Doprovodný příběh k Soutěži v luštění 2009
Pavel Vondruška

Všechny postavy v tomto doprovodném příběhu jsou smyšlené a jakákoliv podobnost se skutečnými osobami je čistě náhodná. Příběh je zcela vymyšlen a nemá reálný podklad. Jediná opravdová reálie je šifrátor ŠD-2. Informace k tomuto šifrátoru můžete najít v e-zinu Crypto-World 78/2009 v článku Vojtěcha Brtníka: Rekonstrukce šifrovacího stroje ŠD-2.

1. JAK SE STAL VÁCLAV PROKOPEC VĚZNĚM

Ve dnech 13. až 25. ledna 1958 se u Státního soudu v Plzni konal proces s Václavem Prokopcem, zaměstnancem Zvláštní správy Ministerstva vnitra, ing. Ondřejem Sýkorou, jeho přímým nadřízeným a Karlem Weberem, synem statkáře, který byl v roce 1945 odsunut do Německa, ale v roce 1957 překročil zpět ilegálně hranice do své vlasti.

Velké procesy padesátých let již skončily, ale prokurátor v podobném duchu hřímal na celý sál:

„...ukázali se být sprostými zločinci, kteří se neštítí pomáhat připravovatelům nové světové války, dodávat jim špionážní zprávy a vyzývat je k válce proti našemu lidu… Chtěli oloupit náš lid o všechny svobody, kterých dobyl, chtěli jej dostat pod vládu statkářů a kapitalistů, chtěli jej zbavit státní samostatnosti.“

Na základě důkazů, které byly u soudu předloženy, byli uznáni všichni tři vinnými. Zaměstnanec Václav Prokopec byl odsouzen za trestný čin velezrady a vyzvědačství k 22 letům odnětí svobody, Karel Weber za stejný trestný čin na 20 let odnětí svobody. Zaměstnanec ing. Ondřej Sýkora byl odsouzen na 3 roky odnětí svobody za nedbalost a neplnění služebních povinností.

Václav Prokopec, který byl převezen k výkonu trestu do Mírova, uléhal na dřevěný tvrdý kavalec ke spánku. Takovýchto nocí strávil ve vězení celkem 8000. Na rozdíl od spoluodsouzených se na něj totiž nevztahovaly amnestie ani rehabilitační procesy, které proběhly v roce 1964-67. Bylo na něj vždy hleděno jako na skutečného špióna, který zradil svůj lid a stát a pro svůj čin nenašel pochopení a odpuštění.

Co vlastně provedl? Jak bylo u soudu prokázáno, vyzradil cizí (americké) rozvědce informace o organizování šifrové služby v Československu, o způsobu a provádění zácviku šifrérů a strukturu a jména osob, kteří na nově zřízené Zvláštní správě Ministerstva vnitra byli zaměstnáni. Tyto informace předával svému známému z dětství, agentu cizí rozvědky Karlu Weberovi. Společně s nimi byl ještě odsouzen také jeho nadřízený, který byl odsouzen za to, že neplnil dostatečně své povinnosti a svým nezodpovědným přístupem umožnil, aby se s těmito informacemi seznámil v rozsahu, který mu nenáležel a navíc i přes některé náznaky na jeho chování neupozornil.

Často, když takto večer uléhal, přemýšlel, proč se v rozsudku neobjevilo také jeho největší provinění, totiž to, že předal podrobné plány sovětského šifrovacího stroje CM-1, který nesl v ČR kódové označení ŠD-2. Říkal si, že asi jeho nadřízený kryptolog ing. Ondřej Sýkora se bál, aby mu nebylo ještě více přitíženo a vše, co se týkalo tohoto stroje, raději popřel a tvářil se, že k úniku nedošlo a nemohlo dojít.

