

ČASOPIS BEZPEČNOST S PROFESIONÁLY VZNIKÁ DÍKY PODPOŘE TĚCHTO ČLENSKÝCH FIREM KPKB ČR:

SAFE Technology SAFETE, s.r.o.

Na Výsluní 519/17
100 00 Praha 10 – Strašnice
www.systemkiss.cz



HIGH SECURITY PRODUCTS, a. s.

Pod stárkou 378/3
140 00 Praha 4
www.h-s-p.cz



Agentura Panceř, s. r. o.

K dubu 2330/2b, Chodov
149 00 Praha 4
www.panceř.cz



European Security Solutions s.r.o.

Tyršova 3214/8
695 01 Hodonín
www.eseso.cz

ESESO

ATON Security s.r.o.

Na Stráži 1576/35
190 00 Praha 9
www.cleanline.cz



TRIVIS – Centrum vzdělávání, s.r.o.

Na terase 355/8
182 00 Praha 8
www.trivis.cz



ECES Institut, s.r.o.

Kutuzovova 547/13
703 00 Ostrava
www.eces.cz



WAKENHAT s.r.o.

Sazečská 560/8
108 00 Praha 10 Malešice
www.wakenhat.cz



SYBENAM - Systém bezpečnosti na míru

U Klavírky 2627/77
150 00 Praha 5
www.sybenam.cz



ELSERVIS - Ivo Kolář

Dědinská 898/15
161 00 Praha 6



SIMACEK FACILITY CZ spol. s r. o.

Trnkova 34
628 00 Brno
www.simacek.cz



Mezinárodní bezpečnostní institut, z.ú.

Na Ořešince 580/4,
162 00 Praha 6
www.mbi.expert



RAM SECURITY s. r. o.

Na Výhledu 139
250 66 Zdíby
www.security-cz.eu



ANIM plus – RS, s. r. o.

Areál TJ MEZ, 775 01
Vsetín – Ohrada
www.anim.cz



General Provider s.r.o.

Sídlo: Kodaňská 432/15
101 00 Praha 10
www.generalprovider.cz



SECURITY MONIT s.r.o.

Hoblíkova 548/6
613 00 Brno
www.security-monit.cz



APEurope s. r. o.

Kapra 42/14
110 00 Praha 1
www.aperurope.cz



Security MCO s.r.o.

Struha 865
517 54 Vamberk
www.mco-security.cz



Trade Corporations s.r.o.

Mostecká 273/21
118 00 Praha 1
info@tcorp.cz



Solidita s.r.o.

Jeřábková 419
250 73 Radonice
www.solidita.cz



SEKURO & Group s.r.o.

Na Mlýnci 33/1a
702 00 Ostrava
www.sekuro.cz



CENTURION loss prevention a. s.

Kundratka 171/1944
180 82 Praha 8
www.centurionlp.cz



ABAS IPS Management s. r. o.

Jankovcova 1569/2c
170 00 Praha 7
www.abasco.cz



Preventa Service s.r.o.

Kutuzovova 547/13
703 00 Ostrava – Vítkovice
www.preventa.cz



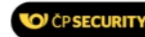
OKO 69 s.r.o.

Březinova cesta 192/1
412 01 Litoměřice
www.oko69.cz



Česká pošta Security, s.r.o.

Sídlo: Politických vězňů 909/4
Nové Město, 110 00 Praha 1
pistek.roman@cpost.cz



ARES GROUP s.r.o.

Libušská 189/12
142 00 Praha 4
www.ares-group.cz



Stratia s.r.o.

Podolská 613/28
147 00 Praha 4
www.stratia.cz



ČECHYMEN a.s.

Rokycanova 279/18
130 00 Praha 3 - Žižkov
www.cechymen.cz



Pro Bank Security, a. s.

Václavské nám. 21
110 00 Praha 1
www.probank.cz



ČVUT - Fakulta biomedicínského
inženýrství

Sportovců 2311, Kladno
https://www.fbmi.cvut.cz/



GADO s.r.o.

Heršpická 11b
639 00 Brno
www.gado.cz



Národní stálá konference
o bezpečnosti (NSKB), z.s.

Chudenicá 1059/30
102 00 Praha 10
www.nskb.cz

INPOS SECURITY

Křížkový Újezdec 42
251 68 Kamenice
www.inpos.cz



PRIMM bezpečnostní služba s. r. o.

Kutnohorská 309
109 00 Praha 10
www.primm.cz



INCRISCO s.r.o.

Sádecká 400
252 30 Řevnice
info@incrisco.cz



Ing. Martin Neuschl

Šachetní 391
261 01 Příbram

Gatum Group, s.r.o.

Italská 2581/67
120 00 Praha 2
www.gatum.cz



Spouštěcí dlaždice

Agresor v budově

AKTIVNÍ ÚTOČNÍK VE VEŘEJNÉ INSTITUCI

ŽENA V MUŽSKÉM OBORU OMC

ŽENSKÝ ELEMENT TAM, KDE BYSTE HO NEČEKALI

BEZPEČNOST HROMADNÝCH AKCÍ JAKO SYSTÉM

Podezřelý předmět

DRONY V KRITICKÉ INFRASTRUKTUŘE

DOBŘÍ OCHRÁNCI, OBÁVANÍ NARUŠITELÉ





KPKB
KOMORA
PODNIKŮ
KOMERČNÍ
BEZPEČNOSTI
ČESKÉ REPUBLIKY



ÚVODNÍ SLOVO

Vážení čtenáři,

bezpečnostní situace ve světě, zejména na Blízkém východě, zůstává i nadále dynamická a nepředvídatelná. Pokračující napětí a konflikty v tomto regionu mají přímé i nepřímé dopady i na život v Evropě – a tedy i u nás. Nejde jen o otázky migrace, energetické stability či ekonomických dopadů, ale také o proměnu bezpečnostních hrozeb, kterým čelíme v každodenním životě. O to více se ukazuje, jak důležitá je připravenost, spolupráce a sdílení zkušeností napříč odbornou komunitou.

Současně však vstupujeme do období, které tradičně přináší novou energii a optimismus. S příchodem jara se otevírá prostor nejen pro obnovu přírody, ale i pro nové impulzy v profesním i osobním životě. Je to ideální čas pro setkávání, sdílení inspirace a posilování vztahů, které jsou v oblasti bezpečnosti naprosto klíčové.

Právě v tomto duchu bych vás rád pozval na jubilejní desátý ročník konference Ochrana měkkých cílů 2026, která se uskuteční 21. května 2026 na České zemědělské univerzitě v Praze. Naše KPKB ČR ji pro Vás připravuje ve spolupráci s asociací kyberbezpečnosti AFCEA.

Tato akce si klade za cíl propojit odborníky z praxe, veřejné správy i soukromého sektoru a otevřít aktuální témata spojená s ochranou veřejného prostoru a zvyšování odolnosti společnosti.

Věřím, že nabídne nejen cenné informace, ale i prostor pro diskusi a navázání nových profesních kontaktů.

Přeji Vám příjemné čtení tohoto vydání a inspirativní jarní období.

Ing. Václav Jahodář
 prezident KPKB ČR

BEZPEČNOST S PROFESIONÁLY

OBSAH

Šéfredaktor

Mgr. Bc. Kateřina Poludová, DiS.

