

BEZPILOTNÉ PROSTRIEDKY A ICH EVENTUÁLNA SPÔSOBILOSŤ OHROZIŤ BEZPEČNOSŤ UTAJOVANÝCH SKUTOČNOSTÍ¹

Miroslav Brvnišťan²

Anotácia: Používanie bezpilotných prostriedkov je súčasťou technického a technologického rozvoja a trendom, ktorý ovplyvňuje vnímanie bezpečnosti a súkromia. Vytvárajú sa tým predpoklady na zavedenie a aplikáciu nových nástrojov a prístupov k riešeniu bezpečnosti, ako aj definovaniu pravidiel bezpečnosti. Ochrana utajovaných skutočností predstavuje nástroj štátu, ktorý má garantovať bezpečnosť skutočností (informácií) spôsobilých ohroziť záujmy štátu. Článok analyzuje možné konzekvencie používania bezpilotných prostriedkov vo vzťahu k ohrozeniu utajovaných skutočností a navrhuje prístupy k hľadaniu vhodných riešení.

KLúčové slová: bezpilotný prostriedok, ochrana utajovaných skutočností, bezpečnostné riziko, bezpečnosť informácií

Anotation: The use of unmanned aerial vehicles (UAVs) is a part of technological and technological developments and a trend that affects the perception of security and privacy. This creates the preconditions for introducing and applying new tools and approaches to address security as well as to define security rules. The protection of classified information is a tool of the state to guarantee the security of the information capable of jeopardizing the interests of the state. The article analyzes the possible consequences of using unmanned aerial vehicles in relation to threats to classified information and suggests approaches to finding suitable solutions.

Key words: unmanned aerial vehicle, protection of classified information, security risk, information security

Úvod

Dynamický rozvoj technológií, meniace sa bezpečnostné prostredie a nové bezpečnostné hrozby kladú čoraz väčšie nároky na schopnosť bezpečnostného systému štátu garantovať bezpečnosť. Moderné technológie menia a nanovo definujú možnosti zaužívaných bezpečnostných nástrojov a opatrení a súčasne kreujú nové. Vytvárajú sa tým elementárne predpoklady pre často neadekvátnu reakciu na rôznych úrovniach riadenia bezpečnostného systému štátu bez ohľadu na to, či ide o rozhodovanie politické alebo odborné.

Očakáva sa jednoznačná, správna a rýchla reakcia, sme však svedkami rozhodnutí, pri ktorých sa nové technológie a meniace bezpečnostné prostredie stávajú prekážkou, na ktorú je ťažké nájsť odpoveď v rámci existujúcich bezpečnostných pravidiel a mechanizmov. To čo bolo historicky zavedené - bezpečnostné postupy, systém všeobecne záväzných právnych predpisov, primeraná rýchlosť reakcie, a vnímané ako záruka bezpečnosti je pod tlakom a spochybňované. Tento stav je do určitej miery logický a pravdepodobne výsledkom neprimeranej zotrvačnosti systému štátu ako takého.

Technologický pokrok zároveň mení postavenie jednotlivca, a to nielen vo vzťahu k individuálnej bezpečnosti (zodpovednosť za vlastnú bezpečnosť), ale najmä vo vzťahu k bezpečnosti spoločnosti, občanov a štátu. Jednotlivec, bez ohľadu na svoje postavenie v spoločnosti, pravdepodobne nikdy v histórii nemal také možnosti ovplyvniť svojím konaním celkovú bezpečnosť spoločnosti, rôznych subjektov, štátov alebo aj nadnárodných zoskupení.

¹ Tento príspevok je podporovaný Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV – 16-0521.

² JUDr. Miroslav Brvnišťan, PhD., Akadémia Policajného zboru v Bratislave, katedra verejnej správy a krízového manažmentu, brvnistan@bmsec.sk.

Určítym prekvapením je však systematické nepripúšťanie si tohto stavu a snaha o dogmatické presadzovanie prekonaných nástrojov a opatrení, vrátane neadekvátneho výkladu platných všeobecne záväzných právnych predpisov.

V súčasnosti sme svedkami „sporu“, ktorý vznikol na jednej strane ako dôsledok rastúceho záujmu o bezproblémové používanie bezpilotných prostriedkov (ďalej len dron) a na druhej strane ako dôsledok snahy štátu o reguláciu - stanovenie pravidiel podľa platnej právnej úpravy v oblasti ochrany utajovaných skutočností - zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení ďalších zákonov (ďalej len zákon o OUS). Ochrana utajovaných skutočností je nesporné integrálnou súčasťou bezpečnostného systému štátu, zabezpečovaná prostredníctvom celého spektra nástrojov a opatrení. Je však vhodná ako nástroj na reguláciu používania dronov? Prečo áno a prečo nie?

Je potrebné mať na pamäti, že základy všeobecne záväzných právnych predpisov, ktorými sa štát snaží regulovať používanie dronov boli vytvorené oveľa skôr ako sa drony začali využívať.

V súvislosti s používaním dronov preto vyvstávajú viaceré legitímne otázky : Môže používanie dronov ohroziť utajované skutočnosti? Aké bezpečnostné riziká drony predstavujú a vie ich systém ochrany utajovaných skutočností eliminovať? Ako je možné na vzniknutú situáciu reagovať?

Predmetné otázky sú len odrazom situácie, kedy moderné bezpečnostné hrozby pravdepodobne presahujú možnosti súčasných bezpečnostných mechanizmov a ich nástrojov, no ich zodpovedanie môže objasniť dôvody „sporu“ a zároveň načrtnúť možnosti riešenia.

