Од тајни до криптоанализе

Др *Светозар Радишић*, пуковник

(Приказ књига Александра Трифонија *Чудесни свет шифара, Разбијањем шифара до истине* и *Обавештајне службе и прислушкивање*[*])

Ретки су људи који нису заинтересовани за тајне, њихову заштиту и начине досезања туђих тајни. То је довољан разлог за знатижељу и тежњу да се сазна шта се крије иза наслова као што су *Чудесни свет шифара*, *Разбијањем шифара до истине* и *Обавештајне службе и прислушкивање*. Вероватно би се наведене књиге читале као и све друге да већ на почетку књиге *Чудесни свет шифара* није наведена мисао француског дипломате Блеза Вижнера (1523–1596), који је сматрао да је све шифра, па и сама природа. Та мисао наводи читаоца да покуша, читајући наведене књиге Александра Трифонија, да живот посматра кроз призму одгонетке света шифара. Дакле, нешто другачије него што нуде класичне научно засноване књиге. Међутим, без обзира на то из којег се света приступа књигама Александра Трифонија и са којом животном мапом се сравњују знања из њих, те књиге садрже нешто ново за сваког читаоца.

Књиге из едиције *Шифре и прислушкивање* треба прочитати из више разлога: 1) зато што су својеврстан уџбеник о обавештајним службама и заштити тајни и нека врста мале енциклопедије; 2) зато што је Александар Трифони приближио јавности једну од најчувени-

[*] Аутор тротомне едиције *Шифре и прислушкивање* Александар Трифони, дипломирани математичар, најпознатији је криптолог на јужнословенском простору. Свој радни век посветио је проучавању шифара, заштити тајности и истинама које се крију у „свету тајни". Објављивањем више стручних и научних радова из области криптологије допринео је популаризацији и бољем научном разумевању те области. Добитник је награде „22. децембар" (1977) за научноистраживачки рад у области војне теорије и праксе. Едицију *Шифре и прислушкивање* издала је „ИДА-М", из Београда, 2001. године.

јих „табу-тема"; 3) аутор је доказани зналац у области криптологије; 4) реч је о теми која је од увек актуелна; 5) боље ће се разумети историја ратовања, али и нове мегатенденције и тзв. нови светски поредак итд.

Помисао на шифре и прислушкивање побуђује машту и читаоце упућује у тајанствени свет у којем су у „врзино коло" ухваћени тајна, заштита тајности, прислушкивање, обавештајне службе и дешифровање у трагању за истином (филмске приче о том свету имају најбројнију и највернију публику). Када читалац само прелиста садржаје књига А. Трифонија стиче утисак да је наишао на зналца који показује да су му блиски и теорија и пракса у области криптологије. Из међунаслова се може много научити и о ауторовим истраживањима. Импресивно је што је професор Трифони користио и литературу о криптографији, која, очевидно, омашком није регистрована ни у веома значајној и вредној Југословенској војној библиографији (1748–1918), у издању Центра за војнонаучну документацију и информације. Наиме, Трифони у богатој коришћеној литератури наводи дело Николе Ј. Дерока, под насловом *Војна криптографија или шифровање и дешифровање депеша*, које је објављено у „Ратнику" у септембру 1905. године, иако је Дерок у наведеној библиографији представљен само једном: као аутор књиге *Пројекат нове сигнализације* из 1907. године. Слично је и са делима Ђорђа Вујића, који се као аутор у наведеној библиографији не помиње, а Александар Трифони је користио следеће његове написе, објављене у војном листу „Ратник": „О криптографији" (јули 1925), „Криптографија у прошлости и садашњости" (јули–август 1926) и „Још нешто о криптографији" (мај 1927). Чини се да је то довољан доказ за ауторов одговоран и студиозан приступ теорији криптологије.

Аутор показује да подједнако добро познаје историјат криптологије и најновија техничка и технолошка постигнућа и решења у тој области. У наведеним књигама описао је све што је сматрао значајнијим – од првих тајни до савремених злоупотреба Интернета, сателита и система као што су „Сигинт" и „Ешелон". Наслови у књигама подсећају на ниску криптолошких бисера: „Шифре чувари тајни", „Почетак криптографије", „Допринос математичара развоју криптографије", „Пет великана француске криптографије", „Кодне таблице и кодови", „Шифровање говора и слике", „Шифре и математика", „Декриптери нису шпијуни", „Афера Драјфус", „Криптографија", „Операција 'Ултра'", „Српски језик као предмет статистичког проучавања", „Обавештајне службе", „Агентурне шифре", „Прислушкивање", „Летеће шпијунске лабораторије", „Стенице", „Ешелон" итд. О сваком наслову аутор би, очевидно, могао да напише књигу. Али, написао је уџбеник из којег сви који знају да читају, без обзира на образовање, могу да науче суштину заштите тајности и основе информационог рата.