Pravda byla však ještě o něco složitější. Vedení Zvláštní správy tušilo, že plány pravděpodobně opravdu unikly. Báli se však sovětské straně toto přiznat, a proto to raději nejen neoznámili, ale během vyšetřování o tom pomlčeli. Přesto provedli určitá opatření. I když kryptografický rozbor stroje neprokázal žádné slabiny, rozhodli se jej v ČR nenasadit. Zdůvodněno to bylo možnými problémy s domácí výrobou, zejména časovou zdlouhavostí, náročností s přepracováním technické a výrobní dokumentace, utajení vlastní výroby, vyškolení techniků a organizováním celého procesu. Možnost sériové výroby těchto šifrovacích strojů v SSSR bylo také nakonec odmítnuto s tím, že nabízená cena za jeden kus šifrátoru je pro náš stát příliš velká. ŠD-2 tak nakonec nebyl v Československu nikdy dále vyvíjen, či nasazen do praxe.

2. JAK SE STAL VÁCLAV PROKOPEC KRYPTOLOGEM

Když večer Václav Prokopec uléhal na svůj vězeňský kavalec, promítal si den po dni svůj život a přemýšlel nad tím, co se vlastně stalo.

Václav vzpomínal:

Bylo mi již 21 let, když jsem ostříhaný dohola 1. října 1952 narukoval k ženistům do starých Fučíkových kasáren v Táboře. Měl jsem absolvovanou měšťanku v Nečtinách a pokračovací školu v Manětíně a vyučen jsem byl jako strojní zámečník. Zde jsem absolvoval tzv. přijímač, složil vojenskou přísahu a začal poddůstojnickou školu. Jako syn partyzána jsem byl považován za spolehlivého a tak když byli hledáni vhodní adepti pro šifranty, byl jsem pozván na PVS, kde jsme dostali k vyplnění speciální testy. Vypadalo to, že zjišťují naši inteligenci. Vůbec jsme netušili, proč nám dávají k řešení tyto rébusy a ptají se nás, zda rádi luštíme křížovky, zda umíme šachy apod.

Pplk. ing. Ondřej Sýkora, který nám na PVS tyto testy rozdal a vedl s námi pohovor, pak vybral mne a ještě jednoho mého kolegu a oznámil nám, že budeme vycvičeni jako pracovníci vojenské šifrové služby. Proč ne? Zdálo se mi to zajímavé a navíc nám sliboval i velmi slušné zacházení a po vojně i práci a zajímavé finanční ohodnocení.

Viz příloha č.1 „Úlohy z PVS“

A tak jsem byl v březnu 1953 vyslán do Administrativního kurzu C v Tloskově u Neveklova, což byl krycí název čtyřměsíčního kurzu šifrantů - důstojníků v záloze. Tehdejším náčelníkem šifrové služby GŠ byl právě ing. pplk. Ondřej Sýkora, kterého jsem již znal z testů. Jeho oddělení čítalo asi 20 osob, bylo to důstojníci - učitelé. Já jsem byl zařazen do první čety, kde nám velel npor. ing. Prachař. V kurzu nás bylo na 300 absolventů ŠDZ (!) ode všech druhů vojsk. Seznámili nás s historií a rozvojem kryptologie (kryptografie), seznámili nás s jednouchými šifrovacími

systémy a jejich luštěním, naučili nás šifrovat ručními prostředky za použití převodových tabulek a písmenkových heslových materiálů, ale také lehce zapamatovatelných klíčů, tvořit signální či hovorové tabulky, naučili nás používat německý diskový šifrovací stroj Enigma, který se stále v naší armádě používal a nakonec jako zvláštní tajemství nám ukázali i diskový šifrovací stroj ANNA, etablovaný na dálnopisných stanicích svazků. Museli jsme se naučit užívat i polní spojovací prostředky včetně sovětské přenosné radiostanice A7b a německého dálnopisu Hell, který byl získaný ve velkém množství jako válečná kořist. Během kurzu byly pořádány tři jednodenní soutěže v luštění jednoduchých úloh (jednoduchá záměna, transpozice apod.). Soutěže se pořádaly vždy v pátek. Tři nejlepší měli za odměnu slíben opušťák na následující sobotu a neděli. Jaké bylo překvapení velitele mé čety a velitele kurzu, když všechny tři soutěže jsem vyhrál já! Kolegové mne dokonce podezírali, že znám výsledky, tak rychle jsem některé úlohy vyřešil…

Viz příloha č.2 „Administrativní kurz C v Tloskově“
Viz příloha č.3 „Administrativní kurz C v Tloskově 2“
Viz příloha č.4 „Administrativní kurz C v Tloskově 3“
Viz příloha č.5 „Administrativní kurz C v Tloskově 4“

Po absolvování kurzu jsem se stal armádním šifrérem. Jako strojař jsem neměl žádné problémy s obsluhou (někdy poněkud uživatelsky nevhodných) šifrovacích a spojovacích zařízení a i jinak jsem byl svými nadřízenými považován za spolehlivého, pilného a chytrého poddůstojníka.

