Bc. Marek Rechtik
Masarykova univerzita v Brně, Fakulta sociálních studií
student magisterského studia
Bc. Jakub Ondrůšek
Masarykova univerzita v Brně, Fakulta sociálních studií
student magisterského studia
Bc. Tomáš Siřinek
Masarykova univerzita v Brně, Fakulta sociálních studií
student magisterského studia

Hrozby vyplývající z použití doručovacích dronů v České republice

Úvod

V posledních letech dochází k výraznému rozmachu bezpilotních leteckých prostředků běžně označovaných jako drony. Stále častěji se dnes přitom uvažuje o využití dronů v oblasti doručovatelství, přičemž řada společností dnes již přistupuje k testovacímu provozu. Velký potenciál této technologie naznačuje, že v budoucnu dojde k masivnímu využívání těchto doručovacích dronů, přičemž tento trend se s velkou pravděpodobnosti nevyhne ani České republice. To s sebou přináší negativní bezpečnostní implikace, protože tyto drony ohrožuje řada intencionálních a neintencionálních hrozeb, které mohou mít negativní dopady nejen na zdraví a životy lidí, ale také na jejich soukromí. Cílem tohoto článku tak bude představit hlavní hrozby, které z využití doručovacích dronů vyplývají. Sekundárním cílem pak bude identifikovat aktéry v rámci ČR, kteří mohou mít zájem na zneužití doručovacích dronů.

Autoři se v úvodu zaměří na současný stav využití dronů v oblasti doručovatelství, mj. v kontextu nově přijatého regulačního rámce na úrovni Evropské unie. V rámci úvodní části bude rovněž krátce nastíněn předpokládaný vývoj využití doručovacích dronů v ČR. Následující kapitola je věnována analýze hrozeb vyplývajících z využití doručovacích dronů, přičemž v úvahu jsou brány jak hrozby kinetické, tak ty kybernetické. Na základě identifikovaných hrozeb se autoři v závěru pokusí o charakterizaci potenciálních rizikových aktérů.

Soudobý stav využití doručovacích dronů a přepokládaný vývoj v rámci ČR

Tento článek se zaměřuje na problematiku bezpilotních létajících prostředků využívaných k přepravě balíků, potravin nebo jiného zboží (běžně nazývaných také jako *doručovací drony*). Bezpilotní letoun *„je letadlo bez posádky, které může být řízeno na dálku, nebo létat samostatně pomocí předprogramovaných letových plánů nebo pomocí složitějších dynamických autonomních systémů.“*[1]

Zatímco pro armádní účely jsou bezpilotní letouny využívány již po několik desítek let, v poslední době dochází k jejich rozmachu i v civilní oblasti, což platí také

[1] Droneweb. (n.d.) Co je dron? (cit. 2021-1-19) (http://www.droneweb.cz/co-je-dron).

pro doručovací služby.[1] Zásadním přelomem ve vývoji v oblasti doručovacích dronů byl rok 2013, kdy Amazon ohlásil záměr přestavit svůj doručovací systém právě na základě doručovacích dronů.[2] Od té doby situace značně pokročila a od roku 2019 řada firem přistoupila k testovacímu provozu na území USA (kromě Amazonu se jedná také o společnosti Alphabet, UPS či AHA).[3] V testovací fázi se nachází také společnost DHL v Číně a některé další společnosti v afrických zemích, kde se zaměřují na donášky vakcín či převoz krevních vzorků.[4]

Právě využití doručovacích dronů v oblasti lékařství má velký potenciál, což potvrzuje také současná pandemie COVID-19. Doručovací drony se staly důležitým nástrojem v boji proti pandemii COVID-19[5] nejen kvůli možnosti donášek zdravotnického materiálu, ale také proto, že pomohly vytvořit odolnější dodavatelské řetězce a zajištění sociálního distancování při doručování. Této skutečnosti si jsou vědomy také regulační úřady v USA, které udělily společnostem provozujícím doručování pomocí dronů řadu regulačních výjimek.[6]

Potenciál bezpilotních letounů v doručovatelství je bezpochyby enormní. Očekává se možnost využití větších či menších dronů i bezpilotních nákladních letadel pro širokou škálu doručovatelských úkolů od donášek jídla přes rozvážení poštovních balíků až po přepravu těžkého vybavení na staveniště, do továren či na námořní plavidla.[7] Mezi hlavní faktory současného rozvoje doručovacích dronů lze řadit zejména nižší náklady a vyšší rychlost oproti tradičním doručovacím prostředkům.[8] Podle některých odhadů jsou provozní náklady na doručování pomocí dronů

---

[1] Transmetrics. (2019). The Evolution of Delivery Drones in Logistics. Trancsmetrics Blog. (cit. 2021-1-19) (https://transmetrics.eu/blog/delivery-drones-logistics/).

[2] E. Oswald. (2017, May 3). Here's everything you need to know about Amazon's drone delivery project, Prime Air. Digitaltrends. (cit. 2021-1-19) (https://www.digitaltrends.com/cool-tech/amazon-prime-air-delivery-drones-history-progress/).

[3] PALMER, A. (2020, August 31). Amazon wins FAA approval for Prime Air drone delivery fleet. CNBC. (cit. 2021-1-19) (https://www.cnbc.com/2020/08/31/amazon-prime-now-drone-delivery-fleet-gets-faa-approval.html).

[4] FEHR & PEERS. (2020). Drone Delivery: How will it affect your community? (cit. 2021-1-19) (https://www.fehrandpeers.com/drone-delivery/).
SANTHANAM, V. (2020, May 8). How drones could change the future of healthcare delivery. World Economic Forum. (cit. 2021-1-19) (https://www.weforum.org/agenda/2020/05/medical-drone-delivery-india-africa-modernize-last-mile/).

[5] Kromě afrických zemí jsou drony v současnosti využívány také pro donášky léků či zdravotnického materiálu např. v USA nebo Irsku. MOLLOY, D. & COPESTAKE, J. (2020, April 30). Drone-to-door medicines trial takes flight in Ireland. *BBC.com*. (cit. 2021-1-19) (https://www.bbc.com/news/technology-52206660).

[6] WOLF, H. (2020, July 6). We're about to see the Golden Age of drone delivery – here's why. World economic forum. (cit. 2021-1-19) (https://www.weforum.org/agenda/2020/07/golden-age-drone-delivery-covid-19-coronavirus-pandemic-technology/).

[7] Transmetrics. (2019). The Evolution of Delivery Drones in Logistics. Trancsmetrics Blog. (cit. 2021-1-19) (https://transmetrics.eu/blog/delivery-drones-logistics/).

[8] GARCIA, O. R.; SANTOSO, A. & JAVADI, M. M. (2019). Drone delivery systems: A comparative analysis in last-mile distribution. Massachusetts Institute of Technology. (cit. 2021-1-19) (https://ctl.mit.edu/sites/ctl.mit.edu/files/theses/20190521_Antonius_Santoso_DDS_research_fest_presentation_v8.pdf).

minimálně o 70% nižší než u dodávky.[1] Co se týče rychlosti, při testovacím provozu firmy DHL v Bavorsku byl jejich dron schopen donášky za pouhých 8 minut na vzdálenost 8 km, zatímco cesta autem by trvala půl hodiny. (DHL 2020) Výhodou je bezpochyby také menší environmentální dopad dronů ve srovnání s automobilovou dopravou.[2]

Tyto zásadní výhody tak logicky vedou doručovací společnosti k intenzivnímu úsilí, které by mělo umožnit rychlý nástup doručovacích dronů ve velkém měřítku. V cestě jim nicméně stojí řada překážek a výzev. Konkrétním bezpečnostním hrozbám spojeným s využíváním doručovacích dronů bude věnována pozornost až v další části, avšak již nyní lze zmínit, že doručovací drony mohou představovat celou řadu rizik. Nebezpečí představují poruchy dronů (porucha sensorů, motoru, logická chyba apod.), kolize (s ostatními drony či jinými objekty) nebo poničení (neintencionální či intencionální).[3] Bezpečnostní rizika navíc nejsou jediným problémem. Jednou z překážek je také hlučnost dronů, která je rovněž předmětem regulací.[4]

Z výše zmíněných důvodů je zřejmé, že regulace v oblasti doručovacích dronů je nezbytná. Narůstající hustota vzdušného prostoru zapříčiněná stále častějším využíváním dronů nicméně vyžaduje nový přístup k certifikaci bezpilotních prostředků.[5] Objevují se názory, že technologická úroveň současných dronů je dostatečná a překážky jsou tak pouze legislativní, nikoli technologické.[6] Andrew Charlton[7] tvrdí, že jádro problému neleží v hardware, ale přímo ve vzdušném prostoru. To, co bude potřeba k zajištění bezpečného provozu doručovacích dronů je tzv. *single*

---

[1] GOASDUFF, L. (2020, May 19). Why Flying Drones Could Disrupt Mobility and Transportation Beyond COVID-19. Gartner. (cit. 2021-1-19) (https://www.gartner.com/smarterwithgartner/why-flying-drones-could-disrupt-mobility-and-transportation-beyond-covid-19/?utm_medium=social&utm_source=twitter&utm_campaign=SM_GB_YOY_GTR_SOC_SF1_SM-SWG-CV&utm_content=&sf234174535=1).

[2] STOLAROFF, J. K. et al. (2018). Energy use and life cycle greenhouse gas emissions of drones for commercial package delivery. Nature communications, 9(1), 1-13. (cit. 2021-1-19) (https://www.nature.com/articles/s41467-017-02411-5).

[3] SCHENKELBERG, F. (2016). How reliable does a delivery drone have to be? 2016 annual reliability and maintainability symposium (RAMS). (cit. 2021-1-19) (https://www.researchgate.net/publication/301574679_How_reliable_does_a_delivery_drone_have_to_be).

[4] CHRISTIAN, A., CABELL, R. (2017). Initial Investigation into the Psychoacoustic Properties of Small Unmanned Aerial System Noise. NASA Langley Research Center (cit. 2021-1-19) (https://ntrs.nasa.gov/citations/20170005870).

[5] WOLF, H. (2018, March 27). Why we need to go back to the drawing board when it comes to regulating drones. World Economic Forum. (cit. 2021-1-19) (https://www.weforum.org/agenda/2018/03/millions-of-drones-will-make-us-air-traffic-unmanageable-within-a-few-years-unless-we-rethink-some-basic-rules/).

[6] Forbes Technology Council. (2018, October 4). Looking Ahead: 11 Predictions On How Drone Deliveries Will Work. Forbes. (cit. 2021-1-19) (https://www.forbes.com/sites/forbestechcouncil/2018/10/04/looking-ahead-11-predictions-on-how-drone-deliveries-will-work/#21492ecf51b3).

[7] CHARLTON, A. (2020, March 25). Getting Locked Down Underlines Why We Must Look Up And Work To Enable Drone Delivery. Forbes. (cit. 2021-1-19) (https://www.forbes.com/sites/andrewcharlton5/2020/03/25/getting-locked-down-underlines-why-we-must-look-up-and-work-to-enable-drone-delivery/#25810f947eeb).

point of truth – způsob, jak zjistit aktuální polohu každého vzdušného prostředku (od největšího komerčního dopravního letadla po nejmenší dron), a to na jedné platformě otevřené všem.

