zachował ostrożność adekwatną do swej skomplikowanej sytuacji i nie dał komunistycznym władzom pretekstu do dalszych szykan⁶¹.

Ze znalezieniem nowej pracy nie miał problemu, ponieważ oceniany był jako bardzo dobry fachowiec. Od 1 kwietnia 1950 r. był zatrudniony jako kierownik referatu ogólnego w Państwowym Przedsiębiorstwie Mierniczym (w 1951 r. przekształconym w Związek Mierniczych w Bydgoszczy). Nie pracował tam długo, ponieważ instytucję podporządkowano Naczelnej Organizacji Technicznej i zaczęto wprowadzać zmiany, których nie akceptował. Od 15 czerwca 1951 r. do 30 września 1954 r. pracował jako starszy księgowy w Związku Spółdzielni Rzemieślniczych, przekształconego w Związek Branżowy Spółdzielni Drzewnych i Wytwórczości Różnej w Bydgoszczy. Kolejna zmiana zatrudnienia związana była z likwidacją Związku Branżowego. W okresie wypowiedzenia został oddelegowany do pracy w Wojewódzkim Związku Spółdzielni Pracy w Bydgoszczy. Tam dał się poznać jako dobry i sumienny pracownik, co zaowocowało zawarciem od 1 października 1954 r. stałej umowy. Początkowo objął stanowisko starszego księgowego, następnie (1 stycznia 1957 r.) awansował na stanowisko instruktora ekonomicznego w Wydziale Inspektoratu Finansowego, a 1 lipca 1966 r. został kierownikiem Inspektoratu Kosztów i Cen w Dziale Księgowości i Finansów. Na tym ostatnim stanowisku pracował do lutego 1967 r., gdy przeszedł na rentę

⁶¹ W. Polak, *Marian Rejewski w optyce władz bezpieczeństwa PRL*, „Czasy Nowożytnie” 2005, t. 18–19, s. 115–127.

(jego sytuacja ustabilizowała się w pełni 16 sierpnia 1970 r., gdy przeszedł na emeryturę)⁶².

Wydaje się oczywiste, że Rejewski nie był usatysfakcjonowany wykonywaną pracą. Przemiany związane z tzw. odwilżą polityczną po śmierci Stalina i Bieruta zachęciły Rejewskiego do próby powrotu do pracy w charakterze kryptologa. 29 kwietnia 1956 r. złożył podanie o przyjęcie do pracy w Biurze Szyfrów Ministerstwa Obrony Narodowej⁶³. Nie wiemy, jakie były powody ubiegania się przez niego o pracę w tej instytucji. Czy była to chęć ustabilizowania sytuacji zawodowej, poprawy warunków materialnych, zajmowania się sprawami związanymi z kryptologią, czy może realizacja zadania wyznaczonego mu podczas szkolenia wywiadowczego z końca 1945 r.?

Podanie Rejewskiego nie zostało przyjęte, prawdopodobnie z powodu wcześniejszego zainteresowania komunistycznych tajnych służb. Poza wspomnianą sprawą „Sztab” w latach 1949–1956 Wydział II Wojewódzkiego Urzędu Bezpieczeństwa Publicznego w Bydgoszczy rozpracowywał Rejewskiego w ramach dwóch innych spraw obiektowych. Pierwsza nosiła kryptonim „Zachód” i obejmowała osoby służące w czasie drugiej wojny światowej w Polskich Siłach Zbrojnych na Zachodzie. Druga sprawa nosiła kryptonim „Targowica” i dotyczyła rozpracowania byłych pracowników i współpracowników Oddziału II Sztabu Głównego Wojska Polskiego. Sprawy te prowadzone były nieumiejętnie, a funkcjonariusze bezpieki nie do końca zdawali sobie sprawę, z kim mają do czynienia. Mimo to intensywnie inwigilowali Rejewskiego, śledzili go, sprawdzali jego kontakty, przeglądali korespondencję, a nawet bezskutecznie usiłowali zwerbować na informatora⁶⁴.

⁶² Archiwum MWL, Teczka personalna Mariana Rejewskiego.

⁶³ AIPN, 2602/3259, Pismo Mariana Rejewskiego do Ministerstwa Obrony Narodowej, 29 IV 1956, k. 28.

⁶⁴ AIPN By, 069/137, t. 1, Tabela nr 2 ewidencji ustalonych pracowników i współpracowników Oddziału II, k. 100, 135; ibidem, Aparat ucisku sprzed 1939 r. Straży Granicznej i P.P., k. 151 (tutaj błędne informacje, że Rejewski po

21 lutego 1956 r. założono kolejną, tym razem indywidualną sprawę ewidencyjno-obserwacyjną o nazwie „Kryptolog”, którą prowadzono do 20 czerwca 1958 r.⁶⁵ Z dokumentów zachowanych w teczce tej sprawy wynika, że również ona prowadzona była nieudolnie i nie dostarczyła resortowi żadnych materiałów, które mogłyby być pretekstem do represjonowania matematyka. Rejewski zdawał sobie sprawę z osaczania go przez komunistyczną bezpiekę. W liście do jednego ze znajomych pisał w 1957 r.: „W bardzo krótkim czasie zorientowałem się, i to na własnej skórze, skąd wiatr wieje, wobec czego zaniechałem wznawiania jakichkolwiek dawniejszych kontaktów, a istniejące ograniczyłem do niezbędnego minimum”⁶⁶. Świadomość potencjalnych zagrożeń i elementarna ostrożność pozwoliły Rejewskiemu uniknąć represji.

W trakcie prowadzonej inwigilacji nie zdołano zebrać obciążających go materiałów. Generalnie stwierdzić można, że wiedza bezpieki na temat kryptologa nie była zbyt głęboka. Funkcjonariusze charakteryzowali go w następujący sposób: „Przynależności do partii oraz udział jaki bierze w życiu społ[eczno]-pol[itycznym] w miejscu zam[ieszkania] nie ustalono. Na tematy polityczne z lokatorami rozmów nie prowadzi. Moralnie prowadzi się dobrze, jest mężczyzną spokojnym. Z rodziną swą i sąsiadami żyje zgodnie, nie wywołuje awantur. Tryb życia prowadzi spokojny i nałogów nie posiada. Opinią w miejscu zam[ieszkania] wśród lokatorów cieszy się dobrą. Żyje w średnich warunkach materialnych,

wojnie był pracownikiem PWRN, kierownikiem Wydziału Gospodarczego); ibidem, Wykaz byłych prac[owników] O[ddziału] II Sztabu Gener[alnego] do 1939 r. w Bydgoszczy, k. 154.

⁶⁵ AIPN By, 044/200, Sprawa ewidencyjno-obserwacyjna kryptonim „Kryptolog”; W. Polak, *Działania władz bezpieczeństwa PRL wobec Mariana Rejewskiego*, [w:] *Rejewski 1905–1980. Życie Enigmą pisane*, red. J.S. Ciechanowski et al., Bydgoszcz 2005, s. 75–88.

⁶⁶ List Mariana Rejewskiego do Stanisława Dobrzyckiego, 22 VII 1957 r. (w zbiorach Janiny Sylwestrzak).

a na swym utrzymaniu ma żonę i jedno dziecko”⁶⁷. W innym dokumencie formułowano podobne opinie na jego temat: „W miejscu zamieszkania opinią cieszy się dość dobrą. Żyje w średnich warunkach materialnych. Moralnie prowadzi się dobrze. Tryb życia prowadzi spokojny”⁶⁸.

Ze względu na to, że nie dostrzeżono w zachowaniu Rejewskiego niczego podejrzanego, postanowiono zakończyć inwigilację. Uzasadniając zakończenie sprawy „Kryptolog”, funkcjonariusz UB stwierdzał, że „w toku rozpracowania nie ustalono by figurant uprawiał jakąkolwiek wrogą działalność w stosunku do PRL. Również utrzymywane przez niego kontakty i obecne miejsce pracy nie dają podstawy do twierdzenia uzasadniającego o ewentualnym jego powiązaniu z wywiadem”⁶⁹. Pomimo pozytywnej dla Rejewskiego opinii był na tyle podejrzany, że podanie o pracę w Biurze Szyfrów MON zostało zaopiniowane negatywnie.

