V ZÁKOPECH digitální války

Moderní konflikty už nerozhodují jen špičkově vybavení vojáci, stratégové či bojoví piloti, ale také IT experti. „Bojovníci od klávesnic“ dokážou vyřadit elektrárnu, nasimulovat něčí smrt či nabourat komunikaci nepřítele. A přesně to již několik let zažívá Ukrajina

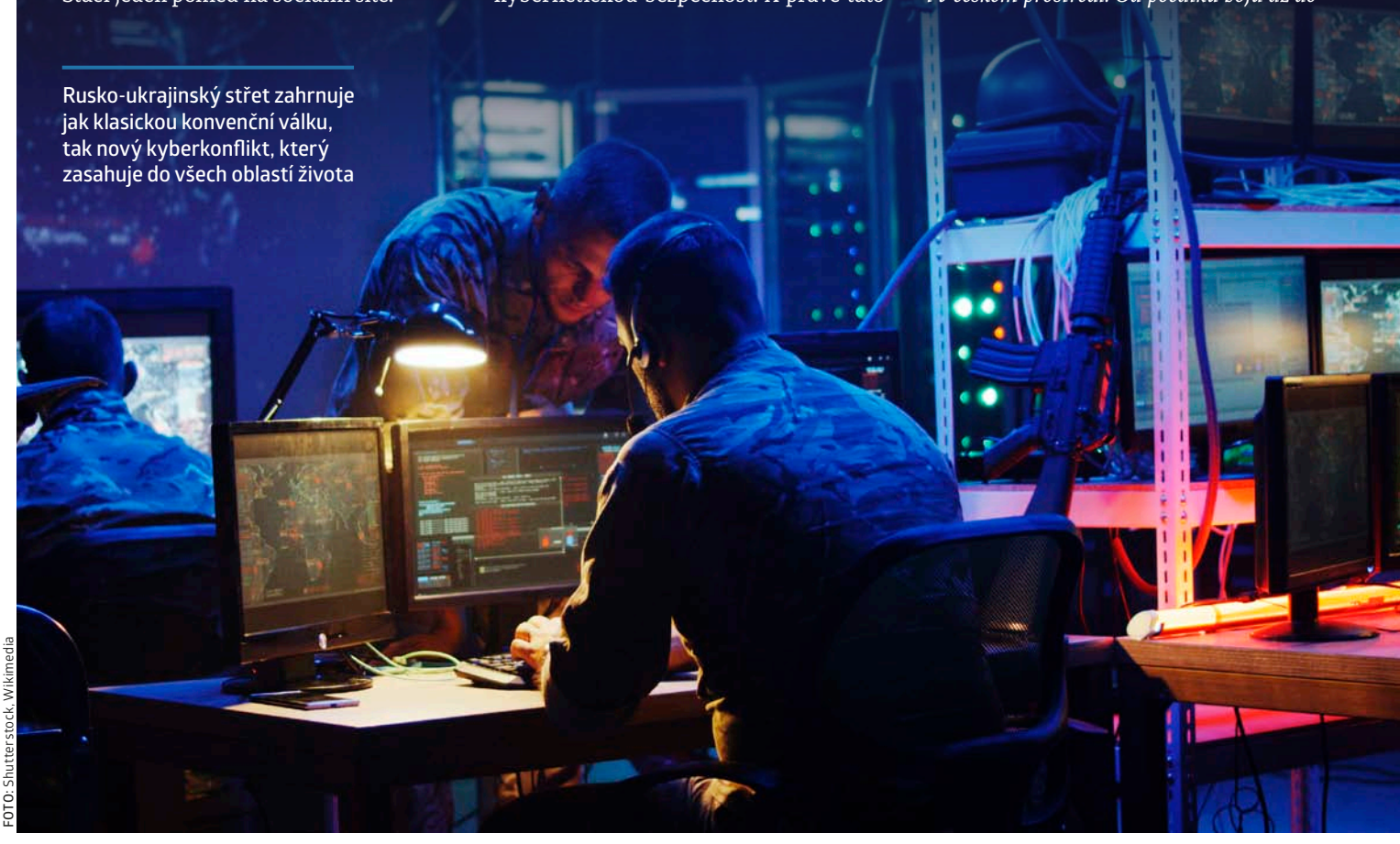
autor | Martin Staroň

Pod pojmem kybernetická válka si část laické veřejnosti představí souboje robotů jako z filmu Terminátor. Ti zkušenější si možná vybaví chytré zbraňové systémy ze světových veletrhů. Jenže bezpečnostní experti to vidí ještě jasněji: Kyberkonflikt totiž není žádné sci-fi, ale boj, který už teď zuří všude kolem nás. Stačí jeden pohled na sociální sítě.