V roce 1955 vznikla Zvláštní správa Ministerstva vnitra, která měla mimo jiné i gesci na vývoj a testování kryptografických prostředků. Vedoucím oddělení, které mělo na starosti vývoj a testování nových kryptografických prostředků, se stal můj „starý známý“ ing. pplk. Ondřej Sýkora. Když hledal vhodné zaměstnance - své podřízené, vzpomněl si na mne, protože si pamatoval, jak jsem v kurzu opakovaně vítězil v soutěžích v luštění jednoduchých šifer. Vyžádal si od mých současných nadřízených na mne reference, a protože jsem byl vylíčen jako oddaný, spolehlivý a schopný šifrér, rozhodl se, že mne zaměstná ve svém oddělení. Po vyřízení příslušných formalit jsem přešel z armády na Ministerstvo vnitra a stal se technickým pracovníkem v oddělení vývoje kryptografických zařízení Zvláštní správy.

Zde jsem zpočátku (během zkušební doby) nedělal nic zajímavého a byl jsem trochu zklamán. Měl jsem však mnohem více volného času než u armády a byl jsem v Praze. Toulal jsem se po tomto nádherném městě a bylo mi dobře. Cítil jsem se mladý, silný a měl život před sebou. Rád jsem si večer poseděl ve vinárně a postupně se ukázalo, že i když jsem měl velmi slušný příjem, stačil jsem jej v tom velkoměstě snadno rozházet. Nemít problémy s penězi, byl jsem dokonale šťastný.

V roce 1957, tedy v době, kdy jsem byl u Zvláštní správy již zaměstnán 2 roky, byla vládou ČSR požádána sovětská strana o pomoc při výrobě šifrátoru. Sovětská strana vyhověla a počátkem listopadu 1957 dodala do Československa k testování dva kusy stroje, které měly představovat vzor pro výrobu šifrátoru s označením ŠD-2. Jednalo se o modifikaci ruského šifrátoru CM-1.

Již jsem měl rok po zkušební době a mjr. Sýkora mne zařadil do týmu, který měl za úkol provést kryptograficko-technický rozbor zařízení. Všichni jsme podepsali

speciální závazek mlčenlivosti, protože nejen, že toto zařízení bylo označeno jako přísně tajné, ale byl zde navíc zájem sovětské strany chránit toto tajemství specifickým způsobem, protože zařízení bylo v Sovětském svazu masově používáno.

3. JAK SE STAL VÁCLAV PROKOPEC ZRÁDCEM

Václav opět po těžkém dnu ve vězení uléhal znaven na svůj kavalec. Před usnutím vzpomínal na dny před svým zatčením. Jak se to vlastně stalo, že přišel o tak zajímavou a dobře placenou práci, že zradil sebe, důvěru a práci svých kolegů - soudruhů a svoji vlast.

Václav byl již druhý rok v Praze. Skončila mu zkušební lhůta a začal pracovat jako plnohodnotný člen kryptografického oddělení. Pro jeho schopnosti kombinovat a luštit jej ing. pplk. Ondřej Sýkora „půjčoval“ majoru Hádkovi z kryptoanalytického oddělení. Václav sice přesně nevěděl, co zde dělají. Pouze předpokládal, že luští zachycené dálnopisy a radiodepeše, ale co skutečně umí luštit a co ne, to nevěděl. Cítil se ve společnosti kryptoanalytiků důležitý. Nevadilo mu, že mu byla dávána jen pomocná práce, kterou nikdo z odborníků nechtěl dělat. Konkrétně mu vždy přinesli svazek dopisů, které byly zasílány na podezřelé vytipované adresy (většinou v cizině). On měl za úkol je přečíst, a pokud se mu zdály nějaké divné, kostrbatě gramaticky napsané apod., tak provést jejich analýzu. Ta spočívala v tom, že vypsal do připravených tabulek např. všechna prvá písmena vět v daném dopise, pak druhá atd., potom obdobně vypisoval poslední, předposlední písmena. Skutečně se stalo, že písmena dávala smysl a někdo (Václav ovšem nevěděl o tom kdo a komu) takto předával utajený text. Kolegové mu jednou prozradili, že mimo tento opravdu jednoduchý systém se používá i mnohem důmyslnější, kdy vypsaná písmena na dohodnutém místě vět tvoří souřadnice šifrovací tabulky.