W kwietniu 1962 r. Rejewscy przeprowadzili się do kamienicy w al. 1 Maja 10 (obecnie ul. Gdańska). Właśnie tam w marcu 1967 r. Rejewski spisał liczące ponad 100 stron wspomnienia. Zawarł w nich charakterystykę pracy dla „dwójki”, koncentrując się na technicznej stronie złamania szyfru Enigmy. Rejewski przekazał maszynopis do Wojskowego Instytutu Historycznego w Warszawie, gdzie początkowo nikt nie zainteresował się jego zawartością. Sytuacja zmieniła się, gdy na Zachodzie zaczęły się ukazywać książki, w których wzmiankowano o sprawie Enigmy i udziale w tym dokonaniu Polaków⁷⁰.

W książce Gustave’a Bertranda wydanej we Francji w 1973 r. autor opisał działania francuskiego wywiadu, polsko-francuską współpracę

⁶⁷ AIPN By, 044/200, Pismo zastępcy naczelnika wydziału „B” do naczelnika Wydziału II WUBP w Bydgoszczy, 15 IV 1955, k. 22.

⁶⁸ Ibidem.

⁶⁹ AIPN By, 044/200, Postanowienie o zakończeniu (zaniechaniu) i przekazaniu do archiwum sprawy ewidencji operacyjnej krypt. „Kryptolog”, 12 VI 1958, k. 58.

⁷⁰ H. Sowińska, *Życie Enigmą znaczone...*, s. 40.

wywiadowczą oraz kulisy złamania kodu niemieckiej maszyny szyfrującej. Wspominając sprawę Enigmy, przyznał, że jej szyfr złamali polscy kryptolodzy, nie wymienił jednak ich nazwisk⁷¹. Sytuacja ta wzbudziła zainteresowanie polskich dziennikarzy, którzy ogłosili w prasie poszukiwania osób znających sekret złamania szyfru Enigmy. Do redakcji zgłosiło się kilka osób, w tym Marian Rejewski; historia Enigmy przestała być tajemnicą. Do drzwi Rejewskich, którzy od 1969 r. mieszkali w Warszawie przy ul. Gdańskiej 2, zaczęli pukać zaciekawieni sprawą dziennikarze, korespondenci prasy zagranicznej, historycy i pasjonaci historii. Chcieli porozmawiać z Rejewskim i wysłuchać jego relacji na temat prac nad łamaniem szyfru Enigmy. Wykorzystując to zainteresowanie, Rejewski odnowił korespondencyjny kontakt z Zygalskim, Bertrendem i innymi osobami związanymi ze sprawą złamania niemieckiej maszyny szyfrującej. Uzyskał wiele informacji, które wykorzystał latem 1974 r. gdy opracowywał uzupełnienie do wspomnień, oraz w opublikowanych następnie tekstach⁷².

Upublicznienie sprawy Enigmy spowodowało presję na uhonorowanie zasług Mariana Rejewskiego. 29 listopada 1978 r. Rada Państwa nadała mu Krzyż Oficerski Orderu Odrodzenia Polski (wręczenie odznaczenia odbyło się 12 grudnia 1978 r. w Ministerstwie ds. Kombatan-tów). W maju 1979 r. minister obrony narodowej wręczył mu srebrny medal „Za zasługi dla obronności kraju”. Przyznanie odznaczeń ukazuje hipokryzję władz komunistycznych; za te same dokonania, za które obecnie Rejewski był nagradzany, kilkadziesiąt lat wcześniej był represjonowany.

Z czasem nadeszły kolejne wyrazy uznania, tym razem spontaniczne i szczerze. 15 września 1979 r. Polskie Towarzystwo Matematyczne

⁷¹ G. Bertrand, *Enigma, ou la plus grande énigme de la guerre 1939–45*, Paris 1973.

⁷² Zob. np. M. Rejewski, *Jak matematycy polscy rozszyfrowali Enigmę*, „Wiadomości Matematyczne” 1980, nr 1, s. 1–28.

przyznało mu honorowe członkostwo. W 1979 r. w kinach wyświetlano film fabularny *Sekret Enigmy*, a telewizja wyemitowała ośmioodcinkowy serial zatytułowany *Tajemnica Enigmy*. Kolejnych honorów Marian Rejewski już nie doczekał. 13 lutego 1980 r. doznał rozległego zawału serca, w wyniku którego zmarł. Został pochowany w asyście kompanii honorowej Ludowego Wojska Polskiego na cmentarzu wojskowym na Powązkach.

Elżbieta Szczuka

O Jerzym Różyckim i jego rodzinie

Kiedy na początku 2016 r. w moim mieście pojawiła się inicjatywa Uczczenia Jerzego Różyckiego, wybitnego absolwenta Gimnazjum Koedukacyjnego Towarzystwa Szkoły Średniej w Wyszkanie nad Bugiem, w 90-lecie zdania przez niego egzaminu dojrzałości, miałam o nim tylko podstawowe wiadomości, o jego rodzinie nie wiedziałam prawie nic. W czasie kilku miesięcy udało mi się jednak zdobyć wiele nigdy niepublikowanych zdjęć i materiałów¹, którymi chcę się podzielić.

Jerzy Witold Różycki, genialny matematyk i kryptolog, najmłodsze dziecko Wandy z Benitów i Zygmunta Różyckich, urodził się 24 lipca 1909 r. o godzinie piątej po południu w Olszanie w guberni kijowskiej. Był nietuzinkową osobowością. Lubił śpiewać, słuchać muzyki, czytać książki, wędrować po górach. W rodzinie wspominają, że miał poczucie humoru, był żartownisiem.

Jego ojciec, **Zygmunt Różycki** herbu Rola, pochodził z ziemiańskiej rodziny. Urodził się, wg kalendarza juliańskiego, 20 kwietnia 1872 r. w majątku Cecylówka, parafia Turzysk, powiat kowelski, gubernia wołyńska. Skończył Wydział Medycyny i Farmacji na Uniwersytecie w Sankt Petersburgu, służył jako oficer medyczno-sanitarny w carskiej armii. Był człowiekiem rzutkim, pełnym inwencji, dobrym biznesmenem. Prowadził apteki na terenie ówczesnej Rosji: w Baku, Kijowie, Sankt Petersburgu i innych miastach. Często zmieniał miejsce zamieszkania. Był też hazardzistą – zdarzało mu się przegrać duże pieniądze w karty lub w kasynie w Monte Carlo.

¹ Za pomoc w zbieraniu materiałów autorka dziękuje: Januszowi Różyckiemu, Maciejowi Grodeckiemu, Jerzemu Krzywaźni, Magdalenie Kolczyńskiej i Andrzejowi Wodzińskiemu.

W 1918 r. wraz z rodziną uciekł z ogarniętych rewolucją terenów byłego Imperium Rosyjskiego do odrodzonej po zaborach Rzeczypospolitej. Przez kilka lat mieszkał w Wyszkanie nad Bugiem. Tu oraz w pobliskich wsiach, Długosiodle i Porębie, prowadził apteki. Apteki zakładał także w: Wąchocku, Opatowie, Kielcach, Gdyni, Kraszewicach. Zmarł w Kraszewicach (Wielkopolska) 22 sierpnia 1931 r. w wieku 59 lat i tam został pochowany.

Matka Jerzego, **Wanda Leopolda z domu Benit**, o 11 lat młodsza od męża, urodziła się 5 listopada 1883 r. w Opatowie (Świętokrzyskie) w rodzinie inteligentnej. Wanda dużo czytała, znała na pamięć całego *Pana Tadeusza*. Jako dziewczyna pisała wiersze i opowiadania do tygodników „Bluszcz” i „Kłosa”. W 1902 r. w kościele parafialnym w Łopusznie wzięła ślub z Zygmuntem Różyckim.

Państwo Różyccy mieli czworo dzieci: Aleksandrę (1903), Halinę (1905), Eugeniusza (1907) i Jerzego (1909). Różne miejsca urodzenia dzieci potwierdzają, że często zmieniali miejsce zamieszkania.

* * *

Jerzy Różycki naukę gimnazjalną rozpoczął w Kijowie, w Polskim Gimnazjum Kresowym, a kontynuował ją w Wyszkanie. Wraz ze starszym o dwa lata bratem Eugeniuszem uczył się w ośmioklasowym prywatnym gimnazjum w Wyszkanie (licea ogólnokształcące powstały dopiero w latach 30. XX w. w ramach Jędrzejewiczowskiej reformy systemu szkolnictwa).