Tímto směrem směřuje také nový regulační rámec EU (ve formě nařízení), který definuje konkrétní požadavky na schopnosti dronů s cílem dosažení maximální bezpečnosti. Jedním z příkladů takových požadavků je právě zajištění individuální identifikace každého dronu, která umožní vnitrostátním orgánům včasně reagovat v případě potřeby.[1] Cílem evropského regulačního rámce je zajistit bezpečný provoz dronů skrze řadu technických a operačních požadavků a zároveň umožnit agilnost a inovativnost a celkový rozvoj celého odvětví. Nařízení také umožňuje členským státům Agentury Evropské unie pro bezpečnost letectví vysoký stupeň flexibility v podobě vymezení zón na svém území, kde bude provoz dronů zakázán nebo omezen. Velký důraz v rámci nařízení je kladen také na dodržování evropské i národní úpravou spojené s ochranou soukromí a ochranou osobních údajů.[2]

Evropský regulační rámec, který se v České republice (a všech ostatních členských státech EU) uplatňuje od 31. 12. 2020, rozděluje tři základní kategorie bezpilotních letounů, a to *otevřenou, specifickou* a *certifikovanou*.

V rámci otevřené kategorie není vyžadováno předchozí povolení[3] příslušného úřadu, ani prohlášení provozovatele bezpilotního letounu před uskutečněním provozu, nicméně je poměrně zásadně omezen jejich provoz. Operátor může s dronem létat pouze na vzdálenost vizuálního dosahu, může létat pouze do výšky 120 m, a to dronem vlastní výroby či dronem splňujícím technické požadavky definované v nařízení[4]. Tato kategorie je pak dále rozčleněna na několik tříd, přičemž pro každou třídu dronů platí další provozní omezení (např. vzdálenost, která musí být udržována mezi dronem a nezúčastněnými osobami).[5]

V rámci specifické kategorie je vyžadováno povolení příslušného úřadu před uskutečněním provozu. Toto povolení lze získat na základě provedení standardizované metody hodnocení rizik a definování mitigačních opatření. Do této kategorie budou typicky spadat zejména drony operující mimo vzdálenost vizuálního dosahu operátora a drony vážící více než 25 kg.[6]

---

[1] Drone Rules. (2019, June 13). EASA: EU wide rules on drones published. (cit. 2021-1-19) (https://dronerules.eu/cs/professional/news/easa-eu-wide-rules-on-drones-published).

[2] Úřad pro civilní letectví. (2020). Příprava společných evropských pravidel. (cit. 2021-1-19) (https://www.caa.cz/provoz/letadla-bez-pilota-na-palube/priprava-spolecnych-evropskych-pravidel/).

[3] Povolení je potřeba rozlišovat od registrace. Zatímco v otevřené kategorii není předchozí povolení vyžadováno, registrovat je potřeba každý dron nad hmotnost 250 g nebo každý dron nesoucí kameru či jiný sensor schopný sběru osobních dat. EASA. (2020a). Civil drones (Unmanned aircraft). (cit. 2021-1-19) (https://www.easa.europa.eu/domains/civil-drones-rpas).

[4] K prokázání souladu s definovanými požadavky budou drony, které lze provozovat v otevřené kategorii, opatřeny identifikačním štítkem příslušné třídy.

[5] Drone Rules. (2020) EU Regulations Updates. (cit. 2021-1-19) (https://dronerules.eu/cs/professional/eu_regulations_updates).

[6] Ibid.

Pravidla vztahující se na kategorii certifikované budou do značné míry stejná jako u letadel ovládaných piloty. Do certifikované kategorie totiž budou spadat velké drony létající v řízeném vzdušném prostoru. U takových bezpilotních systémů bude vyžadována certifikace bezpilotního systému, osvědčení způsobilosti dálkově řídícího pilota a schválení provozovatele příslušným úřadem. V současné době však není tato kategorie blíže specifikována a bude tak předmětem následné etapy vývoje regulačního rámce.[1]

Jak bylo zmíněno výše, hlavní potenciál doručovacích dronů leží v jejich nízkých nákladech. Klíčové je zde přitom snížení nákladů za lidskou pracovní sílu, čehož má být dosaženo pomocí automatizace a autonomizace. *Autonomní dron* je schopen provést bezpečný let bez zásahu pilota (činí tak pomocí umělé inteligence, která mu umožňuje zvládat všechny druhy nepředvídaných a nepředvídatelných mimořádných situací), čímž se liší od *automatických dronů*, které letí předem určené trasy definované operátorem dronu před stanoveným letem. U automatického typu dronu je zásadní, aby vzdálený pilot převzal kontrolu nad dronem a zasáhl při nepředvídaných událostech, pro které dron nebyl naprogramován. Zatímco automatické drony jsou povoleny ve všech kategoriích, autonomní drony nejsou povoleny v kategorii otevřené (spadají do kategorie specifické a certifikované).[2] Právě autonomní drony představují do budoucna cílovou kategorii, která má podle některých odborníků potenciál redefinovat celé dodavatelské odvětví.[3]

Co se týče technické stránky, v současné době nelze nalézt vzorový softwarový design pro dronové systémy a dochází tak k rozvoji řady různých softwarových architektur.[4] Podobně je tomu také v oblasti síťové infrastruktury. V současnosti využívaná infrastruktura zahrnuje point-to-point sítě, celulární sítě, satelitní systémy, do budoucna se však uvažuje například také o cloudové infrastruktuře.[5] V rámci EU nicméně nyní dochází ke snahám o harmonizaci a konvergenci klíčových technologií a softwaru pro autonomní drony (včetně integrované architektury) s cílem vytvoření holistického ekosystému zvaného *U-space*.[6]

---

[1] Drone Rules. (2020) EU Regulations Updates. (cit. 2021-1-19) (https://dronerules.eu/cs/professional/eu_regulations_updates)

[2] EASA. (2020b). FAQ n.116449. (cit. 2021-1-19) (https://www.easa.europa.eu/faq/116449.

[3] SCHRÖDER et al. (2018). Fast forwarding last-mile delivery – implications for the ekosystém. McKinsey & Company. (cit. 2021-1-19) (https://www.mckinsey.com/~/media/mckinsey/industries/travel%20transport%20and%20logistics/our%20insights/technology%20delivered%20implications%20for%20cost%20customers%20and%20competition%20in%20the%20last%20mile%20ecosystem/fast-forwarding-last-mile-delivery-implications-for-the-ecosystem.ashx).

[4] LADEIRA, M.; OUHAMMOU, Y. & GROLLEAU, E. (2020). Towards a modular and customisable model-based architecture for autonomous drones. 2020 IEEE 44th Annual Computers, Software, and Applications Conference. (cit. 2021-1-19) (https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9202678&casa_token=Fell-Mc2L2MAAAAA:DZ51veZ87pRYCMQcWW8AnhkYdhWA16Nmv1VJIQEWEbKmQ5lDlR38eIfTZVaZYHSZrHbjaYOlWw&tag=1).

[5] VORUGANTI, K. (2019, June 24). The Future of: Has the Age of Drones (Finally) Arrived? Equinix. (cit. 2021-1-19) (https://blog.equinix.com/blog/2019/06/24/the-future-of-has-the-age-of-drones-finally-arrived/.

[6] NOUACER, R. et al. (2020). Towards a Framework of Key Technologies for Drones. Microprocessors and Microsystems. (cit. 2021-1-19)

V ČR provoz dronů momentálně reguluje Doplněk X leteckého předpisu L2,[1] nicméně v následujících dvou letech dojde k postupnému přejímání a implementace evropského regulačního rámce. V rámci ČR dochází ke stále častějšímu využívání dronů, a to nejen pro rekreační, ale také pro komerční účely.[2] Drony v Česku využívají také bezpečnostní složky i záchranné sbory,[3] nicméně co se týče doručovacích dronů, je současná situace naprosto odlišná. V roce 2016 došlo k prvnímu testu doručení zásilky pomocí dronu českým e-shopem Mall.cz, který o rok později následoval další český e-shop PoštovnéZDARMA.cz.[4] Oba e-shopy tak učinily pod dohledem Úřadu pro civilní letectví, a ačkoli zkušební test obsáhl celý doručovací proces (od ověření celého procesu objednání zákazníkem přes identifikaci v distribučním centru až po převzetí dronem, který zásilku doručil přímo zákazníkovi) v obou případech šlo spíše o propagační akci. Od té doby totiž k zásadnějšímu pokroku nedošlo a podle provozovatelů výše zmíněných e-shopů byla (a nadále zůstává) hlavní příčinou současná legislativa.[5]

Situace by se tedy měla změnit s nástupem nového regulačního rámce EU, nicméně i přesto nelze v oblasti doručovacích dronů v rámci ČR očekávat převratný vývoj. Naopak, očekávat lze postupný rozvoj kopírující zahraniční trendy. To znamená, že nejprve bude docházet k testovacím provozům doručovatelských společností za dohledu a spolupráce Úřadu pro civilní letectví. Nejpravděpodobnějšími aktéry budou zejména české e-shopy jako např. již zmiňovaný Mall.cz. Nelze vyloučit zájem poboček společností testujících doručovací drony jinde ve světě (např. Amazon, DHL či UPS). Testovací provoz pak bude uskutečňován mimo velká města zejména v řídce obydlených oblastech v rámci vymezených leteckých koridorů. Podle současných odhadů dojde v USA k zavedení běžného provozu zhruba v roce 2025,[6] což znamená,

---

(https://www.sciencedirect.com/science/article/pii/S0141933120303094?casa_token=UfeKHTJIbOwAAAAA:LIfDXIjdWkyL7xn1cZkbH0QyPUuRpTDvuOVPk5vY0sRlNixWjrF7kQRI0fKoBAJsZUy7jXNpdw).

[1] Úřad pro civilní letectví. (2019). Podle kterého předpisu se řídí provoz bezpilotních letadel / systémů? (cit. 2021-5-4) (https://www.caa.cz/provoz-stare/letadla-bez-pilota-na-palube/provoz-ostatnich-letadel-bez-pilota-na-palube/podle-ktereho-predpisu-se-ridi-provoz-bezpilotnich-letadel-systemu/).

[2] LIEBREICH, J. (2020, February 12.) České nebe zaplavují drony. Rekordy lámou i pokuty. E15.cz. (cit. 2021-1-19) (https://www.e15.cz/domaci/ceske-nebe-zaplavuji-drony-rekordy-lamou-i-pokuty-1366693).

[3] Policie České republiky. (2020, March 9). Vybavení Letecké služby PČR novými drony. (cit. 2021-1-19) (https://www.policie.cz/clanek/vybaveni-letecke-sluzby-pcr-novymi-drony.aspx).
HZS ČR. (2020). Hasiči převzali speciální techniku – velitelský vůz s dronem. https://www.hzscr.cz/clanek/hasici-prevzali-specialni-techniku-velitelsky-vuz-s-dronem.aspx).

