TURINYS

Įvadas: šiek tiek apie save 9

1. Istorinės aplinkybės 15
2. Amerikos žvalgybos raida 36
3. Amerikos žvalgybos reikalavimai 62
4. Informacijos rinkimas 73
5. Informacijos rinkimas, padedant specialiems įrenginiams 85
6. Planavimas ir vadovavimas 104
7. Pagrindinis priešininkas – komunistų žvalgybos tarnybos 110
8. Kontržvalgyba 150
9. Savanoriai 164
10. Priešininko supainiojimas 177
11. Kaip panaudojama žvalgybinė informacija 188
12. Žvalgybos darbuotojai 207
13. Mitai, nesėkmės ir eibių priežastys 226
14. Žvalgybos vaidmuo Šaltajame kare 264
15. Saugumas laisvoje visuomenėje 282
16. Žvalgybos tarnyba ir mūsų laisvės 307

Bibliografija 319

5.

INFORMACIJOS RINKIMAS, PADEDANT SPECIALIEMS ĮRENGINIAMS

Žvalgybos tarnybai reikia vyro, kuris kalba suahilių ir prancūzų kalbomis, yra baigęs chemijos inžinerijos studijas, nevedęs, vyresnis nei trisdešimt penkerių ir aukštesnis nei penkių pėdų. Jūs paspaudžiate mygtuką, ir mažiau nei per keturiasdešimt sekundžių įrenginys (panašus į tokį, kuris naudojamas personalo skyriuje) nurodo, ar toks žmogus yra, ir jei taip – papildomai pateikia visus apie jį turimus įrašus. Panašūs įrenginiai naudojami ir rūšiuojant bei renkant žvalgybinę informaciją.

Tai reiškia, kad be analitikų ir vertintojų šiuolaikinėje žvalgyboje dirba asmenys, kurie geba apdoroti duomenis, naudotis kompiuteriais bei kitomis sudėtingomis „mąstančiomis“ mašinomis.

Neturime iliuzijų, kad šios mašinos galėtų pagerinti informacijos pobūdį. Tai visada priklausys nuo šaltinio patikimumo ir analitiko įgūdžių. Tačiau iš milžiniškos informacijos laikmenos galima greitai ir tiksliai išrinkti naujai informacijai įvertinti būtinus duomenis. Iki mechaninių arba elektromechaninių įrenginių išradimo analitikai ištisas savaites ieškodavo ir tyrinėdavo bylas, o dabar mašinos šį darbą atlieka per kelias minutes.

Bet šis darbas įprastas, lyginant su tuo, ką šiais laikais technologijos padaro rinkdamos pačią informaciją. Aš kalbu ne apie kompiuterius ar

kitus įrenginius, o apie specialius įrankius, kurie buvo sukurti pakeisti žmogaus rankas ir akis, t. y. stebėti ir aprašyti įvykius arba patekti į teritorijas, kurių žmogus negali pasiekti.

Šiuolaikinės žvalgybos tikslai yra techninio pobūdžio, todėl kilo poreikis sukurti stebėjimo įrankius. Jei toks tikslas skleidžia kontrolinį garsą, tuomet turi būti stebimas specialiu akustiniu įrankiu. O jeigu kelia smūgių bangas žemėje, tuomet jį aptiks seismografas.

Be to, reikia stebėti ir matuoti mūsų pačių eksperimentus su branduoliniais ginklais ir raketomis, todėl patobulinta įranga, kurią šiek tiek pakeitus galima stebėti kitų valstybių eksperimentus. Pagrindiniai techninio rinkimo įrankiai yra radaras ir tiksli ilgo nuotolio fotografija. O siekiant nustatyti radioaktyvumą atmosferoje, renkami ir analizuojami oro pavyzdžiai. Radioaktyvias daleles vėjas perneša per valstybių sienas, todėl tokių pavyzdžių galime surinkti net nevykdami į priešininko šalį.

1948 metais vyriausybė nurodė visą parą orlaiviu stebėti atmosferą, nes ieškojome eksperimentų su atominiais ginklais. Pirmieji įrodymai apie sovietų įvykdytą atominį sprogimą Azijos žemyninėje dalyje nustatyti 1949 metų rugsėjį, kas nustebino visą pasaulį ir daugelį mokslininkų, iki tol tikėjusių, kad sovietai tais metais „neturės bombos“. Patobulinę instrumentus, sužinojome ne tik apie pirmuosius įvykdytus atominius sprogimus, bet ir detonuoto įrenginio ar ginklo galingumą bei tipą.

Kaip ir buvo galima tikėtis, ilgainiui šie išradimai įkvėpė priešininką, sužinojusį, kad eksperimentai buvo stebimi, imtis aukšto technologinio pobūdžio atsakomųjų priemonių. Dabar įmanoma „uždengti“ po žeme ir didžiulėse aukštumose vykdomus atominius sprogimus, kad nenustatytume charakteristikų, sakykime – dydžio ir tipo. Žinoma, informaciją renkančios šalies technikai sieks sukurti atsakomąsias priemones, kurios padės išvengti technologijų spąstų.

Pastaraisiais metais su sovietais užsitęsė derybos dėl nusiginklavimo bei branduolinių bandymų uždraudimo, kurios susijusios būtent su tokiomis problemomis. Derybų metu atskleisti sudėtingi iki šiol slapta vykdomi tyrimai – ir mes, ir sovietai siekiame slėpti savo eksperimentus su branduoliniais įrenginiais ir aptikti priešininkų bandymus.

Taigi moderniomis technologijomis bandoma stebėti tam tikrus kitų valstybių vykdomus mokslinius ir karinius eksperimentus, susitelkiant į jų

„pašalinius efektus“. Kosmoso tyrinėjimai – tai dar vienas, kiek kitoks stebėjimo būdas. Kosminiai laivai elektroniniais signalais arba telemetrija teikia duomenis apie savo veikimą, sąlygas kosmose arba dangaus kūnus. Šie signalai skiriami orlaivį išsiuntusios šalies bazėms arba stotims. Bet, kaip ir paprastų radijo pranešimų klausymosi atvejais, neįmanoma tinkamą įrangą turintiems neleisti „pasiklausyti“ ir tokių signalų. Akivaizdu, kad tarpusavyje dėl eksperimentų kosmose konkuruojančios valstybės sieks perimti viena kitos telemetriją ir nustatyti, dėl ko vykdomi kitos šalies eksperimentai ir kokie buvo jų rezultatai. Reikia tik teisingai perskaityti signalus.