V RÁJI HACKERŮ

Východ Evropy platí několik posledních let za nejžhavější bojiště kybernetické války vůbec. Poté, co vojáci Ruské federace obsadili počátkem roku 2014 Krym a později zažehli povstání na Donbase, vznikla česká dobrovolnická organizace Team 4 Ukraine. Mezi její členy patří i Tomáš Flídr, v civilním životě expert na kybernetickou bezpečnost. A právě tato specializace se v dalších letech ukázala jako jeden z klíčových prvků v boji s neviditelným útočníkem. Klasický ozbrojený konflikt tam totiž nahradila jeho hybridní verze, jejíž součástí se stala i takzvaná kyberválka.

Flídr vysvětluje: *„Od počátku nás velmi zajímaly formy ruských útoků, abychom na ně v budoucnu dokázali reagovat třeba i v českém prostředí. Od počátku bojů až do*



Rusko-ukrajinský střet zahrnuje jak klasickou konvenční válku, tak nový kyberkonflikt, který zasahuje do všech oblastí života

FOTO: Shutterstock, Wikimedia

roku 2019 jsme také školili místní lidi, často úplně na východě Ukrajiny, tedy přímo na frontové linii. Člověk by si řekl, že civilista trpící bombardováním bude řešit něco úplně jiného. Opak byl pravdou – Rusové či separatisté totiž rozjeli intenzivní kyberválku, která ovlivňovala každodenní život i posledního Ukrajince. Pomáhali jsme dokonce i lidem z druhé strany barikády, tedy z okupovaných území, kde fungují značně nedůvěryhodní internetoví provideři.

Přitom platilo, že čím víc jste se fyzicky blížili k frontě, tím mohutněly útoky na vaše zařízení a digitální entitu – běžné bylo třeba tvoření falešných identit, kradení osobních účtů a tak dále. Navíc platí, že pověstný ráj kyberzločinců leží právě v separatistických republikách DNR a LNR, kde nefunguje žádná právní ochrana digitálního prostoru.“

Těžké hledání: Útočníka lze odhalit tak, že opakovaně používá ty samé nástroje i programátory, kteří mají typický rukopis

ZRÁDNÉ NULY A JEDNIČKY

Klasický konflikt, jež zahrnoval akce dělostřelectva, snajprů či minometných oddílů, tak na východě Evropy již mnoho let doplňují souboje hackerů a IT specialistů. Jak se digitální konflikt projevuje v praxi vysvětluje Tomáš Flídr: *„Jednou věcí je manipulace veřejným míněním, tou druhou drtivý kyberútok na kritickou infrastrukturu nepřítele. Nepotřebujete drahé bojové systémy a vaši vojáci mohou zůstat v kasárnách, nic neostřelují ani neobsazují a úplně se vyhnou boji. Výsledek je ale stejný – nefunkční komunikace, blackout, rozpad infrastruktury, finančního systému a tak dále. Společnost drtí nervozita, ztrácí důvěru ve státní instituce a ze země utíkají investoři. Oběti navíc často chybí přímé důkazy, že šlo zrovna o vaši akci, ať úspěšnou či nikoliv.*

Třeba Ukrajina zažila první mohutný kyberútok během prezidentských voleb v roce 2014, když se hackeři pokusili napadnout servery ústřední volební komise. Ruská státní televize pak bez ohledu na odražení ataku ohlásila vítězství vůdce kontroverzního Pravého sektoru Dmytra Jaroše, který měl získat 37 % hlasů – jenže ve skutečnosti dostal pouhá 3 %! V dalších letech, typicky v zimních měsících, proběhly akce typu black energy, které cílily na distribuci elektřiny, a to i v samotném Kyjevě. Útočníci využili také psychologickou stránku věci, když pomocí DOS útoku zahltili servisní linky, takže zoufalým občanům neměl kdo pomoct. Frustrace rostla a mnozí lidé ztratili důvěru ve schopnosti úřadů zajistit byť i jen základní služby.“

Ráj kyberzločinců najdete v separatistických republikách DNR a LNR, kde nefunguje žádná právní ochrana digitálního prostoru

HALÓ, TADY NEPŘÍTEL!