I. Dron ako bezpečnostné riziko

Používanie dronov sa stáva predmetom čoraz väčšieho množstva diskusií na laickej, odbornej a aj politickej úrovni, často však bez základného porozumenia problematiky a možných konzekvencií. Je nesporné, že téma dronov ako taká, vrátane súvisiacich tém akými sú právna zodpovednosť, zodpovednosť za škodu a aj možné ohrozenie utajovaných skutočností vytvárajú priestor, ktorým sa je potrebné zaoberať a primerane upraviť, a to najmä s ohľadom na rýchly technický a technologický pokrok.

Názov „dron“ sa začal používať v našich zemepisných šírkach na základe prebratia anglického slova „drone“. Ide o zariadenie-lietadlo, ktoré sa oficiálne a spisovne označuje ako Unmanned Aerial Vehicle (možno sa takisto stretnúť so skratkou UAV), teda bezpilotné lietadlo. Dron je teda lietadlo bez posádky, ktoré môže byť riadené na diaľku, alebo lietať samostatne pomocou predprogramovaných letových plánov, prípadne pomocou zložitejších autonómnych subsystémov.³

Pre účely tohto článku sa nebudeme podrobne zaoberať celým spektrom právnej úpravy týkajúcej sa možností využívania dronov a ich regulácie. Dron budeme chápať len ako lietajúce

³Podľa rozhodnutia Dopravného úradu č. 1/2015, ktorým sa určujú podmienky vykonania letu lietadlom spôsobilým lietať bez pilota vo vzdušnom priestore Slovenskej republiky (ďalej len ako „Rozhodnutie“) rozoznávame viacero kategórií bezpilotných lietadiel:

- Autonómne lietadlá – lietadlá bez akéhokoľvek zásahu pilota do riadenia letu;
- Diaľkovo riadené lietadlá – bezpilotné lietadlo, ktorého let je riadený pilotom z iného miesta ako paluby lietadla;
- Modely lietadiel – bezpilotné lietadlá používané na rekreačné, športové, resp. súťažné účely bez komerčného charakteru;
- Hračky – model lietadla do 0,5 kg.

zariadenie spôsobilé niesť určitý náklad, ktorý môže bližšie podmieňovať bezpečnostné riziká. Vychádzame pritom z premisy, že každý dron môže niesť určitý náklad, technické zariadenie, optické alebo iné záznamové zariadenie. Existujúce možnosti závisia od vlastností dronu, jeho technických parametrov (nosnosti, dĺžky prevádzky, letových parametrov) a neposlednom rade od schopností a záujmov osoby, ktorá takýto dron ovláda alebo naprogramovala jeho letovú činnosť.

Takisto je potrebné brať v úvahu, že drony predstavujú akési zhmotnenie spektra moderných technológií, ktoré na prvý pohľad nesúvisia priamo s ich používaním, no majú alebo čoskoro mať budú dopad na modernú spoločnosť. Ide napríklad o schopnosti autonómnej činnosti zariadení - vozidiel alebo lietadiel využívajúcich prvky umelej inteligencie, samoučiace sa zariadenia a pod. Právna zodpovednosť a iné súvisiace konzekvencie sú zatiaľ ťažko predpovedateľné i keď existuje snaha príslušných orgánov vytvoriť primeranú reguláciu najčastejšie prostredníctvom využitia výkladu platnej právnej úpravy⁴. Drony predstavujú problém z právneho hľadiska, množstvo dotknutých zákonov sa mení podľa toho kde dron lieta. Môže ísť o narušenie súkromia, osobnostných práv, letového priestoru, ohrozenie leteckej premávky, poškodenie majetku alebo o ohrozenie utajovaných skutočností. Drony zatiaľ nemôžu byť používané na prepravu osôb⁵.

Vo všeobecnosti je možné konštatovať, že používanie dronov predstavuje výzvu nielen pre právny systém štátu ale aj pre bezpečnostné zložky štátu. Dron a používanie dronov ako takých môže predstavovať rôzne riziká - dron ako zbraň alebo nástroj, či už samostatne alebo v závislosti od neseného nákladu napr. nátražné výbušné zariadenie, nebezpečná látka, strelná alebo iná zbraň, kamera, fotoaparát alebo iné záznamové zariadenie. V závislosti od neseného nákladu je potrebné hodnotiť aj možné riziká a prípadné dôsledky - napr.:

- drony narušujúce vzdušný priestor v okolí verejných miest,
- drony vykonávajúce videozáznam, prenášajúce obrazový záznam
- drony použité na útok, teroristický útok, sabotáž,
- drony ohrozujúce ľudí - plánovane alebo náhodne,
- drony narúšajúce verejné alebo športové podujatia,
- drony narušujúce prácu bezpečnostných zložiek - počas požiaru alebo inej udalosti obmedzujú záchranné zložky v činnosti,
- drony narúšajúce prevádzku lietadiel or letísk,
- drony slúžiace na pašovanie zakázaného tovaru,
- drony na donášanie zásielok väzňom,
- drony prenášajúce zbrane.