Tačiau daugelis svarbių karinių ir techninių taikinių yra stacionarūs, ir jų vietovės arba veiklos pobūdžio negalima nustatyti, atsekti, stebėti ar perimti. Fabrikai, laivų statyklos, arsenalai, statomos raketų bazės neskleidžia signalų, kuriuos būtų galima sekti iš toli. Tam, kad žmogus atrastų tokius įrenginius, turi prie jų priartėti arba skristi tiesiai virš jų labai dideliame aukštyje su ilgo nuotolio kameromis. Toks ir buvo U-2 tikslas – šie orlaiviai gali rinkti informaciją greičiau, tiksliau ir patikimiau nei bet kuris agentas žemėje. Jo atliekamus žygdarbius galima lyginti tik su techninių dokumentų įgijimu tiesiai iš sovietų biurų ar laboratorijų. U-2 mokslinio žvalgybos rinkimo srityje reiškia didžiulį laimėjimą. 1960 metų gegužės 1 d. įvykus U-2 avarijai, Jungtinių Valstijų gynybos sekretorius Thomasas S. Gatesas jaunesnysis 1960 metų birželio 2 dieną Senato užsienio reikalų komitetui teigė, kad:

> „Po šių skrydžių mes gavome informacijos apie aerodromus, orlaivius, raketas, raketų bandymus ir apmokymus, specialiųjų ginklų laikymą, povandeninių įrenginių gamybą, atominių įrenginių gamybą ir su orlaiviais susijusius išradimus, tai yra visų tipų ypatingos svarbos informaciją. Šie rezultatai apsvarstyti mūsų karinėse programose. Mes buvome svarbiausi užsakovai, ir mūsų interesas yra svarbiausias“.

Ne taip seniai labai dideliame aukštyje vykdyti U-2 žvalgybiniai skrydžiai suteikė patikimos informacijos apie sovietų vidutinio nuotolio raketų dislokavimą Kuboje vėlyvą 1962 metų spalį. Jeigu jų nebūtume aptikę dar statant bazes, kol jos nebuvo užmaskuotos, šios bazės būtų tapusios

Amerikiečių žvalgybinis lėktuvas „U-2 Lockheed".

mirtinu pavojumi viso Vakarų pusrutulio saugumui. Įdomu tai, kad klasikinius rinkimo metodus derinant su moksliniais rinkimo metodais buvo gauti itin vertingi duomenys. Įvairūs agentai ir pabėgėliai iš Kubos pranešė, kad statoma kažkas panašaus į raketų bazes, ir nurodė statybos vietą, todėl rinkdami įrodymus pasitelkėme oro žvalgybą.

1964 metų gegužę, kai Nikita Chruščiovas pareiškė, kad Jungtinės Valstijos išvengtų tarptautinės įtampos, atsisakydamos tolesnių U-2 skrydžių virš Kubos, iškilo klausimas, ar pilotuojamus U-2 galėtų pakeisti bepiločiai satelitai, besisukantys aplink pasaulį daug didesniame aukštyje. Chruščiovas teigė, kad kosminiai palydovai atliktų tą patį darbą ir mūsų prezidentui pasiūlė parodyti Amerikos karinių bazių nuotraukas, kurias padarė sovietų „oro šnipai". Abejoju, ar galėtume sutikti su Chruščiovo mintimi, kad kosminiai įrenginiai turėtų pakeisti valdomą lėktuvą visais žvalgybos tikslais. Bet įdomu, kad jis pripažino satelitų naudojimą.

Iškalbingą liudijimą apie mokslinio žvalgybos rinkimo vertę, kuri jau buvo įrodyta šimtus kartų, pateikė Vinstonas Čerčilis, pasakodamas apie Antrąjį pasaulinį karą.* Jis aprašė, kaip 1940 metų rugsėjį per Britanijos mūšį britai panaudojo radarą, bei pasakojo apie Berlyno siunčiamų signalų, kuriais buvo vadovauta Vokietijos orlaiviui, iškraipymą ir falsifikavimą. Čerčilis šį susidūrimą vadino „burtų karu" ir rašė, kad „jei britų mokslas nebūtų pralenkęs vokiečių mokslo, ir jei jo keistų bei grėsmingų resursų nebūtų pavykę panaudoti išgyvenimo mūšyje, mus būtų sumušę ir sunaikinę".

Mokslu, kaip esminiu žvalgybos ginklu, turime kliautis ir ateityje. Dalyvaujame gyvybiškai svarbiose varžybose su komunistinio bloko, ypač Sovietų Sąjungos, mokslininkais, ir privalome dirbti, kad *išliktume* lyderiais. Ateityje mums tai gali būti taip svarbu, kaip britams 1940 metais, kai šie panaudojo radarus.

SEKIMAS GARSO ĮRANGA

Kitokio pobūdžio techninė šnipinėjimo priemonė – paslėptas mikrofonas ir siųstuvas, kuris informacijos tėkmę siunčia į šalia esančią pasiklausymo stotį; žmonės dažnai tai vadina „ūžimu ragelyje", „sekimu" arba „pasiklausymu". Sekti garso įranga, kaip tai vadinama žvalgyboje, reikalinga nepriekaištinga miniatiūrinė elektroninė įranga, išmanūs maskavimo metodai ir agentas – žmogus, kuris patektų į patalpas ir tokią įrangą paslėptų.

Ankstyvą 1960 metų birželį ambasadorius Henry'is Cabotas Lodge'as Jungtinių Tautų būstinėje Niujorke pakabino Didįjį Jungtinių Valstijų herbą, kuris prieš tai kabėjo Amerikos ambasadoriaus biure Maskvoje. Jame sovietai buvo paslėpę miniatiūrinį aparatą, kurį aktyvavus, į sovietų pasiklausymo stotį būdavo persiunčiama viskas, kas kalbėta ambasadoriaus kabinete. Tiesą pasakius, tokio instrumento įstatymas nebuvo didelė sovietų pergalė, nes kiekviena Maskvoje esanti užsienio ambasada yra priversta prašyti vietinių elektrikų, telefonų tinklo specialistų, santechnikų,

* *The Second World War* (Boston: Houghton, Mifflin Co., 1948 – 1953).

valytojų ir panašių darbininkų paslaugų. Sovietams nesudėtinga priversti savo piliečius bendradarbiauti su žvalgyba arba nusiųsti žvalgybos pareigūnus, kurie atliktų darbą persirengę kaip pagalbinis personalas.