Viz příloha č.6 „Zvláštní správa - analýza dopisů“

A tak ubíhal den za dnem. Večer pak Václav chodil do své oblíbené hospůdky na pivo, večeři a pivo a pivo, ale někdy si chtěl zahrát na někoho důležitějšího a to pak šel po městě a hledal nějakou lepší vinárnu. Není divu, že vždy desátého, kdy dostávali výplatu, již netrpělivě čekal u okénka soudružky Hromové, která jim peníze vyplácela.

Byl teplý květnový večer roku 1957. Václav se procházel po Kampě a pak zašel do vinárny u Dvou grošů. Objednal si dvě deci bílého vína a rozhlížel se znuděně po místnosti. V tom uviděl u protějšího stolu svého spolužáka z měšťanky v Nečtinách Karla Webera. Bylo mu to trochu divné, myslel si, že byl odsunut tak, jako ostatní Němci z vesnice Stvolny, kde Karlův otec měl velký statek. Byl však rád, že vidí někoho známého, a protože tam Karel seděl sám, vstal a přisedl k němu. Strávili spolu zajímavý večer, povídali si a vzpomínali na školu a své spolužáky a spolužačky. Řeč přišla i na spolužačku Evu, která se Václavovi tolik líbila. Václav nechtěl kazit ten hezký večer, ale pak si našel odvahu a zeptal se, jak je to možné, že zde Karel je. Byl přece odsunut. Karel se zasmál a řekl: „Neboj, jsem zde legálně. Ale nechce se mi o tom mluvit.“ Jenže vypili další sklenku, tedy přesněji další džbánek a Václav zase stočil řeč na jeho návrat.

„Ty ses vrátil, Karle?“ Karel se na něj podíval a pak po chvilce řekl: „No a proč ne?“ „Myslel jsem, že to nejde“, pokračoval Václav. „Ale jde“ řekl na to Karel a pak mu vyprávěl svoji smyšlenou legendu. Spočívala v tom, že jej v Německu vyhledala naše československá rozvědka a chtěla na něm nějakou službu. Když to udělal, bylo mu dovoleno za odměnu vrátit se zpět do vlasti. Skutečnost však byla úplně jiná. V Německu se jemu ani otci příliš nedařilo. Nakonec se Karel Weber nechal naverbovat americkou rozvědnou službou a působil jako spojka – agent chodec. Již několikráte úspěšně přešel hranice do Československa a pak zpět do Německa. Teď byl v Praze a měl zde za úkol kontaktovat dr.Hromadu a vyzvednout od něj nějaký balíček, který měl co nejdříve přivézt zpět. Měl se s ním sejít právě dnes v této vinárně. Jenže z nějakého důvodu dr. Hromada nepřišel. Právě když chtěl odejít, přisedl k němu jeho bývalý spolužák Václav. Dost dobře se nemohl nechat zapřít a odejít, a tak teď s ním popíjel to mizerné a předražené víno a musel dělat, jak je rád, že jej potkal a poslouchat ty banální vzpomínky a příhody z měšťanky. Vymyslel si kvůli němu i docela slušnou legendu. Věděl, že se zde lidé bojí tajné služby a rozvědky a určitě se jej Václav už na nic více asi nebude vyptávat. Je dost možné, že s ním dokonce nebude chtít mít nic společného. Jenže najednou se přihodilo něco, co skutečně nečekal. Václav se k němu naklonil, podal mu ruku a řekl: „Vítej, tak to jsme skoro kolegové! Já jsem totiž zaměstnán u šifrové služby na Ministerstvu vnitra“. „To není možné!“ reagoval Karel. Pak mu to hned došlo, proboha to je náhoda! Potkat kamaráda, který mu důvěřuje a který má přístup k šifrám. To je prostě náhoda, která se agentovi jen tak nepřihodí. Pokud se mu podaří Václava přimět ke spolupráci, dostanou se jeho chlebodárci k těm nejcennějším tajemstvím a on se z obyčejného agenta – chodce, který neustále riskuje, že bude chycen, stane důležitým a oceňovaným vyzvědačem, kterého budou krýt a po splnění úkolu jej bude očekávat slušná odměna a poklidný život někde v Alpách, kde si s otcem zakoupí malý vysněný statek a zde v klidu stráví zbytek života …

