PROJEKT VENONA I SOVJETSKI AGENTI U INSTITUCIJAMA SAD-a TIJEKOM DRUGOG SVJETSKOG RATA

Robert Derenčin *

UDK: 327.84(73:47+57)
327.54(73:47+57)
355.40(73:47+57)
355.404.5(73:47+57)
Stručni rad
Primljeno: 23. IX. 2016.
Prihvaćeno: 3. V. 2018.

SAŽETAK

Projekt Venona počeo je 1943. kao pokušaj službe za dekriptiranje Kopnene vojske SAD-a (U.S. Army Signal Intelligence Service) da analizom prometa šifriranih poruka između Moskve i sovjetskih diplomatskih predstavništva dođe do nekih saznanja o djelovanju sovjetskih obavještajnih službi u SAD-u. Zahvaljujući jednoj katastrofalnoj sovjetskoj pogrešci dio tih šifriranih poruka je (djelomično) dekriptiran. Zajedničkim radom FBI-a i CIA-je, te srodnih britanskih službi, identificirani su neki od najvažnijih sovjetskih agenata u SAD-u, Britaniji i drugim zemljama. Ipak, činjenica je da je Sovjetski Savez imao svoje agente duboko infiltrirane u društva i institucije zapadnih zemalja, osobito u Velikoj Britaniji i SAD-u, i da su ti agenti pomogli Sovjetskom Savezu da zauzme puno bolje početne pozicije na početku hladnog rata.

Članak pojašnjava kako su ti agenti bili unovačeni i način na koji su Sovjeti šifrirali svoje najtajnije poruke, ali i kako je i najsigurniji sistem nesiguran ako se ne koristi potpuno pravilno.

Ključne riječi: projekt Venona, sovjetska obavještajna služba, NKVD, GRU, dekriptiranje, HUMINT, Drugi svjetski rat.

UVOD: NASTANAK I RAZVOJ PROJEKTA VENONA

Služba za dekriptiranje Kopnene vojske SAD-a (U.S. Army Signal Intelligence Service), prethodnica Nacionalne sigurnosne agencije (National Security Agency – NSA), 1. veljače 1943. otpočela je s projektom proučavanja sovjetskih šifriranih diplomatskih poruka. Kasnije je taj projekt dobio tajni naziv Venona (Benson 2001).

* Robert Derenčin (robert.derencin1@pu.ht.hr) umirovljeni je časnik iz Pule.

Sovjetska diplomatska i ostala službena predstavništva u SAD-a imala su pravo primati i slati šifrirane poruke potpuno legalno, putem lokalnih poštanskih ureda. Amerikanci su te brzojave prikupljali, te su analizom prometa (broj i dužina poruka, učestalost, vrijeme slanja itd.) pokušavali doći do barem nekih saznanja. Znajući da su poruke šifrirane jednokratnom šifrom, Amerikancima se činilo da je dekriptiranje (neovlašteno dešifriranje) tih poruka nemoguće.

Ipak, zahvaljujući jednoj katastrofalnoj pogrešci Sovjeta, Amerikanci su s vremenom uspjeli dekriptirati jedan dio sovjetskih šifriranih poruka, iako je taj proces bio težak i spor. Tek u prosincu 1946. dekripter Meredith Gardner je uspio djelomično dekriptirati dvije poruke koje su poslane u Moskvu 1944. Prva se ticala američkih predsjedničkih izbora, a druga je sadržavala imena vodećih znanstvenika uključenih u projekt Manhattan[1]. Poruku je 2. prosinca 1944. u Moskvu poslao Leonid Kvasnikov (tajno ime Anton), koji je u rezidenturi (obavještajnoj postaji) NKVD-a[2] u New Yorku bio zadužen za špijunažu nuklearne i ostale napredne tehnologije (Benson 2001; Venona #1699). Malo-pomalo dekriptirane su poruke koje su pokazale da unutar američkih institucija neki pojedinci SSSR-u dostavljaju najtajnije podatke. Sovjetski agenti i izvori bili su posvuda, u ministarstvima u Washingtonu, u Kongresu i političkim strankama, medijima, obrambenoj industriji, Uredu strateških službi[3], čak i u Bijeloj kući.

FBI je upoznat s projektom Venona 1947., a CIA (službeno) 1953., i bez suradnje te dvije službe daljnja analiza i eksploatacija dekriptiranih poruka ne bi bila moguća. Britanci su se projektu Venona pridružili 1948. godine. Zajedničkim naporima svih tih službi dekriptiran je dio poruka koje su izmjenjivale rezidenture NKVD-a i GRU-a[4] u inozemstvu (SAD, Meksiko, Južna Amerika, Europa i Australija) i njihova središta u Moskvi. Iako se radilo o porukama koje su uglavnom poslane do kraja 1945. (najkasnije 1948.), NSA je prekinula projekt Venona tek 1. listopada 1980. (Benson 2001).

NAČIN SASTAVLJANJA I ŠIFRIRANJA PORUKA

Da bi se poruka mogla šifrirati, potrebno ju je pripremiti, dovesti u odgovarajući format. To je prvi korak u procesu šifriranja, ali i prvi korak u procesu dekriptiranja, što znači da bez poznavanja načina pripremanja poruke poruku nije moguće dekriptirati. Sistem šifriranja sovjetskih veleposlanstava (i obavještajnih službi) bazirao se na uporabi blokova za jednokratnu uporabu. Šifriranje poruke odvija se na sljedeći način. Prvo, svako slovo otvorene poruke (prema prethodno utvrđenom dogovoru)

[1] Istraživački projekt američke vlade s ciljem izrade atomske bombe.

[2] NKVD (akronim od ruskoga *Narodnyj komissariat vnutrennih del*: Narodni komesarijat unutrašnjih poslova), tijelo sovjetske vlade (1934–1946) zaduženo za poslove državne sigurnosti koje je rukovodilo policijskim i obavještajnim službama, uključujući i obavještajne aktivnosti u inozemstvu.

[3] *Office of Strategic Services* (OSS), osnovan 1942. (CIA je sljednica Ureda strateških službi).

[4] GRU (akronim od ruskoga *Glavnoye razvedyvatel'noye upravleniye*: Glavna obavještajna uprava), vojna obavještajna služba.

ima svoj brojčani ekvivalent. Najjednostavniji sistem je kad slova, prema abecednom redu, zamjenjuju brojevi, pa je A = 01, B = 02, sve do Z = 26. Ipak, da bi se poruka barem donekle skratila, najučestalija slova jednog jezika imaju jednobrojčane ekvivalente, ostala slova imaju dvobrojčane ekvivalente, postoje ekvivalenti za određene znakove interpunkcije, te posebne oznake koje označavaju prijelaz sa slova na brojeve i obratno, prijelaz na uporabu posebne knjige kodova itd. Brojevi u otvorenoj poruci nemaju svoj ekvivalent, već se prilikom pripremanja poruke za konačno šifriranje pišu otvoreno, zbog izbjegavanja pogreške kod dešifriranja ponavljaju se triput, na primjer broj 125 u otvorenoj poruci se prije konačnog šifriranja piše 111 222 555 te se kao takav šifrira.

Svi podaci o navedenim ekvivalentima nalaze se u tablici poznatoj i po imenu „šahovska ploča" (Rijmenants 2016b). Što se tiče najučestalijih slova u ruskom jeziku, radi se o prvih sedam slova ruske riječi *snegopad* (padanje snijega), te su ta slova (s, n, e, g, o, p, a) imala jednobrojčane ekvivalente, a ostala slova (ruske) abecede i oznake imale su dvobrojčane ekvivalente (Kahn 1961; 1979: 381). Knjiga kodova uporabljuje se da bi se poruka dodatno skratila, slučajne skupine od po tri broja zamjenjuju pojedine riječi ili izraze. Nakon što je cjelokupna otvorena poruka pretvorena brojeve, ti se brojevi grupiraju u skupine od po pet brojeva. Zatim slijedi šifriranje na način da se brojevi koji zamjenjuju otvorenu poruku zbrajaju ili oduzimaju od brojeva koji se nalaze u posebnim blokovima za jednokratnu uporabu (engl. *one-time pad*). U tim blokovima nalaze se listovi s otisnutim skupinama od po pet brojeva. Radi se o potpuno slučajnom nizu brojeva koji predstavljaju ključ šifre. Za svaku poruku koristi se samo jedan list koji se nakon šifriranja odmah mora uništiti (Rijmenants 2016b).

