BEZPEČNOSTNÉHO POVEDOMIE V KONTEXTE BOJA PROTI NOVODOBÝM BEZPEČNOSTNÝM HROZBÁM

SECURITY AWARENESS IN THE CONTEXT OF COMBATING MODERN-DAY SECURITY THREATS

Miroslav Brvnišťan[1]

ABSTRACT

The article highlights the need for changes in the approach to the status of an individual in the security system of the State. The importance of understanding this relationship is to be seen especially in the context of new security threats and the dynamic nature of the security environment. Technical and technological developments enable individuals to affect the safety and security system in an unprecedented way. It is necessary that at the state level will be taken appropriate measures. As one of the measures we consider building an adequate security awareness of individual.

Key words:

security awareness, modern-day risks, security education, new models of security measures, security culture.

Úvod

Moderná a dynamická doba prináša nové pohľady na bezpečné fungovanie štátu. Mení sa zaužívané vnímanie bezpečnosti spoločnosťou a jednotlivcami. Bezpečnosť nadobúda nové rozmery súvisiace najmä s technickým a technologickým rozvojom. Moderné technológie menia a nanovo definujú možnosti zaužívaných bezpečnostných nástrojov a opatrení a súčasne kreujú nové. Mení sa postavenie jednotlivca, a to nielen vo vzťahu k individuálnej bezpečnosti (zodpovednosť za vlastnú bezpečnosť), ale najmä vo vzťahu k bezpečnosti spoločnosti a štátu. Jednotlivec, bez ohľadu na svoje postavenie v spoločnosti, pravdepodobne nikdy nemal také možnosnosti ovplyvniť svojím konaním celkovú bezpečnosť spoločnosti, rôznych subjektov, štátov alebo aj nadnárodných zoskupení. Situáciu podmieňujú aj zmeny vo význame chápania hraníc štátov. Bezpečnosť sa stáva globálnou, a preto je potrebné čoraz viac hľadať také riešenia, ktoré nie sú viazané hranicami štátov. Hranice štátov sa stávajú čoraz viac obmedzujúcimi a limitujúcimi. Týka sa to aj

[1]Miroslav Brvnišťan, JUDr. PhD., Akadémia Policajného zboru v Bratislave , Sklabinská č.1, 835 17 Bratislava 35, Slovenská republika, Tel.:+421 910 57423, brvnistan@yahoo.com.

bezpečnostných opatrení, ktorých vynutiteľnosť spravidla nepresahuje hranice štátov, tzv.teritoriálna pôsobnosť. Možný dosah zmien bezpečnostného systému súvisiacich s vývojom a zmenami bezpečnostných rizík vytvára tlak na nové definovanie bezpečnosti jednotlivca, vrátane nových možností jej zabezpečenia. Bezpečnosť sa stáva v kontexte technologického rozvoja komplexnejšou. Nejedná sa len o charakter reakcie bezpečnostného systému na aktuálne bezpečnostné hrozby, ale čoraz viac aj o spôsob zapojenia čo najširších vrstiev spoločnosti do realizácie potrebných zmien a opatrení. Čoraz viac sa bude zohľadňovať individuálna zodpovednosť jednolivcov a ich možností svojim konaním a správaním ovplyvňovať bezpečnosť. Štát sa nachádza v situácii, kedy bude potrebné zohľadniť zmienené aspekty vývoja bezpečnosti a bezpečnostných hrozieb v procese redefinovania postavenia a vzťahu jednotlivca k bezpečnosti a bezpečnostnému systému. Jedným z riešení je aj zavedenie nových prístupov k bezpečnostnému vzdelávaniu jednotlivcov a budovaniu ich bezpečnostného povedomia.

Bezpečnostné povedomie ako integrálna súčasť bezpečnostného systému

Miesto bezpečnostného povedomia jednotlivca ako relevantnej súčasti bezpečnostného systému štátu (podľa nášho názoru platí aj pre iné subjekty - obchodné spoločnosti, organizácie) je odvoditeľné v tom najširšom význame prostredníctvom ľudského faktora. Vychádzame pritom z predpokladu, že účasť jednotlivcov a ich angažovanosť v bezpečnostnom systéme je nespochybniteľná, jednotlivci sú integrálnou súčasťou bezpečnostného systému. Sú nositeľmi adresných úloh a zodpovedností v závislosti napr. od ich spoločenského postavenia, pracovného zaradenia alebo oblasti pôsobenia. To, či sa títo jednotlivci podieľajú na plnení riadiacich, výkonných alebo čiastkových úloh je podľa nášho názoru irelevantné z hľadiska nutnosti ich bezpečnostného vzdelávania a budovania ich bezpečnostného povedomia. Bez adekvátneho bezpečnostného povedomia nebudú jednotlivci schopní plniť stanovené úlohy, čím môže dôjsť k ohrozeniu bezpečnostného systému.