[4] Mall.cz. (2016, November 22). Mall.cz úspěšně otestoval doručování dronem. Balíček předal za 3 minuty. (cit. 2021-1-19) (https://www.mall.cz/tiskova-zprava-16-11-22).
ČESAL, L. (2017, červenec 12). První zásilka dronem doručena. PoštovnéZDARMA.cz. (cit. 2021-1-19) (https://postovnezdarma.cz/blog/535-doruceni-dronem/).

[5] Mall.cz. (2016, November 22). Mall.cz úspěšně otestoval doručování dronem. Balíček předal za 3 minuty. (cit. 2021-1-19) (https://www.mall.cz/tiskova-zprava-16-11-22).
HORČÍK, J. (2017, July 13). Český e-shop umí doručovat zásilky dronem. (cit. 2021-1-19) (http://www.hybrid.cz/cesky-e-shop-umi-dorucovat-zasilky-dronem).

[6] GOASDUFF, L. (2020, May 19). Why Flying Drones Could Disrupt Mobility and Transportation Beyond COVID-19. Gartner. (cit. 2021-1-19)

že rozsáhlejší využívání doručovacích dronů v ČR nelze očekávat dříve než v druhé polovině této dekády.

Přehled hrozeb vyplývajících z využití doručovacích dronů

V současnosti je provoz doručovacích dronů záležitostí testování,[1] řada hrozeb tak doposud zůstává skryta. Aktuálně lze identifikovat pouze hrozby obecného charakteru vyplývající z konceptu účelu využívání této technologie či z proběhlých technologických studií zaměřující se na hrozby komerčním dronům. Specifičtější hrozby doručovacím dronům se začnou manifestovat ve chvíli, kdy bude docházet k testovacím provozům, a plně se manifestují až při plném spuštění provozu. Rovněž celá řada hrozeb vyplývajících z autonomie a na ní závislému konceptu rojení zůstává v tuto chvíli záležitostí úvah. Hrozby vyplývající z aplikací doručovacích dronů lze v současnosti rozčlenit na dvě kategorie:

a) hrozby vůči samotným dronům (primární) a

b) hrozby pocházející od dronů (sekundární).

Hrozby dronům jako doručovacímu systému

Hrozby pocházející z kyberprostoru

Z hlediska kybernetické bezpečnosti lze bezpilotní prostředky zařadit do konceptu internetu věcí (IoT) čelí tedy stejným hrozbám, které se manifestují zde. Jelikož se v modelu IoT, resp. u dronů, klade důraz na efektivitu, dostupné výpočetní kapacity jsou dedikované k provádění esenciálních úkolů potřebných pro fungování systému. Na zabezpečení pak zbývá velmi malá, nebo zcela žádná výpočetní kapacita.[2] Stejný problém se pak týká komunikačních protokolů a sítí, které se mohou pro IoT užívat, např. Bluetooth,[3] ZigBee,[4] Z-Wave,[5] LoRaWAN[6] aj. Hrozby vůči dronům pocházející z kyberprostoru dále rozdělit na útoky na samotný dron a útoky na dodavatelský řetězec.

(https://www.gartner.com/smarterwithgartner/why-flying-drones-could-disrupt-mobility-and-transportation-beyond-covid-19/?utm_medium=social&utm_source=twitter&utm_campaign=SM_GB_YOY_GTR_SOC_SF1_SM-SWG-CV&utm_content=&sf234174535=1).

[1] PALMER, A. (2020, August 31). Amazon wins FAA approval for Prime Air drone delivery fleet. CNBC. (cit. 2021-1-19) (https://www.cnbc.com/2020/08/31/amazon-prime-now-drone-delivery-fleet-gets-faa-approval.html).

[2] GUPTA, B. and Quamara, Megha. (2020). Internet of Things Security. Boca Raton: CRC Press.

[3] CIMPANU, Catlin. (2020). Billions of devices vulnerable to Bluetooth security flaw. Zdnet.com. https://www.zdnet.com/article/billions-of-devices-vulnerable-to-new-blesa-bluetooth-security-flaw/).

[4] KHANJI, Salam et al. (2019). ZigBee Security Vulnerabilities. Ieeexlore.ieee.org. https://ieeexplore.ieee.org/document/8809115).

[5] GUPTA, Pamela and OutSecure. (2019). Mitigating Risks From A to Z-Wave. Securityindustry.org. https://www.securityindustry.org/2019/04/23/mitigating-risks-from-a-to-z-wave/).

[6] YANG, Xueying et al. (2018). Security Vulnerabilities in LoRaWAN. Ieeexlore.ieee.org. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8366983).

Kybernetické útoky na dron mohou v podstatě nabývat trojí podoby:

- unesení (tzv. hijacking),
- zničení a
- zapojení dronů do botnetu.

V případě unesení převezme útočník nad samotným dronem kontrolu, a následně jej může využít pro další aktivity, např. k:

- zisku dat z dronu (identifikační či doručovací údaje zákazníků, informace o letových trasách atp.),[1]
- k manipulaci senzorů dronu (např. vizuálních senzorů k pořizování fotografických či video materiálů),[2]
- ke změně letových tras anebo k celkové manipulaci motorické kontroly nad dronem (a následnému způsobení materiální či fyzické škody).[3]

Řada technických výzkumů ověřující zabezpečení dronů ukazuje, že unést dron je relativně snadné. Některé drony mohou mít slabý autentizační mechanismus, případně může zcela absentovat. Tyto útoky jsou relativně jednoduché, k jejich provedení postačí chytrý telefon.[4] Rovněž se ukazují možnosti unést dron pomocí útoků na jimi využívané komunikační protokoly, případně útoky pomocí laseru, který do dronu vysílá falešné signály (tzv. fault injection).[5] Dalšími možnými způsoby mohou být de-autentizační útoky,[6] rušení signálu (tzv. jamming),[7] vysílání klamných GPS signálů (tzv. GPS spoofing)[8] či malware a zranitelnosti nultého dne.[9] Všechny tyto útoky se týkají napadení jednotlivých dronů, většinu z nich však dokáže provést i relativně nesofistikovaný útočník.

---

[1] AKRAM, Raja N. (2017). Secure Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements. Ieexplore.ieee.org (cit. 2020-11-1) (https://ieeexplore.ieee.org/document/7846999).

[2] BEST, Katharina L. et al. (2020). How to Analyze the Cyber Threat from Drones. Rand.org. (cit. 2020-11-1) (https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2972/RAND_RR2972.pdf).

[3] Ibid.

[4] VALENTE, Junia and Alvaro CADRENAS. (2017). Understanding Security Threats in Consumer Drones Through the Lens of the Discovery Quadcopter Family. Dl.acm.org (cit 2020-11-1) (https://dl.acm.org/doi/pdf/10.1145/3139937.3139943).

[5] AKRAM, Raja N. (2017). Secure Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements. Ieexplore.ieee.org (cit. 2020-11-1) (https://ieeexplore.ieee.org/document/7846999).

[6] VALENTE, Junia and Alvaro CADRENAS. (2017). Understanding Security Threats in Consumer Drones Through the Lens of the Discovery Quadcopter Family. Dl.acm.org (cit 2020-11-1) (https://dl.acm.org/doi/pdf/10.1145/3139937.3139943).

[7] AKRAM, Raja N. (2017). Secure Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements. Ieexplore.ieee.org (cit. 2020-11-1) (https://ieeexplore.ieee.org/document/7846999).

[8] KERNS, Anderw. J. (n.d.). Unmanned Aircraft Capture and Control via GPS Spoofing. Radionavlab.ae.utexas.edu (cit. 2020-11-1) (https://radionavlab.ae.utexas.edu/images/stories/files/papers/unmannedCapture.pdf)

[9] PAGANINI, Pierluigi. (2015, January 27). A hacker developer Maldrone, the first malware for drones. Securityaffairs.co (cit. 2020-11-1) (https://securityaffairs.co/wordpress/32767/hacking/maldrone-malware-for-drones.html).

Závažnější hrozba spočívá v možnosti unést či zmanipulovat roj dronů (tzv. swarm). Koncept rojení přináší do zabezpečení sítí a vzájemné komunikace mezi drony značné problémy, jelikož je potřeba zvažovat efektivitu takové sítě a komunikace. Její bezpečnost tak nemusí být prioritou.[1] V případě, že se útočníkovi podaří nabourat do sítě či komunikace využívané roji, může dojít k manipulaci celého shluku. Přičemž jakákoliv metoda využívaná pro komunikaci roje (rádiová frekvence či LTE) může být relativně snadno narušena či zachycena.[2] Z výše zmíněných útoků lze v současnosti jako prostředek pro napadení celého shluku uvažovat malware, a to kvůli schopnosti jeho proliferace v napadené síťové infrastruktuře dedikované pro drony. Zda bude možné zmanipulovat celý shluk pomocí dalších zmíněných útoku je v současnosti nejisté.

Zničení dronů lze z pohledu kybernetické bezpečnosti v podstatě provést dvěma způsoby (mimo jeho unesení a následný nálet do překážky), a sice pomocí odepření služby (tzv. DoS) či distribuované odepření služby (tzv. DDoS) anebo malware (tzv. bricking). DoS a DDoS jsou široce známé a snadno proveditelný útoky. K jejich provedení existuje na webu řada manuálů i nástrojů,[3] v rámci dark webu lze dokonce poptávat infrastrukturu k provedení DDoS útoků za relativně nízkou cenu.[4] Následkem takového útoku je negativně ovlivněna funkčnost dronů za letu, což může vést k jeho zřícení.[5] Závažnějším útokem je zamrazení (tzv. bricking). Útok spočívá na malwaru, který infikuje cílové zařízení a fakticky jej přivede do stavu trvalé nepoužitelnosti.[6] Závažnost tohoto útok umocňuje možnost, že v případě nakažení jednoho dronu se

---

[1] CAMPION, Mitch et al. (n.d). A Review and Future Directions of UAV Swarm Communication Architectures. Und.edu (cit. 2020-11-1) (https://und.edu/research/rias/_files/docs/swarm_ieee.pdf).
ASHISH, Thomas et al. (2016). Secure Link Establishment Method to Prevent Jelly FIsh Attack in MANET. Ieexplore.ieee.org (cit. 2020-11-1) (https://ieeexplore.ieee.org/document/7546277).

[2] BARTOCK, Michael. (n.d.). LTE Security. Csrc.nist.gov (cit. 2020-11-1) (https://csrc.nist.gov/CSRC/media/Presentations/LTE-Security-How-Good-is-it/images-media/day2_research_200-250.pdf).
HIGGINS, Fiona et al. (2009). Survey on Security Challenges for Swarm Robotics. Ieexplore.ieee.org (cit. 2020-11-1) (https://ieeexplore.ieee.org/document/4976621).

[3] DoS Attack Tutorial. (n.d.). Guru99.com (cit. 2020-11-1) (https://www.guru99.com/ultimate-guide-to-dos-attacks.html).

[4] The Dark Web. (2020, August 26). The Dark Web: DDoS Attacks Sell for as Low as $10 Per Hour. Missioncriticalmagazine.com (cit. 2020-11-1) (https://www.missioncriticalmagazine.com/articles/93185-the-dark-web-ddos-attacks-sell-for-as-low-as-10-per-hour).