1964 metų gegužę šalies Valstybės departamentas viešai paskelbė, kad išsamiai ištyrus mūsų ambasados Maskvoje patalpų vidines sienas, lubas ir grindis, aptikta keturiasdešimt paslėptų mikrofonų. Anksčiau atlikta intensyvi paslėptų elektroninių įrenginių paieška nerado nė vieno tokio mikrofono.

Sovietų Rusijoje ir didžiausiuose satelitinių valstybių miestuose yra specialiai užsienio svečiams paruoštų kambarių, nes juose įrengta stacionari pasiklausymo įranga. Atvykus kokiam nors „įdomiam“ užsieniečiui, nebereikia gaišti laiko. Mikrofonai jau yra, lieka tik įkurdinti užsienietį. Visi viešbučiai priklauso valstybei, ir tarp jų personalo pilna agentų, kurie stebi, kad užsieniečiai būtų apgyvendinti „tinkamuose“ kambariuose.

1955 metų rugsėjį į garsųjį vizitą Maskvoje, kurio metu siekta aptarti diplomatinių ryšių tarp Rusijos ir Vakarų Vokietijos atnaujinimą, kancleris Adenaueris vyko specialiu Vokietijos traukiniu. Kai jis atvyko į Maskvą,

VFR kanclerio K. Adenauerio apsilankymas Maskvoje. 1955 m.

sovietai labai nusivylė sužinoję, kad gudrusis kancleris (tuo metu neveikė ambasada, kurioje jis būtų apsistojęs ir taip užsitikrinęs minimalų saugumą) vizito Maskvoje metu ketino likti traukinyje ir nenorėjo pasinaudoti sovietų „svetingumu“, t. y. apsigyventi vieno iš prabangiausių užsieniečiams skirtų Maskvos viešbučių apartamentuose. Pranešta, kad prieš išvykstant iš Vokietijos kanclerio traukinyje darbavosi technikai, įdiegdami naujausią blokuojančią sekimą įranga.

Už savo šalies ribų žvalgybos tarnyba privalo apsvarstyti galimas pasekmes ir keblumus dėl neteisėtai įvežto oficialaus įrenginio gedimo. Kaip ir visose šnipinėjimo operacijose, tuomet reikia rasti asmenį, kuris galėtų atlikti darbą, turėtų talentą ir motyvą – patriotinį ar piniginį. Kartą sovietams pavyko įtaisyti mikrofonus neutralios Vakarų šalies ambasados biuruose stovinčiuose gėlių vazonuose. Pastato durininkas, turėjęs silpnybę alkoholiui, džiaugėsi galėdamas padėti už mažą piniginį atlygį. Jis ir nežinojo, kas buvo tie, kurie kartkartėmis pasiskolindavo gėlių vazonus, vėliau grąžindavo į vietą, ir ką su jais pasiėmę veikdavo.

Tikriausiai nėra technologinio įrenginio, prieš kurį negalima imtis atsakomųjų veiksmų ir priemonių. Įrenginiai aptinkami ir neutralizuojami, kai kuriais atvejais netgi panaudojami prieš juos įrengusius asmenis. Aptikus tokius įrenginius, juos verta palikti ir tokiu būdu kitai pusei pateikti neteisingą arba klaidinančią informaciją.

Diplomatinėse įstaigose užsienyje sovietai ir jų satelitinės valstybės taip bijo sekimo įrangos, kad paprastai atsisako vietinių darbininkų paslaugų įrengiant telefonus ar netgi įprastą elektros instaliaciją. Kad išvengtų numanomo sekimo, sovietai savo technikus ar elektrikus siunčia kaip laikinai pareigas einančius diplomatus, nurodydami atlikti reikiamas montavimo paslaugas. Kartą įtarę, kad ambasadoje įrengta pasiklausymo įranga, į sostinę netgi atsiuntė darbininkų komandą, kuriems parūpino diplomatinius pasus. Didelei vietos institucijų pramogai, kelias savaites šie darbo rūbais vilkintys „diplomatai“ nešiojosi kastuvus ir aplink ambasados pastatą kasė keturių ar penkių pėdų gylio griovį, ieškodami požeminių laidų, bet taip nieko ir nerado.

KODAI IR ŠIFRAI

„Džentelmenai, – 1929 metais pareiškė valstybės sekretorius Stimsonas, – neskaitykite vieni kitų korespondencijos“, ir taip sakydamas uždarė vienintelę tuo metu funkcionavusią Amerikos kodų dešifravimo tarnybą. Vėliau, Antrojo pasaulinio karo metais, valdant prezidentui Franklinui D. Rooseveltui, eidamas karo sekretoriaus pareigas, jis pripažino žvalgybos svarbą, įskaitant „ryšio kanalų žvalgybą“. Kai kyla pavojus tautai ir jos karių gyvybėms, džentelmenai skaito vieni kitų laiškus, jei tik šie papuola į rankas.

Žinoma, aš nekalbu apie įprastą korespondenciją, nors pašto cenzūra žvalgyboje atliko svarbų vaidmenį. Išskyrus slapto rašto aptikimą, pašto cenzūroje nėra labai jau rimtų technologijų. Kita vertus, moderni ryšio kanalų žvalgyba yra techninė sritis, pasitelkusi geriausius intelektinio karo protus – tokiame kare vyksta mūšiai dėl mokslinės informacijos.

Nepažeidžiamų komunikacijos sistemų sukūrimas ir šių sistemų bei jas valdančio personalo apsauga kelia didelius galvos skausmus kiekvienai vyriausybei. Be to, kiekviena vyriausybė padarys viską, kas yra jos galioje, kad gautų prieigą prie kitų vyriausybių, kurių politika ar veiksmai jai kelia rimtų rūpesčių, komunikacijų. Tokių abiejų pusių pastangų priežastis akivaizdi. Oficialių politinių ar karinių pranešimų apie slaptus reikalus turinys, ypač krizės laikais, yra geriausia ir „karščiausia“ žvalgybinė informacija, kurią viena vyriausybė tikisi surinkti apie kitą.