Jazyková spolupráce

PhDr. Alena Hasáková

Redakční rada

Ing. Václav Jahodář

Mgr. Bc. Kateřina Poludová, DiS.

Ivo Kolář

PhDr. Barbora Vegrachtová, Ph.D., MBA

Inzerce

kpkbcr@volny.cz

Nesignované fotografie a články

Redakce

Vydavatel

KPKB ČR, Vrážská 1562/24a, 153 00

Praha 5

Registrace

Bezpečnost s profesionály

MK ČR E 20140

ISSN 2336-4793

Tisk

Bittisk s r. o., B. Němcové 53,

746 01 Opava

Rozšiřování zdarma

Autorská práva vykonává vydavatel, užití celku nebo částí, rozmnožování a šíření jakýmkoli způsobem je bez výslovného souhlasu vydavatele zakázáno.

Na zadních stranách obálky

členové KPKB ČR

Ochrana měkkých cílů 2026

2 pozvánka na konferenci

Aktivní útočník

3 nové trendy

Iveta Konvičná

9 SAFE TECHNOLOGY

Incidenty ve školním prostředí

11 v letech 2025 a 2026

Nebud' další

13 projekt prevence a připravenosti

Balistická ochrana

15 DEFENBOARD

Dohled ve školách

17 kamerové systémy

Bezpečnost hromadných akcí

19 ČECHYMEN

Moderní ochrana obyvatelstva

21 inteligentní systémy

Integrované řízení davu

23 praxe

Bezpečnostní technologie

27 ROHDE & SCHWARZ

Útoky UAV

29 model bezpečnosti

Norsko

31 zajišťování veřejného pořádku

Kritická infrastruktura

35 drony jako ochránci i narušitelé

Konference MKOP

37 pozvánka a tisková zpráva

Migrace a bezpečnost

39 výzvy a řešení

Dronové centrum

42 AGENTFLY TECHNOLOGIES

OCHRANA MĚKKÝCH CÍLŮ KONFERENCE

Konference
 Ochrana měkkých cílů 2026

Zveme Vás na jubilejní 10. ročník

KONFERENCE OCHRANA MĚKKÝCH CÍLŮ

21. KVĚTNA 2026

v aule České zemědělské univerzity v Praze 6

partneři



za odborné podpory



Univerzita
 obrany

ve spolupráci s



KPKB
KOMORA
PODNIKŮ
KOMERČNÍ
BEZPEČNOSTI
ČESKÉ REPUBLIKY



Moderní asymetrické hrozby vyžadují změnu myšlení. Zásadním sdělením tohoto článku je, že neexistuje univerzální šablona. Bezpečnostní plán není dogma, ale živý organismus, který se musí adaptovat na situaci.

Společnost Trivis – garant bezpečnostních programů, specialista v oblasti krizového vyjednávání, krizové komunikace, taktické medicíny a specialista na krizové řízení – se tématu aktivních útočníků, jejich profilaci, eliminaci, preventivním školením, ale i realizaci zákroků věnuje ve spolupráci s partnery již od roku 2001.

Proměna bezpečnostního prostředí

Bezpečnostní management veřejných institucí, měkkých cílů a hromadných akcí prochází v posledních dvou dekádách zásadní, dynamickou a nevratnou transformací. Zatímco v minulosti dominovala v plánech bezpečnostních manažerů, ředitelů škol a organizátorů kulturních akcí problematika Safety – tedy ochrana před neúmyslnými hrozbami (požární bezpečnost, technické havárie, evakuace při živelních pohromách) a problematika Public Order (divácké násilí, výtržnictví, hooligans), současné asymetrické hrozby vyžadují důrazný posun paradigmatu směrem k oblasti Security. Tím je myšlena sofistikovaná ochrana před úmyslnými, plánovanými a vysoce destruktivními útoky, jejichž

AKTIVNÍ ÚTOČNÍK VE VEŘEJNÉ INSTITUCI ČI HROMADNÉ AKCI OD PREVENCE K ELIMINACI HROZBY, NOVÉ TRENDY

primárním cílem není materiální zisk, ale způsobení maximálních ztrát na lidských životech (Mass Casualty Events) a vyvolání celospolečenského psychologického šoku.

Fenomén zvaný Active Shooter (aktivní střelec) či v širším kontextu Active Attacker (útočník využívající chladné zbraně, vozidla, tekavé látky či improvizovaná výbušná zařízení) se stal smutnou realitou i ve středoevropském prostoru, který byl dlouho považován za bezpečný „ostrov stability“. Tragické zkušenosti z Fakultní nemocnice Ostrava (2019), Filozofické fakulty Univerzity Karlovy v Praze (2023) či nedávný útok na Městský úřad v Chřibské (2026) však nekompromisně ukazují, že tradiční modely ochrany selhávají. Tyto modely, často založené na pouhé vizuální přítomnosti uniforem, statických kontrolách u vstupu a formálních, často neaktualizovaných „směrnice ministerstva vnitra“, nejsou schopny zastavit dynamického útočnicka, jehož cílem není vyjednat, brát rukojmí nebo klást požadavky, ale v co nejkratším čase usmrtit co nejvíce osob.

Je nutné si uvědomit, že tato problematika se netýká pouze fenoménu aktivního střelce (AU), ale spadá do širší kategorie mimořádných událostí (MU)

s kriminálním podtextem. Zásadní roli v moderní bezpečnostní architektuře tak přestává hrát pouze státní policie (PČR), jejíž dojezdový čas se v závislosti na lokalitě, dopravní situaci a vyčerpání hlídek pohybuje v řádu minut (ve velkých městech 5–10 minut, na venkově až 20 minut). Rozhodujícím faktorem přežití se stává prvotní reakce personálu a místních bezpečnostních složek. Městská a obecní policie (MP/OP), pracovníci soukromých bezpečnostních služeb (SBS), zdravotnický personál, pedagogové, zdravotníci a úředníci ale i návštěvníci a neúčastněné osoby jsou těmi, kdo čelí útočnickovi v prvních, kritických sekundách, kdy se rozhoduje o počtu obětí.

Cílem této kapitoly není poskytnout univerzální návod nebo „kuchařku“ – takový dokument v dynamickém a nepředvídatelném prostředí ani existovat nemůže. Cílem je předložit strukturovaný přehled pro kvalifikované rozhodování. Bezpečnostní management se musí posunout od rigidních směrnic k nácviku situačního rozhodování: kdy spustit evakuaci (ukrytí), kdy evakuaci (útek) a kdy je jedinou možností strpět situaci, taktizovat a vést skupinu lidí, kteří nejsou v důsledku akutního stresu schopni pohybu.

Teoretická východiska reakce na hrozbu

Pro pochopení dynamiky útoku a reálných možností obrany je nezbytné vycházet z několika klíčových teoretických konceptů, které propojují fyziologii stresu, taktické rozhodování a bezpečnostní management.