[5] VASCONCELOS, Gabriel et al. (2019). Evaluation of DoS attacks on commercial Wi-Fi-based UAVs. International Journal of Computer Netwok and Information Security (11), no. 1, pp, 212-222 (cit. 2020-11-1) (https://www.researchgate.net/publication/332704018_Evaluation_of_DoS_attacks_on_commercial_Wi-Fi-based_UAVs).
YAACOUB, Jean-Paul et al. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. Ncbi.nlm.nih.gov (cit. 2020-11-1) (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7206421/).

[6] O'DONNELL, Lindsey. (2019, June 27). Thousands of IoT Devices Bricked By Silex Malware. Threatpost.com (cit. 2020-11-1) (https://threatpost.com/thousands-of-iot-devices-bricked-by-silex-malware/146065/).

může malware snadno rozšířit a nakazit ostatní drony či zařízení připojených do stejné sítě. Stejné možnosti zničení lze aplikovat rovněž v případě rojů, byť ty mohou být o něco odolnější vůči útoku odepření služby, jednak kvůli vyššímu nároku na výpočetní kapacity útoku pro ovlivnění sítě, jednak kvůli možnosti zabudovat komplexnější bezpečnostní mechanismy k snížení jeho dopadu.

Poslední z kybernetických hrozeb vůči dronům je jejich zapojení do botnetu pomocí malware. Útočník, který takový botnet ovládá (tzv. botmaster), jej pak může využít k řadě dalších útoků (DDoS, šíření spamu, reklamním podvodům) anebo botnet za úplatu pronajímat jiným.[1] Jak ukazuje řada volně dostupných návodů na webu, vytvoření botnetu je opět jednoduchá záležitost.[2]

Útok na dodavatelský řetězec spočívá ve zneužití zranitelností třetích stran, které primárnímu cíli útoku dodávají služby.[3] Útok lze rovněž rozčlenit do několika kategorií, v závislosti na tom, na jaký článek tohoto řetězce se útočník zaměřuje.

První kategorií je výrobce. Řada komponentů se dnes vyrábí v zahraničí, resp. v zemích s nízkými výrobními náklady. Existuje riziko, že v dronu vyráběném v zahraničí, anebo jeho části, bude přítomný hardware či software umožňující neautorizovaný vzdálený přístup (backdoor).

Druhou kategorií je dodavatel software či dalších služeb, které organizace využívá. Může jít např. o dodavatele software pro pilotování dronů. Útok na dodavatelský řetězec může vyústit ve zcizení dat z dronů, případně i databází využívaných danou společností pro ukládání dat. Rovněž také k unesení či zničení nejen samotného dronu, ale vzhledem k povaze útoku téměř jistě i celého shluku.

Hrozby kinetické povahy

Mimo hrozeb pocházejících z kyberprostoru je možno drony poškodit či zničit i kinetickou silou. Maximální možná výška letu dronu je legislativou ustavena na 120 metrů, jsou tedy sestřelitelné, a to i vzduchovkami či krátkými střelnými zbraněmi.[4] Rovněž může dojít k napadení dronů ptactvem.[5]

---

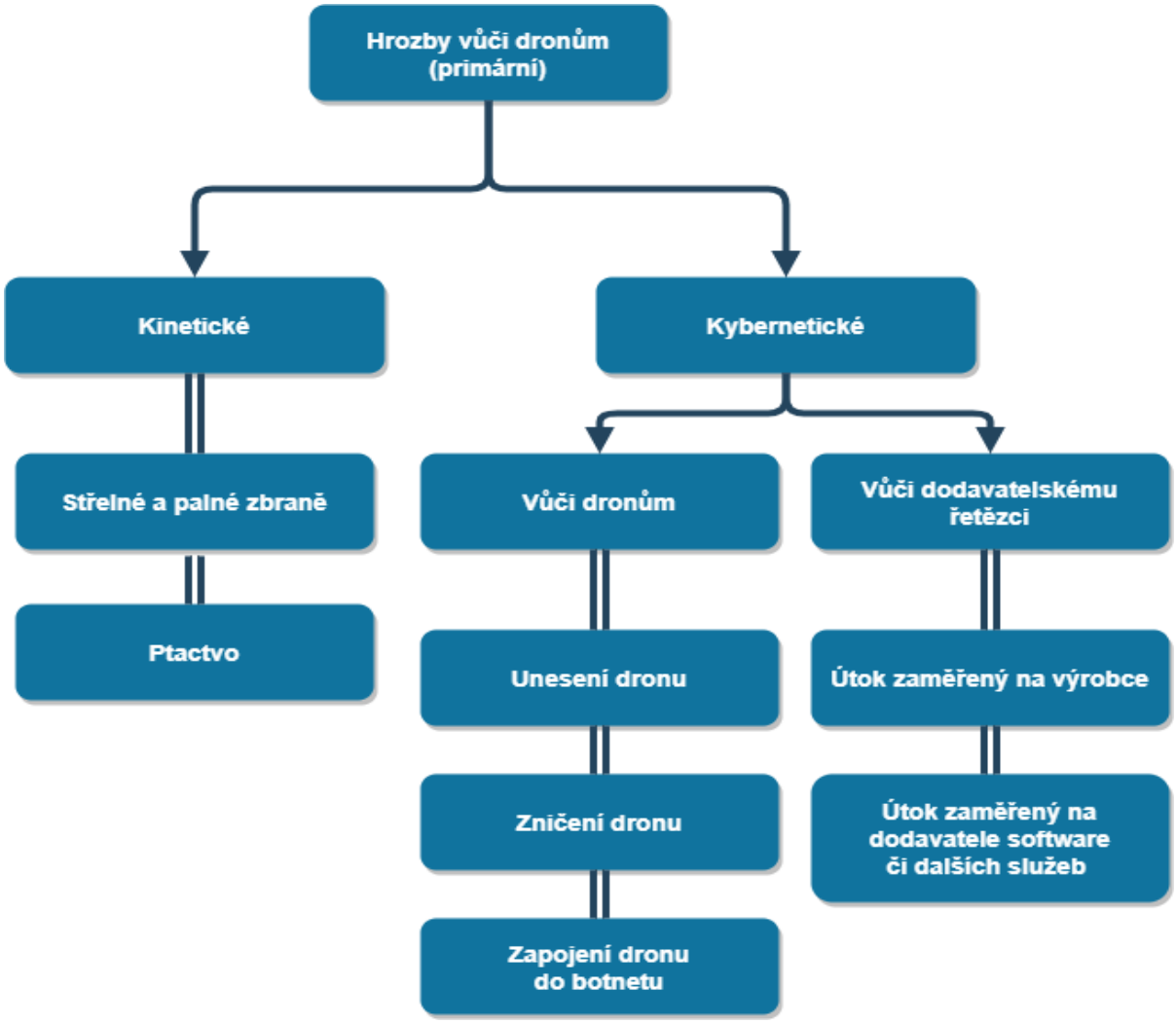
[1] What is a botnet? (2017, December 5). Pandasecurity.com (cit. 2020-11-1) (https://www.pandasecurity.com/en/mediacenter/security/what-is-a-botnet/).
GATES, Megan. (2020 July 1). Flight Risks. Asisonline.org (cit. 2020-11-1) (https://www.asisonline.org/security-management-magazine/articles/2020/07/flight-risks/).

[2] MULLIS, Simon. (2013, August 2). Cybercriminal Intent. Fireeye.com (cit. 2020-11-1) (https://www.fireeye.com/blog/executive-perspective/2013/08/cybercriminal-intent-how-to-build-your-own-botnet-in-less-than-15-minutes.html).

[3] TOWNSEND, Kevin. (2019, September 26). Sky-high concerns. Blog.avast.com (cit. 2020-11-1) (https://blog.avast.com/what-security-threats-are-posed-by-drones).

[4] LIMER, Eric. (2015, August 6). How to Shoot Down a Drone. Popularmechanics.com (cit. 2020-11-1) (https://www.popularmechanics.com/flight/drones/how-to/a16756/how-to-shoot-down-a-drone/).

[5] European Environment Agency. (2020). Drivers of change Delivery drones and the environment. (cit, 2021-1-19). (https://www.eea.europa.eu/publications/delivery-drones-and-the-environment/at_download/file).



Obr. č. 1 Hrozby dronům jako doručovacímu systému

Hrozby vyplývající z využití tohoto systému pro společnost

Hrozby pocházející od dronů směrem ke společnosti lze rozčlenit na:

- hrozby soukromí,
- hrozby kybernetické bezpečnosti a
- hrozby fyzické bezpečnosti.

Hrozby vůči soukromí

Komerční drony jsou zpravidla vybaveny audio-vizuálními sensory.[1] Tyto sensory mohou být účelně zneužity k narušení soukromí obyvatel, resp. mohou pořizovat fotografie či nahrávky, ze strany potenciálních útočníku anebo operátorů doručovacích dronů.

[1] MIAH, Andy. (2020). Drones: The Brilliant, the Bad and the Beautiful. Bingley: sEmerald Publishing.

Drony mají kapacity ke sběru, přenosu a ukládání dat.[1] O jaký konkrétní typ dat jde, záleží na senzorech umístěných na dronu a na účelu jejich nasazení. Téměř jistě budou drony obsahovat přinejmenším identifikační a adresní informace zákazníků, ať už přímo ve své paměti anebo nepřímo v podobě přístupu do databází dané společnosti. Taková data pak mohou být terčem útoku. Jaká další data budou drony z pohledu legislativy moci sbírat a jaký sběr dat bude v zájmu komerčních společností je nejisté.