Sovjeti su prilikom šifriranja zbrajali brojeve otvorene poruke s brojevima iz blokova za jednokratnu uporabu, rezultat je bila šifrirana poruka koja se slala na odredište (Benson 2001). Na odredištu je postupak bio obrnut, brojevi od kojih se sastojala primljena šifrirana poruka oduzimali su se od brojeva iz blokova za jednokratnu uporabu te su se dobivali brojevi koji su predstavljali otvorenu poruku (koji se su pomoću spomenute šahovske ploče i knjige kodova pretvarali u stvarnu poruku).

Zbrajanje i oduzimanje obavlja se bez prebacivanja „desetica", pa je na primjer 5 + 7 = 2 (12, ali se „desetice" zanemaruju), a 2 – 7 = 5 (jer je 12 – 7 = 5) (Rijmenants 2016a). Na primjer, recimo da je neka otvorena poruka (u ovom slučaju sastavljena samo od slova) pretvorena u brojeve, te smo dobili sljedeće tri skupine brojeva: 79226 34749 91690. Te tri skupine moramo šifrirati jednokratnom šifrom koja se sastoji od slučajnog niza brojeva, na primjer: 47757 10126 36660. Sovjeti su kod šifriranja koristili zbrajanje, kod dešifriranja oduzimanje, pa bi u ovom primjeru šifriranje obavljeno na sljedeći način:

Otvorena poruka: 79226 34749 91690

Ključ šifre: + 47757 10126 36660

———————

Šifrirana poruka 16973 44865 27250

Šifrirana poruka glasi „16973 44865 27250" i kao takva šalje se na odredište. Na odredištu se odvija obrnuti postupak, oduzimanje brojeva iz šifrirane poruke s brojevima ključa (šifre):

Šifrirana poruka 16973 44865 27250

Ključ šifre: – 47757 10126 36660

———————

Otvorena poruka: 79226 34749 91690

Zatim se ti brojevi pomoću tablice i knjige kodova (ako je uporabljena) pretvore u stvarnu poruku.

DEKRIPTIRANJE PORUKA ŠIFRIRANIH ŠIFROM ZA JEDNOKRATNU UPORABU

Ako se prilikom šifriranja poštuju sva pravila sigurnosti, poruke šifriranje šifrom za jednokratnu uporabu neprobojne su. Čak i uz pomoć „sirove snage" (neograničeno vrijeme i neograničen broj računala) suprotna strana nikad neće moći otkriti stvarni sadržaj otvorene poruke. Jedino što je (u teoriji) moguće je da se uz primjenu „sirove snage" dobije neograničen broj verzija otvorene poruke. Na primjer, rezultat bi mogao biti da se u otvorenoj poruci mogu nalaziti riječi „danas", „sutra" ili „nikad".

Najvažnija pravila prilikom šifriranja šifrom za jednokratnu uporabu jesu da ključ šifre (niz slučajnih brojeva) mora bit dug barem koliko je duga i poruka, te da se ključ sastoji od doista slučajnog niza brojeva. Nizovi se nalaze otisnuti na stranicama blokova koje imaju samo pošiljatelj i primatelj. Svaki od njih ima posebne blokove, za odlazne i za polazne poruke. Potrebno je imati posebne blokove za dolazne i za odlazne poruke zbog toga što (u teoriji, ali zapravo vrlo moguće) postoji mogućnost da obje strane istovremeno jedna drugoj pošalju poruku šifriranu pomoću istog ključa (iste stranice), što dovodi do situacije da te dvije poruke može dekriptirati neovlaštena strana (Rijmenants 2016b).

Jedan se ključ (stranica bloka) smije uporabiti samo za šifriranje jedne poruke, pa je stoga potrebno ograničiti tiskanje blokova (odnosno stranica) na samo dva primjerka, ali su to pravilo Sovjeti u jednom trenutku prekršili. Naime, zbog pritiska koji je nastao približavanjem Nijemaca Moskvi, oni su izradili oko 35 tisuća duplih stranica, a kad su to otkrili nisu ih uništili, već su ih poslali na geografski udaljena područja misleći da se uporaba iste stranice (ključa) za dvije poruke neće opaziti.

Šifrirane poruke izvana djeluju potpuno nerazumljivo (to im je i zadaća, naravno) pa se čini nemoguće otkriti koje su poruke šifrirane istim ključem, iako je u stvarnosti odgovor na to pitanje vrlo jednostavan, barem u slučaju poruka šifriranih jednokratnim šiframa. Naime, da bi prijemna strana znala koji ključ treba uporabiti kako bi se poruka dešifrirala, polazna strana je o tome treba informirati, a to se radi tako da se (uobičajeno) na početku poruke stavi podatak o uporabljenom ključu – taj se podatak zove indikaor poruke.

Blokovi za jednokratnu uporabu sastoje se od stranica koje sadržavaju skupine od po pet nasumičnih brojeva. Na vrhu svake stranice nalazi se njezin redni broj, npr. 001, 002 itd., koji služi za jednostavnije sastavljanje bloka, te u slučaju jednostavnijeg izvješćivanja ako se određena stranica (ili više njih) mora smjesta uništiti. Međutim, taj se redni broj nikad ne smije koristiti kao indikator poruke, jer bi jednostavnom analizom suprotna strana znala koliko je poruka poslano i njihov redoslijed. Kao indikator poruke koristi se prva skupina od pet brojeva otisnuta na stranici koja se koristi za šifriranje te poruke, i ta se skupina šalje onako kako je otisnuta na toj stranici, bez ikakve promjene. Šifriranje počinje s drugom skupinom nasumičnih brojeva otisnutima na toj stranici (Rijmenants 2016a).

Ipak, jedan je odjel američke službe za dekriptiranje, koristeći tadašnja mehanička računala, obradio početke i krajeve oko pet tisuća sovjetskih poruka, te je u listopadu 1943. došao do prvih saznanja da neke jednokratne šifre (stranice) nisu korištene samo jednom. U studenom 1944. otkriveno je da Sovjeti određene skupine brojeva šalju u porukama nešifrirane, što je pomoglo otkrivanju poruka koje su šifrirane istim (jednokratnim) ključem (Johnson 1995). Nikad nisu pronađene više od dvije poruke šifrirane istim ključem, pa je mogućnost dekriptiranja bila samo teorijska, ali su Amerikanci barem znali da ta mogućnost postoji i nakon toga nisu odustajali. Nije bilo važno odakle su te poruke poslane, kad i za koga. Ako su poruka iz Moskve za New York i poruka iz Canberre za Moskvu imale istu prvu skupinu, na primjer „73018", znalo se da su te dvije poruke šifrirane istim ključem i da ih je moguće dekriptirati.

Moskva je 25. travnja 1944. poslala svim rezidenturama šifriranu poruku o novom načinu sastavljanja indikatora poruke. Od 1. svibnja 1944. indikator poruke sastavljao se tako da je na početak poruke trebalo staviti prvu skupinu (brojeva) koja se nalazila na stranici koja je korištena za šifriranje te poruke, šifriranje poruke počinje drugom (sljedećom) skupinom. Nakon što je cijela poruka šifrirana, trebalo je na njezin kraj staviti skupinu koja je slijedila odmah nakon posljednje (za šifriranje) iskorištene skupine. Obje skupine, i prva koja se nalazila na uporabljenoj stranici i prva neiskorištena, u poruku su stavljane bez ikakve promjene. Ako je šifriranje završilo posljednjom skupinom na stranici, na kraj poruke stavljala se prva skupina sa sljedeće stranice, naravno i ona bez ikakve promjene (*Moscow*…). Za dekriptere ova izmjena nije bila previše važna jer poruke ionako (u većini slučajeva) nisu bile iste dužine, pa i kad su dvije poruke bile šifrirane istim ključem samo je prvi indikator bio isti, dok je drugi (u pravilu) bio različit.