Ten večer se mu podařilo Václava parádně opít. Odvedl jej domů. Ráno pak na něj před domem čekal a rychle mu vysvětlil, že by nebylo dobře, aby se o setkání svým kolegům zmiňoval nebo to dokonce hlásil. Karlovi nadřízení také nechtějí, aby se opíjel po večerech. Navíc, jak by zase Václav vysvětlil, že se schází ve vinárně s odsunutým Němcem, synem statkáře. A říci „pravdu“, že mu jeho dávný spolužák Karel prozradil, že pracuje pro rozvědku, také říci nesmí. Jak by to asi vypadalo, že Karel každému na potkání o tom vypráví. A tak si navzájem slíbili, že o setkání pomlčí.

Karel pak v následujících dnech Václava sledoval, a když zjistil, že chodí pravidelně do blízké hospody a v pátek a sobotu do nějaké vinárničky, nebylo pro něj těžké se s ním zase jakoby náhodou sejít. Setkání a vzájemných flámů přibývalo. Karel začal za Václava platit. Ten zpočátku nechtěl, ale když už mu došly peníze, rád pozvání od kamaráda zase přijal. „Vy teda na té rozvědce jste dobře placeni“ komentoval Václav, když jej Karel zase pozval na flám a když Karel zdůraznil, že to samozřejmě zaplatí.

Na jednom z flámů dokonce Karel hostil Václava i s jeho nadřízeným ing. Ondřejem Sýkorou. Ten flám se o pár měsíců později stal inženýru Sýkorovi osudným. Jeho nadřízení mu vyčítali, že se více nezajímal, s kým vlastně jeho podřízený tráví večery a navíc na něm ulpělo i vážné podezření, že snad věděl, kdo skutečně Karel je a že se nějak sám zapletl.

Vše vypadalo idylicky, ale jen do okamžiku, kdy Karel zcela chladně zaútočil na Václava. „Václave, dost té komedie. Nejsem člen československé rozvědky, ale naopak rozvědky americké!“

Když se Václav vzpamatoval z počátečního šoku, tak jej Karel začal zpracovávat dále. „Opovaž se někomu něco říc! Copak by ti někdo věřil, že jsi trávil tři měsíce po vinárnách se spolužákem, o kterém jsi věděl, že byl odsunut do Německa a nepojal jsi podezření, že zde asi není legálně? Jak bys svým nadřízeným vysvětlil, že jsi nehlásil takový podezřelý styk? A vůbec, chceš si přece užívat. Vol rozumem a místo nepříjemností a možná vězení, ber peníze. Jsem schopen ti zajistit spoustu peněz, a pokud budeš chtít si je užít v bezpečí, zajistím ti i odchod za hranice. Cena je malá. Řekneš mi vše, co o té vaší šifrové službě víš.“

Václav Prokopec váhal, ale nakonec podlehl. V následujících týdnech postupně vyzradil některé informace o službě, kde byl zaměstnán, jak je organizována, jména kolegů, názvy akcí, o kterých věděl, o prováděné kontrole dopisů, které se zúčastnil a také, jaké šifrátory se v armádě používají.

Shodou okolností zrovna v té době dorazila ze Sovětského svazu dodávka dvou šifrátorů CM-1, které dostaly na Zvláštní správě kódové označení ŠD-2 (šifrový dálnopis verze 2). Do týmu, který dostal za úkol provést jeho kryptologicko-technický rozbor, zařadil ing.Ondřej Sýkora i svého oblíbeného podřízeného Václava Prokopce.