Je zrejmé, že drony a ich používanie predstavujú množstvo potencionálnych rizík. K hodnoteniu čo je a čo nieje prípustné je nutné pristupovať vždy s ohľadom na konkrétnu situáciu a chránený

⁴ Napr. Úrad na reguláciu elektronických komunikácií a poštových služieb vydal v roku 2014 správu o tom, že pri kúpe dronu v zahraničí alebo cez internet sa stáva, že si záujemca obstará zariadenia určené pre ázijský alebo americký trh, ktoré majú iné technické parametre a nie je ich povolené používať v krajinách EÚ. V prípade používania nepovolených zariadení hrozí vzájomné rušenie s povolenými zariadeniami. Okrem toho hrozí, že v dôsledku rušenia môže v niektorých prípadoch dôjsť k strate kontroly nad letiacim zariadením, zariadenie sa môže zrútiť a spôsobiť škody alebo zranenie tretím osobám. Úrad upozornil dovozcov, predajcov a výrobcov takýchto zariadení, že podmienkou ich uvedenia na trh a do prevádzky je posúdenie zhody podľa Nariadenia vlády č. 443/2001 Z.z.

Rozhodnutím č. 1/2015, platia pravidlá regulácie, ktoré vydal Dopravný úrad, medzi ktoré patrí pravidlo zodpovednosti, a síce, že prevádzkovateľ akéhokoľvek lietadla spôsobilého lietať bez pilota je zodpovedný za stav bezpilotného lietadla a ako aj jeho letovú spôsobilosť, za prípravu a vykonanie letu. Z uvedeného je preto zrejmé, že aj za prípadné výrobné vady dronu, ktoré spôsobia škodu, bude zodpovedný prevádzkovateľ, ktorý by si následne mohol vymáhať vzniknutú škodu od jeho výrobcu.

⁵Rozhodnutím č. 1/2015, platia pravidlá regulácie, ktoré vydal Dopravný úrad a teda dron nemôže byť použitý na prepravu osôb, nebezpečného nákladu, látok alebo zariadení, ktoré by mohli ohroziť alebo poškodiť zdravie osôb, majetok alebo životné prostredie. Rozhodnutie rozšírilo tento zákaz aj o batožinu a poštové zásielky. Zhadzovanie predmetov z bezpilotného lietadla počas jeho letu a vykonanie letu bezpilotným lietadlom v noci je zakázané.

záujem. Regulácia používania dronov by nemala byť v celkom zjavnom nepomere k možnému spôsobenému následku.

II. Dron ako bezpečnostné riziko pre systém ochrany utajovaných skutočností

Vo vzťahu k systému ochrany utajovaných skutočností a možným bezpečnostným rizikám súvisiacim s používaným dronov je potrebné pristupovať v súlade s platným zákonom č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov (ďalej len zákon o OUS). Zároveň je nutné v úvode tejto časti uviesť, že zákon o OUS je typickou právnou normou, ktorej základy vznikli v minulom storočí⁶, kedy téma dronov ešte neexistovala. Napriek tomu je potrebné zákon o OUS primerane aplikovať. Pripúšťame, že právne inštitúty ktorými zákon o OUS disponuje sú prekonané a preto je potrebné klásť dôraz na adekvátny výklad ustanovení zákona, zohľadňovať reálie súčasnosti a tendencie vývoja. Rígidny výklad a trvanie na jeho dodržiavaní spôsobuje často opačný efekt, bez možnosti nájdania skutočne efektívneho riešenia.

Z hľadiska platnej právnej úpravy oblasti ochrany utajovaných skutočností je potrebné uviesť, že používanie dronov súvisí s viacerými ustanoveniami zákona o OUS. Je však možné obmedziť používanie dronov, nakoľko tieto predstavujú bezpečnostné riziko pre utajované skutočnosti?

V prvom rade bezpečnostné riziká zákon o OUS nedefinuje a ani nedefinuje manažment bezpečnostných rizík. Spôsob ochrany utajovaných skutočností je realizovaný prostredníctvom vytvárania podmienok (nástrojov) na personálnu bezpečnosť, administratívnu bezpečnosť, šifrovú ochranu informácií, fyzickú bezpečnosť, objektovú bezpečnosť, bezpečnosť technických prostriedkov a na priemyselnú bezpečnosť⁷. Realizáciou podmienok a ich vzájomnou kombináciou v závislosti od konkrétnej situácie je možné zabezpečiť ochranu utajovaných skutočností.

Jednotlivé oblasti ochranných opatrení stanovujú opatrenia vyplývajúce z podstaty danej oblasti, napr. personálna bezpečnosť stanovuje opatrenia súvisiace s výberom, určením a kontrolou osôb, ktoré sa môžu oboznamovať s utajovanými skutočnosťami; oblasť objektivej a fyzickej bezpečnosti je systém opatrení slúžiaci na ochranu utajovaných skutočností pred nepovolanými osobami a pred neoprávnenou manipuláciou v objektoch a chránených priestoroch.

Je zrejmé, že ide o pokus zameraný na konečný (fixný) výpočet činností smerujúcich k ochrane utajovaných skutočností. S ohľadom na dynamiku bezpečnostného prostredia sa môže vyskytnúť aj nové riziko (napr. dron), ktoré však bez zmeny zákona o OUS nebude možné zohľadniť vo vzťahu k bezpečnosti utajovaných skutočností⁸. Uvedené konštatovanie je odôvodnené nasledovnými skutočnosťami:

Zákon o OUS priamo nestanovuje pri realizácii jednotlivých oblastí ochranných opatrení povinnosť analýzy rizík, skôr naopak zdá sa, že tvorcovia pri jeho príprave predpokladali, že navrhnu dostatočne robustný systém odolný voči všetkým známym rizikám. Analýza rizík je v niektorých oblastiach ochranných opatrení čiastkovo riešená prostredníctvom vykonávacích vyhlášok k zákonu o OUS⁹, čo však nepredstavuje systémový prístup k ochrane utajovaných skutočností a ani nerieši potrebnú flexibilitu.