Licealne archiwum (kontynuatorem przedwojennego gimnazjum jest I LO im. Cypriana Kamila Norwida) zostało w części zniszczone w czasie drugiej wojny światowej. Najstarszy zachowany katalog pochodzi z roku szkolnego 1916/17, kolejny z roku szkolnego 1923/24. I właśnie w księdze głównej uczniów Gimnazjum Koedukacyjnego Towarzystwa Szkoły Średniej w Wyszkanie nad Bugiem z tego roku wśród uczniów klasy VI, liczącej 27 osób, znajdziemy nazwiska braci Jerzego i Eugeniusza

Różyckich. W księdze głównej z roku szkolnego 1925/26 wśród uczniów klasy VIII jest nazwisko Jerzego Różyckiego z informacją, że został dopuszczony do egzaminu maturalnego. Z 18-osobowej klasy do matury dopuszczono 14 osób. Pisemna informacja o tym, że w maju 1926 r. zdał maturę w Wyszkanie (miał wtedy niecałe 17 lat), pochodzi z archiwum UAM w Poznaniu.

Eugeniusz, brat Jerzego, często chorował, co wiązało się z częstą nieobecnością w szkole. Egzaminu dojrzałości nie doczekał – zmarł w 1925 r. na chorobę niedokrwienną serca. Został pochowany w Wyszkanie. Prawdopodobnie po jego śmierci Różyccy przenieśli się do Kraszewic, a w ostatnim roku nauki Jerzy mieszkał w Wyszkanie na stacji.

W październiku 1926 r. Jerzy Różycki rozpoczął studia na Wydziale Matematyczno-Przyrodniczym Uniwersytetu Poznańskiego. Angażował się w życie studenckie, działał w Korporacji Akademickiej Chrobria skupiającej studentów i absolwentów wyższych uczelni Poznania (dewizą organizacji było hasło „Honor et amicitiae” – dla honoru i przyjaźni), był również członkiem Akademickiego Koła przy Oddziale Poznańskim Polskiego Towarzystwa Tatrzańskiego. W 1929 r. znalazł się w grupie 23 najzdolniejszych studentów matematyki, biegle znających język niemiecki, którzy rozpoczęli utajniony kurs podstaw kryptologii. Organizatorem kursu polecił ich prof. Zdzisław Krygowski, kierujący Instytutem Matematycznym Uniwersytetu Poznańskiego. Z tej grupy tylko ośmiu weszło w skład zespołu kryptologów w filii Biura Szyfrów Sztabu Głównego Wojska Polskiego w Poznaniu. Ostatecznie pozostało w nim trzech: Marian Rejewski, Jerzy Różycki (najmłodszy z nich) i Henryk Zygałski.

Dyplom magistra matematyki Różycki uzyskał w lutym 1932 r. Zdecydował się na studiowanie drugiego kierunku – w grudniu 1937 r. otrzymał dyplom magistra geografii. Prof. Stanisław Pawłowski, wybitny geograf (członek Polskiej Akademii Umiejętności, od 1938 r. wiceprezydent Międzynarodowej Unii Geograficznej), po zdaniu przez Jerzego egzaminu magisterskiego zaproponował mu asystenturę u siebie, na Wydziale Geografii Uniwersytetu Poznańskiego.

Jeszcze jako student matematyki Jerzy Różycki zaczął pracować w zespole kryptologów Biura Szyfrów Sztabu Głównego. We wrześniu 1932 r. poznański zespół przeniósł się do Warszawy. Biuro Szyfrów Oddziału II Sztabu Głównego Wojska Polskiego mieściło się w Pałacu Saskim. Marian Rejewski, Jerzy Różycki i Henryk Zygalski dostali pracę w pełnym wymiarze godzin. Zajmowali się łamaniem niemieckich szyfrów. Praca kryptologów otoczona była ścisłą tajemnicą. Indywidualnym wkładem Jerzego Różyckiego w dekryptaż Enigmy było opracowanie tzw. metody zegara, która pozwalała określić, który z trzech wirników szyfrujących Enigmy jako pierwszy odbiera impulsy z klawiatury.

W 1937 r. Jerzy Różycki poznał **Marię Barbarę Majkę** (bliscy używali jej drugiego imienia). „Radosna, szczęsna, wielka miłość weszła do mej duszy i to było Drezno” – napisał w jednym z listów do niej. Ślub wzięli 2 lipca 1938 r. w Rzeszowie. 10 maja następnego roku urodził się ich syn Jan Janusz.

Żona Jerzego urodziła się w 1910 r. w mieście Wysokie Myto (Czechy). Była spokrewniona z wybitnym scenografem, reżyserem teatralnym i malarzem Józefem Szajną (1922–2008), od 1972 r. profesorem ASP. Ich matki były siostrami. W 1931 r. Maria ukończyła Państwowe Seminarium dla Nauczycielek Rzemiosł w Warszawie, w 1938 r. zdała w Poznaniu egzamin mistrzowski z krawiectwa damskiego. Pracowała jako nauczycielka w szkołach odzieżowych. Po wojnie Maria Różycka m.in. wykładała na Wydziale Tkanin ASP, a w latach 1950–1966 była, w ramach Zakładu Ubioru, kierownikiem Zespołu Odzieży Dziecka w Instytucie Wzornictwa Przemysłowego w Warszawie. Była osobą ciepłą i sympatyczną, wybitną projektantką, została odznaczona Krzyżem Kawalerskim Orderu Odrodzenia Polski. Za mąż ponownie nie wyszła, chociaż miała wielu adoratorów. Zmarła w Rzeszowie 4 października 1991 r., została pochowana w grobie rodzinnym w Stobiernej koło Rzeszowa.

Ostatni raz Maria i Jerzy widzieli się 9 września 1939 r. – pożegnali się na stacji kolejowej w Brześciu nad Bugiem. Jak wyglądały pierwsze dni

września 1939 roku, a zarazem ich ostatnie wspólne dni, wiemy z zapiszków Marii Różyckiej. Zacytuję krótkie fragmenty:

3 września – *Ustawiczne alarmy przeciwlotnicze – żyjemy w stałej wędrówce pomiędzy piwnicą a mieszkaniem (w małej willi na 1. piętrze). Jurek wrócił z biura późnym wieczorem. Przyjechał z Zygą (przyjacielem Henrykiem Zygalskim). Są wstrząśnięci wypadkami przeżytego dnia. Informują nas, że ich biuro opuszcza dotychczasową siedzibę (Pyry pod Warszawą), są już spakowani, jutro wyjeżdżają specjalnym pociągiem do Brześcia n. Bugiem.*

4 września – *Żegnamy się z Jurkiem i Zygą – ogarnia nas smutek, niepewność, czy i kiedy się zobaczymy... Rozstroiło nas pożegnanie Jurka z „Maliznotą” (tak nazywaliśmy naszego synka). Ileż to było pięknych słów wypowiedzianych do czteromiesięcznego dziecka! Wychodzimy wszyscy na taras, powiewamy pieluchami (które się suszyły), krzyczymy słowa pożegnania, dopóki sylwetki ich nie zniknęły z naszych oczów.*

6 września – *O godz. 5 rano przyszedł Jurek. Pociąg ich jeszcze nie może wyjechać. Wpadł na chwilę tylko, aby się upewnić, co się z nami stało. Jest zaszokowany tym, że jeszcze tu jesteśmy. Nie mógł nas w tej sytuacji pozostawić. Zdecydował, że zabierze nas do swojego pociągu – byle tylko wydostać się z Warszawy, a po drodze może łatwiej będzie dotrzeć do rodziny na prowincji. Jurek przyszedł do nas pieszo z dworca Wileńskiego na ul. Ursynowską. Miał okaleczone nogi – nie było czasu na opatrunek, zmienił tylko buty i powiedział, że musi zaraz wracać. Ruszamy najpierw pieszo, po tym różnymi sposobami, wreszcie dostajemy się na dworzec. Za ledwie znaleźliśmy się w wagonie, zaczęło się bombardowanie dworca i pociągów tam stojących. Kryjemy się wszyscy pod wagony. Na razie o wyjeździe nie może być mowy. Tory są uszkodzone i niektóre wagony. Skład pociągu musi być uzupełniony. Jurek poszedł szukać mleka. Jego kolega Marian Rejewski pobiegł jeszcze do domu, do żony i dzieci. Przy nas został Zyga, który tu nikogo nie miał z rodziny – był z Poznania. Wieczorem byliśmy w komplecie. Pociąg ruszył. Z ulgą wyjeżdżamy z dworca w stronę Siedlec.*

9 września – Nareszcie koło południa jesteśmy na dworcu w Brześciu nad Bugiem. Zastajemy ciszę, spokój i przepiękną pogodę. Wychodzimy z pociągu. Ja z Jurkiem biegniemy na poszukiwanie mleka i żywności. Przed dworcem jest wielu sprzedających, można zaopatrzyć się dostatnio – jakby nie było wojny. Nagle słyszymy warkot motorów, po tym ciemną chmurę na niebie – samoloty tuż nad naszymi głowami (W tym pierwszym nalocie na dworzec przyleciało 36 bombowców). Wypadki tego dnia posuwały się jednak zbyt szybko – ciągle naprzód. Przyszedł do nas Zyga, aby nam powiedzieć, że przydzielono ich trójce: Marianowi Rejewskiemu, Henrykowi Zygalskiemu i Jurkowi samochód, i mają rozkaz jak najszybciej przedostać się do Rumunii. We mnie wszystko się buntuje – jak to, po takim wyraźnym ocaleniu znowu rozstanie. Jest to już trzecie z rzędu pożegnanie od wybuchu wojny. Tym razem – na zawsze.