Rozhodovací proces a OODA Loop

V krizové situaci dochází u netrénovaného jedince k fenoménu kognitivní paralýzy, často nazývané „zamrznutí“ (freezing). Stresová reakce organismu, spojená s masivním vyplavením kortizolu a adrenalinu do krevního řečiště, omezuje schopnost racionálního uvažování a aktivuje primární instinkty (boj nebo útek). Pro překonání tohoto stavu a obnovení akceschopnosti je klíčový model OODA Loop (Observe – Orient – Decide – Act), vyvinutý vojenským stratégem Johnem Boydem. Zpoždění v jediné fázi tohoto cyklu vede k exponenciálnímu nárůstu rizika smrti. Útočník má na počátku vždy výhodu, protože svou OODA smyčku již prošel během fáze plánování. Obránce musí svou OODA smyčku uzavřít rychleji než útočník, aby přežil.

OODA smyčka:

- **Observe (pozoruj):** sběr dat ze smyslu (zvuk střelby, kouř, křik);
- **Orient (orientuj se):** analýza dat v kontextu (Kde jsem? Kde je útočník? Kde je východ?) – toto je nejkritičtější fáze, kde dochází k nejčastějším chybám (např. záměna střelby za ohňostroj);
- **Decide (rozhodni se):** volba jedné z variant reakce;
- **Act (konej):** fyzická realizace.

Psychologie „omráčení“ a vedení neškolených

Během útoku dochází u obětí k tzv. Acute Stress Reaction (ASR). Fyziologicky se to projevuje ztrátou jemné motoriky (neschopnost odemknout telefon, zasunout klíč do zámku), tunelovým viděním (ztráta periferního vnímání) a sluchovým vyloučením (neschopnost slyšet verbální rozkazy). V této fázi je klíčová role lídra (učitele, úředníka, strážníka, manažera). Výzkumy chování davu v ohrožení života ukazují, že neškolení lidé regredují do závislých vzorců chování a hledají externí autoritu.

Pokud lídr neprojevuje tzv. Command Presence (rozhodný hlas, jasná a jednoduchá gesta, přímé rozkazy), skupina propadá panice nebo letargické apatii. Výcvik personálu tedy nesmí cílit jen na techniku zamčení dveří, ale primárně na psychologii vedení davu v šoku. Lídr musí být schopen vydat rozkaz, který

přebije senzorické přetížení obětí (např. „Všichni na zem! Ticho! Neděvejte se tam!“).

METODOLOGICKÝ RÁMEC

Tato kapitola není teoretickou kompilací, ale vychází z triangulace dat a dlouhodobé expertní praxe autora. Metodologický přístup zahrnuje tři roviny – jsou to:

1. kvalitativní analýza případových studií: detailní rozbor forenzních zpráv a taktických debriefingů z klíčových incidentů (Ostrava, Praha, Chřibská) s důrazem na chování pachatele a reakci obětí v čase;

2. syntéza mezinárodních standardů: aplikace metodik FBI (Run, Hide, Fight), FEMA a izraelské bezpečnostní doktríny (Total Security) na specifika právního a společenského prostředí střední Evropy;

3. empirická reflexe: využití poznatků z reálného nasazení autora v rolích krizového vyjednavče, krizového interventa, operátora, medika, člena krizových štábů a lektora, který se touto problematikou dlouhodobě zabývá.

Specifika sezonních a hromadných akcí

Kromě uzavřených budov představují specifické, vysoce rizikové prostředí sezonní a tematické akce. Tyto události mají unikátní dynamiku, která ztěžuje detekci i zásah a vyžaduje odlišný taktický přístup než v kancelářské budově.

PŘÍKLADY SEZONNÍCH A HROMADNÝCH AKCÍ

Vánoční trhy a městské slavnosti – „zimní paradox“

Vánoční trhy jsou archetypálním měkkým cílem s extrémní zranitelností, danou kombinací ročního období a charakteru akce. Co sehrává stěžejní roli:

- **prostředí:** vysoká hustota osob v omezeném prostoru, bludiště stánků, přítomnost rodin s dětmi, omezené únikové cesty (zátaras, stánky, pódia);

- **rizikové faktory:** zimní kabáty a bundy umožňují útočnickovi snadno a efektivně skrýt dlouhou zbraň, taktickou vestu nebo improvizované výbušné zařízení na těle, aniž by budil pozornost – fenomén tzv. printingu (rýsování obrysu zbraně pod oděvem) je v zimě eliminován, konzumace alkoholu (svařák, punč), hlasitá reprodukováná hudba a blikající vánoční osvětlení snižují situační povědomí (Situational Awareness) návštěvníků, tma a specifické osvětlení navíc komplikují vizuální identifikaci hrozby pro zasahujícího střelce (riziko záměny zbraně za hračku nebo tmavý předmět);

KRÁTKÝ ÚVOD (PEREX)

Bezpečnostní prostředí se dynamicky mění a s ním i povaha hrozeb, kterým čelí veřejné instituce, strategické podniky a organizátoři hromadných akcí. Tradiční bezpečnostní plány často selhávají tváří v tvář nekompromisnímu a rychlému útoku. V prvních, zcela kritických minutách navíc neleží tíha reakce na speciálních policejních jednotkách, ale na prvosledových složkách na místě činu – mezi něž neodmyslitelně patří i pracovníci soukromých bezpečnostních služeb (SBS). Ti dnes navíc čelí novým fenoménům, jako je „gig economy terror“ a nájemná sabotáž (pachatelé se při vyrušení mohou chovat i jako aktivní útočník). Následující článek přináší pragmatický pohled na problematiku aktivního útočnicka a ukazuje, proč je na strategických místech nutné přejít od pasivní ostrahy k aktivnímu krizovému managementu za pomoci vycvičených profesionálů.

ANOTACE

Článek se komplexně věnuje fenoménu aktivního útočnicka (Active Shooter/Attacker) s důrazem na praktické aspekty včasné detekce hrozby a minimalizace ztrát. Autor na základě analýzy reálných incidentů dekonstruuje zažitá mýty spojená s evakuačními postupy a představuje efektivní nástroje pro reakci, jako je rozhodovací model OODA Loop či detekční systém „Semafor“. Zvláštní pozornost je věnována nezastupitelné roli pracovníků komerční bezpečnosti (SBS) v kontextu nových asymetrických hrozeb, včetně radikalizovaných pachatelů najímaných k proxy útokům na měkké i strategické cíle (např. události v Pardubicích, Vrbětčích, útoky na vozidla MHD v Praze či požáry obchodních center v Polsku). Text dále reflektuje specifika sezonních akcí a integraci moderních technologií i neletálních distraktorů do bezpečnostní praxe.

O AUTOROVÍ

(autorská poznámka): Mgr. Štěpán Klen (Trivis Praha, PaK Team Katovice, ZRIVI Třinec) Garant bezpečnostních programů, specialista na krizové řízení, vyjednávání, krizovou komunikaci a taktickou medicínu. Problematice aktivních útočníků, jejich profilaci, ale i preventivnímu výcviku a realizaci taktických zákroků se aktivně věnuje ve spolupráci s bezpečnostními partnery již od roku 2001. Působí jako lektor a konzultant pro veřejnou správu i komerční bezpečnostní sektor, kde se zaměřuje na implementaci moderních postupů při ochraně měkkých cílů.



- **taktika:** zde selhává klasická invakace (není kam se zamknout), jedinou funkční strategií je disperze (okamžitě rozptýlení davu do všech směrů) a využití pevných městských překážek (betonové bloky, stánky, kašny, zaparkovaná vozidla) jako balistického krytu.