Šioje srityje yra didžiulis skirtumas tarp mėgėjiškos ir profesionalios terminologijos. Vartodamas mėgėjiškus terminus, veikiausiai įžeisiu profesionalus, o vartodamas profesionalius terminus, tikriausiai įkyrėsiu ir sukelsiu sumaištį mėgėjams. Mano pasirinkimas nelengvas, ir aš rašysiu glaustai. Koduose koks nors žodis, simbolis ar simbolių grupė pakeičia visą žodį, žodžių grupę ar net visą mintį. Todėl „XLMDP“ arba „79648“, priklausomai nuo vartojamo raidinio arba skaitmeninio kodo, gali reikšti „karą“, ir ši reikšmė nekinta visame pranešime. Kai 1941 metų gruodį, naudodamasi paprasčiausiais iš anksto sutartais kodiniais žodžiais, Japonijos vyriausybė savo diplomatams Jungtinėse Valstijose sukūrė

žymųjį „Rytų vėjų“ kodą, manėsi pasirengę artėjančiai atakai Ramiajame vandenyne.

Šifruose simbolis, pavyzdžiui, raidė arba skaičius, reiškia vieną žodžio raidę. Taigi „b“ arba „2“ gali reikšti „e“ arba bet kurią kitą raidę. Sudėtinguose šiais laikais naudojamuose šifruose kiekvieną kartą panaudotas tas pats simbolis gali reikšti skirtingą raidę. Kartais pranešimas visų pirma paverčiamas kodu, o tada kodas paverčiamas šifru.

Pirmojo, o kai kuriais atvejais ir Antrojo pasaulinio karo metais korespondencijoje tarp mūšio lauke esančių dalinių Jungtinių Valstijų karinės pajėgos griebėsi gana neįprastų „jau sukurtų“ kodų. Tai buvo Amerikos indėnų, ypač navahų kalba, kuri neturi rašytinių formų, jos niekada išsamiai nestudijavo užsienio mokslininkai. Du tos pačios genties nariai laisvai galėdavo kalbėtis telefonu ir perduoti pranešimus, kurių nesuprato nė vienas klausytojas, išskyrus kitą navahą. Nereikia nė sakyti, kad nei Vokietijoje, nei Japonijoje navahų nebuvo.

Modernioje terminologijoje žodis „kripta“, kuris reiškia „kažką užslėpto“, įtikinamai apibrėžia skirtumą tarp kodų ir šriftų, nes siejasi su „gryno teksto“ arba „aiškaus teksto“ pakeitimo simboliais metodais. Šiandien vartojamas visą sritį apibrėžiantis terminas yra kriptologija. Po šiuo plačiu terminu slypi dvi skirtingos sritys. Kriptografija sudarinėja, išradinėja, kuria ar saugo kodus ir šriftus savo vyriausybės naudojimui. Kriptoanalizė naudojama nulaužti ir dešifruoti kodus

Du navahų kilmės JAV kariuomenės ryšių tarnybos kariai. 1943 m.

ir šifrus, verčiant perimtus pranešimus į reikiamą kalbą. Asmens pranešimų vertimas kodais ar šifrais vadinamas „šifravimu“. O versdami užkoduotus ar šifruotus pranešimus į įprastą kalbą, juos iššifruojame.

Kriptograma yra bet koks užkoduotas ar šifruotas pranešimas. „Ryšio kanalų žvalgybinė informacija“ – tai informacija, gauta sėkmingai atlikus kitų asmenų pranešimų kriptoanalizę. O dabar, visiškai supainioję skaitytoją, galime eiti prie esmės.

Kiekvienos šalies diplomatinės, karinių pajėgų ir žvalgybos tarnybos naudoja slaptus kodus ir šifrus klasifikuotuose ir skubiuose ilgą atstumą keliaujančiuose pranešimuose. Pranešimus galima perduoti komerciniais kabeliais, per radiją arba naudojantis specialiomis vyriausybių sukurtomis schemomis. Radijo pasiklausyti gali kiekvienas. Be to, bent jau krizės laikais vyriausybės gauna kopijas užšifruotų pranešimų, kuriuos jų šalių teritorijoje esantys užsienio diplomatai komerciniais kabeliais siunčia namo. Problemų kelia kodų ir šifrų iššifravimas.

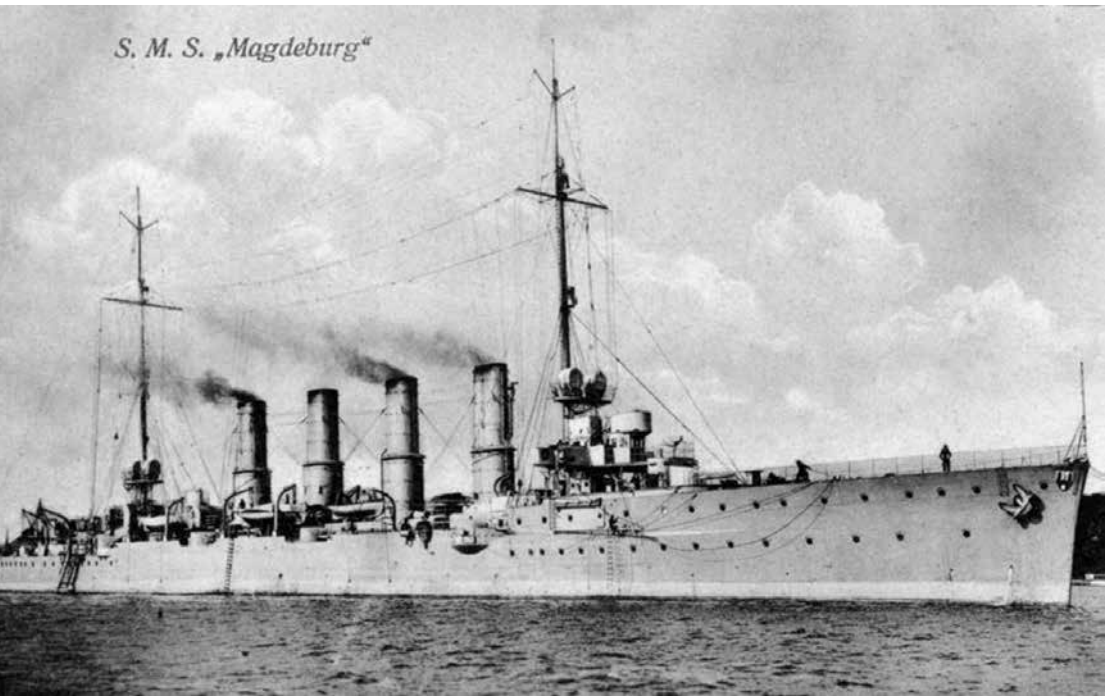
Kai kuriuos kodus ir šifrus galima perskaityti pasitelkiant pranešimų matematinę analizę, t. y. kriptoanalizę, gaunant kodų ar kodų knygų kopijas arba informaciją apie priešininko naudojamas šifravimo mašinas. Naudojama ir šių metodų kombinacija.