Obecně se pak dá odůvodněně předpokládat, že pokud to dovolí legislativní normy, budou drony sbírat taková data, která jim poskytnou nějakou konkurenční výhodu, což se však v důsledku může bít se soukromým fyzických osob. Např. v tomto směru průkopnická společnost Amazon uvažuje, že její doručovací drony budou zachycovat vizuální data z domů, nad kterými proletí. Taková data by se pak dle úvah společnosti daly využívat k upozornění majitelů na případné poškození střech aj.[2]

Hrozby vůči kybernetické bezpečnosti

Hrozby, které drony představují kybernetické bezpečnosti, lze vnímat dvojím způsobem. Jednak mohou kvůli svému nízkému zabezpečení[3] představovat slabý článek, potenciální vstupní bod, který může být využit pro získání přístupu do širších sítí či databází, které jsou primárním cílem aktéra. Komerčně dostupné drony jsou čím dál více sofistikované. Zvyšující se sofistikovanost hardware a software tvoří problémy nejen pro sledování a ověření všech procesů, které na daném dronu probíhají, ale i pro identifikaci možných zranitelností.[4]

O dronech lze rovněž uvažovat jako o nástroji k provádění kybernetických útoků. Drony mohou sloužit jako samostatný nástroj pro infikování jiných zařízení a jejich zapojení do botnetu,[5] případně jako nástroj k vedení útoků na ad hoc sítě využívané pro IoT,[6] jako součástí botnetu mohou být využity pro provádění DDoS útoků[7] anebo

[1] MIAH, Andy. (2020). Drones: The Brilliant, the Bad and the Beautiful. Bingley: sEmerald Publishing.
[2] STERN, Matthew. (2017, August 17). Should drones be used for data collection in addition to deliveries?. Retailwire.com (cit. 2020-11-1) (https://retailwire.com/discussion/should-drones-be-used-for-data-collection-in-addition-to-deliveries/).
[3] WALTERS, Sanders. (2016, October 29). How Can Drones Be Hacked? The updated list of vulnerable drones & attack tools. Medium.com (cit. 2020-11-1) (https://medium.com/@swalters/how-can-drones-be-hacked-the-updated-list-of-vulnerable-drones-attack-tools-dd2e006d6809).
[4] BEST, Katharina L. et al. (2020). How to Analyze the Cyber Threat from Drones. Rand.org. (cit. 2020-11-1) (https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2972/RAND_RR2972.pdf).
[5] REED, T., GEIS, J. (n.d.). SkyNET: a 3G-enabled mobile attack drone and stealth botmaster. Usenix.org (cit. 2020-11-1) (https://www.usenix.org/legacy/event/woot/tech/final_files/Reed.pdf).
[6] RONEN, Eyal et al. (2018). IoT GOes Nuclear. Ieeexplore.ieee.org (cit. 2020-11-1) (https://ieeexplore.ieee.org/document/8283484).
[7] FRUHLINGER, Josh. (2018, March 9). The Mirai botnet explained. Csoonline.com (cit. 2020-11-1) (https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

k odposlouchávání komunikace na jiných zařízeních užívajících bezdrátové protokoly.[1]

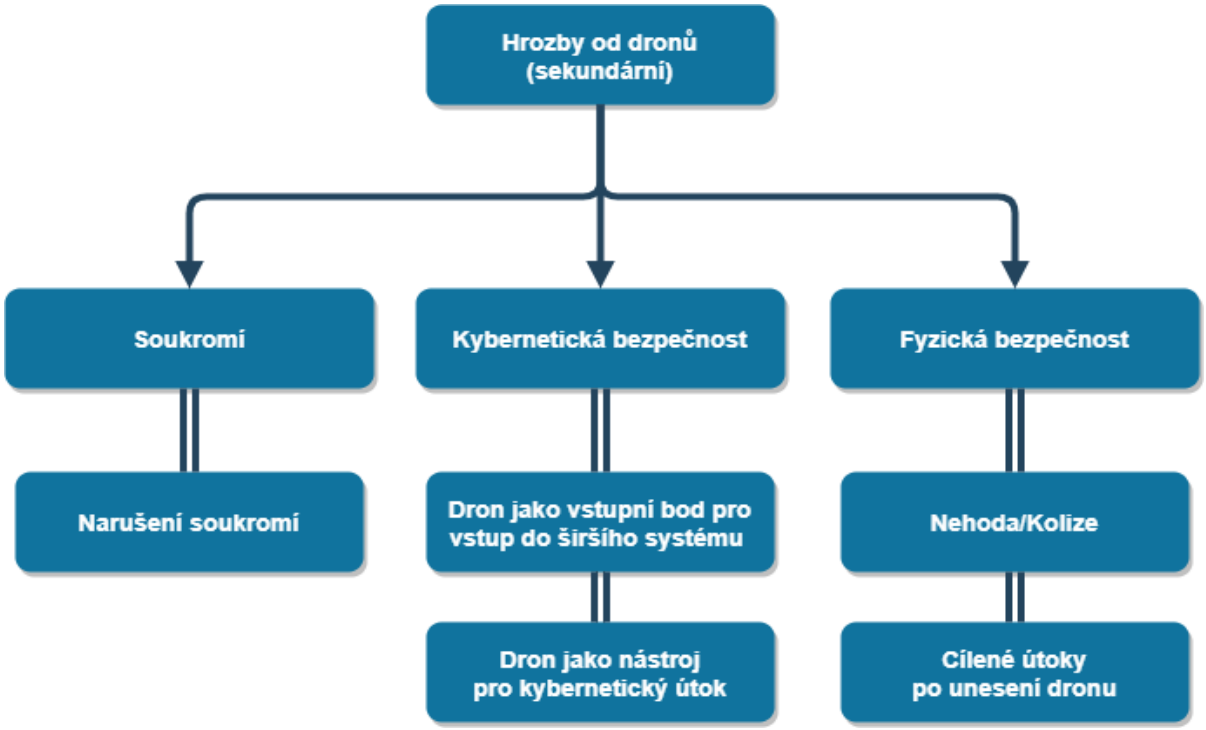
Hrozby vůči fyzické bezpečnosti

Hrozby fyzické bezpečnost mohou nabývat podob od nehod po cílené útoky. K nehodám může docházet, když se dron vymkne kontrole nebo se střetne s ptactvem. Pokud budou drony pilotované operátory, může dojít k lidské chybě, a následné kolizi dronu s jiným dronem či fyzickými objekty anebo lidmi. K takové nehodě došlo např. během triatlonového závodu v Austrálii.[2] Mj. může dojít k poruše hardware či software dronu, které rovněž vyústí v kolizi. To stejné platí v případě autonomních řešení a rojení.

Byť legislativa EU zamezuje dronům let v určitých zónách, tyto restrikce budou vynucovány skrze software, který lze modifikovat, a dronu tak let v zakázaných zónách umožnit.[3] V případě, že útočník dokáže unést roj dronů a tuto restrikci u nich odstranit, otevírá se možnost pro řadu závažných útoků na majetek či osoby. Zejména letištní prostory jsou v případě dronů citlivým cílem, jelikož tamější radary drony zpravidla nezachytí. Přitom kolize dronu s motorem letadla může vyústit ve značné škody na životech i majetku.[4]

K cíleným útokům pomocí dronů může docházet jejich unesením, a následnému náletu na cíl. Pravděpodobnost takového útoku s využitím jednotlivých doručovacích dronů je nejspíše nízká, jelikož si potenciální útočník může dron relativně levně objednat, a následně jej „vylepšit“ ke způsobení větší škody. Nicméně v případě nasazení rojů doručovacích dronů je riziko jejich unesení a následného využití jako prostředku ke způsobení materiální či fyzické škody vyšší, čistě z důvodu jejich množství.

[1] TOWNSEND, Kevin. (2019, September 26). Sky-high concerns. Blog.avast.com (cit. 2020-11-1) (https://blog.avast.com/what-security-threats-are-posed-by-drones).
[2] Tech. (2014, April 7). Australian triathlete injured after drone crash. Bbc.com (cit. 2020-11-1) (https://www.bbc.com/news/technology-26921504).
[3] TRUJANO, Fernando et al. (2016). Security Analysis of DJI Phantom 3 Standard. Courses.csail.mit.edu (cit. 2020-11-1) (https://courses.csail.mit.edu/6.857/2016/files/9.pdf).
[4] ČTK. (2016, srpen 6). Dron se u Mnichova málem srazil s letadlem. Airbus plný lidí minul o deset metrů. Zprávy.aktualne.cz (cit. 2020-11-1) (https://zpravy.aktualne.cz/zahranici/dron-se-u-mnichova-malem-srazil-s-letadlem-airbus-ho-minul-o/r~ac23e1605bd211e6abfa0025900fea04/).



Obr. č. 2 Hrozby vyplývající z využití dronů pro společnost

Rizikoví aktéři potenciálního zneužití doručovacích dronů

Výsledná selekce potenciálních aktérů v ČR je vzhledem k povaze otázky výsledkem zejména na ze současných trendů a expertních znalostí založené metody projekce a brainstormingu autorů. Aktéři, až na některé výjimky, přitom budou charakterizováni hromadně prostřednictvím ‘zájmových skupin’, nebudeme zde proto např. hovořit o jednotlivých jmenovitých skupinách organizovaného zločinu či sítích distribuce drog a jiných zakázaných komodit, nýbrž obecně o těchto množinách, jejich možnostech, motivacích a potenciální rizikovosti vzhledem k zneužívání doručovacích dronů.

Tato část bude zaměřena na aktéry primárního a sekundárního zneužití dronů. Primárním je myšleno takové zneužití, které má za cíl osobní a okamžitý zisk či potěšení z poškození dronu, jeho krádeže či jeho zachycení a uloupení dané zásilky. Sekundárním je poté myšlena komplexnější trestná činnost, která je provozována s využitím zachyceného či jinak ovládnutého doručovacího dronu nebo jeho prostřednictvím. Jak je uvedeno v odpovědi na první otázku, v horizontu pěti let lze očekávat pomalé a postupné zavádění prvních doručovacích dronů, testovací provoz a vylepšování technologie po hardwarové i softwarové stránce, na což si společnost bude postupně zvykat. V tomto období lze předpokládat především aktivitu aktérů primárního zneužití, díky exkluzivitě této nové technologie a předpokládaným nedokonalostem ve fyzickém zabezpečení a letových trasách. K sekundárnímu zneužití je však potřeba, aby se s touto technologií jednotliví aktéři seznámili a uvědomili si její potenciál. Některé hrozby, plynoucí ze sekundárního zneužití, navíc nelze s malým počtem strojů v testovacím provozu realizovat. Nástup potenciálních aktérů sekundárního zneužití doručovacích dronů proto odhadujeme až za více než pět let.

Aktéři primárního zneužití dronů

Lze očekávat, že prvotní zabezpečení doručovacích dronů nebude dokonalé, může proto dojít k případům jejich sestřelení za účelem krádeže zásilek. Způsobů, jak dostat dron ze vzduchu na zem je mnoho, nejsou však nijak primitivní a vyžadují určitý kapitál, znalosti a vybavení.[1] U zloděje balíčků, kterému jde o celkový profit, navíc nelze předpokládat vůli investovat do komplexních uzemňovacích vysílačů či vlastních dronů. Zřícením se navíc náklad pravděpodobně poškodí, a i tak hodnota průměrného balíčku zřejmě nebude nikterak závratná. Můžeme se proto do budoucna setkat s incidenty tohoto charakteru, nejedná se však o nijak lukrativní a spolehlivý způsob ilegálního přivýdělku, bude se tedy nejspíše jednat o výjimečné případy, postihující zejména nízko letící drony.

Spíše než zisk, může být motivací k poškozování a únosům dronů pouhá zábava či uznání. Vandalismus postihuje veškeré veřejně přístupné a sdílené objekty, drony však svou povahou a relativní nedostupností budou lákat spíše útočníky mimo kruh tradičních vandalů. Mezi některými skupinami mládeže se může lov dronů stát populární adrenalinovou zábavou, ať už se jedná o pouliční gangy s improvizovanými lapači a zbraněmi či tzv. *script kiddies*, mladé aspirující hackery, kteří se mohou pro získání prestiže, zkušeností či obdivu okolí snažit se do systému doručovacího dronu nabourat s využitím existujícího malwaru, specificky určeného k jeho ovládnutí.[2] Takový malware či návody jak dron ovládnout na dálku jsou na internetu přitom poměrně jednoduše k dispozici.[3] Je případné očekávat, že právě nahodilí aktéři primitivního primárního zneužití budou největšími nepřáteli doručovacích dronů a incidenty z jejich zapříčinění budou těmi nejčastějšími.