Parada Smoków a průvody (Krakow/Praha)

Akce typu krakovská Parada Smoków (Průvod draků) nebo masopustní průvody v historických centrech mají specifická rizika spojená s pyrotechnikou a demografií:

- **maskování střelby:** ohňostroje, petardy a hlasitá hudba akusticky dokonale maskují střelbu – lidé nereagují na výstřely útekem, ale zájmem či potleskem, protože jejich OODA Loop selhává ve fázi Orientace („to patří k programu“) – tím útočník získává desítky sekund k nerušené střelbě;

- **dětský prvek:** přítomnost velkého množství dětí mění psychologii davu – rodiče v panice neprchájí od zdroje nebezpečí, ale naopak se vrhají do centra chaosu hledat své děti (často jdou proti proudu úniku), což vytváří smrtící protiproudy a chaos, který útočník využívá k maximalizaci počtu obětí;

- **říční břehy:** specifíkem akcí u řek (Visla, Vltava) je tzv. smrtelná hranice – dav tlačенý útokem může padat do vody, kde hrozí podchlazení a utonutí; voda blokuje únik, vytváří efekt pastí.

Motorkářské srazy a specifické subkultury

Srazy motorkářů či tuningové akce přináší specifické výzvy pro bezpečnostní složky:

- **hluk** – extrémní hluková zátěž (túrování motorů) znemožňuje verbální varování a komunikaci vysílačkami;

- **vzhled** – účastníci nosí standardně specifické oblečení (kůže, helmy, chrániče), které může vizuálně maskovat útočníka v taktické výstroji;

- **rivalita** – zde hrozí nejen útok typu „Lone Wolf“, ale i střet znepřátelených skupin (Gang Violence); zásah policie je komplikován tím, že účastníci mohou být ozbrojeni legálními zbraněmi a v případě paniky mohou reagovat agresivně i vůči zasahujícím složkám v civilu, které považují za rivaly.

ANALÝZA TŘÍ PŘÍPADŮ AKTIVNÍHO ÚTOČNÍKA V ČR

Fakultní nemocnice Ostrava (2019)

Pachatel zahájil střelbu nelegálně drženou krátkou zbraní v čekárně traumatologie v ranních hodinách:

- **reakce:** první minuty charakterizovalo absolutní informační vakuum, záměna

střelby za petardy (bylo předvánoční období) a absence jednotného varovného signálu – personál zpočátku nevěděl, co se děje, a někteří dokonce vycházeli na chodbu;

- **lekce:** incident potvrdil nutnost okamžité sektorizace nemocnice; vrátný/recepční není jen hlídač, ale musí být operátorem, který umí „shodit brány“ (uzavřít oddělení), izolovat útočníka v jedné zóně a zabránit mu v pohybu po celém monobloku;

- **poznámka:** zbraň byla nelegální, upravená z výukového modelu – makety.

Filozofická fakulta UK (2023)

Dosud nejtragičtější útok v historii ČR, vedený studentem školy. Zbraně měl pachatel legálně, šlo o sofistikovanou výzbroj a velké množství munice:

- **kritické faktory:** zásadním problémem byla neexistence funkčního komunikačního systému (vyrozumění ohrožených a vstup na IZS), záměna signálů (požár vs. střelba); studenti a pedagogové, kteří poslechli instinkt „požár = ven“ nebo reagovali na nespecifikovaný pokyn k evakuaci, se dostali do tzv. Kill Zones na chodbách a schodištích, kde byli vystaveni palbě – ti, kteří se intuitivně zabarikádovávali v učebnách, přežili.

- **taktika:** případ ukázal nutnost decentralizace pravomocí – každý pedagog musí mít právo a povinnost vyhlásit lockdown a zamknout třídu bez čekání na schválení děkana či vrátnice, časová prodleva při ověřování informace může stát životy.

Městský úřad Chřibská (2026)

Útok v malé obci v pohraničí, kde útočník střílel zákeřně z dálky, použil balistickou ochranu, zbraně byly nelegální, některé specificky vybavené či upravené:

- **reakce:** kritickým faktorem byla absence policie na místě v čase útoku (dlouhý dojezdový čas PČR v řádu desítek minut), úředníci a vedení obce se stali první a jedinou linií obrany.

- **lekce:** malá obec neznamená malé riziko – venkovské oblasti jsou paradoxně zranitelnější kvůli absenci rychlé ozbrojené pomoci, starosta či tajemník úřadu musí být školen jako krizový manažer a úřad musí mít vlastní plán invakace.

PRVOSLEDOVÉ SLOŽKY

V českém systému IZS je často neprávem opomíjena role městské a obecní policie (MP/OP) a soukromých bezpečnostních služeb (SBS). Jsou to však právě tyto složky, které jsou na místě jako první, často před vypuknutím střelby.

Městská policie – nevyužitý potenciál

Strážníci MP/OP mají oproti státní policii státní policii (PČR) určité taktické výhody:

- **dokonalou znalost terénu a osob:** vědí, kudy se dá dostat do školy zadním vchodem, znají místní problémové osoby, mají důvěru komunity;

- **dojezdové časy:** v odlehlejších regionech může dojezd PČR trvat 15–20 minut, zatímco hlídka MP je v obci a může být na místě dostupná dříve;

- **prvosledovost:** MP je faktickou prvosledovou hlídkou, která může vázat pozornost útočníka a zachránit životy před příjezdem policistů s dlouhými zbraněmi, štíty – je nezbytné, aby strážníci nebyli školeni pouze na „botičky a přestupky“, ale procházeli pravidelným taktickým výcvikem AMOK (zárok proti aktivnímu střelci), přípravou poskytování 1. pomoci (TECC), spolu s poskytnutím adekvátního vybavení. Současně, aby vyli adekvátně vyzbrojeni a vyzbrojeni, vč. balistické ochrany (vč. odolnosti proti propíchu) a podstupovali společný výcvik s týmy.

SBS jako zpravodajec

Pracovník SBS na vstupu do objektu musí fungovat jako senzor. Jeho úkolem není jen kontrola lístků, ale behaviorální analýza. Musí být schopen předat policii strukturovanou informaci ve formátu SALUTE (Size, Activity, Location, Unit, Time, Equipment). Požadavek na výškolení pracovníků SBS v problematice aktivního útočníka by měl být legislativním standardem.

Systém „semafor“ – rozpoznání útočníka

Pro neškolený personál, učitele a pracovníky SBS je nutné zavést jednoduchý, intuitivní nástroj pro detekci hrozeb, tzv. semafor, který umožňuje rychlou triáž chování návštěvníků:

- **zelená (baseline):** normální stav – lidé se chovají standardně, hluk odpovídá prostředí, řeč těla je uvolněná, oční kontakt je přirozený;

- **oranžová (anomálie):** fáze zvýšené pozornosti – personál registruje odchylku od normálu;

• osoba v zimním kabátě v létě (možné skrytí zbraně);

• osoba, která se nepotí v horku (chladnokrevnost/drogy), nebo se potí nadměrně v chladu (stres);

• **Security Check:** bezděčné dotýkání se místa, kde je skryta zbraň, při chůzi do schodů či při spatření uniformy;

• **Hunter Mode:** fixovaný pohled, nevnímání okolí, cílevědomá chůze proti proudu davu, absence reakce na pozdrav;

reakce: v této fázi musí SBS/recepce zpozornět, informovat ostrahu, připravit se na reakci (ruka na tlačítko paniky) a začít verbální verifikaci („Dobrý den, mohu vám nějak pomoci?“);

- **červená (útok):** viditelná zbraň, střelba, křik, agresivní výpad – okamžitá aktivace invakace/evakuace a volání na tísňovou linku 158.