⁶ Brvnišťan, M. : Ochrana utajovaných skutočností v spektre historického vývoja, Tlačiareň Ministerstva vnútra SR, Bratislava 2013.

⁷ §6 ods. 2 zákona o OUS.

⁸ Pozri bližšie v Brvnišťan, M.: **Vybrané problémy analýzy bezpečnostných rizík v systémoch ochrany informácií**, In Zborník vedeckých a odborných prác, 9. Medzinárodná vedecká konferencia Národná a medzinárodná bezpečnosť 2018, Akadémia ozbrojených síl generála Milana Rastislava Štefánika.

⁹ Pozri napr. Vyhláška č. 336/2004 Z. z. o fyzickej bezpečnosti a objektivej bezpečnosti, Vyhláška 339/2004 Z.z. o bezpečnosti technických prostriedkov.

Odlišná situácia je v prípade relevantných predpisov EU a NATO. Ide pritom často o ochranu tých istých utajovaných informácií, vznikajúcich na rovnakom teritóriu, v rovnakom bezpečnostnom prostredí a rámci jedného nadnárodného integračného zoskupenia (organizácie).

Podľa bezpečnostnej politiky NATO - C-M(2002)49 je predmetom ochrany utajovaná informácia alebo materiál, ktorý vyžaduje *ochranu pred neautorizovaným zverejnením*¹⁰. Definuje sa tu základný princíp ochrany, ktorým je manažment bezpečnostných rizík a vybudovanie bezpečnostnej autority zodpovednej za zber a hodnotenie spravodajských informácií týkajúcich sa špionáže, sabotáže a podvratných hrozieb¹¹.

Zámerom tvorcov bolo implementovať systém manažmentu rizík priamo do bezpečnostnej politiky NATO (záväznej pre členské krajiny). Zároveň sú jednoznačne definované a pomenované kľúčové bezpečnostné riziká.

Podľa záväzných predpisov EÚ je spôsob ochrany realizovaný rozhodnutím Rady EÚ, ktorým sa ustanovujú základné zásady a minimálne normy bezpečnosti na ochranu utajovaných skutočností EÚ (jednotlivé oblasti ochranných opatrení sú obdobné ako v systéme SR a NATO)¹². *Zároveň sa definuje riadenie bezpečnostných rizík, ktoré sa uskutočňuje ako proces*. Tento proces sa zameriava na určenie známych bezpečnostných rizík, stanovenie bezpečnostných opatrení na zníženie týchto rizík na prijateľnú úroveň. Bezpečnostné opatrenia na ochranu utajovaných skutočností EÚ počas celého ich životného cyklu zodpovedajú najmä ich stupňu utajenia, podobe a množstvu informácií alebo vecí, miestu, kde sa nachádzajú zariadenia, v ktorých sa utajované skutočnosti EÚ uchovávajú, a ich konštrukcii, stanovenej lokálnej úrovni ohrozenia škodlivými a/alebo trestnými činnosťami vrátane **špionáže, sabotáže a terorizmu**¹³. Opätovne je tu jednoznačne určený systém analýzy a manažmentu bezpečnostných rizík a sú pomenované kľúčové bezpečnostné riziká.

V prípade predpisov NATO a EÚ možno konštatovať, že ochrana utajovaných informácií zohľadňuje bezpečnostné riziká, ktoré môžu vyplývať z používania dronov.

V jednotlivých systémoch OUS OUS (berúc v úvahu aj predpisy NATO a EÚ) je analýza rizík definovaná a následne využívaná rôzne. Z hľadiska eliminácie rizík vyplývajúcich z prevádzky dronov nie je pri súčasnom stave zákona o OUS a jeho výklade (vrátane absencie inštitútu analýzy bezpečnostných rizík) možné predpokladať prijatie relevantných opatrení. To je možné v súčasnosti iba prostredníctvom platných predpisov nadnárodných zoskupení, ich aplikácia sa však v praxi neuskutočňuje!¹⁴

V zásade je možné konštatovať, že systém OUS vytvára podmienky na ochranu utajovaných skutočností tak, aby nedošlo k ich ohrozeniu. Ak by však aj boli drony identifikované ako potencionálne riziko systém OUS by to riešil využitím nástrojov a ochranných opatrení podľa platného zákona o OUS, prijatím takých opatrení aby toto riziko bolo eliminované.

Možno konštatovať, že vzhľadom na rigidnosť súčasného systému OUS je takmer nemožné predpokladať prijatie účinných opatrení. Absentujúci manažment bezpečnostných rizík a následná identifikácia nových foriem bezpečnostných rizík priamo ovplyvňujú možnosti ich eliminácie. Na to aby bolo používanie dronov hodnotené ako bezpečnostné riziko pre oblasť OUS nemá platný

¹⁰ Príloha "A" Annex 1 písm. a) bezpečnostnej politiky NATO.

¹¹ Pozri bližšie bod 5.1 a 5.2. Bezpečnostnej politiky NATO.

¹² Článok 1 Rozhodnutia Rady z 23. septembra 2013, č. 2013(488)EU o bezpečnostných predpisoch na ochranu utajovaných informácií.

¹³ Článok 5 Rozhodnutia Rady z 23. septembra 2013, č. 2013(488)EU o bezpečnostných predpisoch na ochranu utajovaných informácií.