Aktéři sekundárního zneužití dronů

Vlastnické korporace

První rizikovou skupinou mohou být překvapivě právě samotné doručovací, velkoobchodní či jiné korporace, které budou drony provozovat. Pokud bude legislativa v oblasti využití bezpilotních prostředků nedostatečně konkrétní, resp. najdou-li se v ní početné skuliny, některé korporace mohou pod různými záminkami či ve skrytu přistoupit ke sběru dat zákazníků bez jejich svolení pro získání konkurenční výhody.[4] Nejednalo by se přitom o žádnou novinku - excesy sociálních sítí, online vyhledávačů či statistických firem týkající se nakládání s daty uživatelů jsou poslední dobou velmi častým tématem.[5] Společnost Amazon, jeden z průkopníků využívání autonomních

[1] COOMBS, Casey. (2020, leden 1). From zappers to nets, this gear gives drones that sinking feeling. WIRED. (cit. 2021-1-19) (https://wired.me/science/how-to-down-a-drone/).
[2] SÝKORA, Petr. (2018, červenec 16). Ataky dronů z nebe začínají být na hraně zákona: jak se můžeme bránit? TechFocus.cz. (cit. 2021-1-19) (https://techfocus.cz/112-ataky-dronu-z-nebe-zacinaji-byt-na-hrane-zakona-jak-se-muzeme-branit.html).
[3] LEHOVEC, Matěj. (2017). Analýza možností teroristického útoku za použití bezpilotních leteckých prostředků. (Diplomová práce). Praha: ČVUT.
[4] Ibid.
[5] LOVELACE, Ryan. (2020, únor 25). Big Tech companies insist spying on users, government is inadvertent. The Washington Times. (cit. 2021-1-19) (https://www.washingtontimes.com/news/2020/aug/2/big-tech-companies-insist-spying-on-users-governme/).

doručovacích dronů, se dle některých analýz již v současnosti pohybuje s některými technologiemi v šedé zóně. Kromě případů skrytého nahrávání AI asistentem Alexa se jedná např. o technologii rozeznávání obličejů *Rekongition* či odesílání soukromých dat Amazonem vlastněnou aplikací *Ring*.[1] Není si proto tak těžké představit, že Amazon svou flotilu doručovacích dronů bude obdobně využívat i k vedlejším účelům. Prozatím si lze představit nedovolený sběr vizuálních dat o zákazníkovi, okolí jeho bydliště či po celou dobu letu, do budoucna však firmy mohou přijít na další způsoby, jak drony využívat i mimo jejich primární určení. Zda bude nějaká taková nadnárodní korporace, působící na území ČR, své vlastní drony popsanými způsoby zneužívat, pak závisí spíše na obecném mezinárodním prostředí a nejvyšším vedení dané korporace, bezpečnostní prostředí ČR se proto v tomto případě prolíná s ostatními státy, kde by korporace působila, a rizikovost aktéra lze jen obtížně odhadnout.

Hackeři

Flotila doručovacích dronů jedné společnosti bude pravděpodobně řízena komplexním systémem, který bude s jednotlivými stroji komunikovat a dálkově je řídit. Nabízí se proto přirozeně možnost kompromitace tohoto systému. Kybernetický útok, vedený zvenku na centrální systém, nebo skrze méně zabezpečené spojení dronu se systémem, by mohl celou flotilu vyřadit z provozu nebo dokonce zcela ovládnout. Motivací takového sofistikovaného útoku by pak ze strany zločineckých hackerských skupin mohla být snaha ze společnosti vydíráním dostat finanční prostředky. Nemusí však zůstat pouze u pasivního převzetí, ovládnuté drony mohou páchat škody a narušovat činnost dalších subjektů, ať už se jedná o záměrné blokování provozu na letišti, zahlcení kapacity radiolokátorů nebo jen demonstraci kontroly. Ve všech těchto případech je předmětné počítat s požadavky na výkupné. Státem kontrolované hackerské skupiny by pak o zisk kontroly nad sítí doručovacích dronů mohly mít zájem např. s ohledem na možnost získávání vizuálních informací z oblastí, které jsou vlastním prostředkům zapovězeny. Možností je nakonec i hacking s využitím dronu jakožto transportního prostředku vysílače k fyzicky obtížně přístupnému ale jinak nezabezpečenému uzlu, např. u výškových budov.[2] V ČR se však dle expertního odhadu autorů tito aktéři v tomto ohledu příliš angažovat nebudou a případné aféry budou spíš výjimkou.

Černý trh a distribuce drog

Distribuce drog a jiných ilegálních komodit pomocí dronů je již poměrně zažitou záležitostí, nejvíce incidentů přitom probíhá na hranicích USA a Mexika.[3] Obdobné případy jsou však známé po celém světě.[4] Nejedná také o pouhou distribuci drog, drony lze využít k anonymizovaným donáškám jakéhokoli materiálu, jsou tedy ideálním

[1] ANDERSON, Bruce. (2020, únor 26). Is Amazon spying on you? Martechcube. (cit. 2021-1-19) (https://www.martechcube.com/is-amazon-spying-on-you/).
[2] LEHOVEC, Matěj. (2017). Analýza možností teroristického útoku za použití bezpilotních leteckých prostředků. (Diplomová práce). Praha: ČVUT.
[3] Ibid.
[4] SÝKORA, Petr. (2018, červenec 16). Ataky dronů z nebe začínají být na hraně zákona: jak se můžeme bránit? TechFocus.cz. (cit. 2021-1-19) (https://techfocus.cz/112-ataky-dronu-z-nebe-zacinaji-byt-na-hrane-zakona-jak-se-muzeme-branit.html).

prostředkem pro dopravu artiklů, zakoupených na tržištích Darknetu.[1] Mimoto se objevují zprávy o pokusech propašovat rozličný kontraband pomocí dronu do věznic, v tomto případě je však nutno vyzdvihnout preemptivní úsilí české Vězeňské služby, která se na tento začínající fenomén připravuje budováním bezletových zón nad věznicemi a spolu s ČVUT vyvíjí drony na polapení těch pašeráckých.[2] Ačkoli si pašeráci povětšinou mohou dovolit zakoupit drony vlastní, krádež či ovládnutí firemního doručovacího dronu by mohla jejich ilegální aktivity lépe zamaskovat. Komerční doručovací dron nesoucí balíček nikomu nebude podezřelý a pašeráci by navíc mohli využít i integrované transportní navigace a síť tras a adres. Tito aktéři by v ČR mohli být z těch sekundárních nejvíce aktivní, ač nejméně organizovaní a viditelní, vzhledem k jejich snaze o maximalizaci anonymity.

Terorismus

Komerční bezpilotní letouny se v posledních letech staly běžnou součástí arzenálu teroristických a povstaleckých skupin na Blízkém východě, jejich využívání např. hnutím Hizballáh však sahá ještě dále. Mimo bombardování a „kamikadze" útoky drony nesoucími výbušniny je povstalci používají k distribuci propagandy, komunikaci či sběru dat o protivnících.[3] Reflektuje to obecně se zlepšující úroveň technických znalostí a profesionalizace teroristických skupin, které jsou schopny si drony upravovat a programovat dle svých potřeb. Proč by však měli mít zájem o korporátní doručovací drony? Benefity z jejich použití jsou v tomto případě stejné, jako při využití k transportu kontrabandu – maskování a potenciální ztráty na životech při hromadném útoku hejnem ovládnutých strojů, kterému lze jen obtížně zabránit – kromě toho však útočníkům do karet opět hraje software dronů, který by bylo možno využít k plánovaným autonomním útokům bez vyvolání podezření. Doručovací drony navíc budou stavěné na transport zásilek nezanedbatelné váhy, unesou tedy pravděpodobně více výbušnin, než průměrný komerční stroj. Možnosti teroristických útoků na kritickou infrastrukturu či měkké cíle na evropské či americké půdě pak závisí pouze na fantazii extremistů. Vzhledem k historicky i aktuálně poměrně nízkému riziku teroristického útoku a obecně problematice terorismu v ČR však zneužití doručovacích dronů teroristy u nás není v blízké budoucnosti příliš reálné.

Závěr

V současné době dochází ve světě k rozsáhlému testování možností provozu doručovacích dronů. V ČR došlo k prvním testům doručovacích dronů již v roce 2016, nicméně od té doby nedošlo k významnějšímu pokroku. Změnu však může přinést nový regulační rámec EU, který vstoupil v platnost na konci roku 2020.

---

[1] Darknet je souhrnné označení pro ilegální část deep webu – sítě, dostupné pouze skrze anonymizující software se znalostí konkrétních adres. Je využíván pro anonymní komunikaci, úniky, ilegální sdílení a černé trhy.

[2] SHABU, Martin. (2019, listopad 11). Česko by se mělo připravit na pašování zásilek drony do věznic. ČeskáPozice.Lidovky.cz. (cit. 2021-1-19) (https://ceskapozice.lidovky.cz/tema/cesko-by-se-melo-pripravit-na-pasovani-zasilek-drony-do-veznic.A191107_132852_pozice-tema_lube).

[3] KUBÍK, Tomáš. (2019, listopad 13). Bezpilotní letouny na Blízkém východě v rukou teroristů. Security Outlines. (cit. 2021-1-19) (https://www.securityoutlines.cz/bezpilotni-letouny-na-blizkem-vychode-v-ruckou-teroristu)/.

Lze předpokládat, že budoucí vývoj využití doručovacích dronů v ČR bude kopírovat zahraniční trendy (testovací provoz za dohledu a spolupráce národní autority v rámci vymezených leteckých koridorů apod.). Nasazení doručovacích dronů do běžného provozu nicméně nelze očekávat dříve než v roce 2025.

Hrozby vyplývající z použití dronů lze rozčlenit do dvou kategorií, a sice hrozby dronům jako doručovacímu systému a hrozby vyplývající z využití tohoto systému pro společnost. Doručovací systém je vystaven hrozbám kybernetické i kinetické povahy, přičemž řadu z nich dokáže provést i nesofistikovaný útočník. Hrozby směrem ke společnosti dělíme na hrozby soukromí, hrozby kybernetické a fyzické bezpečnosti. Jako nejrizikovější hrozby se jeví zejména unesení či zničení dronu využitím kybernetických prostředků.

Závěrem lze konstatovat, že v ČR se pravděpodobně nachází aktéři, kteří by mohli na zneužití doručovacích dronů mít zájem. Povahou se však především jedná o typ primárního zneužití, resp. únosů a poškozování dronů za účelem osobního zisku či zábavy. Mezi nejaktivnější aktéry sekundárního zneužití, tedy provozování trestné činnosti s použitím doručovacích dronů, budou v našem prostředí patřit dealeři drog a kriminální skupiny operující v prostředí černého trhu či ilegálních internetových tržišť, pro které by transport ilegálního zboží pomocí ovládnutých doručovacích dronů mohl být lákavý z hlediska značného navýšení anonymity, která u těchto skupin hraje prim. Ostatní aktéři sekundárního zneužití budou vzhledem k současnému stavu a vývoji v ČR spíše vzácní a trendy v této oblasti bude určovat zahraničí.