Ankstyvosiomis mūsų diplomatinės tarnybos dienomis, iki Pirmojo pasaulinio karo, kodų klausimas spręstas daugiau mažiau atmestinai, ir pasekmės dažniausiai būdavo liūdnos. Kai buvau jaunas užsienio reikalų skyriaus pareigūnas, man papasakojo vieną istoriją. Ramiomis 1913 metų dienomis mūsų pasiuntinys Rumunijoje buvo gerbiamas politikas, puikiai ėjęs pareigas Vidurio Vakaruose. Todėl buvo įvertintas ir išsiųstas į Bukareštą. Šioje srityje jis buvo naujokas, ir kodai bei šifrai jam nedaug ką reiškė. Tuo metu mūsų pagrindinė sistema buvo paremta kodų knyga, kurią vadinsiu „Rožiniu kodu“, nors, kai galvojome jai pavadinimą, pasirinkta ne ta spalva. Prie šios knygos aš praleidau tūkstančius kankinančių valandų. Jos nemačiau daugiau nei keturiasdešimt metų, bet iki šiol prisimenu, kad „periodui“ pavadinti turėjome šešis ar septynis žodžius. Vienas jų buvo „PIVIR“, kitas „NINUD“. Likusių keturių ar penkių nepamenu. Tuo metu naiviai galvojome, kad jei turėsime šešis ar septynis žodžius, supainiosime priešą, ir jis nežinos, kur pradedame ir baigiame sakinius.

Mūsų pasiuntinys iš Vašingtono išvyko dideliame užantspauduotame voke turėdamas „Rožinį kodą“ ir saugiai pasiekė Bukareštą. Planavome jį saugoti viename iš delegacijos seifų. Tačiau seifo kombinacijos nebuvo naujojo pasiuntinio stiprioji pusė, ir jis pagalvojo, kad patogiau laikyti kodą po čiužiniu, kur šis sėkmingai išbuvo keletą mėnesių. Vieną dieną visa kodų knyga – vienintelė, kurią turėjo ministras – dingo. Manoma, kad ji iškeliavo į Petrogradą.

Naujasis pasiuntinys atsidūrė keblioje padėtyje, kurią jis, kaip politikas, išsprendė labai išradingai. Tomis dienomis į Bukareštą siųsti gana nereikšmingi koduoti pranešimai, daugiausia emigrantų iš Rumunijos ir Besarabijos klausimais. Tad surinkęs pusę tuzino koduotų pranešimų, naujasis pasiuntinys sėsdavo į traukinį, kuris vykdavo į Vieną, ir ten užsukdavo pas mūsų ambasadorių. Pokalbio metu svečias iš Bukarešto atsitiktinai užsimindavo, kad prieš pat išvykimą gavo kelis pranešimus, kurių nespėjo iššifruoti, ir pasiskolindavo ambasadoriaus „Rožinį kodą“. (Tais senais gerais laikais tas pačias kodų knygas siųsdavome į beveik visas diplomatines misijas.) Tuomet ministras Bukarešte iššifruodavo pranešimus, parengdavo ir užkoduodavo atitinkamus atsakymus, išvykdavo į Bukareštą ir atitinkamu laiku išsiųsdavo užkoduotus atsakymus. Kurį laiką viskas vyko sklandžiai. Kodų knygos praradimo paslaptis sėkmingai išsaugota iki 1914 metų rugpjūčio, kai iš Vašingtono ėmė plūsti gausybė pranešimų, nes įsisiūbavo dramatiški įvykiai, privedę iki Pirmojo pasaulinio karo. Ministro padėtis buvo tragiška – kelionių į Vieną nebeužteko. Jis pripažino aplaidumą ir grįžo į Amerikos politiką.

Kartais dėl nekontroliuojamų įvykių ir karo katastrofų vienos pusės kriptografinę medžiagą panaudoja kita pusė. Štabas arba forpostas gali būti užimtas, o kodų knygos pamirštos atsitraukiant. Pirmojo pasaulinio karo metais įvyko daug tokių įvykių, dėl kurių britai gavo gyvybiškai svarbios informacijos apie vokiečių karinius ir diplomatinius planus. Karo pradžioje rusai paskandino vokiečių kreiserį „Magdeburg“ ir iš paskendusio jūrininko rankų ištraukė vokiečių jūrų laivyno kodų knygą, kurią nedelsdami perdavė sąjungininkams britams. Britų vykdomų paskendusių vokiečių povandeninių laivų gelbėjimo metu aptikta panašių radinių. 1917 metais, grįždami iš mūšio prieš Angliją, du vokiečių dirižabliai papuolė į audrą ir nukrito Prancūzijos teritorijoje. Tarp rastos medžiagos



Vokiečių kreiseris „Magdeburg“. Iš jame rastų slaptų knygų britams ir rusams pavyko nustatyti vokiečių slaptus kodus.

buvo užkoduoti žemėlapiai ir vokiečių povandeniniuose laivuose Atlanto vandenyne naudotos kodų knygos.

Antrojo pasaulinio karo pabaigoje Amerikos jūrų laivynas įvykdė žygdarbį, po kurio sužinojome apie gautus priešo kodus ir šifrus. Tai buvo ne atsitiktinumas, o gerai pavykęs kruopštus planas. 1944 metų birželio 4 dieną Jungtinių Valstijų jūrų laivynas, kuriam vadovavo kontradmirolas Danielis V. Gallery'is, ties Prancūzijos valdomais Vakarų Afrikos krantais užgrobė nepažeistą vokiečių povandeninį laivą U-505.