Václav velmi brzy pochopil obrovský význam, jaký mají plány tohoto šifrátoru, který byl v Sovětském svazu používán. Kontaktoval Karla a o šifrátoru mu řekl. Slíbil, že plány překreslí a vše, co mu bude o zařízení známo, předá. Současně si však vymínil, že to bude ta poslední věc, co pro něj udělá. Žádá za to pak ihned zařízení přechodu do Německa a slušnou sumičku peněz. Karel vše do centrály ohlásil, počkal na pokyny a za týden se s Václavem opět sešel.

Viz příloha č.7 „Zpráva centrále“

Oznámil mu, že je vše zařízeno. „Přines plány a budeme se bavit, kdy a kde přejdeš.“ Václav Karla nečekaně překvapil. Plány již měl obkresleny a dokonce je přinesl na schůzku s sebou. Beze slova je teď vyndal a zabalené v Rudém Právu je dal Karlovi. Po chvilce mlčení překvapenému Karlovi pak řekl: „Jsme tedy domluveni, zajisti mi odchod a příští pátek mi řekni, kdy a kde!“ S tím se také ten večer rozloučili.

Jenže pak se to stalo. Tím, že byl Václav zařazen do týmu, kde se požadovala absolutní mlčenlivost, protože sovětská strana přikládala předaným podkladům velký význam, bylo rozhodnuto o speciální prověrce všech účastníků projektu. Všichni byli v tajnosti prolustrováni. Kontrarozvědka zjišťovala, s kým se stýkají, kdo se kolem nich pohybuje a jaký vedou život. Tím se samozřejmě dostala na stopu Karlovi Weberovi.

Pak již šlo vše ráz na ráz. Na schůzku do vinárny U dvou hrochů, kde se měli oba spiklenci sejít a domluvit konkrétní datum útěku z republiky, již Karel nepřišel. Místo něj však přišli na místo setkání dva příslušníci státní tajné bezpečnosti a Václava Prokopce zatkli.

Zatčen byl druhý den i jeho nadřízený, protože dle vyšetřovatelů nebylo možné, aby netušil, že se děje něco nepatřičného. Navíc bylo zjištěno, že se sám jedné ze schůzek dokonce zúčastnil a přitom nic podezřelého nenahlásil. Nezodpovědně dokonce zařadil Václava Prokopce na jeden z nejdůležitějších úkolů odboru. Mělo se však všeobecně za to, že Václav Prokopec byl zatčen dříve, než se pořádně seznámil s plány šifrátoru a že nebylo možné, aby je stačil obkreslit a předat cestou Karla Webera cizí rozvědce. Ing. Ondřej Sýkora sice tušil, že to mohl stihnout, neboť mu umožnil, aby se s plány seznámil ještě dříve, než celý projekt oficiálně startoval, ale ve vlastním zájmu mlčel a ani u soudu se o tom on nebo Karel Weber nezmínil.

Možná i díky tomu, že předané informace byly vyhodnoceny jako sice přísně tajné, ale přece jen takového rázu, že nemohly zásadním způsobem poškodit šifrovou službu a bezpečnost státu a také možná proto, že již končila krutá padesátá léta, nebyl v následujícím soudním procesu Václav Prokopec odsouzen k trestu smrti, dokonce ani na doživotí.

4. JAK BYL PROLOMEN ŠIFROVÝ TEXT ZAŠIFROVANÝ POMOCÍ CM-1

Šifrátor CM-1 byl na svoji dobu velmi dobrým kryptografickým zařízením. Z šifrového textu nešlo ani při znalosti dokonalého popisu šifrátoru jej prolomit. Ovšem dokonalý popis stroje umožnil americké rozvědné službě postavit jeho funkční repliku. Pak již stačilo úkolovat agenty, aby získali nastavení šifrátoru na příslušný měsíc. Pokud se jim jej podařilo získat, pak již snadno rozvědka dešifrovala všechny zachycené texty, které byly pod tímto klíčem zaslány. Šifrátory tohoto typu se v Sovětském svazu používaly dlouhých třicet let od roku 1956 do roku 1986. Během této doby se podařilo americké rozvědce klíče získat relativně často. Zejména díky seržantu Kulikovovi, který je po celých 15 let pravidelně dodával, ale to je již zcela jiný příběh.

Viz příloha č.8 „Dešifrace ŠD-2 / CM-1“