¹⁴ Pozri bližšie v Brvnišťan, M.: Legal basis for the protection of the European union classified information, In Police Theory and Practice, ročník XXVI., Bratislava 1/2018.

zákon vytvorený potrebný mechanizmus. Tento stav je neakceptovateľný a pravdepodobne sám o sebe predstavuje bezpečnostné riziko¹⁵.

Neakceptovanie tohto stavu a hľadanie náhradných riešení prostredníctvom "flexibilného" výkladu platných ustanovení zákona o OUS neprinesie riešenie a účinnosť realizovaných opatrení bude drahá a pochybná.

III. Inštitút utajenia ako nástroj ochrany pred následkami používania dronov

Ochrana utajovaných skutočností podľa zákona o OUS predstavuje komplex špecifických ochranných opatrení zameraných na elimináciu bezpečnostných rizík vo vzťahu k informáciám štátu. Nejde však o všetky informácie štátu, ale len tie, ktoré sa týkajú realizácie záujmov štátu a ak v dôsledku neoprávnenej manipulácie s nimi by mohla vzniknúť škoda na záujmoch štátu¹⁶. Samotná podstata systému utajenia vychádza zo základných princípov (teoretických východísk) systémov ochrany. Zákon o OUS je z tohto hľadiska len prirodzeným zhmotnením dostupných vedomostí, znalostí a možností ovplyvnených spoločenskými požiadavkami a situáciou v čase jeho spracovania.

Ochrana utajovaných skutočností nadobúda v súčasnej modernej dobe na význame, je reálnym dôsledkom nielen exponenciálneho rastu množstva informácií a ich charakteru, ale aj zmenami a vývojom bezpečnostného prostredia v ktorom sa Slovenská republika nachádza. Ako subsidiárne je možné vnímať v tomto kontexte technologický pokrok a technický vývoj prostriedkov a nástrojov určených na jednej strane na ochranu informácií, na strane druhej na ich protiprávne získavanie (ohrozenie). Správne nastavenie systému utajenia, jeho teoretických a právnych základov tak, aby zodpovedali požiadavkám modernej spoločnosti je dnes, ako bude aj v budúcnosti kľúčovým.

Ochrana utajovaných skutočností prostredníctvom režimu utajenia je pritom jediným komplexným nástrojom ochrany informácií štátu. Pri realizácii utajenia je potrebné jednotlivé opatrenia citlivo zvažovať, aby opatrenia súvisiace so zabezpečovaním režimu utajenia a miera utajovania informácií neprekročila únosnú hranicu medzi potrebou utajiť dôležité informácie štátu a vice versa umožnila občanom aktívne realizovať svoje práva.

Rozhodnutie o utajení je z hľadiska režimu utajenia pravdepodobne najdôležitejší akt, zakladajúci celý rad vzájomne podmienených krokov a ich dôsledkov, ktoré podmieňujú účinnosť ochrany režimom utajenia. Utajenie samotné je pritom realizované komplexom špecifických opatrení¹⁷, ktoré zabezpečujú to, že daná informácia je prístupná len určitému presne definovanému okruhu dôveryhodných (preverených) osôb. Predpokladá sa, že režim utajenia následne eliminuje celé spektrum rôznych bezpečnostných rizík, medzi ktoré môžeme zaradiť napr. stratu informácie, špionáž alebo jej možné vyzradenie a využíva na to špecifické formy a metódy činnosti, vrátane spravodajských. Z tohto hľadiska štát využíva, teda má vytvorený „systém“, ktorý zabezpečuje potrebnú úroveň bezpečnosti režimu utajenia.

¹⁵ Pozri bližšie Buzalka, J., Blažek, V., Dworzecki, J., Urbanek, A. a kol.: Rozvoj bezpečnostných rizík a tvorba krízových scenárov pre verejnú správu, Vedecká monografia, Akadémia PZ v Bratislave 2014, str. 23.

¹⁶ Bližšie pozri §3 zákona č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.

¹⁷ § 6 ods.2 zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov znie: Ochranou utajovaných skutočností je vytváranie podmienok na personálnu bezpečnosť, administratívnu bezpečnosť, šifrovú ochranu informácií, fyzickú bezpečnosť, objektívnu bezpečnosť, bezpečnosť technických prostriedkov a na priemyselnú bezpečnosť.

Môže byť systém utajenia využitý (zneužitý) na elimináciu bezpečnostných rizík súvisiacich s používaním dronov? Mohlo by k tomu dôjsť prostredníctvom zneužitia inštitútu utajenia.

Je zrejmé, že systém OUS by nemal byť zneužívaný na dosiahnutie regulácie používania dronov, ak to priamo nesúvisí z bezpečnosťou utajovaných skutočností. Zároveň však platí, že systém OUS v súčasnosti nedokáže reagovať na nové bezpečnostné riziká bez zmeny zákona o OUS a napr. identifikovať dron ako bezpečnostné riziko pre režim utajenia, najmä s ohľadom na absenciu systému analýzy bezpečnostných rizík.

Môže byť rozhodnutím o utajení zamedzené používaniu dronov? Odpoveď môže byť prekvapujúca.

Konštrukcia samotného systému OUS utajením vychádza priamo z ustanovení Ústavy SR – zák. č. 460/1992 Zb. (Ústava SR), ktorá definuje, kedy je možné obmedziť právo na informácie¹⁸. Zákon o ochrane utajovaných skutočností, umožňuje realizáciu tohto ustanovenia v praxi, vytvorením uceleného právneho rámca. Bezpečnosť informácií je Ústavou SR povýšená nad akýkoľvek iný záujem, vrátane Ústavou SR garantovanému slobodnému prístupu k informáciám¹⁹, ako aj prostredníctvom ustanovení Listiny základných práv a slobôd²⁰. Z pohľadu štátu je teda zabezpečené, že občan má vo všeobecnosti prístup k všetkým informáciám, okrem tých, o ktorých bolo rozhodnuté, že budú chránené utajením.