Nakon što je Igor Guzenko, koji je do 5. rujna 1945. radio kao šifrant GRU-a u sovjetskom veleposlanstvu u Ottawi (Kanada), prebjegao (zatražio azil u Kanadi, što je nakon prvobitnih problema i dobio), jedan je dekripter iz projekta Venona poslan da ga ispita. Guzenko mu je detaljno opisao proces šifriranja (Johnson 1995). Vjerojatno bi Amerikanci s vremenom i sami došli do tih saznanja, ali na ovaj način doznali su više i brže. Doznali su način pripremanja otvorene poruke za šifriranje, te koje su poruke šifrirane istim jednokratnim ključem.

Nakon toga slijedio je najvažniji dio dekriptiranja – trebalo je odrediti riječ (engl. *crib*) koja se nalazi u jednoj od tih dviju (otvorenih) poruka. Uz pretpostavku te riječi,

i pretpostavku na kojem se mjestu nalazi u jednoj od poruka, mogao se odrediti dio ključa na tom mjestu te poruke. Zatim je taj ključ primijenjen za dešifriranje dijela druge poruke, na istom mjestu na kojem se otkriveni (još uvijek pretpostavljeni) ključ nalazio u prvoj poruci. Ako bi to dešifriranje otkrilo barem djelomični suvisao tekst (možda tek dio neke veće riječi) u drugoj poruci, dekripter je znao da je na dobrom putu. Ako je u drugoj poruci otkrio dio neke veće riječi, mogao je odrediti nešto veći (duži) dio ključa, to bi primijenio vrativši se na prvu poruku, otkrivajući veći dio otvorenog teksta te prve poruke istovremeno otkrivajući još veći dio ključa, zatim bi se vratio na drugu poruku sve dok obje poruke ne bi (u savršenom slučaju) bile potpuno dekriptirane. Zapravo je potpuno dekriptirana poruka mogla biti samo ona kraća, jer je usporedbom dviju poruka šifriranih istim ključem mogao biti određen samo onaj dio ključa koji se „protezao" kraćom porukom. Naravno, riječ je o dugotrajnom i iscrpljujućem poslu, o sistemu pokušaja i pogrešaka, gdje dekripter mora biti spreman na razočarenja, koristeći samo papir, olovku i svoju imaginaciju (Rijmenants 2016b).

Otkrivanje moguće riječi u otvorenoj poruci najvažnije je za dekriptiranje, a do tih riječi Amerikanci su dolazili i pomoću iskaza nekih bivših sovjetskih agenata, npr. Elizabeth Bentley, dugogodišnje sovjetske agentice koja se u studenom 1945. predala FBI-u i odala imena pojedinaca zaposlenih u državnim institucijama koji su SSSR-u (preko nje) dostavljali dokumente. Nekoliko godina nakon toga dekriptirane sovjetske poruke potvrdile su njezine tvrdnje, u njima se nalazilo i njezino tajno ime, kao i imena sovjetskih obavještajaca i agenata koje je odala.

U svezi tajnih imena treba imati na umu činjenicu da je postojalo više vrsta tajnih imena te da su se ona ponekad (s vremena na vrijeme) mijenjala. Glavni ilegalni rezident NKVD-a u Sjedinjenim Državama tijekom Drugog svjetskog rata bio je Ishak Abdulovič Ahmerov. Radilo se o ilegalcu, što znači da je u SAD-u boravio pod lažnim identitetom (a ne kao sovjetski građanin). Njegovo tajno ime u šifriranim porukama koje su izmjenjivale rezidentura i Moskva bilo je Mer, a od 1944. Albert. Imena pod kojima je živio bila su od 1937. do 1945. William Greinke, Michael Green, Michael Adamec itd., a njegova „ulična" imena, pod kojima su ga znali njegovi kontakti, bila su Michael i Bill. Elizabeth Bentley znala ga je jedino kao Billa (Benson 2001). Barem u ovom slučaju ulična su imena bila ista kao imena aliasa (Bill je skraćeno od William). Usto, jedno od imena u porukama bilo je dio njegovog pravog prezimena – Mer. Iako su sovjetski obavještajci vjerovali u to da su njihove šifre neprobojne, u svojim su porukama (kad su to mogli) osobe navodili pod njihovim tajnim imenima, što je bila dobra odluka. U slučaju Elizabeth Bentley to je značilo da je ona mogla imenovati Ahmerova kao Billa i nikako više, a to se ime nije nalazilo u sovjetskim porukama i nije moglo pomoći Amerikancima u dekriptiranju.

Navođenje agenata i izvora u porukama pod njihovim tajnim imenima skraćivalo je poruke i povećalo je sigurnost ne samo od mogućeg dekriptiranja poruke, već vjerojatno ni sami sovjetski obavještajci nisu (barem ne uvijek) znali prava imena agenata i izvora. Tajna imena nisu imali samo agenti i izvori, nego i druge osobe, pa je predsjednik SAD-a Roosevelt imao tajno ime Kapetan (u originalu: Kapitan). Tajna imena koristila su se i za neke institucije (Ministarstvo vanjskih poslova SAD-a bilo je

Banka) i gradove (San Francisco bio je Babilon), a projekt Manhattan bio je Enormoz, itd. Ponekad su sami dekripteri otkrivali što koje tajno ime znači, a identifikacija agenata i izvora obavljala se analizom i istraživanjem „na terenu". U početku je to radio FBI, zatim su se pridružile britanske službe i od 1953. i CIA (Benson 2001).

Za mnoga tajna imena u dekriptiranim porukama nikad nije ustanovljeno kome pripadaju, što pokazuje da je potrebno koristiti tajna imena čak i kad se vjeruje u sigurnost šifri. To važno pravilo treba potpuno primjenjivati, a osobe za koje još nije određeno tajno ime u porukama se ne smiju spominjati, već se sve u vezi njih javlja na drugi način. Na primjer, u jednoj od dekriptiranih poruka navedeno je da se Liberalova (tajno ime Juliusa Rosenberga) supruga zove Ethel, što je bilo njezino pravo ime. FBI je identificirao Juliusa i Ethel Rosenberg 1950. (Benson 2001). Tu poruku je 27. studenog 1944. iz New Yorka u Moskvu poslao već spomenuti Leonid Kvasnikov (tajno ime Anton). S obzirom na to o kako se važnim agentima radilo, nevjerojatno je koliko se podataka nalazilo u poruci. Usto što je navedeno da je pravo ime Liberalove supruge Ethel, navedeno je i da Ethel nosi suprugovo prezime, da ima 29 godina, u braku je pet godina, ima završenu srednju školu, članica je Komunističke parije SAD-a od 1938. Da ne bi bilo zabune, zatim je slijedio podatak da Ethel zna za djelovanje svog supruga, te za uloge još dvojice agenata, ali da zbog slabog zdravlja ne sudjeluje u tom djelovanju (Venona #1657). Ova poruka pravi je primjer da se neki podaci ne smiju navoditi u porukama koliko god se smatralo da je sistem šifriranja siguran.

Usto što su poruke sadržavale tajna imena (osoba, ustanova i mjesta), postojala je i knjiga kodova koja je sadržavala riječi i fraze predstavljene skupinom brojeva (Benson 2001). To je dodatno skraćivalo poruke i povećavalo njihovu sigurnost. U Drugom svjetskom ratu Sovjeti su koristili dvije verzije knjige kodova: 1942., 1943. i početkom 1944. koristila se jedna verzija, a zatim je 1944. u uporabu ušla nova verzija knjige kodova (Benson 2001). Prvu verziju knjige kodova (zapravo njezinu fotokopiju) pronašli su Amerikanci na samom kraju rata u Njemačkoj, te su je uspjeli skloniti prije nego što je područje u kojem su bili preuzela sovjetska vojska. Inače su Nijemci originalnu knjigu kodova pronašli 22. lipnja 1941. u sovjetskom konzulatu u Petsamu (Finska), knjiga je bila djelomično spaljena jer su je pripadnici NKVD-a u konzulatu pokušali uništiti. Drugi američki tim je na drugom mjestu u Njemačkoj također pronašao srodan kriptološki materijal.