Jerzy Różycki z kolegami z Biura Szyfrów ewakuowali się do Rumunii, a potem do Francji. Tu przebywał pod nazwiskiem Julien Rouget. Polacy współpracowali z francuskim wywiadem przy łamaniu szyfrów (kryptolodzy zostali oddelegowani przez Armię Polską we Francji do służby w armii francuskiej na czas wojny). Od 1940 r. pracowali w zamku des Fouzes, ośrodek miał kryptonim Cadix. Jesienią 1941 r. Jerzy Różycki na kilka miesięcy popłynął do Algieru, gdzie była ekspozytura Cadixu, żeby rozszyfrować przechwycone depesze radiowe. Z powrotem do Francji wypłynął 6 stycznia 1942 r. na parowym statku pasażerskim „Lamoriciere”. W trakcie podróży rozpętał się sztorm.

W archiwach zachował się dokument z 1942 r. podpisany przez Henri Materona (Henryk Paszkowski):

Rozmawiałem z nim na kilka chwil przed opuszczeniem mnie na zawsze. Skarżył się na wyczerpanie fizyczne spowodowane chorobą morską, bezsennością i jednocześnie brakiem posiłków. To prawdopodobnie skłoniło go do zawarcia ze mną umowy, jaką zawarłem ubiegłej nocy ze Smolnym. Miała ona obowiązywać każdego z nas. Prośba Rouget'a brzmiała

następująco: „Jeśli się uratujesz, powiedz moim przyjaciółom w Fouzes, żeby nie zapomnieli o mojej rodzinie. Czuję się bardzo niespokojny i trudno jest mi się opanować”.

9 stycznia na Morzu Śródziemnym w pobliżu Balearów statek zatonał. O śmierci męża Maria Różycka dowiedziała się dopiero w maju 1942 r. z listu Henryka Zygalskiego.

Wanda Różycka przeżyła syna prawie 20 lat. Okupację niemiecką spędziła w Warszawie wraz z córkami i ich rodzinami. W tym trudnym czasie bardzo pomagali im, zaopatrując w produkty rolne, mieszkający w Somiance (wieś gminna w powiecie wyszkowskim) kuzynka Zofia i jej mąż Franciszek Wróbel, zarządca pól miejscowego majątku. Wanda Różycka zmarła 19 grudnia 1960 r. w Warszawie w wieku 77 lat, została pochowana na Cmentarzu Bródnowskim.

Syn Jerzego Różyckiego, **Jan Janusz**, dla bliskich „Jancyk”, to absolwent Liceum Plastycznego i warszawskiej Akademii Sztuk Pięknych. W latach 1968–1973 na Wydziale Malarstwa ASP był asystentem prof. Tadeusza Dominika (1928–2014), wybitnego malarza i grafika. Zasiągnął jako malarz, scenograf, ale też jako znakomity sportowiec – w latach 60. Janusz Różycki był jednym z najlepszych polskich szermierzy, wielokrotnym mistrzem Polski we florecie i szabli, wicemistrzem świata i wicemistrzem olimpijskim.

Upamiętnienie Jerzego Różyckiego

W kwietniu 2016 r. na budynku I Liceum Ogólnokształcącego im. Cypriana Norwida odsłonięto pamiątkową tablicę. Imię Jerzego Różyckiego nosi też sala matematyczna w I LO, a szkoła co roku organizuje konkursy matematyczne jego imienia.

W listopadzie 2016 r. radni miejscy podjęli uchwałę w sprawie nadania imienia „Jerzego Różyckiego, matematyka i kryptologa” rondu na skrzyżowaniu ulic Tadeusza Kościuszki i Stefana Okrzei w Wyszkowie.

W kwietniu 2017 r. na budynku nr 4 przy ul. Woronicza w Warszawie, gdzie w latach 1937–1938 mieszkał Jerzy Różycki, zawisła pamiątkowa tablica.

W październiku 2018 r. w Parku Karola Ferdynanda Wazy w Wyszkowie, w pobliżu nieistniejącego już budynku Gimnazjum, stanęła ławeczka Jerzego Różyckiego autorstwa rzeźbiarza Karola Badyny.

W lutym 2020 r. Jerzy Witold Różycki został patronem Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni.



Fot. 1. Od góry: Jerzy Różycki z ojcem Zygmuntem, w środku: Wanda Różycka, Halina Skierczyńska z córką Wandą i mężem Marianem, Kraszewice, 1928.

Źródło: Zbiory prywatne Macieja Grodeckiego

Patryk Piłasiwicz

Henryk Zygałski i muzyka szyfrów

„Czy świat potrwa jeszcze trzy kwadransy?...”

Henryk Zygałski, Trebeurden, 1955

Historia zmagania kryptologów z szyframi Enigmy budzi wiele emocji. Uważnego badacza przeszłości prowadzi w mroczny świat wydarzeń przemilczanych, a przed naukowcem odkrywa niewyczerpane pole matematycznych eksploracji. Postrzegana niezmiennie jako metafora tajemnicy, Enigma stała się symbolem nowej epoki technologicznej i kulturowej, przepowiednią narodzin sztucznej inteligencji.

Wojenny exodus polskiego Biura Szyfrów i bezprecedensowy sukces kryptologiczny trójki superbohaterów: Mariana Rejewskiego, Jerzego Różyckiego i Henryka Zygałskiego przez lata ukrywany był w cieniu przemilczeń i manipulacji. Mozolne odkrywanie prawdy o udziale Polaków w wyścigu kryptologicznym przypominało walkę z szyframi w przestrzeni wojennej konfrontacji. Dało jednak zdumiewający efekt – dzięki wysiłkowi wielu osób i instytucji prawdziwa historia złamania Enigmy wreszcie ujrzała światło dzienne. Poszczególne jej aspekty analizowane są coraz intensywniej na forach naukowych. Podejmowana refleksja dotyczy historii, rozwoju technologii czy szyfrowania danych w niemal wszystkich obszarach życia społecznego. Jej elementem nieodmiennie jest zachwyt nad potęgą ludzkiego umysłu, zdolnego pokonać niemal wszystkie ograniczenia.