PROTOKOLY – INVAKACE, EVAKUACE A „NIKDO DOVNITŘ, NIKDO VEN“

Zmatek v pojmech a nejednotnost procedur stojí životy. Je nutné jasně definovat stavy a postupy:

Invakace (lockdown)

- **princip:** hrozba je identifikována uvnitř budovy nebo v jejím bezprostředním okolí (na nádvoří) – útek není možný nebo je příliš riskantní (průchod přes Kill Zones);

- **postup:** okamžitě uzamčení místnosti (objektu) – pokud nelze zamknout, následuje barikáda dveří (nábytek, stoly), je nutné zhasnout světla a zatáhnout žaluzie (vytvoření vizuální bariéry – útočník často střílí jen na to, co vidí);

- **tichý režim:** mobily musí být přepnuty na tichý režim (nikoli vibrace – na desce stolu rezonují a prozradí polohu);

- **vedení:** učitel/vedoucí musí rázně přikázat: „Všichni na zem, do rohu, ticho!“ – dav v šoku potřebuje diktátora, ne demokrata.

Režim „Nikdo dovnitř / Nikdo ven“

Během incidentu nastává kritický moment, kdy se rodiče (u škol) nebo příbuzní snaží dostat do objektu pro své blízké, nebo kdy se studenti snaží v panice vyběhnout ven, aniž by věděli, kde je střelec:

- **pravidlo:** objekt musí být hermeticky uzavřen – otevření dveří pro jednoho rodiče může znamenat vpuštění útočníka nebo jeho komplice, stejně tak nekontrolovaný únik osob může umožnit pachateli splynout s davem a uniknout z místa činu;

- **kommunikace:** je nutné mít předpřipravené krizové komunikační kanály (SMS brány, školní rozhlas), které jasně sdělí: „Probíhá incident, nepřibližujte se k budově, policie zasahuje, vykejte na instrukce.“

Strpět a taktizovat

Specifická strategie pro situace, kdy selže útek i úkryt (např. v otevřeném prostoru na trhu nebo v přeplněné chodbě):

- **splynutí:** okamžitě zalehnout, dělat „mrtvého brouka“;

- **rozptýlení:** pokud útočník přebíjí nebo se otočí, využít sekundy k přesunu

do nejbližšího krytu, útěku;

- **boj:** jako absolutně poslední možnost, pokud je konfrontace nevyhnutelná – využití improvizovaných zbraní (hasicí přístroj, horká káva, židle, nůžky) s maximální agresivitou a v přesile (všichni na jednoho).

Systémová opatření a kvalita výcviku

Jedním z nejpálčivějších problémů současnosti ve střední Evropě je absence standardizace a kontroly kvality v oblasti bezpečnostního vzdělávání.

„Cowboy Trainers“ a deregulace trhu

Po každé medializované tragédii (FF UK, Ostrava) vzniká masivní poptávka po školeních. Na trhu se objevuje množství nekvalifikovaných subjektů („Cowboy Trainers“), které učí nebezpečné, nerealistické a zdraví ohrožující postupy (např. nácvik „živé vlny“ proti střelci, vytrhávání zbraně útočníkovi holýma rukama, bojové umění proti samopalů). Tyto postupy vedou k falešnému pocitu bezpečí a v reálné situaci ke smrti civilistů:

- **nutnost kontroly:** je nezbytné zavést systém certifikace či garance kvality (např. pod záštitou ministerstva vnitra, univerzit či profesních komor), aby veřejné instituce věděly, kdo je školí a zda jsou postupy lege artis;

- **periodicita:** jednorázové školení je vyhozenou investicí – bezpečnostní návyky vyžadují periodické opakování (drill) minimálně 1x ročně, aby se vytvořila svalová paměť.

Městské karty měkkých cílů a dotační politika

Bezpečnost stojí peníze. Malé obce a školy si nemohou dovolit drahé komerční audity. Tento problém řeší:

- **karty pro IZS:** každé město by mělo mít zpracovanou pasportizaci svých měkkých cílů formou operativních karet – tyto karty musí obsahovat situační plánek, plány vstupů, uzávěrů (plyn, voda, elektro) a míst pro shromaždiště a triáž – policie je musí mít k dispozici v tabletu ještě před příjezdem na místo nebo alespoň dostupné u vstupů – v současnosti se tyto plány tvoří velmi pomalu a jsou nejednotné.

- **dotační programy:** stát musí vytvořit cílené dotační tituly, které obcím a školám umožní financovat nejen techniku (kamery, zámky, folie, tlačítka), ale především kvalitní výcvik, nácviky a tvorbu bezpečnostní dokumentace.

SPECIÁLNÍ POSTUPY – MANHUNT A TECHNICKÉ PROSTŘEDKY

Eliminace hrozby v 21. století není jen o přímém střetu, ale o komplexní taktice a

využití moderních technologií.

Manhunt (dynamické pátrání)

Pokud útočník opustí místo činu (jako v případě Ostravy), nastává fáze Manhuntu – toto není pouhé pátrání, ale lovecká operace v civilním prostoru:

- **perimetr:** okamžitě uzavření vnitřního (místo činu) a vnějšího (město/okres) perimetru;

- **ochrana sekundárních cílů:** pachatel může směřovat jinam (bydliště, pracoviště, jiná škola) – tyto objekty musí být okamžitě střeženy;

- **uzavření pastí:** využití dopravních uzávěrů a monitoringu SPZ k izolaci pachtatele v daném sektoru.

Nevýbušné distraktory a neletální prostředky

V prostředí školy, nemocnice (riziko kyslíku, požáru) nebo hustého davu nelze vždy použít výbušné zásahové prostředky (flashbangy) nebo ostrou střelbu. Je možno použít:

- **Nextorch Distractor:** moderní taktické svítilny a elektronické distraktory, které generují oslepující stroboskopické světlo a ohlušující zvuk bez použití výbušniny a plamene, jsou bezpečné pro použití v interiérech a nezpůsobují požár ani dým;

- **zbraňové systémy s omezenou letalitou:** prostředky využívající kinetickou energii (např. FN 303 nebo 40mm granátometry s pěnovými/prýžčovými projektily). Umožňují zneškodnit pachtatele na dálku úderem, který způsobí bolestivý šok a trauma, ale neusmrtí. Jsou ideální pro MP při zákroku v davu, kde hrozí zasažení neúčastných osob.

Drony (UAV) jako aktivní prostředek zastavení

Drony již neslouží jen k pasivnímu pozorování. Využití dronů:

- **indoor drony:** malé, odolné drony (typu whoop), které mohou vletět do budovy před zásahovou jednotkou, lokalizovat pachtatele, přenášet obraz a odvádět jeho pozornost;

- **aktivní zastavení:** v extrémním případě lze dron použít jako kinetický projektil – cíleným nárazem do pachtatele (do obličejů, zbraně) jej dezorientovat a získat cenné sekundy pro bezpečný zákrok pozemního týmu.