Prva verzija knjige kodova bila je kompliciranija od druge verzije. Iako su Amerikanci vidjeli samo prvu verziju knjige kodova, većina dekriptiranih poruka bila je iz godina kad su Sovjeti koristili drugu verziju knjige kodova. Objašnjenje za to je jednostavno. Sovjeti su „duple" jednokratne blokove za šifriranje vrlo malo koristili 1942., nešto više 1943., da bi 1944. i 1945. koristili (relativno) puno „duplih" jednokratnih blokova, pa je bilo više uspješno dekriptiranih poruka. Veći dio sovjetskih poruka poslanih 1944. i 1945. dekriptirano je između 1947. i 1952. Poruke poslane 1942. i 1943. dekriptirane su kasnije, počevši od 1953/1954. Tek nakon toga se povezalo knjigu kodova pronađenu u Njemačkoj s tim ranijim porukama!Potkraj 1944. je u Stockholmu održan sastanak Amerikanaca s predstavnicima finskog SIGINT-a (*Signals Intelligence*). Na tom su sastanku Finci Amerikancima predali

jednu njemačku Enigmu (stroj za šifriranje) s pripadajućim rotorima, te su opisali svoje uspjehe u svezi sovjetskih komunikacija (Benson 2001). Izgleda da su na tom sastanku Finci predali Amerikancima i sovjetsku knjigu kodova (ili sličan materijal povezan sa sovjetskim šiframa). Tadašnji američki ministar vanjskih poslova Edward Stettinius to je doznao, te je u prosincu 1944. uspio uvjeriti predsjednika Roosevelta da ovaj zapovijedi Uredu strateških službi (OSS) da se materijal preda Sovjetima kao znak dobre volje (Haynes i Klehr 2013).

SOVJETSKI AGENTI U INSTITUCIJAMA SAD-a

Kad je 1951. istražno povjerenstvo američkog Senata zatražilo od generala Douglasa MacArthura da objasni kako je napad Sjeverne Koreje na Južnu Koreju mogao iznenaditi Amerikance, MacArthur je odgovorio kako on ne vidi mogućnost da se predvidi takav napad, osim u slučaju da postoji netko u najvišim krugovima neprijatelja koji je spreman dostaviti takav podatak (Orlov 1963). S ovom izjavom neki se ne bi složili, jer uz klasičan obavještajni rad (HUMINT) postoji i elektroničko izviđanje (SIGINT), snimanje iz zraka, analiza otvorenih izvora itd. Međutim, MacArthurova izjava u potpunosti se slagala s „filozofijom" sovjetskih obavještajnih službi prema kojoj je jedini „pravi" obavještajni rad bio onaj na terenu, u inozemstvu. Podatke dobivene na taj način (izvješća agenata i ukradeni dokumenti) Sovjetski Savez je i cijenio najviše.

NKVD je svoje djelovanje u inozemstvu u potpunosti bazirao na tajnim izvorima i prikrivenim agentima. GRU je proučavao inozemne vojne i znanstvene časopise, vojne priručnike itd., ali je barem 80% svog truda koncentrirao na izgradnju i održavanje mreža svojih agenata u inozemstvu i na dobavljanju (krađi) tajnih dokumenata (Orlov 1963). Da bi sovjetske službe mogle djelovati u inozemstvu, trebali su im pojedinci koji su u svojim zemljama bili spremni raditi kao agenti ili izvori. Radilo se o članovima ili simpatizerima lokalnih komunističkih partija koji su u Sovjetskom Savezu prije svega vidjeli simbol, a ne stranu državu. Oni su radili iz uvjerenja, ne za novac, svoj su rad vidjeli prvenstveno kao pomoć prvoj zemlji socijalizma i svjetskoj revoluciji. Takvih je pojedinaca, voljnih da postanu sovjetski agenti, bilo i u Sjedinjenim Državama. Neki od njih bili su izvori, neki su bili kuriri, neki su vodili svoje mreže agenata, a neki su se popeli nevjerojatno visoko unutar pojedinih institucija SAD-a, gdje su imali pristup najvažnijim podacima i gdje su mogli utjecati na donošenje odluka. Ponekad kod agenata koji rade iz uvjerenja (a ne zbog novca, ucjene i slično) dolazi do razdoblja krize, kad se pitaju postupaju li ispravno, vjerojatno je to bio slučaj i sa sovjetskim agentima u Sjedinjenim Državama.

Kad je 23. kolovoza 1939. u Moskvi potpisan njemačko-sovjetski pakt o nenapadanju i kad je Sovjetski Savez zauzeo baltičke države i istočnu Poljsku, vjerojatno su ti agenti vjerovali (ili su željeli vjerovati) kako se radi o „mudroj politici druga Staljina" i da je rat u Europi rat buržoazija u kojem proletarijat ne treba sudjelovati, iako ti agenti s proletarijatom uglavnom nisu imali nikakve veze. Situacija se preokrenula 22. lipnja 1941. kad je Njemačka napala SSSR. Nakon toga sovjetski agenti nisu imali

nikakve sumnje u ispravnost svojeg djelovanja, bili su uvjereni da upravo SSSR najviše pridonosi borbi protiv fašizma i nacizma, te da mu u tome treba pomoći. Pred kraj rata, kad se već znalo tko će u ratu pobijediti, sovjetski su agenti nastojali osigurati ono mjesto i utjecaj u poslijeratnom svijetu za koje su mislili da SSSR zaslužuje.

Na Jaltskoj konferenciji 1945. u američkoj se delegaciji nalazio barem jedan sovjetski agent.

U poruci koju je 30. ožujka 1945. sovjetski rezident u Washingtonu poslao u Moskvu piše da je agent „Ales" nakon konferencije odletio u Moskvu, gdje se navodno (kako je Ales rekao sovjetskom obavještajcu s kojim je razgovarao nakon povratka u SAD) susreo sa zamjenikom ministra vanjskih poslova SSSR-a Andrejem Višinskim (bio je i na Jaltskoj konferenciji), koji mu je prenio izjavu zahvalnosti GRU-a (Venona #1822). Logično je da je GRU zamolio Višinskog da prenese njihovu zahvalnost Alesu, jer razgovor dvojice diplomata, vjerojatno tijekom nekog neformalnog druženja ili prijema, sam po sebi nije toliko sumnjiv.

Poruka je kasnije dekriptirana, te je zaključeno da je Ales vjerojatno Alger Hiss, visoki službenik u Ministarstvu vanjskih poslova SAD-a (Johnson 1995). Tom je zaključku „pomogla" i činjenica da je nekoliko bivših sovjetskih agenata izjavilo da je Hiss godinama bio sovjetski agent. U toj poruci od 30. ožujka 1945. Gromov (tajno ime Vadim, rezident NKVD-a u Washingtonu) izvješćuje Moskvu o Alesu koji je neprekidno od 1935. bio agent druge sovjetske službe (vjerojatno GRU-a). Ales (i skupina nižih agenata koje je vodio) je dostavljao podatke vojne prirode toj drugoj službi, koja je navodno bila malo zainteresirana za podatke iz „Banke" (tajno ime za američko Ministarstvo vanjskih poslova), pa je te podatke Ales dostavljao neredovito. Obavještajac koji je obavio razgovor s Alesom je (vjerojatno) bio Ahmerov (u poruci se navodi kao „A"), glavni ilegalni rezident NKVD-a u SAD-u, i vjerojatno se ispitivala mogućnost da Ales prijeđe iz GRU-a u NKVD (Benson 2001).

Rezident GRU-a u New Yorku koji je djelovao pod krinkom sovjetskog vicekonzula u New Yorku, čije je tajno ime bilo Moliere, poslao je 28. rujna 1943. poruku u Moskvu. Poruka, koja je kasnije djelomično dekriptirana, uz ostalo je sadržavala podatak da je „susjed" (tj. pripadnik NKVD-a ili, možda, mornaričkog GRU-a) spomenuo osobu „iz Ministarstva vanjskih poslova po imenu Hiss" (Venona #1579). U to vrijeme su u Ministarstvu radila samo dva Hissa, Alger i njegov brat Donald. Ako se radilo o Algeru Hissu, i ako je on doista bio sovjetski agent (sam Hiss je sve do svoje smrti to poricao), zašto se u poruci navelo njegovo pravo prezime umjesto tajnog imena? Odgovor je jednostavan. Ako je Ales doista bio Hiss, onda je on cijelo vrijeme bio agent GRU-a, te je vođen iz rezidenture GRU-a u Washingtonu. Ostale službe, NKVD i mornarički GRU, nisu ni smjele znati za njegov rad. Vjerojatno za to nije znao ni rezident GRU-a u New Yorku, te je zato poslao poruku da je „susjed" spomenuo Hissa iz Ministarstva vanjskih poslova.