V červnu 2017 zase proběhla akce zvaná NotPetya, když patrně ruská hackerská skupina Sandworm napadla účetní systém pro podávání daňových přiznání, který používalo mnoho ukrajinských společností. Jeho prostřednictvím poslali do soukromých interních sítí škodlivý malware, jež likvidoval počítačové harddisky. Tento vir typu wiper doslova zamořil nejen domácí firmy, ale nakonec se přes jejich filiálky rozšířil i do zahraničí, a to včetně samotného Ruska. Výsledkem byly mnohamiliardové škody po celém světě.

Ukrajinci se během let museli vypořádat také s psychologickými operacemi proti své armádě. Hackeři totiž pomocí falešných stanic BTS získali data z tamních mobilních telefonů a poté rozeslali rodinám daných vojáků zprávy, že dotyční padli. Vyděšení lidé pak okamžitě volali svým synům a otcům zpět, čímž potvrdili jejich pozice – a Rusové či separatisté je

Z ČR AŽ NA BOJIŠTĚ

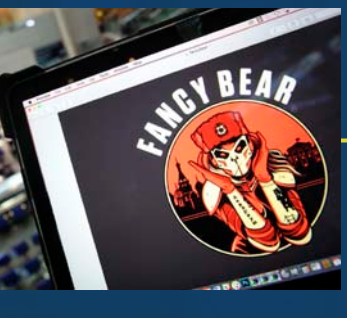
Organizace Team 4 Ukraine pomáhá Ukrajině jak penězi, tak humanitární pomocí či obranným materiálem. Všechny darované či nakoupené věci se dobrovolníci snaží dodat přímo do rukou konkrétním lidem v místech bojů, aby si nad celým procesem udrželi permanentní kontrolu. Tito nadšenci pracují bez nároku na odměnu a své aktivity dokumentují na sociálních sítích.
Více na **www.team4ukraine.eu**

KDYŽ KOUSNE MEDVĚD

K nejznámějším hackerským a špionážním skupinám takřka jistě napojeným na GRU patří APT 28 neboli Fancy Bear (Medvěd fešák), která se specializuje na diplomatické cíle v zemích s ruskými zájmy. Jde o velké množství špičkových programátorů, kteří disponují drahými technologiemi a moderními nástroji. Viry šijí na míru cílovým prostředím a často je konfigurují tak, aby používaly místní e-mailové servery. K jejich úkolům zdaleka nepatří jen šíření propagandy: Například v letech 2014–2016 napadla skupina řízení raketových sil a dělostřelectva ukrajinské armády. Použila k tomu malware pro aplikace Android, který původně sloužil ke kontrole zaměřovacích dat pro 122mm houfnice D-30. Škodlivý software pak způsobil asi 15–20 % ztrát, když automaticky posílal informace o rozmístění děl na druhou stranu fronty.

Hackeři od Fancy Bear zaútočili také na pořadatele Zimních olympijských her 2018 v Koreji, případně na Světovou antidopingovou agenturu (2016), která odhalila rozsáhlé porušování pravidel ze strany ruských sportovců. O klidný spánek připravili také vedení amerických vojensko-průmyslových gigantů od Boeingu až po Lockheed Martin či mnohé novináře kritizující putinovský režim. Digitální diverzanti se také pokusili vyděsit západní společnost akcemi neexistující skupiny hackerů CyberCaliphate, jež o sobě tvrdila, že bojuje ve prospěch teroristů z Islámského státu. Moskvu popudili také novináři spojení se skupinou Bellingcat, která zkoumala sestřelení letadla Malaysia Airlines 17 nad Ukrajinou (červenec 2014) – ruští hackeři na ně podnikli phishingový útok za účelem vylákání důvěrných informací. A pak tu byl také špionážní útok proti Ministerstvu zahraničních věcí ČR z roku 2016 – útočníky zajímaly hlavně e-mailové schránky nejvyšších představitelů úřadu, do nichž vstupovali dokonce opakovaně. Kdo je Ruskem vnímán jako hrozba, má zkrátka o zábavu postaráno…

Infikovaná verze mobilní aplikace pro řízení palby 122mm houfnic D-30 způsobila ukrajinským silám značné ztráty



Jedna z nejčastějších stylizací loga ruské skupiny Fancy Bear. Samotní hackeři pochopitelně žádný veřejný symbol nepoužívají…

Elektronický boj může mít stejně devastující účinky jako dělostřelecký přepad

pak zasypali dělostřeleckými granáty. Jindy se na displejích mobilů ukrajinských vojáků v různých jednotkách objevilo sdělení, že jejich velitel dezertoval a oni ať se rozhodnou, jestli se v poklidu vrátí domů anebo padnou za fašistickou juntu. I když tomu většina mužů nevěřila, na psychické pohodě jim to rozhodně nepřidalo.