Na začiatku režimu utajenia by malo byť rozhodnutie (akt) o utajení informácie, ako zásadné rozhodnutie, ktoré zabezpečí ochranu informácie tak, aby táto bola prístupná len definovanému okruhu osôb.

Zákon o OUS rámcovo vytvára mechanizmus, ktorý umožňuje informácie utajiť pri súčasnom splnení dvoch základných podmienok: informácia musí byť spôsobilá ohroziť záujmy štátu²¹, a zároveň táto vzniká v oblasti, ktoré ustanovila vláda SR svojim nariadením²². Predmetné nariadenie vlády SR zároveň v § 2²³ stanovuje podmienku vymedzenia utajovaných skutočností vedúcim vznikajúcich v právnickej osobe. Výsledkom je zoznam utajovaných skutočností²⁴, určený ich stupeň utajenia, vrátane dôvodov utajenia. Tým je explicitne popísaný mechanizmus umožňujúci utajiť vybrané informácie.

Po podrobnejšej analýze možno konštatovať, že tento mechanizmus je síce na prvý pohľad v poriadku, no v skutočnosti vo svojej podstate umožňuje utajiť akúkoľvek skutočnosť. De jure je pravdepodobne všetko v poriadku. Tento stav je ešte umocnený tým, že pravdepodobne neexistuje mechanizmus, ktorý by umožňoval rozhodnutie o utajení informácie spochybníť, respektíve

¹⁸ Čl. 26 ods. 4 Ústavy SR „Slobodu prejavu a právo vyhľadávať a šíriť informácie možno obmedziť zákonom, ak ide o opatrenia v demokratickej spoločnosti nevyhnutné na ochranu práv a slobôd iných, bezpečnosť štátu, verejného poriadku, ochranu verejného zdravia a mravnosti“.

¹⁹ Čl. 26, 45 a 34 zák. č. 460/1992 Zb. Ústava SR (Ústava SR).

²⁰ Čl. 17,25 a 35 ústavný zák. č. 23/1991 Zb. Listina základných práv a slobôd.

²¹ Pozri bližšie §3 Stupne utajenia zákona č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.

²² Nariadenie vlády SR č. 216/2004 Z.z. ktorým sa ustanovujú oblasti utajovaných skutočností.

²³ §2 nariadenia vlády č. 216/2014 Z.z. znie: (1)Vedúci vymedzí podľa §1 tohto nariadenia utajované skutočnosti vznikajúce v právnickej osobe v rámci pôsobnosti ustanovenej podľa osobitného predpisu. Určené utajované skutočnosti vedúci zaraďuje do zoznamu utajovaných skutočností právnickej osoby.

(2) Zoznam utajovaných skutočností právnickej osoby podľa odseku 1 vydáva vedúci písomne. Jeho obsahom je konkrétne určenie utajovaných skutočností s príslušným stupňom utajenia podľa § 3 zákona, zaradených do oblastí podľa § 1 tohto nariadenia a odôvodnenie potreby ich označenia príslušným stupňom utajenia.

(3) Zoznam utajovaných skutočností právnickej osoby je verejný.

²⁴ Pozri napr. Zoznam utajovaných skutočností Ministerstva vnútra SR, Nariadenie MV SR z 30.6.2015 o zozname utajovaných skutočností v znení nariadenia MV SR č. 112/2015 a nariadenia MV SR č. 14/2016.

korigovať. Takéto konštatovanie je založené pritom priamo na ustanoveniach zákona o OUS, ktoré ani v prípade súdneho konania neumožňujú bez súhlasu pôvodcu odtajniť informáciu. Vychádzame pritom z predpokladu, že súd by bol pri svojom rozhodovaní viazaný už zmieneným mechanizmom utajenia informácie a išlo by teda vo svojej podstate len o posúdenie dodržania procesných pravidiel utajenia informácie²⁵.

Zároveň je potrebné poukázať na systémový nedostatok platnej právnej úpravy OUS, nakoľko napriek vytvoreniu zákonného predpokladu na utajenie vecí ako výrobok, zariadenie, nehnuteľnosť²⁶ neboli od nadobudnutia účinnosti zákona o OUS vypracované potrebné vykonávacie predpisy, ktoré by to umožnili. Znamená to, že napriek teoretickej možnosti rozhodnúť o utajení objektov ako napr. letisko, budova toto nie je možné vzhľadom na absenciu nástrojov. Napriek tomu napr. zoznam utajovaných skutočností MO SR obsahuje v bode 16. predmet utajenia zariadenie alebo nehnuteľnosť (predpokladaný stupeň utajenia V-T)²⁷.

Zároveň je na mieste otázka aké iné utajované skutočnosti môžu byť ohrozené prostredníctvom dronov? Môže to byť napr. režimové opatrenia ochrany objektov, preprava citlivých materiálov alebo zbraní, taktika výcviku, odpozeranie utajovaných písomností?

Na základe uvedeného možno konštatovať, že rozhodnutím o utajení by mohlo dôjsť k utajeniu takých skutočností, kedy by v záujme dodržania režimu utajenia mohla byť obmedzená prevádzka dronov. Platilo by to však len v prípade, že systém OUS by s takouto alternatívou rátal a mal vytvorené potrebné nástroje. Takýmto nástrojom by mohli byť ustanovenia § 63 a § 64 zákona o OUS zaoberajúce sa reguláciou fotografovania, filmovania a leteckého snímkovania.