Međutim, ako je Hiss doista bio sovjetski agent, zašto nije bio agent NKVD-a, kome bi kao službenik Ministarstva vanjskih poslova bio puno korisniji, već je bio agent GRU-a? Odgovor je jednostavan: u obavještajnom poslu postoji nešto što bi se moglo nazvati pravom prvenstva. U Hissovom slučaju to znači da ga je unovačio

pripadnik GRU-a, te je mogao prijeći u NKVD samo ako bi GRU na to pristao, pa je vjerojatno razgovor u ožujku 1945. i održan s namjerom da Hiss postane agent NKVD-a. Alger Hiss nije mogao biti od (pre)velike koristi GRU-u, ali to ne znači da nije mogao biti koristan SSSR-u. Naime, unutar Ministarstva vanjskih poslova Hiss je vjerojatno djelovao kao tzv. agent utjecaja.

Agenti utjecaja (engl. *influence agents*) bili su komunistički simpatizeri zaposleni u institucijama (političkim, državnim, kulturnim itd.) svojih zemalja, koji su sabotirali i/ili usmjeravali djelovanje tih institucija. Agente je najlakše otkriti praćenjem kretanja (i kontakata) poznatih stranih obavještajaca (ili onih za koje se pretpostavlja to da jesu) u pojedinoj zemlji, te praćenjem tijeka novca (za isplatu agenata, podmirivanje troškova itd.). Agenti utjecaja djelovali su samostalno, po svom nahođenju, te su održavali vrlo malo osobnih kontakata sa sovjetskim obavještajcima, a njihove plaće i materijalne troškove ionako su podmirivale institucije u kojima su radili, iste one institucije koje su ti agenti lukavo i pažljivo sabotirali. Sabotaža se sastojala od toga da je pojedini agent utjecao na to da se na ključna mjesta postavljaju komunistički simpatizeri (a da ovi u pravilu nisu znali tko im je i zašto pomogao) ili oni za koje su bili uvjereni da su nesposobni. Zatim, svojim utjecajem ti su agenti određivali smjer djelovanja svojih institucija, promicanje nevažnih ili kontraproduktivnih projekata, a zanemarivanje onih doista važnih itd. Agente utjecaja vrlo je teško otkriti, te im je praktički nemoguće dokazati ikakvu krivnju, osim za pogrešan ili loš rad, a za tako nešto se, barem u uređenim državama, ne ide u zatvor (Geschwind 1963).

Postojao je i agent (tajno ime „19") koji je barem u jednoj prigodi imao pristup predsjedniku Rooseveltu. Glavni ilegalni rezident NKVD-a Ahmerov je preko „legalne" rezidenture NKVD-a u New Yorku 29. svibnja 1943. u Moskvu poslao poruku potpisanu svojim tajnim imenom Mer. U poruci navodi kako ga je „19" izvijestio da su „Kapetan" (u originalu: Kapitan) i „Nerast" (ili Vepar, u originalu: Kaban) tijekom razgovora u Sjedinjenim Državama pozvali „19" da se pridruži njima i „Zamjeniku" (u originalu: Zamestitel), te da su razgovarali o otvaranju drugog bojišta u Europi (Venona #812). Radilo se o sastanku američkog i britanskog vodstva u Washingtonu, u razdoblju između 12. i 25. svibnja 1943., a delegacije su vodili osobno Roosevelt i Churchill. Tajno ime predsjednika Roosevelta bilo je Kapetan, britanskog premijera Winstona Churchilla Nerast, a Zamjenik je vjerojatno tadašnji potpredsjednik SAD-a Henry Wallace.

Postoje razne teorije tko su zapravo bili „Zamjenik" i agent „19". Prema nekima, agent „19" bio je Harry Hopkins, najbliži suradnik predsjednika Roosevelta tijekom Drugog svjetskog rata, kojem je Roosevelt potpuno vjerovao te ga ovlastio da vodi program vojne i ekonomske pomoći Velikoj Britaniji i Sovjetskom Savezu. Hopkins je bio izrazito prosovjetski orijentiran i to nije krio. Međutim, dva detalja iz djelomično dekriptirane poruke isključuju Hopkinsa bilo kao „Zamjenika", bilo kao agenta „19". Naime, u poruci se navodi da je „Zamjenik" pobornik otvaranja drugog bojišta, ali kako „19" misli da Roosevelt ne izvješćuje „Zamjenika" o bitnim vojnim odlukama. To što je Zamjenik bio pobornik otvaranja drugog bojišta (misli se na invaziju na Francusku) moglo bi upućivati na to da je „Zamjenik" Hopkins, jer je otvaranje drugog bojišta (i to što prije) želio i SSSR, ali podatak da Roosevelt nije izvješćivao

„Zamjenika" o bitnim vojnim odlukama isključuje Hopkinsa kao „Zamjenika" jer pred njim Roosevelt nije imao tajni. Zbog toga se može skoro sa sigurnošću zaključiti da je „Zamjenik" bio potpredsjednik SAD-a Wallace.

To što „19" misli da Roosevelt ne izvješćuje „Zamjenika" o bitnim vojnim odlukama isključuje Hopkinsa i kao agenta „19", jer da je „19" bio Hopkins onda ne bi „mislio", već bi „znao" – jer je znao sve. Harry Hopkins (preminuo je u siječnju 1946.) vjerojatno je bio „korisna budala" (engl. *useful idiot*). Tako se nazivaju pojedinci koji propagiraju određenu stranu (npr. ideologiju ili državu) ne shvaćajući njezinu pravu prirodu. Zaista bi bilo glupo od Sovjeta da su pokušali unovačiti čovjeka koji im je i inače vjerovao i pomagao.

Najvjerojatnije je agent „19" bio Laurence Duggan, od 1930. do 1944. zaposlen u Ministarstvu vanjskih poslova SAD-a, nakon čega odlazi na rad u UNRRA-u[5], a za kojeg je dokazano da ga je 1935. unovačio NKVD. To bi objasnilo i razlog zašto je pozvan da se pridruži Rooseveltu, Churchillu i Wallaceu. Naime, Duggan i Wallace bili su prijatelji, te je Wallace od Duggana često tražio savjete u svezi vanjskopolitičkih pitanja. Tijekom svoje karijere sovjetskog agenta Duggan je održavao kontakte s nekoliko operativaca NKVD-a, ali najviše (kad je ovaj bio u SAD-u) s Ahmerovim, koji je i potpisao navedenu dekriptiranu poruku (Haynes i Klehr 2013). Izgleda da je Ahmerov jedini znao kako pristupiti Dugganu, koji je potkraj 1930-ih, nakon što je doznao za čistke u SSSR-u, imao period osobne krize.

U svakom slučaju, Sovjeti su pratili Duggana i nakon što je u srpnju 1944. otišao u UNRRA-u. Duggan se pojavljuje u nekoliko dekriptiranih brzojava, ali ne kao „19", već kao Frenk, Šervud i Knjaz (imena se navode kao u originalu). Sovjeti nisu bili zadovoljni Dugganovim odlaskom iz Ministarstva, ali su računali na njegovo prijateljstvo s Wallaceom i na mogućnost da jednog dana zbog tog prijateljstva dođe na neku visoku poziciju (Venona #1114; 1251; 1613). Uostalom, dali su mu i tajno ime Knjaz. Da je u trenutku Rooseveltove smrti Wallace bio potpredsjednik SAD-a (a radilo se o samo 82 dana „razlike"), Wallace bi postao predsjednik SAD-a, te bi skoro sigurno imenovao Duggana ministrom vanjskih poslova. Vjerojatno je Duggan otišao iz Ministarstva kako bi izbjegao tu mogućnost jer ga kao ministra vanjskih poslova Sovjeti ne bi pustili na miru, i dalje bi morao biti sovjetski agent, a izgleda da on to više nije želio. Duggan je 20. prosinca 1948., nekoliko dana nakon što su ga u njegovom domu ispitali agenti FBI-a, smrtno stradao namjernim ili slučajnim padom kroz prozor svog ureda na šesnaestom katu jedne zgrade u New Yorku. Možda se doista radilo o samoubojstvu. Pritisak je postao prejak, s jedne strane Amerikanci i vjerojatno odlazak u zatvor, s druge strane SSSR i bijeg u Moskvu. U trenutku smrti imao je 43 godine, suprugu i četvero djece.