Vzhledem k tomu, že se tento článek částečně zaměřuje na blízkou budoucnost, je nutné počítat s tím, že korespondující závěry a prezentované názory jsou probabilistického charakteru. To je dáno mj. také značnou dynamikou v oblasti vývoje a využívání bezpilotních leteckých prostředků. Co se nakonec týče možností dalšího navazujícího výzkumu v oblasti, nabízí se zejména výzkum zaměřený na reálné možnosti zabezpečení doručovacích dronů, potažmo případové studie jednotlivých bezpečnostních incidentů ve spojitosti s jejich zneužitím.

Seznam použitých zdrojů

AKRAM, Raja N. (2017). Secure Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements. Ieexplore.ieee.org (cit. 2020-11-1) (https://ieeexplore.ieee.org/document/7846999).

ANDERSON, Bruce. (2020, únor 26). Is Amazon spying on you? *Martechcube. (*https://www.martechcube.com/is-amazon-spying-on-you/).

ASHISH, Thomas et al. (2016). Secure Link Establishment Method to Prevent Jelly FIsh Attack in MANET. Ieexplore.ieee.org (cit. 2020-11-1) (https://ieeexplore.ieee.org/document/7546277).

BARTOCK, Michael. (n.d.). LTE Security. Csrc.nist.gov (cit. 2020-11-1) (https://csrc.nist.gov/CSRC/media/Presentations/LTE-Security-How-Good-is-it/images-media/day2_research_200-250.pdf).

BEST, Katharina L. et al. (2020). How to Analyze the Cyber Threat from Drones. Rand.org. (cit. 2020-11-1) (https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2972/RAND_RR2972.pdf).

BURSZTYNSKY, J. (2020, April 27). CVS and UPS will use drones to deliver prescriptions in a retirement community amid coronavirus outbreak. *CNBC*. (cit. 2021-1-19) (https://www.cnbc.com/2020/04/27/coronavirus-cvs-ups-delivering-prescriptions-with-drones.html).

CAMPION, Mitch et al. (n.d). A Review and Future Directions of UAV Swarm Communication Architectures. Und.edu (cit. 2020-11-1) (https://und.edu/research/rias/_files/docs/swarm_ieee.pdf).

COOMBS, Casey. (2020, leden 1). From zappers to nets, this gear gives drones that sinking feeling. *WIRED.* (cit. 2021-1-19) (https://wired.me/science/how-to-down-a-drone/).

CIMPANU, Catlin. (2020). Billions of devices vulnerable to Bluetooth security flaw. Zdnet.com. https://www.zdnet.com/article/billions-of-devices-vulnerable-to-new-blesa-bluetooth-security-flaw/).

ČTK. (2016, srpen 6). Dron se u Mnichova málem srazil s letadlem. Airbus plný lidí minul o deset metrů. Zprávy.aktualne.cz (cit. 2020-11-1) (https://zpravy.aktualne.cz/zahranici/dron-se-u-mnichova-malem-srazil-s-letadlem-airbus-ho-minul-o/r~ac23e1605bd211e6abfa0025900fea04/).

ČESAL, L. (2017, červenec 12). První zásilka dronem doručena. *PoštovnéZDARMA.cz.* (cit. 2021-1-19) (https://postovnezdarma.cz/blog/535-doruceni-dronem/.

DHL. (2020). Historie inovací. (cit. 2021-1-19) (https://www.dhl.com/cz-cs/home/o-nas/nase-vize.html).

DoS Attack Tutorial. (n.d.). Guru99.com (cit. 2020-11-1) (https://www.guru99.com/ultimate-guide-to-dos-attacks.html).

Drone Rules. (2019, June 13). EASA: EU wide rules on drones published. (cit. 2021-1-19) (https://dronerules.eu/cs/professional/news/easa-eu-wide-rules-on-drones-published).

Drone Rules. (2020) EU Regulations Updates. (cit. 2021-1-19) (https://dronerules.eu/cs/professional/eu_regulations_updates.

Droneweb. (n.d.) Co je dron? (cit. 2021-1-19) (http://www.droneweb.cz/co-je-dron.

EASA. (2020a). Civil drones (Unmanned aircraft). (cit. 2021-1-19) (https://www.easa.europa.eu/domains/civil-drones-rpas).

EASA. (2020b). FAQ n.116449. (cit. 2021-1-19) (https://www.easa.europa.eu/faq/116449).

European Environment Agency. (2020). Drivers of change Delivery drones and the environment. (cit, 2021-1-19). (https://www.eea.europa.eu/publications/delivery-drones-and-the-environment/at_download/file).

Fehr & Peers. (2020). Drone Delivery: How will it affect your community? (cit. 2021-1-19) (https://www.fehrandpeers.com/drone-delivery/).

Forbes Technology Council. (2018, October 4). Looking Ahead: 11 Predictions On How Drone Deliveries Will Work. *Forbes*. (cit. 2021-1-19) (https://www.forbes.com/sites/forbestechcouncil/2018/10/04/looking-ahead-11-predictions-on-how-drone-deliveries-will-work/#21492ecf51b3).

FRUHLINGER, Josh. (2018, March 9). The Mirai botnet explained. Csoonline.com (cit. 2020-11-1) (https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html).

GARCIA, O. R.; SANTOSO, A. & M. M. JAVADI. (2019). Drone delivery systems: A comparative analysis in last-mile distribution. Massachusetts Institute of Technology. (cit. 2021-1-19) (https://ctl.mit.edu/sites/ctl.mit.edu/files/theses/20190521_Antonius_Santoso_DDS_research_fest_presentation_v8.pdf).

GATES, Megan. (2020 July 1). Flight Risks. Asisonline.org (cit. 2020-11-1) (https://www.asisonline.org/security-management-magazine/articles/2020/07/flight-risks/).

GOASDUFF, L. (2020, May 19). Why Flying Drones Could Disrupt Mobility and Transportation Beyond COVID-19. *Gartner*. (cit. 2021-1-19) (https://www.gartner.com/smarterwithgartner/why-flying-drones-could-disrupt-mobility-and-transportation-beyond-covid-19/?utm_medium=social&utm_source=twitter&utm_campaign=SM_GB_YOY_GTR_SOC_SF1_SM-SWG-CV&utm_content=&sf234174535=1).

GUPTA, Pamela and OutSecure. (2019). Mitigating Risks From A to Z-Wave. Securityindustry.org. https://www.securityindustry.org/2019/04/23/mitigating-risks-from-a-to-z-wave/).

GUPTA, B. and Megha QUAMARA. (2020). Internet of Things Security. Boca Raton: CRC Press.

HIGGINS, Fiona et al. (2009). Survey on Security Challenges for Swarm Robotics. Ieexplore.ieee.org (cit. 2020-11-1) (https://ieeexplore.ieee.org/document/4976621).

HORČÍK, J. (2017, July 13). Český e-shop umí doručovat zásilky dronem. (cit. 2021-1-19) (http://www.hybrid.cz/cesky-e-shop-umi-dorucovat-zasilky-dronem).

HZS ČR. (2020). Hasiči převzali speciální techniku – velitelský vůz s dronem. https://www.hzscr.cz/clanek/hasici-prevzali-specialni-techniku-velitelsky-vuz-s-dronem.aspx).

CHARLTON, A. (2020, March 25). Getting Locked Down Underlines Why We Must Look Up And Work To Enable Drone Delivery. *Forbes*. (cit. 2021-1-19) (https://www.forbes.com/sites/andrewcharlton5/2020/03/25/getting-locked-down-underlines-why-we-must-look-up-and-work-to-enable-drone-delivery/#25810f947eeb).

CHRISTIAN, A.; CABELL, R. (2017). Initial Investigation into the Psychoacoustic Properties of Small Unmanned Aerial System Noise. *NASA Langley Research Center* (cit. 2021-1-19) (https://ntrs.nasa.gov/citations/20170005870). KERNS, Anderw. J. (n.d.). Unmanned Aircraft Capture and Control via GPS Spoofing. Radionavlab.ae.utexas.edu (cit. 2020-11-1) (https://radionavlab.ae.utexas.edu/images/stories/files/papers/unmannedCapture.pdf).

KHANJI, Salam et al. (2019). ZigBee Security Vulnerabilities. Ieeexlore.ieee.org. https://ieeexplore.ieee.org/document/8809115).

KUBÍK, Tomáš. (2019, listopad 13). Bezpilotní letouny na Blízkém východě v rukou teroristů. *Security Outlines.* (cit. 2021-1-19) (https://www.securityoutlines.cz/bezpilotni-letouny-na-blizkem-vychode-v-ruckou-teroristu/).

LADEIRA, M.; OUHAMMOU, Y. & E. GROLLEAU. (2020). Towards a modular and customisable model-based architecture for autonomous drones. 2020 IEEE

44th Annual Computers, Software, and Applications Conference. (cit. 2021-1-19) (https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9202678&casa_token=Fell-Mc2L2MAAAAA:DZ51veZ87pRYCMQcWW8AnhkYdhWA16Nmv1VJIQEWEbKmQ5lDlR38eIfTZVaZYHSZrHbjaYOlWw&tag=1).

LEHOVEC, Matěj. (2017). *Analýza možností teroristického útoku za použití bezpilotních leteckých prostředků.* (Diplomová práce). Praha: ČVUT.

LIEBREICH, J. (2020, February 12.) České nebe zaplavují drony. Rekordy lámou i pokuty. *E15*.cz. (cit. 2021-1-19) (https://www.e15.cz/domaci/ceske-nebe-zaplavuji-drony-rekordy-lamou-i-pokuty-1366693).

LIMER, Eric. (2015, August 6). How to Shoot Down a Drone. Popularmechanics.com (cit. 2020-11-1) (https://www.popularmechanics.com/flight/drones/how-to/a16756/how-to-shoot-down-a-drone/).

LOVELACE, Ryan. (2020, únor 25). Big Tech companies insist spying on users, government is inadvertent. *The Washington Times.* (cit. 2021-1-19) (https://www.washingtontimes.com/news/2020/aug/2/big-tech-companies-insist-spying-on-users-governme/).

Mall.cz. (2016, November 22). Mall.cz úspěšně otestoval doručování dronem. Balíček předal za 3 minuty. (cit. 2021-1-19) (https://www.mall.cz/tiskova-zprava-16-11-22).

MIAH, Andy. (2020). Drones: The Brilliant, the Bad and the Beautiful. Bingley: sEmerald Publishing.

MOLLOY, D. & J. COPESTAKE. (2020, April 30). Drone-to-door medicines trial takes flight in Ireland. *BBC.com*. (cit. 2021-1-19) (https://www.bbc.com/news/technology-52206660).

MULLIS, Simon. (2013, August 2). Cybercriminal Intent. Fireeye.com (cit. 2020-11-1) (https://www.fireeye.com/blog/executive-perspective/2013/08/cybercriminal-intent-how-to-build-your-own-botnet-in-less-than-15-minutes.html).

NOUACER, R. et al. (2020). Towards a Framework of Key Technologies for Drones. Microprocessors and Microsystems. (cit. 2021-1-19) (https://www.sciencedirect.com/science/article/pii/S0141933120303094?casa_token=UfeKHTJIbOwAAAAA:LIfDXIjdWkyL7xn1cZkbH0QyPUuRpTDvuOVPk5vY0sRlNixWjrF7kQRI0fKoBAJsZUy7jXNpdw).