UMÉST CESTU DO PEKLA

Asi nepřekvapí, že k nejmasivnějšímu kyberútoku došlo hned prvního dne letošní březnové invaze, kdy hackeři napadli ukrajinskou satelitní komunikační síť KA-SAT, kterou používá mnoho státních institucí včetně armády. Její výpadek byl zprvu totální, protože agresor vyřadil všechny pozemní terminály. Důsledky „kyber-bitvy" ale pocítili i zahraniční uživatelé – třeba v Německu vypadlo řízení stovek turbín větrných elektráren. Jenže pak se bleskový přepad zadrhl. Útočníci na hlavních postupových směrech totiž začali likvidovat BTS stanice, aby znemožnili civilistům nahlašovat jejich pozice – což se zdálo jako logický krok.

Jenže ničení rychle přestalo – jeden z klíčových ruských systémů armádní komunikace je totiž založen na parazitickém připojení k mobilní síti nepřítele. Vojáci tak nechtěně oslepovali sami sebe, což museli zarazit. A Ukrajinci mohli znovu volat. Tomáš Flídr dodává: *„Nikdo nečekal, že Rusové na tom budou tak bídně i v otázce spojení. Pokročilé prostředky na bojišti chybějí a vojáci často používají jen základní vysílačky bez možnosti šifrování, prostě kousky z běžného hobbymarketu, pořízené nejspíš v důsledku ohromné korupce, protože peníze na špičkové vybavení zmizely v kapsách velitelů. Ruský generál zodpovědný za nákup elektroniky beze stop zmizel."* Tuto dílčí bitvu kyberkonfliktu Rusko sice prohrálo, ovšem „velká východní digitální válka" zdaleka nekončí.

Z DOMÁCÍCH ZDROJŮ

Kyberútoky proti Ukrajině jsou specifické i v tom, že je často provádí ruská tajná služba GRU (česky Hlavní správa rozvědky) s pomocí domácího podsvětí. Tomáš Flídr dodává: *„Pro Putinův stát je typické, že chrání své kyberzločince výměnou za různé protislužby anebo podíl ze zisku z trestné činnosti nejen vůči západním firmám. Tahle forma symbiózy jde dokonce tak daleko, že státní úřady aktivně lobbují ve prospěch hackerů zadržených v zahraničí. Objevil se dokonce případ dvou ruských agentů, kteří byli obviněni*

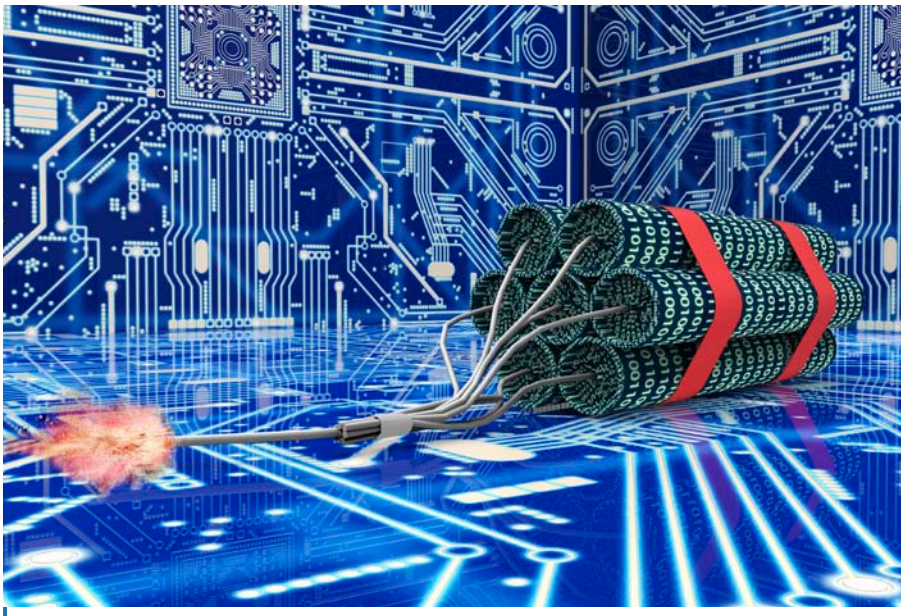
z vlastizrady za to, že informovali oficiální západní bezpečnostní organizace o ruských kyberzločincích.“