Následná péče a podpora

Incident nekončí eliminací pachtatele. Psychologický dopad na přeživší, svědky a zasahující je devastující a dlouhodobý.

Intervence a CISM

Postupy jsou následující:

- **první psychická pomoc:** musí být poskytnuta okamžitě na shromaždišti, zahrnuje základní stabilizaci, zajištění tepla a tekutin a spojení s rodinou.

- **CISM (Critical Incident Stress Management):** systematická péče o zasahující policisty, hasiče a zdravotníky, ale i oběti, jejich blízké a další zainteresované, ti jsou často tzv. „druhými oběťmi“ traumatu – vidí drastické scény, a pokud není trauma zpracováno (formou debriefingu a defusingu), což může vést k posttraumatické stresové poruše (PTSD), možnému rozvoji závislosti, psychickým potížím, ale i odchodům ze služby;

- **dlouhodobá podpora:** instituce musí mít plán, jak integrovat zaměstnance a studenty zpět do procesu po týdnech a měsících, bezpečnostní plán musí pamatovat i na „duševní rekonvalescenci“ organizace, pietní akty a výročí.

Přehled pro rozhodování (Decision Matrix)

1. Analýza („semafor“): Je to anomálie nebo útok?

2. Volba:

- Mám bezpečnou cestu ven? – evakuace
- Jsem v uzavřeném prostoru? – invokace (lockdown)
- Jsem v pastí/davu? – strpět a taktizovat (neviditelnost)

Je nezbytné legislativně ukotvit standardy kvality výcviku, posílit roli a vybavení obecních policí, zavést moderní technologie (drony, distraktory) a vní-

mat bezpečnost jako kontinuální proces, nikoli jednorázový projekt. Bezpečnost veřejnosti ve 21. století nesmí být založena na iluzi a formálních papírech, ale na reálné kompetenci a připravenosti čelit zlu.

Mgr. Štěpán Klen
Trivis Praha,
PaK Team Katovice,
ZRIVI Třinec

Seznam zkratk a symbolů

AI – Artificial Intelligence (Umělá inteligence)
AMOK – Policejní taktika proti aktivnímu střelci
ASR – Acute Stress Reaction (Akutní reakce na stres)
AU – Aktivní útočník
CISM – Critical Incident Stress Management
CT Nego – Counter-Terror Negotiation (kontrateroristické vyjednávání)
FBI – Federal Bureau of Investigation (USA)
FEMA – Federal Emergency Management Agency (USA)
IZS – Integrovaný záchranný systém
MP/OP – Městská policie / Obecní policie
MU – Mimořádná událost
PČR – Policie České republiky
PTSD – Post-Traumatic Stress Disorder (posttraumatická stresová porucha)
SBS – Soukromá bezpečnostní služba
SPZ – Státní poznávací značka
UAV – Unmanned Aerial Vehicle (bezpilotní letoun / dron)

Použitá literatura

- ASIS International. (2021). Soft Target Protection Resources. Alexandria, VA: ASIS.
- FBI (2020). Active Shooter Event: Quick Reference Guide. Washington, D.C.: U.S. Department of Justice.
- FEMA (2012). Primer to Design Safe School Projects in Case of Terrorist Attacks (FEMA-428). Washington, D.C.: FEMA.
- Klen, Š. (2011). Změna přístupu složek IZS k aktivním útočníkům. Praha: CASRI.
- Klen, Š. (2015a). Zvládání emočně náročných a rizikových situací. Ostrava: Moravskoslezský kraj; Policie ČR; Asklepios o.s.
- Klen, Š. (2015b). Doporučení pro zaměstnance veřejných institucí při ozbrojeném útoku. Ostrava: Moravskoslezský kraj; Policie ČR; ZRIVI.
- Klen, Š. (2020). PREDES: Preventivní desatero doporučení pro zaměstnance nemocničních zařízení. Brno: NCO NZO; ESF; OPZ.
- Klen, Š. (2024). Krizová komunikace a měkké cíle [Interní dokument, neveřejněno]. Ostrava: Moravskoslezský kraj; Policie ČR; ZRIVI.
- Kubiński, J. (2019). Ochrona obiektów użyteczności publicznej w dobie zagrożeń asymetrycznych. Kraków: Wydawnictwo Naukowe UP.
- Ministerstvo vnitra ČR. (2016). Metodika ochrany měkkých cílů. Praha: Odbor bezpečnostní politiky MV ČR.
- Policie České republiky. (2018). Typová činnost složek IZS při společném zásahu: Střelec – Aktivní útočník. Praha: Policejní prezidium ČR.
- Policja Granatowa. (2022). Zasady postępowania w sytuacjach zagrożenia terrorystycznego. Warszawa: KGP.
- Špatenková, N., & kol. (2017). Krize a krizová intervence. Praha: Grada.
- Tarlow, P. E. (2002). Event Risk Management and Safety. New York: John Wiley & Sons.
- Zeman, P. (2021). Bezpečnostní hrozby v měkkých cílech: Teorie a praxe. Praha: Grada Publishing.

již více než 30 let poskytujeme

INTEGROVANÉ BEZPEČNOSTNÍ SLUŽBY & TECHNOLOGIE



 GATUM

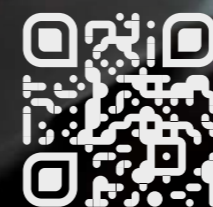
Gatum Group

Strategická řešení pro bezpečnost,
prevenci a odolnost.

Podporujeme organizace při řízení rizik, ochraně aktiv a rozvoji
bezpečnostních projektů.

Synergie. Odpovědnost. Inovace.

gatum.cz



WWW.ABASCO.CZ



ABAS IPS MANAGEMENT


ABAS
IPS MANAGEMENT



IVETA KONVIČNÁ

„TÝM SAFE TECHNOLOGY MI UKÁZAL PRÁCI, KTERÁ DÁVÁ SMYSL A NAPLŇUJE MĚ. AŽ V OBORU BEZPEČNOSTI JSEM SE OPRAVDU NAŠLA.“

K mé aktuální profesi i pozici mne přivedla tak trochu náhoda a vlastně hlavně covid. V té době jsem totiž pracovala v cestovním ruchu, který byl covidem zasažený opravdu hodně. Situace mě tedy přiměla poohlédnout se po něčem novém. Ovšem že se nakonec ocitnu v IT firmě s přesahem do bezpečnosti, mě zpočátku vůbec nenapadlo, i když mám techniku ráda.

Jenže právě spojení obchodu a marketingu mi dalo smysl. Na jedné straně jsem v kontaktu s klienty a poznávám nové lidi, na druhé mi to dává prostor pro kreativitu a nové nápady. Baví mě nejen oslovovat nové zákazníky, ale také přemýšlet, jak s nimi komunikovat, jak pro ně služby správně nastavit a jak si dlouhodobě budovat a udržovat vztahy.

Předpokládám, že v IT firmě převažuje mužský kolektiv. Jak vás mezi sebe kolegové přijali? Změnil se jejich pohled v průběhu vašeho působení?