Razne su sudbine razotkrivenih agenata. Oni s jakim (prijateljskim ili obiteljskim) vezama umirove se ili se premjeste na neko mjesto na kojem ne mogu nanositi štetu,

[5] UNRRA (akronim od engl. *United Nations Relief and Rehabilitation Administration*), Uprava UN-a za pomoć i obnovu ratom opustošenih zemalja, osnovana 1943. sporazumom 44 države s ciljem pružanja pomoći civilima na područjima oslobođenima od okupacije sila Osovine. Prestala djelovati 1949.

na način da izvana sve djeluje normalno, možda čak i kao promaknuće. Nijednoj državi nije lako priznati da je netko u njezinom vrhu radio za drugu stranu, pa se to, ako je ikako moguće, zataška. Oni manje važni i bez osobnih veza završe drugačije. Julius i Ethel Rosenberg osuđeni su na smrtnu kaznu i pogubljeni na električnoj stolici, iako je, kako se vidi iz dekriptirane poruke, Ethel Rosenberg bila sporedna u toj priči. Alger Hiss je za davanje lažne izjave (krivokletstvo) pod prisegom osuđen na dvije istovremene petogodišnje kazne zatvora, u zatvoru je proveo tri godine i osam mjeseci, ostao je živjeti u Sjedinjenim Državama i do kraja života ponavljao da nije bio sovjetski agent. Činjenica da nije otišao u Moskvu, gdje bi ga sigurno dočekale počasti i (za sovjetske prilike) ugodan život, na prvi pogled bi mogla dokazivati da doista nije bio sovjetski agent, ali stvari nisu bile tako jednostavne.

Ne može se reći da je SSSR loše primio svoje zaslužne agente. Svi su oni dobili (za sovjetske uvjete) lijepe stanove u Moskvi i dače (ladanjske kuće) u okolici Moskve. Međutim, nije bilo lako pripadniku, npr., britanske više srednje klase prilagoditi se životu u Moskvi u jednoiposobnom stanu s kuhinjom i kupatilom, kojim je Sovjetski Savez pokazao zahvalnost svom dugogodišnjem borcu. Oni su do dolaska u Moskvu živjeli puno luksuznije, a dača u okolici Moskve imala je malo sličnosti s ladanjskim kućama u Britaniji, u kojima su nekad provodili vikende. Zbog toga su u SSSR odlazili agenti kojima je to bio jedini način da izbjegnu suđenje i zatvor, dok su ostali radije ostajali na Zapadu. Naravno, nisu svi sovjetski agenti na Zapadu pripadali srednjim i višim slojevima društva, ali neki jesu, i baš su ti agenti SSSR-u bili najdragocjeniji.

Kako je moguće da takve osobe iz ideoloških razloga rade za zemlju (sistem) koja negira njihov način života i da izdaju svoju zemlju u kojoj, na kraju krajeva, sasvim dobro žive? Odgovor je jednostavan. Većina Britanaca i Amerikanaca, koji su iz ideoloških razloga bili sovjetski agenti, unovačeni su 1930-ih, kad je u svijetu vladala velika ekonomska kriza. Iako su živjeli privilegiranim načinom života i školovali se na najprestižnijim sveučilištima, ti su (tada još potencijalni) sovjetski agenti dobro vidjeli kako u njihovim zemljama žive najsiromašniji, nezaposleni i gladni. Jedino što je trebalo bilo je uočiti potencijalne kandidate, pametno im pristupiti i unovačiti ih, a SSSR je izgleda imao jako dobre osobe za taj posao.

Jedan od njih bio je sovjetski obavještajac Arnold Deutsch, izuzetno obrazovan, s odličnim uspjehom doktorirao je kemiju na Sveučilištu u Beču, a studirao je i psihologiju i filozofiju, koji je 1934. došao u Veliku Britaniju s ciljem novačenja agenata. U tome je bio jako uspješan, prema sovjetskim dokumentima tijekom boravka u Britaniji Deutsch je unovačio dvadeset agenata (Andrew 2009: 173). Prema Deutschu, a njegovu je strategiju Moskva odobrila, radikalne (vrlo) ambiciozne studente vodećih sveučilišta trebalo je kultivirati (obrađivati) prije nego što počnu napredovati. Deutsch je bio svjestan da postoji mogućnost da se netko jednog dana sjeti da je taj-i-taj na sveučilištu bio komunist, ali je vjerovao se to može objasniti kao prolazan mladenački hir, osobito ako se radi o potomku buržoazije (Andrew 2009: 170).

Elitna sveučilišta pripremaju mlade ljude da jednog dana preuzmu najodgovornije pozicije u svojim zemljama. Barem je tako bilo do Drugog svjetskog rata, kasnije se taj elitizam donekle izgubio, ali ne sasvim. U Velikoj Britaniji takva su sveučilišta Oxford

i Cambridge. Prvi agent kojeg je Deutsch unovačio bio je Kim Philby, bivši student na Cambridgeu. Philby je preporučio Donalda Macleana i Guya Burgessa, Burgess je preporučio Anthonyja Blunta, a ovaj Johna Cairncrossa – i nastala je „petorka s Cambridgea" (Andrew 2009: 170–173). Članovi „petorke s Cambridgea" nikad ne bi toliko napredovali (u institucijama u kojima su radili) da nisu pohađali „prave" škole i da nisu bili članovi „pravih" klubova (Moran 2011). Ironično, barem na prvi pogled. Da nisu pripadali privilegiranim slojevima jedne kapitalističke i vrlo klasno raslojene zemlje, da nisu bili „buržuji", članovi „petorke" ne bi mogli toliko dobro služiti „prvoj zemlji socijalizma".

Ono što su u Britaniji bili Cambridge i Oxford, to su u Sjedinjenim Državama bili Harvard, Yale i ostala *Ivy League*[6] sveučilišta. Vjerojatno je način novačenja agenata na tim sveučilištima bio sličan načinu na koji je u Britaniji novačio Arnold Deutsch. Uostalom, i Alger Hiss i Laurence Duggan studirali su na Harvardu.

ZAKLJUČAK: TEHERAN I JALTA

Sovjetski agenti unutar američkih institucija koristili su Sovjetskom Savezu na dva načina – dostavljali su izuzetno vrijedne podatke, te su koristeći svoj utjecaj poboljšavali položaj SSSR-a u odnosu na ostale saveznike. Trebalo je imati prave ljude na pravom mjestu, a SSSR ih je imao.

Jedan od tih ljudi bio je i Alger Hiss. Hiss je bio član američkog izaslanstva na Jaltskoj konferenciji u veljači 1945., a nakon toga je bio vršitelj dužnosti privremenog glavnog tajnika Organizacije Ujedinjenih naroda na osnivačkom sastanku koji se održavao od 25. travnja do 26. lipnja 1945. u San Franciscu. Potkraj 1946. Hiss je napustio Ministarstvo vanjskih poslova te je postao predsjednik jednog instituta za istraživanje međunarodnih odnosa. Moguće je da je Hiss otišao iz državne službe nakon što su ga Sovjeti upozorili da postoji mogućnost da bude razotkriven, a vođenje jednog nevladinog, ali utjecajnog instituta omogućilo mu je da barem donekle „ostane u igri". Ipak, nakon što su optužbe da je bio sovjetski agent postale ozbiljne, Alger Hiss je u svibnju 1949. bio prisiljen napustiti taj institut.

Naravno da je SSSR-u njihov agent unutar američkog izaslanstva na Jaltskoj konferenciji bio koristan. Međutim, sve ono što se u Jalti događalo rezultat je višegodišnjeg djelovanja svih sovjetskih agenata unutar institucija SAD-a. Taj sovjetski agent u Jalti, tko god on bio, možda je mogao donekle utjecati na neke američke odluke, te je mogao SSSR-u dostaviti određeni podatak, iako je to vrlo opasno i moglo ga je razotkriti. Uostalom, Sovjetima nije ni trebao agent koji bi dojavljivao o čemu razgovara američko izaslanstvo u Jalti, jer su to oni vrlo dobro znali i sami.