Z pohľadu bezpečnostného systému a jeho vzťahu k jednotlivcovi je situácia zložitejšia. Na niektoré širšie súvislosti sa pokúsime ďalej poukázať. Jednotlivec je bezpochyby účasníkom všetkých relevantných vzťahov v rámci bezpečnostného systému a jeho primerané bezpečnostné povedomie tu zohráva kľúčovú rolu. Niektoré dôsledky chýbajúceho bezpečnostného vzdelania a primeraného bezpečnostného povedomia sú evidentné. Pri predpokladanom správnom fungovaní bezpečnostného systému by mal exitovať explicitný (priamy) vzťah medzi zistenými aktuálnymi bezpečnostnými rizikami a realizovanými opatreniami. Tieto by mali byť realizované čo najskôr s ohľadom na možné negatívne dopady a škody. Do uvedeného vzťahu však vstupuje z úrovne bezpečnostného systému spravidla viacero “externých” faktorov.

Za jeden z najvýraznejších považujeme ignorovanie úlohy riadiacich a strategických dokumentov pre riadenie a systematický rozvoj bezpečnostného systému štátu a jeho nahrádzanie ad-hoc rozhodnutiami, často bez ohľadu na aktuálnu bezpečnostnú situáciu alebo udržateľnosť. Neaktuálnosť strategických dokumentov[2] podporuje celkový chaotický stav v rozvoji budovania bezpečnostného systému. Situácia je o to zložitejšia, ak dochádza k nesúladu strategických dokumentov SR a strategických dokumentov schvaľovaných v rámci nadnárodných integračných zoskupení - Severoatlantickej aliancie (ďalej len "NATO") a Európskej únie (ďalej len "EÚ"). Uvedený stav len poukazuje na fakt, že štát zlyháva pri realizácii systematického rozvoja bezpečnostného systému a jeho riadenia. Takýto stav by nemal byť všeobecne akceptovaný i keď veľmi rozšírená argumentácia typu "nič sa nestalo" je čoraz viac zaužívaná, ako vysvetlenie dôvodov prečo nie je potrebné daný stav systematicky meniť. Ak by sme uvedené akceptovali, mohli by sme jednoducho konštatovať, že dynamika bezpečnostných hrozieb je relatívne nemenná (resp. mení sa veľmi pomaly), a teda nie je potrebná žiadna nová reakcia bezpečnostného systému. Z hľadiska identifikácie nových bezpečnostných hrozieb je následne možné uviesť, že ak bezpečnostný systém negeneruje poznatky a informácie o nových bezpečnostných rizikách zrejme je všetko v poriadku a opätovne nie je potrebné nič meniť. Takýto stav však nepovažujeme za akceptovateľný, a to najmä nie v situácii, kedy je zrejmé, že je potrebné systémovo reagovať na nové bezpečnostné hrozby akými sú napr. asymetrické vedenie boja, informačná vojna, kybernetická vojna a iné. Na nové bezpečnostné hrozby je potrebné reagovať vytvorením nových bezpečnostných nástrojov. Rýchlosť reakcie bezpečnostného systému priamo podmieňuje konečnú efektívnosť realizovaných opatrení. Ak štát nie je schopný zabezpečiť rozvoj bezpečnostného systému v situácií relatívne nemenných bezpečnostných hozieb ako zvládne situáciu v kontexte prebiehajúcich konfliktov napr. na Ukrajine alebo v Sírii, kde dochádza k využívaniu moderných nástrojov a spôsobov vedenia boja ako informačná vojna a kybernetické útoky? Dochádza tu k využívaniu neštandardných prostriedkov a nástrojov s dôrazom na využívanie, resp. zneužívanie informácií. Informačná vojna vedená za využitia moderných a sofistikovaných technických a technologických nástrojov a vojna prebiehajúca v kybernetickom prostredí sú už viac ako integrálnou súčasťou moderného vedenia boja. Na základe dostupných informácií je možné konštatovať, že štandardné, zaužívané spôsoby riadenia bezpečnosti a bezpečnostného systému nie sú efektívne. Vysporiadať sa s uvedenými fenoménmi by malo byť cieľom koordinovaných aktivít bezpečnostných zložiek štátu. To, že štát nereaguje primerane na riadiacej a koncepčnej úrovni a ani na operačnej, je zrejmé. Môže byť riešením tejto situácie bezpečnostné vzdelávanie a budovanie bezpečnostného povedomia jednotlivcov ?