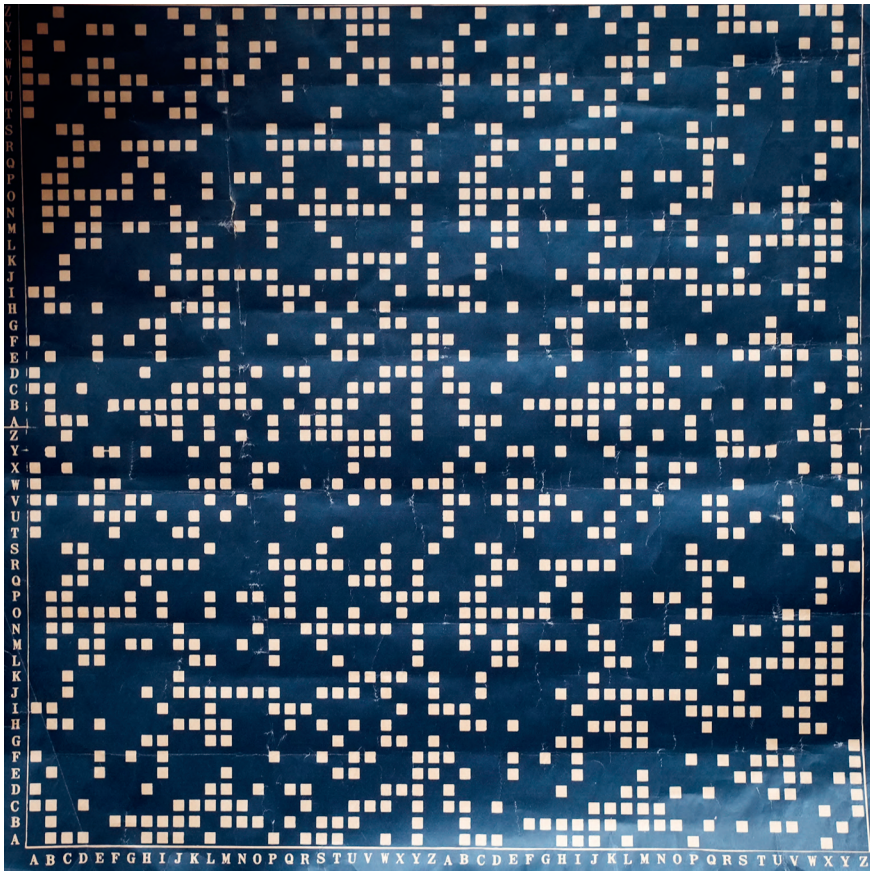
Jako muzyk – kompozytor, wykonawca i dyrygent – podzielam ten zachwyt i zadaję sobie pytanie o granice możliwości kreatywnych człowieka. Akt zwycięstwa nad Enigmą postrzegam jednak w nieco innym świetle niż kryptolog czy historyk. Wpływ na to mają moje własne

ograniczenia – nie dysponuję umysłem matematycznym ani umiejętnościami kryptologicznymi. Historia jest dla mnie przestrzenią tylko częściowo poznaną, a doniosłość wydarzeń kluczowych dla danej epoki angażuje mnie w mniejszym stopniu niż niuanse życia poszczególnych ludzi – bohaterów chętnie zapominanych i pomijanych. Myśl inżynierska w moim wydaniu mogłaby sprawić więcej kłopotów niż pożytku, więc sprowadzam ją do działań koniecznych, wykonywanych z poświęceniem, lecz chaotycznie. Enigma fascynuje mnie jednak i uzależnia, inspiruje do tworzenia muzyki i określa sposób jej percepcji. Kiedy myślę o historii kryptologów, ich szaleńczej podróży po ogarniętej wojną Europie, w mojej wyobraźni rozpościera się mapa miejsc i wydarzeń, które tworzą swoisty algorytm tajemnicy, narracji opartej na okrucinach życia, wspomnieniach i obrazach.



Fot. 1. Henryk Zygalski.
Fotografia z archiwum rodzinnego
Marii i Gerharda Bryschaków

Moim bohaterem stał się Henryk Zygałski. Ujrzałem w nim człowieka o charakterze otwartym, nieskrępowanym, pełnym życia i światła. Jego płachty – perforowane arkusze papieru służące do deszyfrażu – skojarzyłem z wielkoformatowymi stronami partytur. Treść partytury, umieszczona na pięcioliniach i złożona ze skomplikowanych symboli, jest równie nieczytelna jak arkusz płachta Zygałskiego. Oba obiekty mają ze sobą jednak coś wspólnego – ich sens spotyka się w angielskim słowie *sheet*. Partytury są zaszyfrowanym nośnikiem dźwięku, jednokrotnym i niepowtarzalnym (mimo wyjściowej powtarzalności



Fot. 2. Egzemplarz płachty Zygałskiego. Archiwum autora

zapisu nutowego), ponieważ prowadzą do wykonania dzieła muzycznego *tu i teraz* – w sposób jednokrotny, naznaczony ulotną mieszanką emocji słuchaczy i interpretacji muzyków (dyrygenta i orkiestry). Przypominają *one-time-pad* – sposób szyfrowania, w którym niemożliwe jest powtórzenie. Płachty Zygałskiego „czytane” są dzięki obecności światła – promienia prześwietlającego szereg nałożonych na siebie perforacji i prowadzących do odczytania kluczowych informacji. Wykorzystanie światła w procesie deszyfrazu przy użyciu płacht jest poetyckim śladem, znaczącym poza intencją znaczenia, ale posiadającym niezwykle siłę artystycznej inspiracji.

Podobnie jak w przypadku deszyfrazu, w procesie tworzenia muzyki kluczowym elementem jest czas. Można powiedzieć, że czas stanowi substancję muzyki, nadaje kształt przeżyciom słuchaczy i prowadzi ich przez narrację lub stan zawieszenia (zatrzymania) do celu. Głównym celem muzyki (oprócz dostarczenia bodźców estetycznych, emocji lub stworzenia tła rozmaitych wydarzeń) jest zmiana, która dokonuje się w słuchającym. Głębokiemu przeżyciu muzyki towarzyszy przeobrażenie – dźwięki docierają do samej istoty emocji i otwierają je jak algorytm. Doniosłość tych zmian zrozumiała jest dla każdego, kto choć raz w życiu doświadczył szczerego muzycznego uniesienia, podczas którego myśli, uczucia, wyobrażenia i wspomnienia tworzą architekturę czystej harmonii. W tym sensie każde wykonanie (wysłuchanie) muzyki jest jak nadanie (odbiór) szyfrogramu i poddanie go procesowi deszyfrazu, który może się udać lub nie.

Współczesne partytury przypominają często skomplikowane szyfrogramy. Dwudziesty wiek zrezygnował z monopolu klasycznego zapisu nut na pięciolinii – pojawiły się nowe techniki notacji muzycznej, wykorzystujące enigmatyczne symbole z pogranicza grafiki, malarstwa, rysunku i kaligrafii. Takie partytury graficzne są często tworzone jednokrotnie – dany sposób zapisu obowiązuje wyłącznie w odniesieniu do jednego utworu, a do odczytania (odszyfrowania) partytury niezbędny jest klucz – legenda ze szczegółowym opisem każdego symbolu.

20 SCULPTURE (Skalpel) 4:30 1:1

DB^b A INTRO ~164
 Db^b A ad lib
 G^b Db Ab Db^b (0.47) (this then...)
 A (0.52) Db^b (add 9) 16
 B (1.10) Db^b A (add 9) 16
 C A₂ (1.39) Db^b A (add 9) 16

D (2.03) 16 Db^b A (add 9)
 E (2.26) 16 Db^b A (add 9)
 F (2.49) 15 Db^b A (add 9) 16
 G (3.13) 16 Db^b A (add 9) 16
 H (3.36) 15 Db^b A (add 9) 16

I (3.59) 16 Db^b A (add 9)
 J (4.23) 16 Db^b A (add 9)

NO DRUMS percussion (delicate), vi/bs ten
 Lector-text: (this time is strophonic...)
 LET RING.

Coda
 Meher „Das Buchiel” - kowidaka
 Attack po „On The Road.”
 SKALPEL Liquid
 BIG BAND
 simple chords, un-expected orchestration (soft)
 Steve Reich. New York Counterpoint?

Layering not improvising
 Loop notes
 Bass clarinet
 Clarinet
 Flute
 Flugelhorn
 Vibes

INTRO - quasi-Cadenza (piano) u/vibes (ad lib upper melodic line)
 Double Bass - arco Db (pedal note)
 phage-like