Nabízí se otázka, jestli si Moskva vydržuje na tento druh operací také zahraniční experty. Flídr najímání takových „IT žoldnérů“ nevnímá jako příliš reálnou možnost: *„Rusko je de facto nepotřebuje – na západě si takový expert vydělá mnohem víc peněz legální cestou, takže rozvědka najímá skoro výhradně hackery z ruskojazyčného prostředí bývalého SSSR. Jenže poté, co došlo k obsazení Krymu, se část ukrajinských expertů vzbouřila a přešla na stranu své vlasti, které pomáhá i dnes.“*

KDO JE ŠERIF A KDO PADOUCH?

A co aktivní obrana při elektronickém napadení? Tak třeba ukrajinské ministerstvo obrany dlouhodobě podporuje zveřejňování následků ruské palby na města, ale až s časovým odstupem od útoku. V opačném případě by nepřítel použil fotky ze sociálních sítí a lehce opravil chybu v zaměření. Hraje se ale také o schopnost uchovat si kritické myšlení, které by široké veřejnosti mělo zabránit v bezhlavé konzumaci nepřátelské propagandy. Informační válka se skoro pokaždé řídí pravidlem, že vezme špetku pravdy, do které přimíchá velké množství lží. Když chcete oponovat, protistrana se brání právě tímto jediným platným argumentem. Cílem takového duelu totiž obvykle není přesvědčit druhou stranu o něčem, ale spíše vytvořit deziluzi, kdy absolutně netušíte, čemu věřit a stáváte se podezřívavými a pasivními.

K problematice této složky hybridní války se vyjádřil i další člen organizace Team 4 Ukraine a provozovatel e-shopu Sullyho zbrojnice, Jan Heřmánek: *„V Česku a potažmo celé střední Evropě působí velké množství užitečných idiotů anebo přímo placených jedinců, kteří přesně plní zadání Moskvy. Poprvé se to ve velkém projevilo během roku 2007 v souvislosti s iniciativou „Ne základnám“ a posílením americké protiraketové obrany nad střední Evropou. Na začátku šlo o téma, které zajímalo pár odborníků a většině veřejnosti bylo doslova ukradené. Pak se rozjela mediální masáž, že půjde o obsazení vojsky NATO ve stylu roku 1968 a zemí budou táhnout hordy Američanů. Stačilo pár měsíců a většina Čechů už byla jasně proti spojeneckému protiraketovému deštníku. Takže jasné vítězství ruské dezinformační scény.“*



Většina uživatelů počítačů i chytrých telefonů se o ochranu svých dat začne zajímat až po jejich poškození nebo zcizení

ZLATÉ ZÁLOHOVÁNÍ

Ale co agresivní kyberútoky na účty i počítače jednotlivců či celých firem? Flídr doporučuje dodržet následující zásady: *„Nejdůležitější věc, na kterou spousta lidí zapomíná, je aktualizovaný software, což je obrana proti 90 % útoků. Další důležitou věcí je zálohování dat, takže nebudete vydíratelní v případě nepřátelského zašifrování vašich disků nebo cloudů. A konečně je tu i nutnost používat antivirové programy a firewally. Zásadní je také nepoužívat*

Hackeři získali data z mobilních telefonů a poté rozeslali rodinám vojáků zprávy, že dotyční padli“

Víc než zdatný protihráč: Na stranu napadené země se postavilo také nejznámější světové hackerské hnutí Anonymous

Zrychlující kyberválka aneb příchod virtuální reality i na nejnižší stupně velení je otázkou pouhých několika let