Tijekom Teheranske konferencije u studenom 1943. Roosevelt je boravio u zgradi tamošnjeg sovjetskog veleposlanstva, dok je u Jalti u veljači 1945. boravio u bivšoj

[6] Osam znanstveno i društveno najuglednijih, najstarijih i najbogatijih privatnih američkih sveučilišta, smještenih na sjeveroistoku SAD-a. Studenti tih sveučilišta imaju velik utjecaj u poslovnom, političkom i društvenom životu zemlje.

ljetnoj rezidenciji ruskog cara. Sve prostorije u kojima su boravili Roosevelt i njegovi najbliži suradnici bile su ozvučene, svako jutro je Staljin izvješćivan o razgovorima Amerikanaca prethodne večeri kako bi se bolje pripremio za taj dan. Na Teheranskoj konferenciji Churchill je boravio u britanskom veleposlanstvu, dok su u Jalti Britanci morali prihvatiti boravak u palači koju su im Sovjeti dodijelili, pa su Sovjeti i njih prisluškivali.

U svojoj politici prema Sovjetskom Savezu i Staljinu Roosevelt je bio nevjerojatno naivan. Jednostavno, vjerovao je onima koji su ga uvjeravali da Staljin želi sigurnost za svoju zemlju i ništa više, a nije vjerovao onima koji su ga upozoravali na prirodu Staljinova režima i njegove namjere. Jedan od onih koji su Roosevelta upozoravali na Staljina bio je William Bullitt, prvi veleposlanik SAD-a u Sovjetskom Savezu (1933–1936). U jednom pismu Roosevelt je Bullittu odgovorio kako ima predosjećaj da Staljin nije onakav kakvim ga je Bullitt opisao (ne negirajući činjenice koje je Bullitt naveo), te da misli da ako on (Roosevelt) da Staljinu sve što mu može dati i ništa ne traži zauzvrat, Staljin neće pokušati ništa pripojiti i s njim (Rooseveltom) će raditi na uspostavi demokracije i mira u svijetu (Kern 2003). Roosevelt je u to doista vjerovao odnosno vjerovao je osobama u svojoj blizini koje su ga uvjeravale u Staljinove poštene namjere, a te su osobe bile ili sovjetski agenti, ili su u njihovoj blizini bili sovjetski agenti koji su utjecali na njih, ili su bile korisne budale.

Joseph E. Davies, veleposlanik SAD-a u Moskvi od 1936. do 1938., za razliku od svog prethodnika Bullitta bio je izrazito naklonjen Sovjetskom Savezu i Staljinu. U svibnju 1943. Roosevelt je bez da je prethodno o tome izvijestio tadašnjeg veleposlanika SAD-a u Moskvi admirala Standleyja, u Moskvu poslao Daviesa kako bi on osobno (nasamo) prenio Staljinu koliko ga Roosevelt poštuje i koliko želi izgraditi specijalne odnose među njima, te da se želi osobno susresti s njim. Davies je naglasio američko neodobravanje britanskog imperijalizma i prilično jasno nagovijestio da SAD i Sovjetski Savez mogu vladati svijetom bez Britanaca (Kern 2003).

Roosevelta je njegovo osoblje upozorilo da ga u Teheranu vjerojatno prisluškuju. Jedan pripadnik NKVD-a, koji je svako jutro izvješćivao Staljina o rezultatima prisluškivanja, ponekad je imao dojam da se Roosevelt putem mikrofona obraća direktno Staljinu (Kern 2003). Vjerojatno je bio u pravu. Kad je 1937. u veleposlanstvu SAD-a u Moskvi pronađen prislušni uređaj iznad radnog stola tadašnjeg veleposlanika Josepha Daviesa, Davies se nasmijao i rekao svojim suradnicima da „ako Sovjeti žele prisluškivati, jedino što će dobiti bit će dokaz iskrene želje SAD-a za suradnjom". Ako ovi detalji o Daviesovom i Rooseveltovom (blago rečeno) toleriranju prisluškivanja izgledaju nevjerojatno, kako tek izgleda podatak da je William Bullitt upozorio Roosevelta na to da su Alger i Donald Hiss sovjetski agenti, ali da Roosevelt nakon toga nije ništa poduzeo (Kern 2003).

Projekt Venona trajao je dugo jer dekriptiranje tako šifriranih poruka nije jednostavno. Ponekad se dekriptira samo dio poruke i taj dio pomaže u dekriptiranju neke druge poruke, što dovodi do dekriptiranje treće poruke itd. Na kraju se dekripter vraća prvoj poruci i imajući više podataka i iskustva ponekad je može dekriptirati u cijelosti. Radi se o sistemu pokušaja i pogrešaka, potrebna je velika strpljivost,

spremnost na razočaranja i znanje – lingvističko prije svega, ali i znanje o načinu razmišljanja određene strane (u ovom slučaju – sovjetske), ponekad čak i znanje o pojedincu iz neke rezidenture, njegov (njezin) način razmišljanja, izražavanja, sastavljanja poruke.

Poruke nikad nisu dekriptirane u realnom vremenu, u najboljem slučaju radilo se o porukama koje su poslane nekoliko godina prije (Benson 2001). Međutim, budući da se radilo o porukama koje su sadržavale podatke o sovjetskim agentima i izvorima koji su se nalazili duboko unutar institucija SAD-a, jasno je da je realno vrijeme doista relativno. Sovjetski Savez je već 1944. imao ograničena saznanja o projektu Venona, kasnije su uz pomoć svojih agenata unutar američkih i britanskih službi došli do više podataka (Benson 2001). Naravno da štetu koja je nastala njihovom pogreškom nisu mogli popraviti, ali ponekad su je mogli umanjiti upozoravajući svoje agente za koje su vjerovali da su identificirani, ili da je identifikacija moguća.

Projekt Venona započela je Američka kopnena vojska u vrijeme kad je predsjednik SAD-a i vrhovni zapovjednik oružanih snaga bio Franklin D. Roosevelt (do 12. travnja 1945.), te kasnije Harry Truman (1945. – 1953.). Međutim, projekt je bio toliko tajan da za njegovo postojanje nisu znali ni Roosevelt, ni Truman. Truman je bio upoznat s rezultatima projekta Venona kroz uobičajena izvješćivanja FBI-a, CIA-e i Ministarstva pravosuđa, ali mu nije rečeno da se ti rezultati baziraju na dekriptiranju sovjetskih poruka. To je bila odluka vrha Kopnene vojske, i bila je opravdana kad se zna koliko je sovjetskih agenata bilo u i oko Bijele kuće.

Sasvim sigurno su oni koji su tu odluku donijeli bili svjesni da krše pravila demokratskog sustava. Međutim, bili su svjesni i (sasvim realne) mogućnosti da SSSR praktički odmah dozna rezultate projekta Venona, kao i (opet vrlo realne) mogućnosti da jedan ili drugi predsjednik, po nagovoru nekog od savjetnika (koji je lako mogao biti sovjetski agent ili barem korisna budala), donese odluku o prekidu programa. Zapravo se nešto tako i dogodilo jer je nekoliko mjeseci prije kraja Drugog svjetskog rata netko iz Bijele kuće (naravno, neslužbeno) pokušao zaustaviti projekt Venona, ali u tome nije uspio (Johnson 1995: 159).

U sklopu projekta Venona dekriptirano je, djelomično ili potpuno, oko 3000 sovjetskih šifriranih poruka. Međutim, i taj relativno mali broj pružio je Amerikancima uvid u djelovanje sovjetskih obavještajnih službi u SAD-u, te je uspješno identificirano više od 200 osoba povezanih s NKVD-om i GRU-om (*VENONA: An Overview*). Otkriveni su važni sovjetski agenti u SAD-u, Britaniji, Australiji i drugim zemljama. Njihovim otkrivanjem nije mogla biti popravljena nanesena šteta, ali su barem onemogućeni u daljnjem radu.