Score

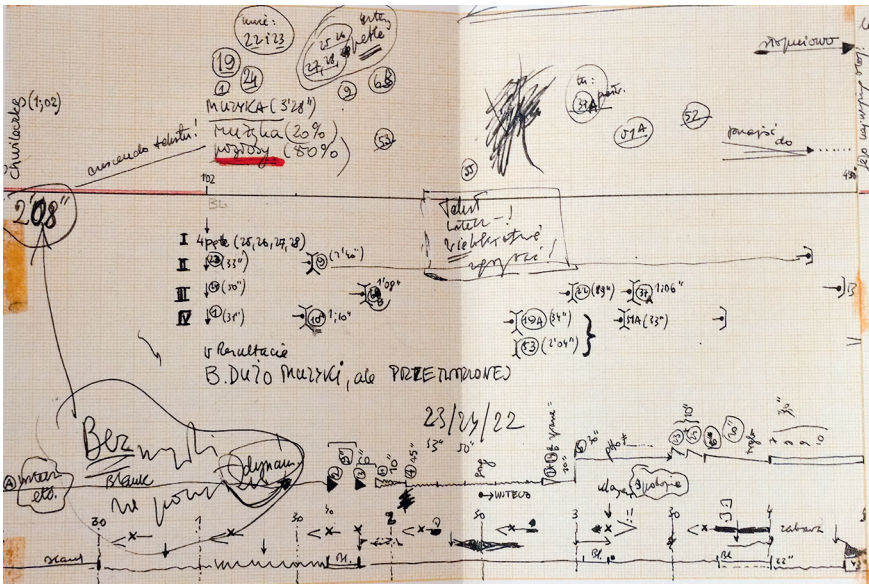
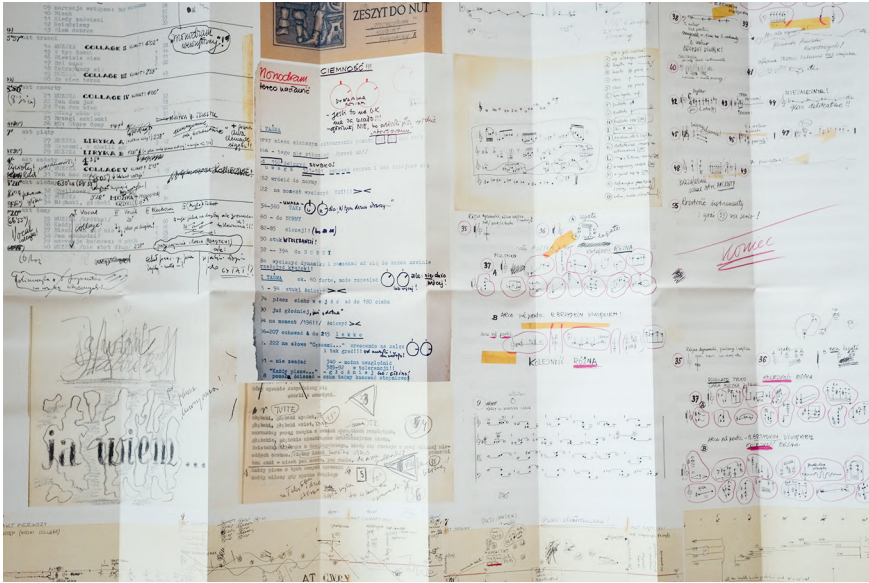
Sculpture VIBES - moc!
 Skalpel
 Patryk Piłasiwicz

ORCHESTRA LOW, SHARP, NO CRESC.

COUNT 1, 2, 3 (double time) (TPT)

Flute
 Alto Sax
 Clarinet Bb
 Bass Sax
 Bass Clarinet
 Flugelhorn 1
 Flugelhorn 2
 Horns 1
 Horns 2
 Vibraphone
 Drum Set
 Percussion
 Electric Piano
 Gong
 String Bass

Fot. 3a, 3b. Przykład partytury graficznej oraz jej „odszyfrowanego” odpowiednika. Opracował Patryk Piłasiwicz



Fot. 4a, 4b, 4c. Partytura kompozycji Bogusława Schaeffera *Monodram* (fragment), Requiem Records, 160/2018

Kolejność wykonania poszczególnych części utworu może zależeć od wielu czynników. Niektóre kompozycje Johna Cage'a, Kazimierza Serockiego czy Bogusława Schaeffera wymagają każdorazowego układania fragmentów partytury i głosu orkiestrowego przez muzyków¹. Proces superimpozycji segmentów z zapisem w celu odzwierciedlenia muzycznej narracji przypomina nakładanie kolejnych płacht Zygalskiego podczas próby deszyfrażu.

Postrzeżenie działań kryptologów z perspektywy muzycznej wydaje się uzasadnione nie tylko w kontekście zapisu i odczytu zaszyfrowanych informacji. Obraz soniczny szyfrogramów jest odrębnym źródłem

¹ Przykładem takiej kompozycji jest *Non stop* Bogusława Schaeffera. Utwór, oryginalnie skomponowany na fortepian (1957), może być wykonywany za pomocą specjalnej aplikacji przeznaczonej na mobilne urządzenia (telefony, tablety) oraz przez dowolną obsadę instrumentalną. <http://aureaporta4schaeffer.pl/non-stop> [dostęp: 28.09.2018].

inspiracji dla współczesnych kompozytorów, grafików i twórców interdyscyplinarnych. Proces szyfrowania i deszyfrowania miał przecież postać dźwiękową, a Enigma przeznaczona była do działania w eterze – przestrzeni radiowego nasłuchu.

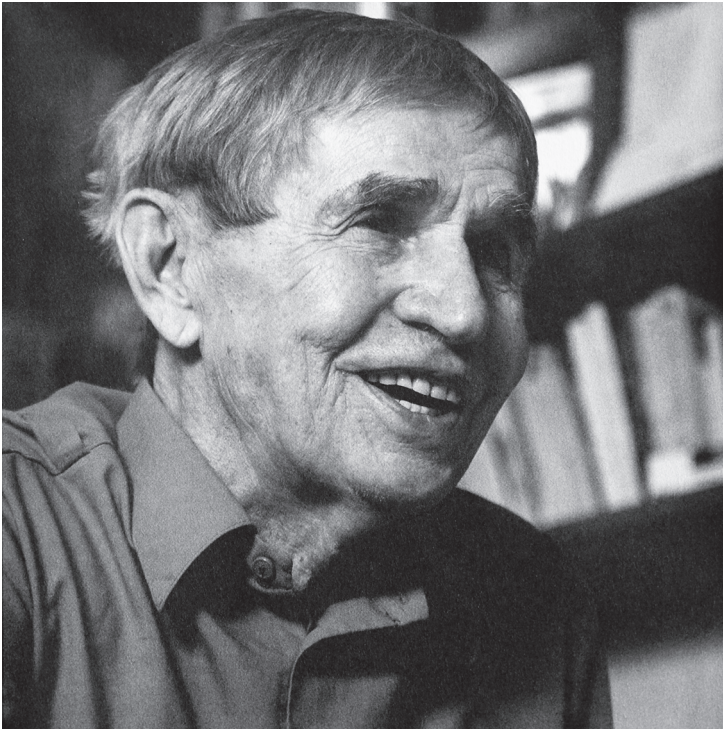
Kryzys klasycznych środków wyrazu, którymi posługiwała się muzyka dziewiętnastowieczna, stał się początkiem poszukiwań nowych obszarów ekspresji. Wartości do tej pory odrzucane lub pomijane, takie jak: hałas, szum (*noise*), przypadkowość, peryferyjność, błąd, usterka (*glitch*), stały się bazą do tworzenia nowych muzycznych pojęć, kluczowych dla pionierów współczesnej muzyki eksperymentalnej. Zmianom w sposobie myślenia o muzyce towarzyszyły nowe rozwiązania techniczne, oparte na najnowszych urządzeniach do rejestracji i emisji dźwięku. Budowano nowe instrumenty, szukano rozwiązań umożliwiających jak najpełniejsze odzwierciedlenie obrazu dźwiękowego rzeczywistości i wyrażenie emocji towarzyszących odczuwaniu świata. Tendencję tę zapoczątkował Luigi Russolo, włoski malarz i kompozytor, który w 1914 r. zbudował *intonarumori* – ogromny instrument generujący kontrolowane „harmoniczne wibracje i hałas”². W wydanej w 1913 r. traktacie *L'arte dei rumori (Sztuka hałasu)* Russolo podjął próbę ujęcia zjawiska *noise'u* w kategorii tworzenia muzyki³.

Początkowo soniczne eksperymenty futurystycznego kompozytora i malarza postrzegane były jako odchylenia i dziwactwa. Okazały się jednak uzasadnione – kilkadziesiąt lat później jego śladami podążyli tacy twórcy, jak: Milton Babbitt, Luciano Berio, Karlheinz Stockhausen czy Pierre Schaeffer. Europejskie ośrodki eksperymentalne stały się zalążkami nowych szkół kompozytorskich. Obok paryskiego *Groupe de Recherches Musicales*, prowadzonego przez Pierre'a Schaeffera, kołońskiego *Studio für elektronische Musik*, w którym królował Karlheinz Stockhausen, i dowodzonego przez Luciano Berio mediolańskiego

² <https://patches.zone/the-art-of-noise> [dostęp: 28.09.2018].

³ https://pl.wikipedia.org/wiki/Luigi_Russolo [dostęp: 28.09.2018].