Vykstant Antrajam pasauliniam karui, sąjungininkai sunaikino daugiau nei septynis šimtus vokiečių povandeninių laivų. U-505, kuris šiuo metu eksponuojamas Čikagos mokslo ir pramonės muziejuje, buvo vienintelis, kurį pavyko ištempti į krantą nepažeistą. Vokietijos povandeninių laivų įgula, jei būdavo priversta iškilti į paviršių ir pasiduoti, turėjo užtikrinti,

kad po įgulos išsilaipinimo povandeninis laivas nuskęs. Tačiau šiuo atveju kruopščiai parengta admirolo D. V. Gallery'o grupė sugebėjo įlipti į U-505 kaip tik tuo metu, kai atidariusi sklendes įgula ruošėsi jį palikti. Rizikuodami gyvybėmis ir nežinodami, kiek sekundžių liko iki paskutinio povandeninio laivo panirimo, dešimt vyrų iš Amerikos jūrų laivyno įlaipinimo grupės užvėrė liuką ir paskutinę minutę uždarė vožtuvus. Vėliau išsigelbėti jiems padėjo vokiečių jūrininkas. Jis buvo iššokęs už borto ir plaukė greta skęstančio povandeninio laivo, kai įlaipinimo grupės narys įtraukė jį atgal ir privertė atskleisti stebėjimo bokštelio, kuris buvo įtrauktas į amerikiečių išsigelbėjimo maršrutą, veikimo principą. Įmesdami jį atgal į vandenį, grupės nariai tylomis dėkojo, bet netrukus jam ir kitiems vokiečių įgulos nariams suteikta pagalba.

Visi povandeniniame laive buvę įrašai, bylos ir techninė įranga, įskaitant kodus ir šifrus, buvo išgelbėti, o povandeninis laivas saugiai nutemptas į Bermudus.

Bet istorija tuo nesibaigia. Jei naciai būtų sužinoję, kad povandeninis laivas nenuskendo ir nebuvo sunaikintas, tuomet būtų supratę, kad laive buvę kodai ir šifrai paimti, ir niekada daugiau jų nenaudoję. Keli tūkstančiai operacijoje dalyvavusių Amerikos jūrų laivyno darbuotojų žinojo faktus, ir daugeliui tai buvo puiki karo laikų istorija. Priversti šiuos jūreivius suvokti, kad užgrobimą gyvybiškai svarbu laikyti paslaptyje buvo dar sunkiau nei užgrobti patį povandeninį laivą. Bet tai sėkmingai pavyko. Vokiečiai tikėjo, kad laivas palaidotas jūroje kartu su paslaptimis, kurios mums puikiai pasitarnavo.*

Tačiau karinės operacijos, vykdomos iššifruotų kodų pagrindu, dažnai priešininkui kelia įtarimų. Kai vykstant Pirmajam pasauliniam karui vokiečiai pastebėjo, kad jų povandeniniai laivai apsupami stebėtinai dažnai, nesunkiai nuspėjo, jog jų povandeniniam laivynui skirti pranešimai skaitomi. Tad visi kodai nedelsiant pakeisti. Todėl visada kyla klausimas, kaip elgtis su tokiu būdu įgyta informacija. Siekiant greitos karinės ar diplomatinės naudos galima rizikuoti prarasti naudingą šaltinį, arba galima susilaikyti ir kaupti žinias apie priešo manevrus bei veiksmus, ir taip vėliau jam būtų padaryta maksimali žala.

---

* Pasakojimas apie šį jūrų laivyno žygdarbį aprašytas Daniel'io V. Gallery'io „*Twenty Billion Tons Under the Sea*“ (Čikaga: Henry Regnery Co., 1954).

Amerikiečių jūreiviai pozuoja ant užgrobto vokiečių povandeninio laivo U-505.

Dažniausiai siekiama išsaugoti tikrąjį šaltinį, kuo ilgiau juo naudotis ir pateikti priešui klaidingų žinių, kad reikiama informacija buvo gauta iš kitur. Kartais nesiimama priešininkui nuostolingų operacijų, jei taip šis sužinotų, kad jo pranešimai skaitomi.

Pirmojo pasaulinio karo metais pirmasis rimtas amerikiečių kriptoanalitinis sumanymas pradėtas įgyvendinti vadovaujant Karo departamentui. Oficialiai vadinamas Karinės žvalgybos 8-uoju skyriumi, jis mėgdavo pasivadinti „Juoduoju kambariu“ – šį pavadinimą ilgus šimtmečius naudojo didžiausių Europos valstybių pašto cenzūros slaptieji organai. Pradėjusi nuo nulio, buvusio telegrafo operatoriaus Herberto Yardley‘aus vadovaujama genialių mėgėjų grupė iki 1918 metų tapo aukščiausios

klasės profesionalų organizuota grupe. Po Pirmojo pasaulinio karo vienas didžiausių jos pasiekimų buvo Japonijos diplomatinių kodų iššifravimas. 1921 metais Vašingtono konferencijoje vykusių derybų metu Jungtinės Valstijos labai norėjo susitarti su japonais dėl 10:6 jūrų laivyno proporcijos. Japonai atvyko į konferenciją, iš anksto tikėdamiesi išlaikyti 10:7 koeficientą. Diplomatijoje, kaip ir visose kitose derybose, turite milžinišką persvarą, jei žinote, kad reikalui esant jūsų oponentas yra pasirengęs nusileisti. „Juodasis kambarys“ iššifravo tarp Vašingtono ir Tokijo vykusius japonų diplomatinius susirašinėjimus ir pateikė informaciją mūsų vyriausybei, kad jei tvirtai laikysimės pozicijos – japonai sutiks. Todėl šiuo klausimu galėjome laikytis savo pozicijos nerizikuodami sužlugdyti konferencijos.