[2] Bezpečnostná stratégia SR bola schválená v roku 2005-pozn. autora.

Niektoré aspekty bezpečnostného vzdelávania a budovania bezpečnostného povedomia

Dôležitosť budovania bezpečnostného povedomia nám potvrdzuje aktuálna bezpečnostná situácia, nové bezpečnostné hrozby a riziká. Zmeny bezpečnostného prostredia zohrávajú priamu rolu nielen vo vzťahu k štátu a jeho bezpečnostnému systému. Čoraz viac je zrejmé, že niektoré aktuálne hrozby, napr. sofistikované spôsoby vedenia boja sú zamerané širokospektrálne a masovo, s dôrazom na využívanie technických a technologických výdobytkov ľudstva. Takými sú napr. internet, mobilná komunikácia, sociálne siete, dostupnosť šifrovania, možnosti monitorovania pohybu osôb a ich komunikácie, rýchlosť a kapacita prenosu dát. Je nesporné, že čoraz viac sa integrálnou súčasťou moderného vedenia boja stáva jednotlivec, ako základný stavebný prvok spoločnosti, systému proti ktorému je samotný boj vedený. Často nejde len o jednotlivcov priamo zaangažovaných na bojových operáciách, práve naopak, prostredníctvom využívania psychologických nástrojov ako súčasti vedenia boja sa ovplyvňujú široké masy (verejnosť) za účelom získaniea náklonnosti verejnej mienky a tým nepriamo dosiahnutia požadovaného cieľa. Jednolivec môže byť cieľom nielen ako priama (aktívna alebo pasívna) súčasť bezpečnostného systému (napr. vojak, riaditeľ, veliteľ), ale aj ako nepriama (napr. verejnosť).

Možnosti využívania alebo zneužívania jednotlivcov z hľadiska dosahovania stanovených cieľov tým však nie sú zdaľeka vyčerpané. Jednotlivec môže byť aj prostriedkom alebo nástrojom na dosiahnutie cieľa. Útoky na jednotlivcov (napr. prostredníctvom sociálnych sietí, sociálne inžinierstvo) môžu byť zamerané na zmenu a formovanie jeho postojov, viery alebo názorov, získavanie podporných informácií alebo údajov, čím môže dochádzať k dosahovaniu stanovených cieľov (požadovaného správania) v rôznych skupinách obyvateľov, širšej spoločnosti alebo štátoch. Takéto útoky sú spravidla veľmi sofistikované a realizované skrytým spôsobom, pre jednotlivca ťažko odhaliteľným - napr. prostredníctvom cieľených web stránok poskytujúcich "pravdivé" informácie k prebiehajúcim konfliktom[3]. Jednotlivec sa stáva "ľahkou obeťou". Dochádza však aj k útokom a následnému zneužívaniu individuálnych technických prostriedkov jednotlivcov - počítačov, komunikačných mobilných zariadení alebo iných technických zariadení. Tieto zariadenia sú využívané na realizovanie rôznych, často nezákonných aktivít

[3] V súčasnosti bolo podľa rôznych verejných zdrojov identifikovaných približne 40 web stránok poskytujúcich skreslené alebo cielene zamerané informácie, týkajúce sa vojnových konfliktov, rôznych konšpiračných teórií o politických cieľoch veľmocí a vojenských zoskupení. Pravdivosť tvrdení je často ťažko overiteľná a v kontexte množstva rôznorodých informácií dostupných jednotlivcom tieto poskytujú dostatočnú páku na spochybnenie spoločnosťou všeobecne akceptovaných informácií - pozn. autora.

napr. hromadných počítačových útokov[4], šírenie vírusov, získavanie informácií a ich následné zneužívanie, krádeže identity alebo korporátnych informácií. Špionáž je vo všeobecnosti zaužívaný termín na pomenovanie takýchto aktivít súvisiacich s cieleným zneužívaním technických a technologických prostriedkov a nástrojov za účelom získania informácií ako súčasť otvorených konfliktov alebo ako príprava na ne. Aká by v takýchto prípadoch mala byť úloha štátu?