IV. Dron ako zariadenie vykonávajúce fotografovanie, filmovanie a letecké snímkovanie

Zákon o OUS sa v § 63 a § 64 explicitne zaoberá špecifickými činnosťami, ktoré by pravdepodobne mohli ohroziť režim utajenia. Je to však naozaj tak?

Pri hľadaní odpovede je potrebné analyzovať pôvod citovaných ustanovení. Už zo samotného znenia je zrejmé, že sa jedná o ochranu všeobecného záujmu - § 63 obrany a bezpečnosti štátu a § 64 reguláciu leteckého snímkovania a vykonávanie geodetických a kartografických prác. Predmetné ustanovenia priamo neobsahujú zmienku o ochrane utajovaných skutočností. Prečo? Odpoveď je možné identifikovať v pôvode týchto ustanovení. Už prvá právna úprava oblasti ochrany informácií štátu zákon č. 102/1971 Zb. o ochrane štátneho tajomstva v §21 upravovala zákaz fotografovania a filmovania, v § 17 upravovala zariadenia na obranu vlasti a v §18 upravovala ich zoznam. Ustanovenia je v prvom rade potrebné vnímať v kontexte doby a vtedajších technických možností. Zároveň je možné predpokladať, že aj vynútiteľnosť zákazu fotografovania bola omnoho jednoduchšie realizovateľná. Princíp bol založený na vzťahu štátny záujem - dôležitý objekt - režim utajenia. Dôležité objekty a zariadenia boli chránené režimom utajenia, často bola utajovaná nielen ich primárna funkcia, ale utajovaná aj ich fyzická existencia. Zákon č. 102/1971 Zb. platil až do roku 1996, kedy bol nahradený zákonom č. 100/1996 Z.z. o ochrane štátneho tajomstva, služobného tajomstva, o šifrovej ochrane informácií a o zmene a doplnení Trestného zákona v znení neskorších predpisov. Tento už len prevzal ustanovenia o zákaze fotografovania a filmovania - §29 a doplnilo sa ustanovenie o leteckom snímkovaní a

²⁵ Bližšie v Brvnišťan, M. : Rozhodnutie o utajení ako základný predpoklad realizácie ochranných opatrení, In Zborník vedeckých a odborných prác, 8. Medzinárodná vedecká konferencia Národná a medzinárodná bezpečnosť 2015, Akadémia ozbrojených síl generála Milana Rastislava Štefánika 2017.

²⁶ Pozri bližšie §2 písm. c.) zákona o OUS.

²⁷ Pozri bližšie Zoznam utajovaných skutočností MO SR na <https://www.mod.gov.sk/data/files/560.pdf>

vykonávaní geodetických a kartografických prác - §30, ktoré v podstate s menšími zmenami platia až do dnešnej doby. §30 vznikol v dôsledku potreby riešiť novú situáciu, kedy sa právnické osoby (obchodné spoločnosti) budú podieľať na štátnych zákazkách, a teda im budú postupované utajované skutočnosti.

Platný zákon o OUS sa v § 63 zaoberá zákazom fotografovania a filmovania napriek tomu, že z objektívnych dôvodov je ustanovenie ťažko vynútiteľné. Jedným z dôvodov je aj technický a technologický pokrok, masové využívanie technológií, ktoré už nie sú pod kontrolou štátu (satelitné snímkovanie, navigácia, mobilné technológie, možnosti filmovania a záznamu a pod.). Obdobne v § 64 zákon o OUS upravuje ochranu snímkového materiálu, nakoľko sa predpokladá, že tento môže obsahovať utajované skutočnosti. Pri posudzovaní relevantnosti ustanovení § 63 a §64 je potrebné brať v úvahu, ako už bolo uvedené, aj praktickú nemožnosť utajenia objektov a zariadení podľa platnej legislatívy, vrátane posudzovania trestno-právnej zodpovednosti v prípade úniku alebo odcudzenia snímkového materiálu, ktorý má ochranu ako by išlo o utajenú skutočnosť²⁸.

V čase vzniku analyzovaných ustanovení problematika používania dronov neexistovala. Oblasť ochrany objektov štátneho významu a činnosti regulované v predmetných ustanoveniach boli s ohľadom na technický a technologický vývoj relatívne ľahko vynútiteľné a kontrolovateľné. Platila predstava, že v štátnom záujme je možné čokoľvek utajiť, a ak šlo o objekty a zariadenia bolo možné utajiť aj ich fyzickú existenciu. Zároveň existovali nástroje ako to zabezpečiť na rozdiel od súčasnosti platného zákona o OUS. Napr. príslušnému vedúcemu bolo umožnené rozhodnúť aj o „ďalších metódach ochrany“²⁹.

Napriek tomu, že problematika týkajúca sa oblasti fotografovania, filmovania a leteckého snímkovania je vskutku komplexná, možno konštatovať, že nebola snaha nájsť komplexné riešenie. Problémy vyplývajúce z aplikácie ustanovení § 63 a §64 zákona o OUS sa stali najviac vypuklými práve s rozvojom moderných technológií a masovým rozšírením používania dronov.

Čo by sa stalo ak by ustanovenia § 63 a §64 v platnom zákone neboli? Ako už bolo uvedené ich realizovateľnosť a vynútiteľnosť je pochybná. Bez prepojenia a vytvorenia väzieb na ostatné časti zákona o OUS a prípadne aj na iné oblasti je ich existenciu možné považovať za obsolétu.