„Juodasis kambarys“ dirbo daugiausia Valstybės departamentui iki 1929 metų, kai sekretorius Stimsonas nebeleido departamentui naudotis jo paslaugomis. Stimsono biografas McGeorge‘as Bundy‘is pateikia tokį paaiškinimą:

> „Užsienio politikoje Stimsonas laikėsi principo visada remtis asmeniniais ryšiais, kitaip tariant, jis manė, kad norint užsitikrinti asmenų patikimumą, reikia jais pasitikėti. Vadovaudamasis šiuo principu, jis priėmė sprendimą, dėl kurio vėliau buvo rimtai kritikuojamas – uždarė vadinamąjį Juodąjį kambarį. Šio veiksmo jis niekada nesigailėjo. Stimsonas, kaip valstybės sekretorius, džentelmeniškai elgėsi su džentelmenais, kuriuos draugiškos tautos buvo atsiuntusios kaip ambasadorius ir ministrus.“*

Laimei, mūsų kariuomenė ir jūrų laivynas vis dar sprendė kriptoanalizės problemas, skirdami didelį dėmesį Japonijai, kadangi tuo metu Amerikos karininkai numatė, kad Japonija bus pagrindinis potencialus Jungtinių Valstijų priešas bet kokiame artėjančiame kare. Iki 1941-ųjų, tai yra Perl Harboro metų, mūsų kriptoanalitikai buvo iššifravę daugelį svarbių Japonijos jūrų laivyno bei diplomatinių kodų ir šifrų. Todėl dažniausiai žinodavome apie planuojamus Japonijos veiksmus Ramiajame vandenyne dar iki jų pradžios.

---

* Henry L. Stimson ir McGeorge Bundy „On Active Service in Peace and War“ (Niujorkas: Harper&Brothers, 1948).

1942 metų birželį įvykęs Midvėjaus mūšis – jūrų laivyno karo Ramiajame vandenyne lūžis – buvo kova, kurios mes laukėme, nes iššifravę pranešimus sužinojome, kad didžiausios Japonijos imperatoriškojo jūrų laivyno pajėgos rinkosi Midvėjuje. Turėdami žvalgybinės informacijos apie priešo pajėgų galią ir išdėstymą, galėjome juos nustebinti netikėtais jūrų laivyno veiksmais.

Po Perl Harboro susidūrėme su specifine problema – kaip nuslėpti, kad skaitome japonų kodus. Tyrimai, kaltinimai, kerštо troškimas dėl baisių amerikiečių praradimų kėlė šiam „stebuklui" grėsmę ir susirūpinimą, kad nesužinotų visuomenė ir neatskleistų paslapties japonams. Kol vandenyne neturėjome tinkamo karinio jūrų laivyno, kovoje su Japonija vienas iš nedaugelio mūsų turėtų pranašumų buvo gebėjimas skaityti japonų pranešimus. Pasitaikė keli atsitiktiniai nutekėjimai, bet nebuvo jokių jų neginčijamų įrodymų.

1944 metais Thomasas E. Dewey'is, kuris prezidento rinkimuose kovėsi su F. D. Rooseveltu, kaip ir daugelis federacinei vyriausybei artimų žmonių, sužinojo, kad skaitome japonų kodus, tačiau iki Perl Harboro mes nesugebėjome pasinaudoti turima informacija. Baimintasi, kad Thomasas E. Dewey'is apie tai prabils savo rinkimų kampanijoje. Vos pagalvoję apie tokią grėsmę Generalinio štabo vadai tirtėdavo iš baimės. Tuomet pats generolas Marshalas parašė asmeninį laišką Dewey'ui, kuriame nurodė, kad japonai iki šiol nežino, jog esame nulaužę kodus, o skaitydami jų pranešimus skiname karines pergales. Dewey'is niekada neužsiminė apie sėkmingą japonų šnipinėjimą. Paslaptis buvo išsaugota.

Vienas įspūdingiausių ėjimų ryšių kanalų žvalgyboje padarytas 1917 metų sausį, kai Jungtinės Valstijos buvo ant Pirmojo pasaulinio karo slenksčio: britai iššifravo vadinamąją Cimermano telegramą.* Darbą atliko „40 kambario", t. y. britų karinio jūrų laivyno kriptoanalizės štabo ekspertai. Pranešimą Vokietijos pasiuntiniui į Meksiką iš Berlyno išsiuntė Vokietijos užsienio reikalų sekretorius Cimermanas. Jame nurodytas planas 1917 metų vasarį atnaujinti povandeninių laivų karą, nes taip būtų galima priversti Jungtines Valstijas kariauti, ir būtina Meksikai pasiūlyti įsitraukti į karą kartu su Vokietija, o po pergalės atgauti „prarastas teritorijas Teksase, Naujojoje Meksikoje ir Arizonoje".