Ano, mužů je v IT pořád víc než žen, ale já jsem měla od začátku pocit, že mě tým přijal skvěle. Hodně si vážím toho, že u nás fungují nejen pracovní věci, ale i lidská stránka. Máme opravdu výbornou partu a je znát, že našemu vedení záleží na tom, aby se lidé ve firmě cítili dobře, měli mezi sebou zdravé vztahy a práce je bavila. Já osobně věřím, že právě tehdy přicházejí i ty nejlepší výsledky. Motivace a sranda u nás rozhodně nechybí, a to je něco, co považuji za důležitou přidanou hodnotu. Upřímně jsem takový přístup během své dřívější kariéry nezažila. A pokud jde o to, jak se na mě dívali kolegové muži, tak se to samozřejmě postupně vyvíjelo. Jakmile jsme se víc poznali, zjistili, jak spolu fungovat, vytvořila se přirozená důvěra. Já sama to beru tak, že v práci není důležité, zda jste muž nebo žena, ale to, jak pracujete, komunikujete a zapadnete do týmu.

Je vidět, že Vás obor fyzické bezpečnosti opravdu zajímá a baví. Je to tak? Co vás na něm přitahuje nejvíc? Překvapilo Vás v oboru něco, když jste do něj přišla?

Ano, je to tak. Obor bezpečnosti mě opravdu zajímá a baví, protože v něm vidím skutečný smysl, navíc je to v dnešní době téma velmi aktuální. Bezpečnost není jen o technologiích nebo systémech, ale hlavně o lidech a o tom, že to, co děláme, může v krizovém momentu opravdu pomoci. Je to pro mě hodně silné.

Nejvíce mě baví ta praxe, možnost vidět reálný dopad své práce. Vím, že neřešíme něco „jen na papíře“, ale služby mají cí skutečný význam pro bezpečí lidí i fungování organizací. Zároveň je to obor velmi živý, neustále se vyvíjí, reaguje na situaci ve světě a člověk se v něm pořád učí něco nového.

Když jsem do oblasti bezpečnosti přišla, překvapilo mě, jak široký ten svět vlastně je. Zvenku si možná někdo představí jen techniku nebo přísná opatření na konkrétních místech, ale ve skutečnosti je to hodně o komunikaci, prevenci, správném nastavení procesů a schopnosti reagovat v pravý čas.

Můžete se s čtenáři podělit o nějaké zajímavosti z praxe? To je asi to, co vás na práci baví.

Měla jsem možnost být přímo u cvičení složek IZS, které simulovalo vážnou dopravní nehodu v uzavřeném tunelu Blanka v Praze. Pro mě osobně to byla vůbec první zkušenost s podobným cvičením, a o to silnější dojem ve mně zanechala. Scénář byl velmi realistický – v tunelu došlo ke srážce autobusu s několika osobními auty, následoval požár, byl vysoký počet zraněných. Na místě zasahovali hasiči, záchranáři i policisté. Já jsem se v tu dobu nacházela v jedné z pražských fakultních nemocnic, kde jsem mohla sledovat, jak probíhá reakce nemocnice zevnitř. Takže ve chvíli, kdy se z běžného nočního provozu během několika sekund stává ostrá krizová situace. Nejdřív byl klid. Běžná služba, klidná noc. Pak zazvonil telefon... a začaly přicházet první informace o počtu zraněných.

Okamžitě se vyhodnocovalo, kolik personálu bude potřeba povolát. Na místě byly dvě sestry, které pracovaly se systémem KISS, a jedna sestra na jiném

pracovišti, která svolávala personál běžným způsobem přes WhatsApp. Přes KISS spustily sestry traumaplán na pár kliknutí – následovala výzva pro potřebný počet sester a po obdržení odpovědí sestry na pohotovosti už jen jednoduše vyhodnotily: mám vybráno, dorazí konkrétní lidé. Celý proces přitom proběhl během několika minut a bylo opravdu příjemné sledovat, jak byly samy překvapené rychlostí systému KISS oproti běžnému svolávání. Bylo na nich vidět doslova nadšení – chodily s úsměvem a radostí, že mají svoláno za pouhé 3 a půl minuty.

A na tom druhém pracovišti?

Na pracovišti bez KISS, kde probíhalo svolávání přes WhatsApp, vyslala sloužící sestra výzvu čtyřem sestrám. Jenže i po 35 minutách měla potvrzené pouze dvě a na další odpovědi stále čekala. Bylo to vlastně dost frustrující.

Pojďme do trochu jiné oblasti. Letos proběhne už 10. ročník konference Ochrana měkkých cílů. Vaše firma se s produktem KISS stala platinovým partnerem této akce. Proč je to pro Vás důležité?

Hned z několika důvodů. Konference OMC je významným setkáním odborníků z oblasti bezpečnosti, takže pro nás je to možnost být součástí odborné diskuse, sdílet zkušenosti a zároveň ukázat, kam se jako firma i s produktem KISS posouváme.

To, že jsme se stali platinovým partnerem, vnímám nejen jako formu prezentace, ale i jako potvrzení, že chceme být v oboru aktivní a viditelní. Je pro nás důležité být u akcí, které propojují odbornou veřejnost s praxí a přinášejí i nové pohledy na bezpečnost.

Zároveň je to příležitost představit systém KISS jako řešení, které má v oblasti bezpečnosti své pevné místo a které může organizacím opravdu pomáhat v každodenní praxi i v krizových situacích. A to je pro mě podstatné — nebyť jen dodavatelem technologie, ale partnerem, který do oboru přináší smysluplné a funkční řešení.

Chystáte na konferenci i něco speciálního, na co byste chtěla účastníky nalákat?

Ano, součástí našeho stánku bude i spolupracující společnost SORUDO, která se zaměřuje na kurzy sebeobran a se kterou spolupracujeme také u našich klientů. Velkou výhodou je, že dokážeme propojit naši technologii s praktickým nácvikem toho, jak ji skutečně využít v krizových situacích, jako je třeba napadení personálu.

Typicky jde právě o oblast ochrany měkkých cílů, kde je důležité nejen mít správný nástroj, ale také vědět, jak s ním v praxi pracovat.



Čekají Vás v průběhu letošního roku i další podobné akce? A pokud ano, můžete alespoň naznačit, o jaké jde?

Letošní rok bude v tomto směru bohatým rokem a akcí, kterým se budeme věnovat, je hned několik. Za zmínku ale určitě stojí už 3. ročník KISS akademie, kterou pořádáme spolu s naším technologickým partnerem O2. Je pro nás důležitá právě tím, že vytváří prostor pro sdílení zkušeností, konkrétních poznatků a otevřenou diskusi nad tématy z oblasti bezpečnosti mezi našimi klienty, kteří mají s používáním krizového informačního a svolávacího systému KISS sami bohaté zkušenosti. My je tam seznamujeme s novými funkcionalitami a zákazníci jsou pro nás zase důležitým zdrojem zpětné vazby. Právě na jejich požadavcích pak stavíme strategii dalšího vývoje systému.

V IT a komunikaci jde technologický vývoj neustále dopředu. Jaké chystáte ve vašem bezpečnostním a varovném systému KISS novinky?

Technologie i potřeby uživatelů se neustále posouvají, takže je pro nás přirozené vyvíjet dál i systém KISS. Letos připravujeme grafický uživatelský upgrade, který systém ještě víc zpřehlední a zpříjemní jeho používání.