Z hľadiska prevádzky dronov považujeme skôr za zásadné zaoberanie sa možnosťami identifikovania dronov, jeho majiteľa, respektíve osobu, ktorá dron ovláda.

Záver:

Drony a ich používanie sú oblasťou, ktorá poukazuje na nutnosť zaoberania sa využívaním nových, moderných technológií v bezpečnostnej praxi. Drony pre bezpečnostný systém štátu predstavujú abstraktné zhmotnenie spektra moderných technológií a ich možných dopadov na modernú spoločnosť.

V súčasnosti prebieha tzv. 4. technologická revolúcia, ktorá má potenciál položiť nové základy pre tvorbu bezpečnostných systémov. Víťazmi budú tí, ktorí budú schopní adekvátne reagovať na moderné bezpečnostné fenomény reprezentované novými technológiami. Nástup novej generácie technológií vo všeobecnosti formuje našu spoločnosť a bezpečnostný systém štátu. V minulosti moderné technológie a technologický náskok “západu” porazili “východ”, reprezentovaný najmä neschopnosťou efektívne reagovať na pokrok a z neho vyplývajúce bezpečnostné riziká. Nástup používania dronov reprezentuje podľa nášho názoru obdobnú situáciu v súčasnosti, preto by sme sa mali poučiť z minulosti a adekvátne reagovať. Nájsť vhodné a akceptovateľné riešenie nie je jednoduché, no je takmer isté, že problém nie je možné prehliadať. Technický a technologický pokrok je nezastaviteľný a bude vytvárať neustály tlak na zavedené

²⁸ Pozri bližšie § 64 ods.2 zákona o OUS.

²⁹ Zákon č. 100/1996 Z.z. umožňoval prostredníctvom napr. § 6 vytváranie aj ďalších podmienok ochrany.

bezpečnostné mechanizmy a právne prostredie. Možno konštatovať, že dynamika bezpečnostného prostredia sa neustále mení a je v príkrom protiklade so “stabilitou” bezpečnostného systému a právneho prostredia. Neefektívne a pomalé riadenie oblasti bezpečnosti a zbytočná byrokratizácia sú prekážkami na prijímanie efektívnych riešení. Dôsledky sa prejavujú v neschopnosti bezpečnostných systémov identifikovať hrozby a následne správne a včas reagovať na aktuálne hrozby. Uvedený stav je možné považovať za jedno z najzásadnejších bezpečnostných rizík súvisiacich s rozvojom a riadením bezpečnostných systémov. O to viac, ak ide o tak citlivé otázky, akými je oblasť ochrany informácií utajením. Je to potrebné zmeniť.

Za kľúčové preto považujeme vytvorenie mechanizmu, ktorý dokáže včas identifikovať potencionálne hrozby vyplývajúce z nových technológií a navrhnuť efektívne riešenie. Štát sa však nachádza v komplikovanej situácii, zaostáva. Súkromný sektor bude neustále prinášať nové technológie a riešenia. Súčasťou riešenia preto musí byť aj hľadanie efektívneho modelu spolupráce medzi štátnym a súkromným sektorom, zmeny v systéme regulácie a pravdepodobne aj čiastočné prenesenie zodpovednosti za bezpečnosť na súkromný sektor.

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.: Vybrané problémy analýzy bezpečnostných rizík v systémoch ochrany informácií, In Zborník vedeckých a odborných prác, 9. Medzinárodná vedecká konferencia Národná a medzinárodná bezpečnosť 2018, Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 25. - 26. október 2018, ISBN 978-80-8040

Brvnišťan, M.: Legal basis for the protection of the European union classified information, In Police Theory and Practice, ročník XXVI., Bratislava 1/2018, ISSN 1335-1370, str. 83-97

Brvnišťan, M. : Rozhodnutie o utajení ako základný predpoklad realizácie ochranných opatrení, In Zborník vedeckých a odborných prác, 8. Medzinárodná vedecká konferencia Národná a medzinárodná bezpečnosť 2015, Akadémia ozbrojených síl generála Milana Rastislava Štefánika 2017, ISBN 978-80-8040-515-1, str.33-41

Národná stratégia manažmentu bezpečnostných rizík Slovenskej republiky, schválená uznesením vlády SR č.3 z 13.1.2016

Rozhodnutie Rady z 23. septembra 2013, č. 2013(488)EU o bezpečnostných predpisoch na ochranu utajovaných informácií, OJ L 274/1 z 15.10.2013, Prístupné na internete: www.nbusr.sk, 2017 R

Security within the North Atlantic Treaty Organization (NATO) Bezpečnosť v rámci NATO, C-M(2002)49, NATO Archives – public version, rístupné na internete: www.nato.int, 2017

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

Zákon č. 143/1998 Z.z. o civilnom letectve a o zmene a doplnení niektorých zákonov

Rozhodnutie Dopravného úradu č. 1/2015, ktorým sa určujú podmienky vykonania letu lietadlom spôsobilým lietať bez pilota vo vzdušnom priestore Slovenskej republiky

Zákon č. 45/2011 Z.z. o kritickej infraštruktúre

Zákon č. 215/2014 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov

Nariadenie vlády č. 216/2004 Z.z, ktorým sa ustanovujú oblasti utajovaných skutočností

Zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Nariadenie Európskeho parlamentu a rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)

Vyhláška č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti

Vyhláška č. 339/2004 Z.z. o bezpečnosti technických prostriedkov