У књизи *Чудесни свет шифара* аутор дефинише основне појмове из криптологије и скида вео мистификације, укида „привилегије" одређених људи из обавештајне струке, разоткрива табу-теме у вези са шифровањем и декриптовањем и описује историјат заштите тајних података и информација. Историјат шифрованих порука Трифони је започео описом једне „шифрантске досетке" извесног Хистаја, с краја 5. века п. н. е., који је на глави свог роба записао поруку коју је роб, када му је коса довољно порасла, пренео до Аристагоре, тиранина из Милета. У тој књизи аутор наводи и вечне дилеме везане за криптологију. На пример, у време витешког, отменог и племенитог понашања Роберт Лансинг и Хенри Стимсон, амерички министри иностраних послова, били су противници увођења декриптерске службе „јер џентлмени не читају туђе поруке". У књизи су описани прва осмишљена шифра „Скитале", којом су се служили Лакедемонци, шифре Гаја Јулија Цезара, развој теорије о шифрама, њени оснивачи, као што су Енеја Тактичар, Роџер Бекон, Џефри Чосер, Леон Батиста Алберти, Јоан Батиста Порта, Гироламо Кардано, Ђовани Сестри, Јакоп Силвестри итд. Сви наведени начини шифровања изузетно су занимљиви и поучни, побуђују машту и подстицајни су за креативну визуелизацију.

Читањем књиге *Разбијањем шифре до истине* стиже се, у имагинацији, у „свет шпијунаже". Аутор почиње књигу преводом „Расправе о шифри" Леона Батисте Албертија, из 1568. године – рукописом који се чува у Ватикану. После цитата, Трифони закључује: „'Расправа о шифри' је актуелна и данас, јер свако ко жели да научи тајне декриптирања мора усвојити запажања и закључке које излаже Алберти". Према Трифонијевим истраживањима, највећи мајстори дешифровања били су математичари, попут Џона Волиса, и за декриптовање школовани ентузијасти, фанатици, као што је био Херберт Јардли. Све тајанствене методе шифровања, описане у првој књизи, имају одговарајуће, правовремено или са закашњењем откривене методе дешифровања које је аутор објавио у другој књизи едиције *Шифре и прислушкивање*. Посебни бисери објављени у књизи *Разбијањем шифара до истине* јесу примери дешифровања у операцијама *Ultra* и *Magic*, затим криптографија у Србији и приказ могућности (де)шифровања у савременим рачунарским мрежама.

Књига *Обавештајне службе и прислушкивање* може да се прикаже са неколико занимљивих навода. Онима који инсистирају на отвореном друштву и боре се против затворености обавештајних служби и служби безбедности, према приговору сопствене или нечије савести, аутор је дао прилику да размисле о будућности своје државе у реалном амбијенту, у којем је један од директора ЦИА (Џон Дојч) отворено, у два наврата, 24. фебруара и 21. јула 1996, изјавио: „ЦИА има право да не узме у обзир забрану злоупотребе новинарске професије у изузетно осетљивим случајевима, па да ангажује професионал-

ног новинара као агента, или да одобри професионалном обавештајцу да се званично представља као новинар. Исти принцип може се применити и на припаднике мировних мисија и – свештенство".

Александар Трифони је записао: „У годинама уочи Другог светског рата није се знало ко има више посла, МИ5 или МИ6. МИ5 се борио са све већим бројем немачких шпијуна који су на британска острва просто надирали као туристи, трговци или дописници разних листова... Прослављена 'Соба 40' поред декриптовања ухваћених шифрованих телеграма била је преплављена писмима проблематичне садржине или наизглед безазленог садржаја испод кога је невидљивим мастилом била исписивана тајна порука. МИ6 је прикупљао информације које су слале британске амбасаде и шпијуни широм земаљске кугле...".

Следећи цитат свима је јасан: „Према тврђењима стручњака и произвођача НСА је успела да угради, у све верзије оперативних система *Windows,* посебне кодове приступа. Поставља се питање коме то све треба!? Одговор је једноставан – Сједињеним Америчким Државама... НСА одређује норме фирмама које производе уређаје за шифровање без обзира да ли су америчке или неких других држава. Уколико се не прихвате те норме, те фирме бивају искључене са дела тржишта које контролишу САД, а то значи више од три четвртине светског тржишта...".

О дометима прислушкивања, које званично није дозвољено сем у неким случајевима, може се закључити из следећег цитата: „У садашње време и ласерима се може прислушкивати. Ласерски зрак се, на пример, усмери на стакло прозора просторије из које се жели чути разговор. Вибрације стакла, узроковане разговором, 'хвата' осетљиви ласерски пријемник, а затим их претвара у разумљив говор".

Свет у којем живимо може да се посматра и кроз визуру техничких и технолошких могућности на почетку трећег миленијума: „НСА је патентирала нову технологију која омогућава једновремено прислушкивање милиона међународних и домаћих телефонских разговора. Патент је регистрован под бројем 5937422, а патентно право је добијено 10. августа 1999... Вест о глобалном прислушкивању стигла је до парламентараца... ". Међутим, креатори стављања свега под контролу сетили су се нове формуле: „прислушкивање и пресретање информација је оправдано, јер је намењено борби против тероризма, спречавању корупције, трговине дрогом и оружјем и друго".

Многима се чини да живимо у контролисаном свету, препуном мистике и шифара, а у књигама Александра Трифонија *Чудесни свет шифара, Разбијањем шифара до истине* и *Обавештајне службе и прислушкивање* та димензија живота је верно описана, поједностављена, одгонетнута и приближена обичним људима.