Sme svedkami procesov, pri ktorých sa meniace bezpečnostné prostredie stáva výzvou, na ktorú je čoraz ťažšie nájsť odpoveď v rámci existujúcich bezpečnostných opatrení. Úloha jednotlivca zohráva a pravdepodobne bude zohrávať čoraz dôležitejšiu rolu pri eliminácii moderných bezpečnostných hrozieb. Jednotlivec bez ohľadu na jeho postavenie v bezpečnostnom systéme môže byť prínosom, ale aj enormným bezpečnostným rizikom.

Miesto bezpečnostného povedomia v bezpečnostnom systéme a jeho charakteristika

Vzťah medzi dynamikou bezpečnostného prostredia a možnosťami a schopnosťmi bezpečnostného systému eliminovať bezpečnostné hrozby a riziká bude podľa nášho názoru určujúcim pre hľadanie efektívneho riešenia. Jednou zo zavedených možností ako sa s uvedeným pokúsiť vo vzťahu k "ľudskému faktoru" vysporiadať, je rozvoj spôsobilostí bezpečnostného systému štátu zameraných na bezpečnostné preverenie a na správnu a rýchlu identifikáciu rizikových jednotlivcov (napr. bezpečnostné previerky podľa zákona č. 215/2004 Z.z. o ochrane utajovaných skutočností, preukazovanie bezúhonnosti podľa zákona č. 473/2005 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov). Je však takýto spôsob eliminácie bezpečnostných rizík vo vzťahu k jednotlivcom postačujúci? Bezpečnostné previerky jednotlivcov nie sú novodobý fenomén. Ich princíp je veľmi jednoduchý, založený na skutočnosti, že ak poznáme (predpokladáme) možné bezpečnostné riziká osôb, tak v procese previerky ich vo vzťahu ku konkrétnemu jednotlivcovi zisťujeme, posudzujeme a hodnotíme. Ak sa ich existencia potvrdí jednotlivec je rizikovým a sú prijaté náležité opatrenia. Obdobne pri prijímaní do zamestnania sa potencionálny zamestnanec preukazuje výpisom z registra trestov. Po jeho posúdení sa rozhodne či bude prijatý alebo nie. Už z podstaty uvedených procesov je zrejmé, že vo vzťahu k novým bezpečnostným hrozbám a ich dynamike je takýto postup nedostatočný. Takéto preverovacie procesy dokážu eliminovať stabilné /statické bezpečnostné hrozby a riziká, čomu zodpovedá aj časovo náročný proces preverovania. V súčasnom neustále sa meniacom bezpečnostnom prostredí sú

[4] Najčastejšie tzv. DDOS - Distributed Denial of Services - technika útoku na internetové služby, pri ktorej dochádza k zahlteniu serverov množstvom požiadaviek na komunikáciu, a tým k znefunkčneniu, nedostupnosti systému alebo služby, Výkladový slovník kybernetickej bezpečnosti, Policejní Akademie ČR v Praze, str. 33

však takéto procesy nedostatočné. Primerané bezpečnostné povedomie sa javí ako možný efektívny nástroj na elimináciu moderných bezpečnostných rizík. Jedným z dôvodov, ktorý poukazuje na dôležitosť bezpečnostného povedomia jednotlivcov je využívanie tohto nástroja v niektorých špecifických oblastiach bezpečnosti.

Pojem bezpečnostné povedomie je historicky najčastejšie spájané s informačnou bezpečnosťou, bezpečnosťou informačných systémov a bezpečnosťou informácií. V týchto oblastiach ide o proces zavedený s ohľadom na praktické skúsenosti či už súkromného alebo verejného sektora. Dôležitosť budovania bezpečnostného povedomia v týchto oblastiach podčiarkuje aj fakt, že napr. podľa prieskumu stavu informačnej bezpečnosti z roku 2004 bolo viac ako dve tretiny bezpečnostných incidentov zapríčinených zlyhaním ľudského faktora[5].