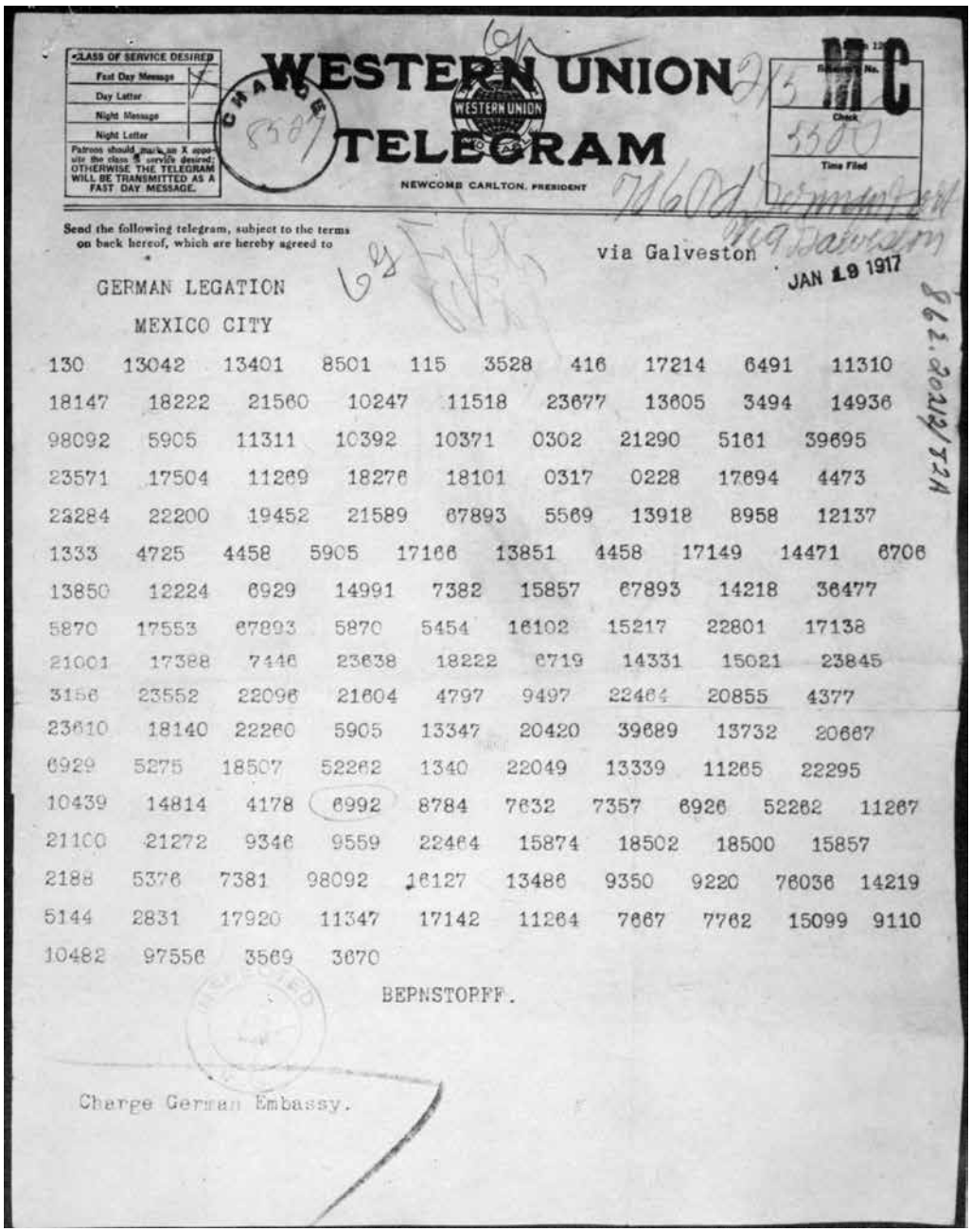
---

* Pasakojimas pateikiamas Barbaros Tuchman knygoje. Žr. bibliografiją.

Legendinis britų jūrų laivyno žvalgybos vadas admirolas Hallas laikė šį pranešimą rankose daugiau nei mėnesį. Jis galvojo, kaip perduoti iššifruotą pranešimo turinį amerikiečiams, kad šie patikėtų jo autentiškumu, o vokiečiai nesužinotų, kad britai skaito jų kodus. Galiausiai britų užsienio reikalų sekretorius lordas Balfouras oficialiai perdavė Cimermano pranešimą Amerikos ambasadoriui Londone. Jis tapo sensacija Baltuosiuose rūmuose ir Valstybės departamente bei sukėlė rimtų problemų mūsų vyriausybei – kaip patikrinti pranešimo tikrumą ir tinkamai paskelbti, kad visuomenė nemanytų, jog tokiu būdu anglai ir amerikiečiai siekia įtraukti Jungtines Valstijas į karą. Mano dėdė Robertas Lasingas, kuris tuo metu ėjo valstybės sekretoriaus pareigas, vėliau man pasakojo apie kelias dienas vykusius dramatiškus įvykius, priartinusius Ameriką prie karinių veiksmų.

Situaciją apsunkino tai, kad vokiečiai naudojosi Amerikos diplomatinėmis ryšio priemonėmis perduoti pranešimą ambasadoriui grafui Bernstorffui. Pats ambasadorius tą patvirtino kolegai Meksike. Prezidentas Wilsonas leido vokiečiams naudotis mūsų tarpatlantinėmis ryšių priemonėmis su sąlyga, kad tokiuose pranešimuose bus teikiami taikos pasiūlymai – jais Wilsonas buvo suinteresuotas.

Prezidento nusivylimas buvo dar didesnis, kai suprato, kokiems tikslams vokiečiai naudojosi jo kanceliarija. Bet paaiškėjo, kad ši keista situacija labai naudinga. Buvo galima teigti, kad Valstybės departamentas turėjo užkoduotos Cimermano telegramos kopiją, kurią persiuntė Bernstorffui, nežinodamas kurstomojo turinio. Užkoduotas tekstas buvo aptiktas ir persiųstas ambasadai Londone, kur kažkuris admirolo Hallo pavaldinys jį iššifravo ambasados atstovo akivaizdoje, todėl abejonių dėl turinio autentiškumo nekilo. Iššifruotos telegramos kopijas vokiečių diplomatai matė ir Vašingtone, ir Meksike, o tai mums padėjo išspręsti svarbią problemą, kuri sukėlė tiek daug rūpesčių admirolui Hallui, t. y. kaip apkvailinti vokiečius, kad šie nesuprastų, kaip iš tiesų gavome šią informaciją. Galiausiai vokiečiai patikėjo, kad pranešimas nutekintas dėl neatsargumo ar pavogtas kažkurioje Vokietijos ambasadoje ar biure Meksike. Jie ir toliau naudojo tuos pačius kodus, parodydami mums naudingą savo vaizduotės trūkumą. 1917 metų kovą Valstybės departamentas atskleidė telegramos turinį „Associate Press“ agentūrai. Amerikos visuomenėje kilo šurmulys. O balandį paskelbėme karą Vokietijai.



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter
Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

CHARGE 8307

Check 3300

Time Filed

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

Britų perimtas slaptas Cimermano pranešimas tapo lemiamu veiksniu, paskatinusiu JAV stoti į Pirmąjį pasaulinį karą.

Lyginant šiais laikais naudojamas kriptografijos sistemas su Pirmojo pasaulinio karo sistemomis, kurias pasitelkusios vyriausybės siuntė svarbiausias ir didžiausias paslaptis, pastarosios atrodo mėgėjiškos dėl pasikartojančių simbolių grupių, kurios kriptoanalitikui atskleisdavo, kad už simbolių slepiasi svarbus ar dažnai vartojamas žodis. Kai admirolo Hallo kriptoanalitikai Cimermano telegramoje pamatė kombinaciją „67893“, ją atpažino ir suprato, kad ši reiškia „Meksiką“. Vokiečių sistemoje šios kombinacijos reikšmė niekada nekito. Šiais laikais tokia šifrų grupė niekada nepakeistų to paties žodžio daugiau nei vieną kartą.

Dabar visi oficialūs vyriausybės pranešimai rašomi ir šnipų komunikacija vykdoma pasitelkiant saugias ir sudėtingas kriptografines sistemas. Pavyzdžiui, siųsdami informaciją į Maskvą, sovietų agentai naudoja labai sudėtingus šifrus. Šioje ir kitose srityse tobulėjant gynybos priemonėms, tobulėja ir atsakomieji veiksmai.