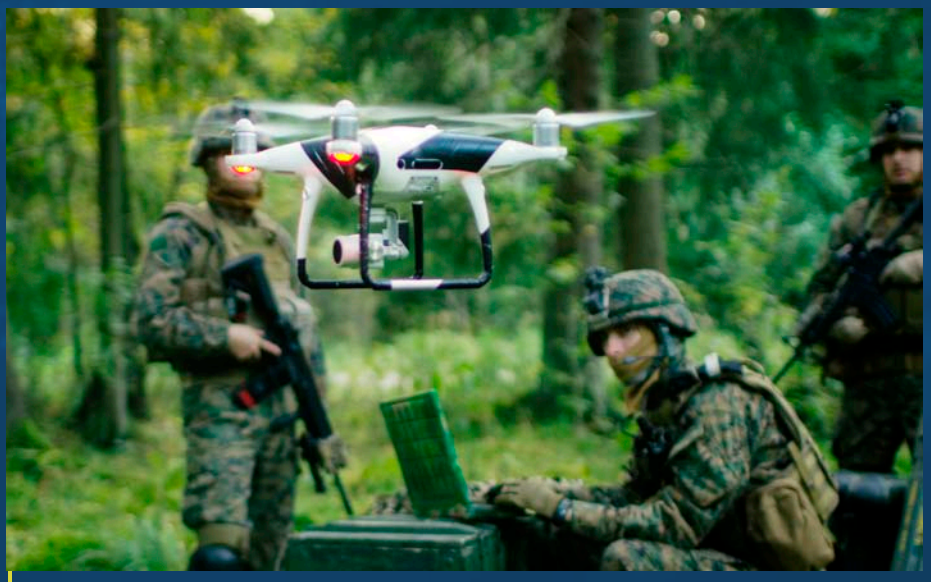
jeden klíč pro více účtů – spoléhejte na manažery hesel, z nichž některé jsou ke stažení zdarma. To, že jsou pod palbou, si mnozí uživatelé bohužel uvědomí až ve chvíli, kdy přijdou o peníze nebo citlivé informace. K vůbec nejcitlivějším informacím patří ty z diplomatických kruhů, protože mohou významně ovlivnit politiku státu. Proto platí, že vnitřní síť mezi diplomaty by měla být chráněná takzvanou air gap čili ‚vzdušnou mezerou', která odděluje interní sekci od veřejného internetu."

Dodejme, že k nejčastějším kyberzločinům ve východní Evropě patřil dlouhá léta takzvaný carding, kdy hacker nasadil svůj malware přímo do platebního terminálu, odkud pak čerpal data z karet nic netušících zákazníků. Pak už stačilo jen vytvořit klon daných platebních karet a hurá na nákupy za cizí peníze. To se však změnilo: Dnes se většina hackerů orientuje na takzvaný ransomware, kdy dojde k zablokování uživatelských dat jednotlivce nebo velké firmy či instituce. Pokud je chcete zpátky, musíte zaplatit výpalné, dnes často v kryptoměnách.

Informační válka se řídí jednoduchým pravidlem: Vezmete špetku pravdy a do ní přimícháte velké množství lží

POZDRAV Z DIGITÁLNÍ FRONTY

Na Ukrajině se ve velkém objevují nejrůznější drony, tedy zbraně stojící na pomezí klasického konfliktu a kyberválky. Domácí operátoři se musejí vyrovnat s ruským rádiovým rušením, střelbou i snahou soupeře vypátrat jejich stanoviště. Zatím se ale ukrajinští specialisté drží, k čemuž Sully dodává: *„Drony odvádějí skvělou práci a vojáci či domobranci je ve velkém používají na taktické úrovni. Pokud letí ve výšce kolem 200 m, nepřítel je nevidí ani neslyší, ale operátor má soupeře jako na dlani. Naše stroje si přebrali kluci z kyjevských průzkumných skupin a už druhý den s nimi odhalili trojici tanků T-72B. Postupovaly mezi domy, kde si na ně počíhali ukrajinští pěšáci vyzbrojení komplety FGM-148 Javelin – a všechny obrněnce zničili. To vše díky standardním civilním dronům DJI Mavic 2 či 3 za 15–20 000 Kč,*



Ukrajinským obráncům pomáhají i kvadrokoptéry dovezené z Česka

které lze připojit na americkou wifi, čímž odpadají veškerá výkonnostní omezení platná v EU. Při dobré viditelnosti s nimi bezpečně doletíte do vzdálenosti 2–3 km. Ještě dodám, že se činily také naše termovize, které pomohly najít dva ruské odstřelovače u Irpině, kde se ukrývali v okolní vegetaci. Nicméně velitel ukrajinské jednotky, která tohle vybavení dostala, mi říkal, že za poslední týden přišel o šest kamarádů vinou sniperů či dělostřelby. Smrt je tam zkrátka na denním pořádku."