Bezpečnostné povedomie je v oblasti informačnej bezpečnosti definované ako: "Poznanie potreby ochrany informácie a informačnej a komunikačnej infraštruktúry, ako aj povinnosti osobne sa na nej podieľať[6]." Univerzálnejšia definícia bezpečnostného povedomia znie: "Uvedomenie si a postoj členov organizácie vo vzťahu k ochrane rôznych hodnôt organizácie" alebo "Dosiahnutie udržateľného postoja zamestnancov vo vzťahu k bezpečnosti a zároveň budovanie dôvery vo vlastnú organizáciu"[7]. **Mať príslušné bezpečnostné povedomie v súlade s týmito definíciami teda znamená, že jednotlivec: 1. Chápe podstatu bezpečnosti, 2. Uvedomuje si potencionálne hrozby, 3. Má vedomosť ako o tom ako hrozbám predchádzať, 4. V prípade, že takéto okolnosti nastanú vie ako reagovať.**

Špecificku oblasťou je systém ochrany utajovaných skutočností, ktorý síce priamo v zákone o ochrane utajovaných skutočností nepracuje s pojmom bezpečnostné povedomie no nahrádza ho poučením. Poučenie samotné nezodpovedá obsahovej a funkčnej náplni termínu bezpečnostné povedomie. No zároveň záväzné akty Európskej únie napr. Rozhodnutie Rady č. 2013/488/EÚ alebo Rozhodnutie Komisie č. 2015/444/EÚ, Euroatom v oblasti ochrany utajovaných informácií tento termín poznajú[8]. Je v nich už podrobnejšie rozpracované, čo je to bezpečnostné povedomie a čo má byť súčasťou bezpečnostného vzdelávania - napr. pravidelné oboznamovanie sa s aktuálnymi hrozbami, dôsledkami kompromitácie informácií, prostredníctvom uceleného programu bezpečnostného vzdelávania a budovania bezpečnostného povedomia. Takýto program má využívať moderné, cielené a zrozumiteľné prístupy k výučbe, tréningu a systematickému vzdelávaniu v oblasti bezpečnosti s cieľom meniť postoj členov organizácie vo vzťahu k ochrane hodnôt organizácie

---

[5] Podľa prieskumu informačnej bezpečnosti v roku 2013 je jednotlivec príčinou takmer 90% bezpečnostných incidentov. Bližšie MF SR, Prieskum stavu informačnej bezpečnosti vo verejnej správe v SR v roku 2013.

[6] Podrobnejšie pozri normu ISO 27001:2013 Systém riadenia bezpečnosti informácií, Organizácia bezpečností informácií, Bezpečnosť z hľadiska ľudských zdrojov - Povedomie, vzdelávanie a príprava.

[7] www.sansecurity.com, 2015

[8] Podrobnejšie Rozhodnutie Rady č. 2013/488/EÚ z 23.9.2013 článok 7(5) a časť IV Prílohy 1.

(najčastejšie informácie alebo majetok). Časovo nenáročným, nevtieravým a pritom systematickým spôsobom postupne meniť vnímanie bezpečnosti a budovať dlhodobo udržateľný postoj jednotlivca vo vzťahu k bezpečnosti a dôvere k vlastnej organizácii (štátu). Bezpečnostné povedomie je v systéme ochrany utajovaných skutočností súčasťou tzv. pyramídy bezpečnosti, kde prvý stupeň tvorí bezpečnostná previerka (statické riziká), bezpečnostné povedomie (dynamické riziká) a princíp "need-to-know". Obdobne by malo byť primerané bezpečnostné povedomie komplexne integrované aj do bezpečnostného systému štátu.

Bezpečnostné povedomie je však možné vnímať ucelenejšie a aj na kvalitatívne vyššej úrovni. Potom možno hovoriť o tzv. kultúre bezpečnosti (organizácie alebo štátu). Kultúra bezpečnosti vo všeobecnosti vypovedá o miere a spôsobe naplnenia a osvojenia si cieľov a úloh v oblasti bezpečnosti, ich dosahovania, kontroly a rozvoja. Kultúra bezpečnosti určuje rozsah a vzory základných riešení, hodnôt, noriem, štandardov, symbolov a názorov, vplývajúcich na spôsob prístupu k bezpečnostným výzvam a k riadeniu bezpečnosti na všetkých hierarchických úrovniach bezpečnostného systému štátu. Zavádza stereotypy pre bezpečné správanie sa ľudí ako v každodennom živote doma, na verejnosti, či na pracovisku, tak aj v krízových situáciách. Je súčasťou jednotného vzťahu: "Kultúra bezpečnosti-bezpečnostné povedomie-bezpečné správanie"[9].