Da Sovjetski Savez nije napravio pogrešku uporabljujući iste ključeve za dvije poruke, vjerojatno bi većina tih agenata nastavila svoj rad, neki od njih sigurno i na višim i odgovornijim pozicijama. SSSR je računao na to da je mala vjerojatnost da će netko opaziti da poruke poslane, na primjer, iz New Yorka u Moskvu i iz Moskve u London počinju istom prvom skupinom brojeva (tj. da imaju isti indikator poruke), osobito ako je između slanja jedne i druge poruke proteklo određeno vrijeme, mjeseci ili čak godine. Međutim, oni koji odlučuju o šiframa morali bi znati da ako

postoji i najmanja mogućnost da netko primijeti neku pogrešku ili slabu točku u šifriranju, da će se to i dogoditi.

U Drugom svjetskom ratu njemački su šifranti napravili tek nekoliko pogrešaka prilikom rada s uređajima za šifriranje (Enigma i teleprinterska šifra Lorenz), ali su te pogreške Britanci uočili i nakon toga iskorištavali. Na temelju samo jedne pogreške operatera na predajnoj strani radio-teleprinterske veze između (vjerojatno) Atene i Beča, 30. kolovoza 1941., a koja je bila opažena u britanskoj prislušnoj postaji u Knockholtu (Kent, Engleska), stručnjaci u Bletchley Parku (središtu britanske službe za dekriptiranje u Drugom svjetskom ratu) shvatili su način rada Lorenzovog uređaja za šifriranje teleprinterskih poruka SZ-40, te su do kraja rata dekriptirali poruke najviših zapovjedništava njemačke vojske (Sale). Doslovno se radilo o porukama koje su izmjenjivali Hitler i njegovi generali i feldmaršali.

Sovjetski Savez nije smio ništa prepustiti slučaju, pogotovo jer se radilo o sigurnosti njegovih najvažnijih agenata u inozemstvu, osobito u SAD-u i Velikoj Britaniji. Britanski i američki dekripteri su u Drugom svjetskom ratu pokazali da kad se jednom uvjere da se neka šifra može „razbiti", od toga ne odustaju. Jednom kad su Amerikanci opazili da su neke (nikad više od dvije) sovjetske poruke šifrirane istim ključem, ništa ih više nije moglo zaustaviti.

LITERATURA

Andrew, Christopher. 2009. *The Defence of the Realm: The Authorized History of MI5*. London: Penguin.

Benson, Robert L. 2001. The Venona Story. Center for Cryptologic History, National Security Agency. https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/publications/coldwar/assets/files/venona_story.pdf (pristupljeno 20. rujna 2016.).

Geschwind, C. N. 1963. Wanted: An Integrated Counter-intelligence. *Studies in Intelligence* 7(3). https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol7no3/html/v07i3a02p_0001.htm (pristupljeno 20. rujna 2016.).

Haynes, John Earl i Harvey Klehr. 2013. Was Harry Hopkins a Soviet Spy? Frontpage Mag, 15. kolovoza. http://www.frontpagemag.com/fpm/200900/was-harry-hopkins-soviet-spy-john-earl-haynes (pristupljeno 20. rujna 2016.).

Johnson, Thomas R. 1995. *American Cryptology during the Cold War, 1945–1989. Book I: The Struggle for Centralization, 1945–1960*. Center for Cryptologic History, National Security Agency. https://www.nsa.gov/news-features/declassified-documents/cryptologic-histories/assets/files/cold_war_i.pdf (pristupljeno 20. rujna 2016.).

Kahn, David. 1961. Number One From Moscow. *Studies in Intelligence* 5(4). https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol5no4/html/v05i4a09p_0001.htm (pristupljeno 20. rujna 2016.).

Kahn, David. 1979. *Šifranti protiv špijuna*, 3. sv. Zagreb: Centar za informacije i publicitet – Liber.

Kern, Gary. 2003. How "Uncle Joe" Bugged FDR. *Studies in Intelligence* 47(1). https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no1/article02.html (pristupljeno 20. rujna 2016.).

Moran, Christopher R. 2011. Coming to Clarity – The Pursuit of Intelligence History: Methods, Sources, and Trajectories in the United Kingdom. *Studies in Intelligence* 55(2). https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-55-no.-2/pdfs-vol.-55-no.-2/Moran-HistoriographyofIntelinUK-7%20June2011.pdf (pristupljeno 20. rujna 2016.).

Moscow [unnumbered], 25 April 1944. Keypad indicator change. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/venona-soviet-espionage-and-the-american-response-1939-1957/b26.gif/image.gif (pristupljeno 20. rujna 2016.).

Orlov, Alexander. 1963. The Theory and Practice of Soviet Intelligence. *Studies in Intelligence* 7(2). https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol7no2/html/v07i2a05p_0001.htm (pristupljeno 20. rujna 2016.).

Rijmenants, Dirk. 2016a. The complete guide to secure communications with the one time pad cipher. Cipher Machines and Cryptology. http://users.telenet.be/d.rijmenants/papers/one_time_pad.pdf (pristupljeno 20. rujna 2016.).

Rijmenants, Dirk. 2016b. One-time Pad. Cipher Machines and Cryptology. http://users.telenet.be/d.rijmenants/en/onetimepad.htm (pristupljeno 20. rujna 2016.).

Sale, Tony. The Lorenz Cipher and how Bletchley Park broke it. http://www.codesandciphers.org.uk/lorenz/fish.htm (pristupljeno 20. rujna 2016.).

VENONA: An Overview. Cryptologic Almanac 50th Anniversary Series. https://www.nsa.gov/news-features/declassified-documents/crypto-almanac-50th/assets/files/VENONA_An_Overview.pdf (pristupljeno 20. rujna 2016.).

Venona #812. https://www.nsa.gov/news-features/declassified-documents/venona/dated/1943/assets/files/29may_roosevelt_churchill.pdf (pristupljeno 20. rujna 2016.).

Venona #1114. https://www.nsa.gov/news-features/declassified-documents/venona/dated/1944/assets/files/4aug_laurence_duggan_unra.pdf (pristupljeno 20. rujna 2016.).

Venona #1251. https://www.nsa.gov/news-features/declassified-documents/venona/dated/1944/assets/files/2sept_covername_changes.pdf (pristupljeno 20. rujna 2016.).

Venona #1579. https://www.nsa.gov/news-features/declassified-documents/venona/dated/1943/assets/files/28sep_gru_sources.pdf (pristupljeno 20. rujna 2016.).

Venona #1613. https://www.nsa.gov/news-features/declassified-documents/venona/dated/1944/assets/files/18nov_lawrence_duggan.pdf (pristupljeno 20. rujna 2016.).

Venona #1657. https://www.nsa.gov/news-features/declassified-documents/venona/dated/1944/assets/files/27nov_mrs_rosenberg.pdf (pristupljeno 20. rujna 2016.).

Venona #1699. https://www.nsa.gov/news-features/declassified-documents/venona/dated/1944/assets/files/2dec_manhattan_project_scientists.pdf (pristupljeno 20. rujna 2016.).

Venona #1822. https://www.nsa.gov/news-features/declassified-documents/venona/dated/1945/assets/files/30mar_kgb_interviews_gru_agent.pdf (pristupljeno 20. rujna 2016.).

VENONA PROJECT AND SOVIET AGENTS INSIDE THE U.S. INSTITUTIONS DURING WW2

Robert Derenčin

SUMMARY

Venona Project began in 1943 as an attempt of the code-breaking service of the US Army (U.S. Army Signal Intelligence Service) that by means of traffic analysis of ciphered messages between Moscow and Soviet diplomatic representations obtain some knowledge about activities of Soviet intelligence services in the U.S. Thanks to one catastrophic Soviet mistake part of the Soviet ciphered messages was (at least partially) decrypted. By means of joint work of American code-breakers, FBI, CIA and their British counterparts some of the most important Soviet agents in the U.S., Britain and other countries were identified. Nevertheless, the fact is that the Soviet Union had its agents deeply infiltrated into societies and institutions of the western countries, and that those agents helped the Soviet Union to take much better staring positions in the beginning of the Cold war. The article explains how the Soviets recruited those agents and on which way the Soviets ciphered their most secret messages, but it also explains how even the most secure system is actually insecure if not used completely properly.

Keywords: Venona Project, Soviet intelligence, NKVD, GRU, code-breaking, HUMINT, WW2.