Studio di Fonologia Musicale znalazło się warszawskie Studio Eksperymentalne Polskiego Radia. Założone z inicjatywy Józefa Patkowskiego, kojarzone jest przede wszystkim z osobą charyzmatycznego inżyniera, kompozytora i realizatora Eugeniusza Rudnika. Współtwórca dzieł Krzysztofa Pendereckiego (m.in. *Psalmus 161*, *Ubu Król*) i kompozytor muzyki do dzieł teatralnych, spektakli i słuchowisk określał swój sposób działania jako tworzenie „(...) muzyki podłych materii, muzyki zrobionej z dźwięków nieszlachetnych”⁴.



Fot. 5. Eugeniusz Rudnik, fot. Krzysztof Mariański,
[w:] Eugeniusz Rudnik, *Miniatury*, Requiem Records

⁴ <https://culture.pl/pl/artykul/studio-eksperymentalne-polskiego-radia-i-poczatki-muzyki-elektroakustycznej-w-polsce> [dostęp: 28.09.2018].

Modus operandi Rudnika polegał na odrzuceniu „bagażu doświadczeń klasycznie wykształconego kompozytora”⁵ i świeżym, nieskrępowanym podejściu do zastanej materii dźwiękowej. Pracował z użyciem (dosłownie) skrawków taśm wyjmowanych z kosza na śmieci, odpadków dźwiękowych, wszystkiego, co dla klasycznie wykształconego kompozytora było muzycznym śmietnikiem. „Ocalone” obiekty dźwiękowe poddawał obróbce i przez zestawienie nadawał im nowe, zaskakujące znaczenia, w pewien sposób je deszyfrował. Proces ten przypominał działanie Rejewskiego, Różyckiego i Zygalskiego, którzy zmuszeni byli bazować na skąpych danych wyjściowych i nie tylko tworzyć algorytmy częściowych rozwiązań, ale opracowywać zupełnie nowy sposób myślenia, wchodzący w obszar nieznanych dotąd kryptologicznych znaczeń. Czas pokazał, że stał się on fundamentem nowej ery technologicznej w historii ludzkości.

Przedstawione powyżej analogie stanowią zaledwie punkt wyjścia do dalszych rozważań. Ich aspekt muzykologiczny jest intrygujący, zwłaszcza że współcześni kompozytorzy i przedstawiciele różnych stylów coraz odważniej eksplorują mroczne tajemnice kryptologii. Jednym z najbardziej rozpoznawalnych zjawisk muzycznych związanych z kryptologicznymi tajemnicami jest *The Conet Project*. Sześciopłytkowy album, na który składa się kolekcja nagrań radiostacji numerycznych, zrealizowany został przez brytyjskie wydawnictwo Irdial Records⁶. Twórcy, tacy jak: Kronos Quartet, Boards of Canada, Johann Johannsson czy Cameron Crowe, wykorzystali brzmienie radiostacji numerycznych w swoich kompozycjach i dziełach filmowych. Trudno jest jednak znaleźć artystyczne ślady historii polskich kryptologów i opis ich udziału w walce z szyframi Enigmy. Tym bardziej trudno o rzetelną artystyczną metaforę procesu twórczego, jakim była syzyfowa, kryptologiczna praca Biura Szyfrów.

⁵ Ibidem.

⁶ https://en.wikipedia.org/wiki/The_Conet_Project [dostęp: 28.09.2018].

Naznaczona walką z czasem, obarczona ryzykiem porażki i ulotnością efektów, z pewnością nie kojarzyła się nikomu z pisaniem symfonii czy tworzeniem operowych librett.

Przypuszczać można jednak, że bez udziału artystycznej wyobraźni, niemal poetyckiej intuicji językowej, wrażliwości na dźwiękowe i graficzne frazy geniusz matematyczny Rejewskiego, Różyckiego i Zygalskiego mógł okazać się niewystarczającą bronią w walce z tak wymagającym przeciwnikiem. Dzięki zachowanym materiałom archiwalnym dowiedzieć się można, że bohater, który wprowadził mnie w świat zmagania z Enigmą – Henryk Zygaliski – nie tylko znakomicie słyszał muzykę i był melomanem, ale również grał na instrumentach – skrzypcach i fortepianie. Muzyka w jego życiu była obecna *non stop* – jako inspiracja, pasja i sposób spędzania wolnego czasu.

Konsekwencją kilkuletnich poszukiwań, spotkań z rodziną Henryka Zygalskiego i pracy badawczej nad zachowanymi dokumentami⁷ stał się projekt interdyscyplinarny, zatytułowany: „Czy świat potrwą jeszcze trzy kwadransy?...”. W ramach projektu powstały makietki książki fotograficznej inspirowanej powojennymi losami kryptologa oraz spektakl interdyscyplinarny.

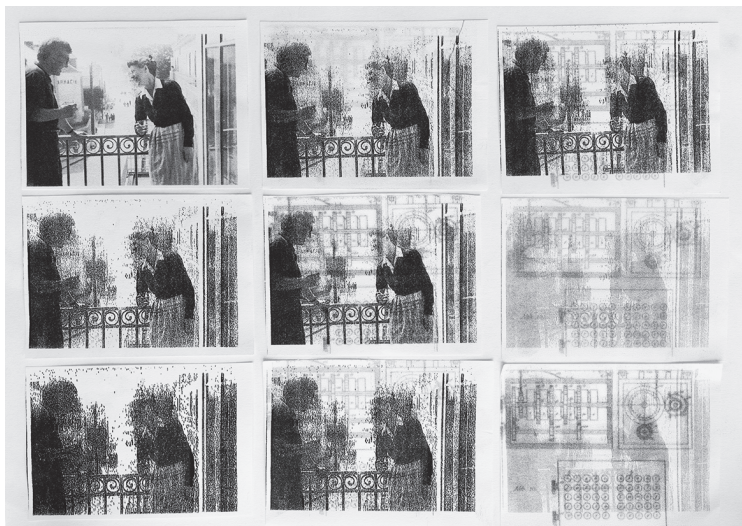
⁷ W okresie od 2013 do 2017 r. współpracowałem z państwem Marią i Gerhardem Bryschakami. Dzięki ich uprzejmości i życzliwości zyskałem dostęp do zasobów archiwum rodzinnego. Opracowałem i poddałem digitalizacji ponad 400 obiektów: listów, pocztówek, fotografii, notatek i dokumentów związanych z Henrykiem Zygalskim. Miałem wielokrotnie zaszczyt i przyjemność uczestniczyć w rozmowach, w trakcie których dowiadywałem się kolejnych szczegółów z życia Henryka Zygalskiego, przede wszystkim związanych z powojennym losem kryptologa.



Fot. 6a. Fragment scenografii spektaklu, C.K. Zamek, Poznań



Fot. 6b. „Czy świat potrwa jeszcze trzy kwadransy?...” – przygotowania do spektaklu, Poznań 2014. Na zdjęciu Andrzej Konieczny



Fot. 7a, 7b. Materiały archiwalne stanowiące bazę projektu
„Czy świat potrafi jeszcze trzy kwadransy?...” Archiwum autora



Fot. 8. Henryk Zygałski i Bertha Blofield, Quiberon, 1947.
Fotografia z archiwum Marii i Gerharda Bryschaków

Opis projektu

Projekt „Czy świat potrwa jeszcze trzy kwadransy?...” jest umiejscowiony na obrzeżach fotografii, muzyki i historii. Jego tematem jest postać Henryka Zygałskiego – wybitnego matematyka, kryptologa, który pracował nad złamaniem szyfrów Enigmy. Autor genialnej metody, nazwanej od jego nazwiska płachtami Zygałskiego, po wojnie zamieszkał w Anglii, gdzie podjął próbę zbudowania życia na nowo – pracował jako nauczyciel w college’u, znalazł swoją miłość i dom. Niestety, nie podzielił losu i kryptologicznej sławy swoich amerykańskich i brytyjskich kolegów; podobnie jak cała ekipa polskiego Biura Szyfrów – BS 4 – stał się postacią marginalną, niepotrzebną i pomijaną w historycznych rozważaniach dotyczących zmagania z Enigmą. Aby podjąć pracę jako zwykły nauczyciel, musiał powtórzyć w Anglii studia matematyczne.

Nikt – do tej pory – nie zainteresował się powojennym rozdziałem życia Henryka Zygałskiego, udokumentowanym skrupulatnie w listach, pocztówkach i fotografiach, które systematycznie (wraz ze skromnymi paczkami) trafiały z Anglii do jego rodziny, do kamienicy przy ul. Matejki w Poznaniu. Sposób opisu zdjęć robionych przez samego Henryka, pełen barwnych zwrotów i szczegółów język jego listów, częstotliwość korespondencji i jej nastrój świadczą o poczuciu humoru, dystansie i bezpretensjonalności ich autora. Wyczuwalna jest w nich również nuta żalu, tęsknoty, subtelna ironia człowieka, który zdaje sobie sprawę, że świat, dla którego poświęcił najlepsze lata i siły, obchodzi się z nim niesprawiedliwie.