O'DONNELL, Lindsey. (2019, June 27). Thousands of IoT Devices Bricked By Silex Malware. Threatpost.com (cit. 2020-11-1) (https://threatpost.com/thousands-of-iot-devices-bricked-by-silex-malware/146065/).

OSWALD, E. (2017, May 3). Here's everything you need to know about Amazon's drone delivery project, Prime Air. *Digitaltrends*. (cit. 2021-1-19) (https://www.digitaltrends.com/cool-tech/amazon-prime-air-delivery-drones-history-progress/).

PAGANINI, Pierluigi. (2015, January 27). A hacker developer Maldrone, the first malware for drones. Securityaffairs.co (cit. 2020-11-1) (https://securityaffairs.co/wordpress/32767/hacking/maldrone-malware-for-drones.html).

PALMER, A. (2020, August 31). Amazon wins FAA approval for Prime Air drone delivery fleet. *CNBC.* (cit. 2021-1-19)

(https://www.cnbc.com/2020/08/31/amazon-prime-now-drone-delivery-fleet-gets-faa-approval.html).

Policie České republiky. (2020, March 9). Vybavení Letecké služby PČR novými drony. (cit. 2021-1-19) (https://www.policie.cz/clanek/vybaveni-letecke-sluzby-pcr-novymi-drony.aspx).

REED, T., GEIS, J. (n.d.). SkyNET: a 3G-enabled mobile attack drone and stealth botmaster. Usenix.org (cit. 2020-11-1) (https://www.usenix.org/legacy/event/woot/tech/final_files/Reed.pdf).

RONEN, Eyal et al. (2018). IoT GOes Nuclear. Ieeexplore.ieee.org (cit. 2020-11-1) (https://ieeexplore.ieee.org/document/8283484).

SAMMERS, Nick. (2016, October 28). Icarus machine can commandeer a drone mid-flight. Engadget.com (cit. 2020-11-1) (https://www.engadget.com/2016-10-28-icarus-hijack-dmsx-drones.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAK-K1bv58EDrmWOkjTwlm4vNM031ehWbtuDi6cZNxs3ib0bcLefYePJ8QIQJLKA7QpOyH8jsOiykHQC_Pk5L5XW5bBRtveAUhaSXD7-UGzKQEpCIgt3AmuBsl5Q6vma_G-SRTxjDx0I-EB87Z7Q9jybgXt4Rt3MccJ8Nws-9Y6RM).

SANTHANAM, V. (2020, May 8). How drones could change the future of healthcare delivery. *World Economic Forum*. (cit. 2021-1-19) (https://www.weforum.org/agenda/2020/05/medical-drone-delivery-india-africa-modernize-last-mile/).

SHABU, Martin. (2019, listopad 11). Česko by se mělo připravit na pašování zásilek drony do věznic. *ČeskáPozice.Lidovky.cz.* (cit. 2021-1-19) (https://ceskapozice.lidovky.cz/tema/cesko-by-se-melo-pripravit-na-pasovani-zasilek-drony-do-veznic.A191107_132852_pozice-tema_lube).

SCHENKELBERG, F. (2016). How reliable does a delivery drone have to be? *2016 annual reliability and maintainability symposium (RAMS)*. (cit. 2021-1-19) (https://www.researchgate.net/publication/301574679_How_reliable_does_a_delivery_drone_have_to_be).

SCHRÖDER et al. (2018). Fast forwarding last-mile delivery – implications for the ekosystém. *McKinsey & Company*. (cit. 2021-1-19) (https://www.mckinsey.com/~/media/mckinsey/industries/travel%20transport%20and%20logistics/our%20insights/technology%20delivered%20implications%20for%20cost%20customers%20and%20competition%20in%20the%20last%20mile%20ecosystem/fast-forwarding-last-mile-delivery-implications-for-the-ecosystem.ashx).

STERN, Matthew. (2017, August 17). Should drones be used for data collection in addition to deliveries?. Retailwire.com (cit. 2020-11-1) (https://retailwire.com/discussion/should-drones-be-used-for-data-collection-in-addition-to-deliveries/).

STOLAROFF, J. K. et al. (2018). Energy use and life cycle greenhouse gas emissions of drones for commercial package delivery. *Nature communications*, *9*(1), 1-13. (cit. 2021-1-19) (https://www.nature.com/articles/s41467-017-02411-5.

SÝKORA, Petr. (2018, červenec 16). Ataky dronů z nebe začínají být na hraně zákona: jak se můžeme bránit? *TechFocus.cz.* (cit. 2021-1-19) (https://techfocus.cz/112-ataky-dronu-z-nebe-zacinaji-byt-na-hrane-zakona-jak-se-muzeme-branit.html)

Tech. (2014, April 7). Australian triathlete injured after drone crash. Bbc.com (cit. 2020-11-1) (https://www.bbc.com/news/technology-26921504).

The Dark Web. (2020, August 26). The Dark Web: DDoS Attacks Sell for as Low as $10 Per Hour. Missioncriticalmagazine.com (cit. 2020-11-1) (https://www.missioncriticalmagazine.com/articles/93185-the-dark-web-ddos-attacks-sell-for-as-low-as-10-per-hour).

TOWNSEND, Kevin. (2019, September 26). Sky-high concerns. Blog.avast.com (cit. 2020-11-1) (https://blog.avast.com/what-security-threats-are-posed-by-drones).

Transmetrics. (2019). The Evolution of Delivery Drones in Logistics. *Trancsmetrics Blog*. (cit. 2021-1-19) (https://transmetrics.eu/blog/delivery-drones-logistics/).

TRUJANO, Fernando et al. (2016). Security Analysis of DJI Phantom 3 Standard. Courses.csail.mit.edu (cit. 2020-11-1) (https://courses.csail.mit.edu/6.857/2016/files/9.pdf).

Úřad pro civilní letectví. (2019). Podle kterého předpisu se řídí provoz bezpilotních letadel / systémů? (cit. 2021-5-4) (https://www.caa.cz/provoz-stare/letadla-bez-pilota-na-palube/provoz-ostatnich-letadel-bez-pilota-na-palube/podle-kterehо-predpisu-se-ridi-provoz-bezpilotnich-letadel-systemu/).

Úřad pro civilní letectví. (2020). Příprava společných evropských pravidel. (cit. 2021-1-19) (https://www.caa.cz/provoz/letadla-bez-pilota-na-palube/priprava-spolecnych-evropskych-pravidel/).

VALENTE, Junia and Alvaro CADRENAS. (2017). Understanding Security Threats in Consumer Drones Through the Lens of the Discovery Quadcopter Family. Dl.acm.org (cit 2020-11-1) (https://dl.acm.org/doi/pdf/10.1145/3139937.3139943).

VASCONCELOS, Gabriel et al. (2019). Evaluation of DoS attacks on commercial Wi-Fi-based UAVs. International Journal of Computer Netwok and Information Security (11), no. 1, pp, 212-222 (cit. 2020-11-1) (https://www.researchgate.net/publication/332704018_Evaluation_of_DoS_attacks_on_commercial_Wi-Fi-based_UAVs).

VORUGANTI, K. (2019, June 24). The Future of: Has the Age of Drones (Finally) Arrived? Equinix. (cit. 2021-1-19) (https://blog.equinix.com/blog/2019/06/24/the-future-of-has-the-age-of-drones-finally-arrived/).

WALTERS, Sanders. (2016, October 29). How Can Drones Be Hacked? The updated list of vulnerable drones & attack tools. Medium.com (cit. 2020-11-1) (https://medium.com/@swalters/how-can-drones-be-hacked-the-updated-list-of-vulnerable-drones-attack-tools-dd2e006d6809).

What is a botnet? (2017, December 5). Pandasecurity.com (cit. 2020-11-1) (https://www.pandasecurity.com/en/mediacenter/security/what-is-a-botnet/).

WOLF, H. (2018, March 27). Why we need to go back to the drawing board when it comes to regulating drones. *World Economic Forum*. (cit. 2021-1-19) (https://www.weforum.org/agenda/2018/03/millions-of-drones-will-make-us-air-traffic-unmanageable-within-a-few-years-unless-we-rethink-some-basic-rules/).

WOLF, H. (2020, July 6). We're about to see the Golden Age of drone delivery – here's why. *World economic forum*. (cit. 2021-1-19) (https://www.weforum.org/agenda/2020/07/golden-age-drone-delivery-covid-19-coronavirus-pandemic-technology/).

YAACOUB, Jean-Paul et al. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. Ncbi.nlm.nih.gov (cit. 2020-11-1) (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7206421/).

YANG, Xueying et al. (2018). Security Vulnerabilities in LoRaWAN. Ieeexlore.ieee.org. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8366983).

R E S U M É

Tento článek se zabývá problematikou bezpečnosti doručovacích dronů a zaměřuje se na hrozby, které mohou vyplývat z jejich budoucího využívání. Hromadné komerční využití doručovacích dronů s sebou přináší celou škálu hrozeb, které lze rozdělit na hrozby dronům jako doručovacímu systému a hrozby vyplývající z využití tohoto systému pro společnost. Za nejrizikovější lze přitom považovat hrozby únosu či zničení dronu prostřednictvím kybernetických prostředků, jelikož takto lze dron zneužít k další trestné činnosti. V rámci ČR lze identifikovat řadu potenciálních rizikových aktérů, kteří mohou mít na zneužití dronů zájem. Pomalejší zavádění těchto doručovacích prostředků v ČR spíše až v pozdějších vlnách, kdy by ty nejvíce kritické slabiny této technologie již měly být vyřešeny, a také dobrá bezpečnostní situace v ČR však přispívají k zjištění, že většina z nich by na národní úrovni neměla představovat významné riziko. Nejpravděpodobnější je pak aktivita aktérů primárního zneužití, kteří mohou zneužívat drony především za účelem osobního zisku či zábavy.

Klíčová slova: bezpilotní letecké prostředky; UAV; kybernetické hrozby; doručovací drony.

S U M M A R Y

RECHTIK, Marek; ONDRŮŠEK, Jakub; SIŘINEK, Tomáš: THREATS ARISING FROM THE USE OF DELIVERY DRONES IN THE CZECH REPUBLIC

This article deals with the issue of delivery drones security and focuses on threats emanating from their use in future. The use of delivery drones brings a whole range of threats which can be divided into threats to the drones themselves and threats for the society resulting from the use of these systems. The authors consider the threats of hijacking or destroying a drone by cyber means as the most dangerous, as they can be subsequently used in further crimes. Within the Czech Republic, a number of potential risk actors, who might be interested in abusing drones, can be identified. A slower introduction of these delivery tools in the Czech Republic, probably in later phases, when the most critical weaknesses should have already been compensated, and also the high level of security in the Czech Republic, do contribute towards the general finding that most of these actors should not pose a meaningful threat on the national level. Finally, it seems that the actors of primary abuse, who may abuse drones for their personal gain or entertainment, will be the most active ones.

Keywords: unmanned aerial vehicles, UAV, cyber threats, delivery drones.