Pri dostatočne etablovanej kultúre bezpečnosti a primeranom bezpečnostnom povedomí jednotlivcov je možné vytvoriť efektívny systém predchádzania a eliminovania moderných bezpečnostných hrozieb.

Záver:

Každý moderný a demokratický štát by mal využívať (za podmienky dodržiavania príslušných pravidiel a zákonov) všetky dostupné nástroje a prostriedky na dosiahnutie potrebnej úrovne bezpečnosti. **Samotné stanovovanie pravidiel nie je vždy efektívne, naopak kladenie zodpovednosti a pozitívne vplývanie a vzdelávanie (pod hrozbou sankcie) by mohlo byť primeraným riešením.** Uvedomenie si potreby dodržiavania pravidiel je prvým krokom k ich akceptácii a ich ďalšiemu pozitívnemu šíreniu. Stupeň bezpečnostnej kultúry na úrovni štátu sa prejavuje najmä v obsahu a zameraní prijímaných dokumentov do oblasti zaisťovania vnútornej a vonkajšej bezpečnosti. Prijaté a osvojené zásady kultúry bezpečnosti sa odrážajú v obsahu a zameraní strategickej kultúry bezpečnosti štátu, vyjadrujúcej najmä prístup politickej reprezentácie štátu k zaisteniu svojej vnútornej a vonkajšej

[9]Hofreiter, L.: Kultúra bezpečnosti a riadenie bezpečnosti, In Zborník z 20. Vedeckej konferencie s medzinárodnou účasťou Riešenie krízových situácií v špecifickom prostredí, Fakulta špeciálneho inžinierstva Žilinskej univerzity v Žiline, 2015,str.65

bezpečnosti. V strategickej kultúre štátu sa odrážajú najmä ideové, náboženské a kultúrne hodnoty, historická skúsenosť, naratívna história, ale aj vojenské spôsobilosti a vymedzenie hierarchie chránených záujmov štátu. Odraz kultúry bezpečnosti a bezpečnostného povedomia jednotlivcov je realizovaný vo všeobecnej rovine prostredníctvom strategických dokumentov štátu.

Jednotlivec sa stáva zásadným činiteľom pre bezpečnosť, vrátane svojej vlastnej bezpečnosti. Ako už bolo konštatované, môže byť prínosom ale aj rizikom. Bez ohľadu na to či je aktívnou alebo pasívnou súčasťou bezpečnostného systému, či je nástrojom alebo cieľom nepriateľských opatrení, alebo len vlastníkom zneužitých technických prostriedkov.

Bezpečnostné povedomie jednotlivca zohráva a bude zohrávať čoraz dôležitejšiu rolu v oblasti bezpečnosti.

Literatúra:

Brvnišťan, M.: Ochrana utajovaných skutočností v spektre historického vývoja, Tlačiareň Ministerstva vnútra SR, Bratislava 2013, 160 str., ISBN 978-80-8054-561-1

Brvnišťan, M.: Možností ochrany informácií SR, In Zborník príspevkov z VI. medzinárodnej vedeckej konferencie v Banskej Bystrici 6. – 7. februára 2013, II. Zväzok, Fakulta politických vied a medzinárodných vzťahov UMB, 2013, ISBN 978-80-557-0497-5, str. 556 – 565

Hofreiter, L.: Kultúra bezpečnosti a riadenie bezpečnosti, In Zborník z 20. Vedeckej konferencie s medzinárodnou účasťou Riešenie krízových situácií v špecifickom prostredí, Fakulta špeciálneho inžinierstva Žilinskej univerzity v Žiline, 2015, ISBN 978-80-554-1024-1, str. 36-43

Nečas, P., Ušiak, J.: Nový prístup k bezpečnosti štátu na začiatku 21. storočia, In Vedecká monografia, Akadémia ozbrojených síl generála M. R. Štefánika v Liptovskom Mikuláši, 2010, ISBN 978-80-8040-401-7

Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a o doplnení niektorých zákonov

Zákon č. č. 473/2005 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov

Bezpečnostná stratégia SR, 2005, www.mosr.sk

Bezpečnostná stratégia NATO, www.mosr.sk, 2015

Európska bezpečnostná stratégia, www.mosr.sk, 2015

Rozhodnutie Rady z 23. septembra 2013, č. 2013(488)EU o bezpečnostných predpisoch na ochranu utajovaných informácií, OJ L 274 z 23.9.2013