Zbiór niepublikowanych fotografii archiwalnych i dokumentów udostępniony mi przez rodzinę matematyka stał się punktem wyjścia do zbudowania opowieści prowadzonej na granicy snu i jawy. Ścieżka intymnych wspomnień zapisanych w listach i opisach zdjęć tworzy abstrakcyjną mapę, tajemniczą, częściowo zatartą. W jej obszarze istnieje pole negocjacji prawdy historycznej, opartej na twardych, znaczących faktach, z ulotną prawdą ludzkiego życia i pamięci, pomijaną przez historyków. Przestrzeń ta jest zaszyfrowana, ukryta. Dostrzeżenie jej struktury wymaga szczególnie uważnego spojrzenia – dyskretnego i pytającego, które „nałoży” (jak płachty do deszyfrazu) ślady przeszłości na mapę dziejącą się i przeżywaną przez odbiorcę teraźniejszości.

Zestawienie zdjęć archiwalnych, notatek i listów Zygałskiego z oryginalnymi szyfrogramami, dokumentacją techniczną Enigmy, materiałami propagandowymi z czasów II wojny światowej i artykułami prasowymi tworzy warstwę wizualną projektu, uporządkowaną narracyjnie i zamkniętą w makietę książki. Jej dopełnieniem jest cykl „progresji”, których tłem i inspiracją są degradacja pamięci oraz tworzenie się i przenikanie wspomnień. W progresjach „nałożone” zostały fotografie rodzinne oraz fragmenty szkiców technicznych Enigmy.

Kontrapunktem całej sfery wizualnej jest projekcja z muzyką. Warstwa dźwiękowa składa się z zaszyfrowanych do postaci dźwiękowej fotografii, zapisanych i nadanych alfabetem Morse’a notatek Zygałskiego, nagranych atmosfer i pejzaży dźwiękowych z miejsc, w których

odbywały się zajęcia kursu kryptologicznego (podziemia Zamku w Poznaniu) oraz czytanych, poddanych degradacji brzmieniowej tekstów-komentarzy do fotografii. Wplecione w przestrzeń brzmieniową radiowych szumów i słów cytaty muzyczne (Bach i Chopin w wykonaniu Edwina Fischera i Władysława Szpilmana) oraz improwizacje instrumentalne podczas live-actu tworzą przestrzenny soundscape, ściśle związany z warstwą wizualną projektu. Treść projekcji stanowią sekwencje powojennych fotografii rodzinnych poddanych interwencji koszmaru „wspomnienia” Enigmy ukazującego się poprzez fragmenty schematów maszyny, detali i rysunków.

Cały zamysł projektu polega na „wejściu” w rolę kryptologa, który odszyfrowuje to, co ukryte w (pozornym) chaosie, i ukrywa w (pozornym) chaosie to, co widzialne, oczywiste, przyswajalne w akcie bezpośredniego odbioru. To ukrycie ma dodatkowy wymiar/cel – przez konieczność ponownego odszyfrowania skłania do rezygnacji z podejścia schematycznego, odbioru konwencjonalnego, pozbawionego refleksji. W ten sposób budzi wrażliwość „widzenia/słyszenia peryferyjnego” – zamiast podawać konkretne, ważne w konwencji historycznej „fakty”, uczy „zerować na okruchach” i wyławiać z nich sens, tropy, ślady i znaczenia. Odbiera podejściu historycznemu ton pewności, zastępując go pytaniem, świadomością ryzyka i uznaniem, że prawda ma wymiar subiektywny, intymny i daleki od hegemonii niepodważalnych faktów.

Muzyka konkretna – poprzez atmosferę poszczególnych miejsc, ich dźwiękową architekturę – opisuje to, co niewyraźne, zatrzymuje czas i brzmi w ciszy – wrażliwej, wyczekującej, pytającej, sprowadza doświadczenie do „bycia tutaj” i uświadamia zasadniczą samotność każdego człowieka, podstawę wymiaru egzystencjalnego. Wybór Bacha i Chopina jako dopełnienia tej skonkretyzowanej, zakotwiczonej w miejscach (Zamek w Poznaniu) architektury dźwiękowej jest gestem wskazującym na historyczny wymiar, horyzont, z którego wyłania się doświadczenie niemieckości (Bach) i polskości (Chopin), dodatkowo odczuwane z konkretnych perspektyw: przedwojennej, postromantycznej (Fischer) i powojennej, postapokaliptycznej (Szpilman). Te dwa spojrzenia określają granice pola znaczeniowego (wspólnego pola uczestnictwa) i delikatnie rzeźbią

światłem głębię kontekstu ku-przeszłości i ku-przyszłości, uprzestrzeniają w innym wymiarze historię Henryka i jego miłości – Berthy – oraz całą historię Enigmy.

Tytuł projektu: „Czy świat potrwa jeszcze trzy kwadranse?...” jest cytatem z notatek Henryka Zygałskiego. Warstwę muzyczną skomponował Andrzej Konieczny, a muzykę wykonał duet GRIT. Wszelkie materiały zostały użyte w projekcie za zgodą właścicieli.

Prezentacja publikacji oraz projekcja, live-act i spotkania z publicznością miały już miejsce w Poznaniu w grudniu 2014 r. Przestrzenią wystawy i spotkania była Scena Nowa w poznańskim Centrum Kultury „Zamek” – miejscu, w którym Henryk Zygałski, Marian Rejewski i Jerzy Różycki studiowali matematykę.

Realizacja projektu była koniecznym gestem ze strony człowieka, dla którego historia walki polskich kryptologów z Enigmą ma głębokie znaczenie. Kilka lat po realizacji spotkań, spektakli i opublikowaniu pilotażowej serii albumu mam świadomość ulotności podejmowanych wysiłków. Jednocześnie wiem, że ulotność ta jest obrazem walki z czasem, zmagania się z naturą przemijalnych zdarzeń, gestów i osób. Muzyczna metafora łącząca obszary kryptologii, historii i piękna prowadzi mnie dalej – w ogród pamięci, dzięki któremu krucha, chwilowa obecność człowieka i istnienie świata potrwają dłużej niż trzy kwadranse...

Dziękuję za pomoc i życzliwość: Państwu Marii i Gerhardowi Bryschakom, dr. Markowi Grajkowi oraz prof. dr. hab. Piotrowi Pogonowskiemu.

PATRYK PIŁASIEWICZ, 2018

O autorach

Jan Stanisław Ciechanowski – dr, Wydział „Artes Liberales” Uniwersytetu Warszawskiego.

Marek Grajek – dr, informatyk, dziennikarz i historyk. W pierwszym obszarze specjalizuje się w zastosowaniach kryptologii, w drugim – w badaniach historii służb specjalnych, a w szczególności historii kryptologii.

Kamil Kulesza – dr inż., Instytut Matematyczny PAN. Ukończył z wyróżnieniem University of South Africa w Pretorii i uzyskał dyplom w zakresie: informatyka, matematyka, fizyka teoretyczna. Doktoryzował się w Instytucie Podstawowych Problemów Techniki PAN, gdzie obronił z wyróżnieniem pracę z zakresu kryptografii teoretycznej. Po doktoracie przez kilka lat przebywał na University of Cambridge (Department of Applied Mathematics and Theoretical Physics oraz Isaac Newton Institute for Mathematical Sciences). Po powrocie do Polski założył Centrum Zastosowań Matematyki i Inżynierii Systemów działające w ramach Polskiej Akademii Nauk. Łączy naukę z biznesem – na działalność badawczą zarabia, rozwiązując problemy firm i instytucji przy użyciu matematycznego sposobu myślenia.

Krzysztof Osiński – dr, Instytut Pamięci Narodowej, Delegatura w Bydgoszczy.

Patryk Piłasiewicz – dr hab., Akademia Muzyczna im. Ignacego Paderewskiego w Poznaniu.

Elżbieta Szczuka – absolwentka LO w Wyszkowie, Politechniki Warszawskiej i studiów podyplomowych w Szkole Wyższej im. Pawła Włodkowica w Płocku, dziennikarka tygodnika lokalnego „Nowy Wyszkowiak”. Zgłębia i propaguje historię lokalną, opisuje sylwetki ludzi związanych z regionem.