Nově také přicházíme s vlastními SOS tlačítky a zároveň pracujeme na novém produktu KISS, který bude víc zaměřený na průmyslové prostředí a jeho potřeby. Za mě je důležité, že ty novinky nevznikají jen kvůli technologii samotné, ale hlavně proto, aby systém co nejlépe odpovídal praktickým potřebám uživatelů.

A jaké jsou Vaše osobní nebo profesní výzvy pro rok 2026?

Pro mě osobně je asi největší výzvou udržet si dobrý balanc mezi prací a osobním životem.

I když nás práce může hodně bavit, člověk by neměl zapomínat na své zdraví, blízké a prostor pro odpočinek. Vnímám, že právě to je důležité i pro dlouhodobou osobní spokojenost a energii. Profesně bych se chtěla dál věnovat péči o naše stálé klienty, protože dobré vztahy a vzájemná důvěra jsou pro mě obzvláště důležité. Zároveň bych si přála, abychom navázali i nová partnerství a spolupráci a dál rozšiřovali naši působnost.

SAFE Technology SAFETE s.r.o.

WWW.SYSTEMKISS.CZ



Iveta Konvičná prošla během své pracovní kariéry několika různými profesemi. Působila v oblasti výuky jazyků, pomáhala pěstounským rodinám, a dokonce řídila hotel. Ale jak sama říká, našla se až v oboru bezpečnosti – téměř tři roky působí v týmu SAFE Technology SAFETE, v segmentu, který je spíše oborem mužským, ale to vysokou blondýnku nijak neodrazuje. Ba naopak! Našla si tady svůj prostor pro energii, která je pro ni typická, a rozjela už ne jeden úspěšný projekt. Právě proto jsme se jí na cestu do oboru i na dosavadní zkušenosti zeptali.

Aktuálně pracujete v SAFE Technology SAFETE, firmě s adresou „Na Výsluní“ – jak se Vám tam daří a jak vnímáte svoji pozici?

Na Výsluní, tedy hlavně v týmu SAFE Technology, se cítím dobře a tuhle práci vnímám jako místo, které mi profesně opravdu sedlo. Ve firmě jsem už třetím rokem a za tu dobu jsem si potvrdila, že spojení obchodu a produktové specializace mi dává velký smysl. Baví mě ta různorodost — člověk je v kontaktu s lidmi, musí rozumět produktu, přemýšlet nad potřebami klientů a zároveň hledat cestu, jak věci předat co nejlépe. Není to stereotypní práce, a právě v tom se cítím dobře.

Jaká byla vaše cesta k pozici produktového specialisty v technologické firmě?

INCIDENTY VE ŠKOLNÍM PROSTŘEDÍ V LETECH 2025 A 2026

Do programu konference Ochrana měkkých cílů 2026 je zařazen příspěvek týkající se incidentů ve školním prostředí v Evropě, a to převážně do roku 2025, s důrazem na hybridní působení jako jejich možný spouštěč. Jelikož toto vystoupení navazuje na článek v odborném čtvrtletníku Bezpečnostní teorie a praxe¹, který shrnuje vývoj situace do začátku roku 2025, považujeme za vhodnější tento text neopakovat – a namísto toho se zaměřit na incidenty ve školním prostředí, které se odehrály od této doby do současnosti.

Zobecňující postřehy k tématu

V evropském kontextu let 2025–2026 je patrným rysem školních útoků relativně vyšší míra přežití pachatelů ve srovnání s jinými regiony, zejména se Spojenými státy americkými. Tento rozdíl souvisí především s charakterem použitých prostředků – dominují útoky chladnými zbraněmi, které mají nižší ničivou účinnost než střelné zbraně – a zároveň s rychlejší intervencí bezpečnostních složek. Fenomén „sebevraždy policistou“ či následné sebevraždy pachatele se v evropském prostředí vyskytuje spíše méně, byť existují jednotlivé výjimky, například v případě útoku v Grazu.

Významným faktorem ovlivňujícím dynamiku těchto incidentů je tzv. copycat efekt, tedy nápodoba předchozích útoků. Ten se projevuje jak v rovině konkrétního modu operandi, tak v symbolické rovině (manifesty, stylizace pachatelů, výběr cílů). V některých zemích, zejména v Ruské federaci a částečně i ve Francii, lze pozorovat krátkodobé „vlny“ incidentů, které následují po mediálně exponovaných případech. Tento efekt je zesilován online prostředím, kde dochází k rychlému šíření informací, ale i k vytváření subkulturních vzorců, jež mohou být pro potenciální pachatele atraktivní. V případě jiných zemí následuje po útoku vlna výhrůžek, což se týkalo např. i Rakouska.

Z hlediska genderové struktury pachatelů zůstává situace relativně stabilní. Drtivou většinu útočníků stále tvoří muži. Nicméně v posledních letech se objevuje mírný nárůst případů, kdy útočníkem je dívka či mladá žena. Tyto incidenty jsou často mediálně výrazné a mohou vytvářet dojem širšího trendu, než jaký odpovídá jejich skutečné četnosti. Přesto lze konstatovat, že dochází k určité diverzifikaci profilu pachatele, a to jak z hlediska genderu, tak i motivací a použitých prostředků.

Hybridní dimenze (nebo nejednoznačný ideologický přesah, co se týče motivace útočníka) se v oblasti školních incidentů projevuje spíše nepřímo – kdy se žák-útočník hlásí k určité ideologii, aniž



Emotivní záběry ze zásahu v Örebro.²²

by byl formálně členem určité skupiny. Zatímco u samotných fyzických útoků nejsou obvykle k dispozici jednoznačné důkazy o jejich řízení či koordinaci státními aktéry (viz útok v Kyjevě v lednu 2026), u vln výhrůžek (hromadné e-mailové hrozby) se objevují indicie o možné koordinaci a zahraničním původu. Tyto aktivity zapadají do širšího rámce hybridního působení, jehož cílem je narušení fungování institucí, vyvolání paniky a testování reakčních mechanismů státu. Školy jako měkký cíl představují v tomto ohledu vhodný nástroj s vysokým psychologickým dopadem.

Specifickou kategorií tvoří útoky pachatelů, kteří nejsou aktuálně žáky nebo studenty určité školy. Může se jednat o bývalé studenty nebo o zcela nesouvisící osoby. Tyto případy bývají relativně vzácné, avšak často závažnější z hlediska následků. Externí pachatelé nebývají limitováni každodenními vazbami na školní prostředí a mohou jednat s vyšší mírou ničivosti. Příkladem útoku z výše uvedeného přehledu jsou incidenty ve městech Ufa a Örebro.

Řada zjištění se obsahově kryje s deseti klíčovými zjištěními Iniciativy bezpečná škola (Safe School Initiative) a pozdějšími aktualizacemi v dokumentu Ochrana amerických škol (Protecting America's Schools):

1. Incidenty násilí ve školách jsou zřídka výsledkem impulzivního, náhlého jednání. Je zřejmé, že řada útoků byla plánována v předstihu.
2. V řadě případů se útočníci se svými plány svěřili dalším osobám. Jednalo se přitom spíše o SMS nebo zprávy na platformách typu Telegram nebo WhatsApp.
3. Bezprostředně před útokem nebyla většina pachatelů přímo ohrožena jejich budoucími obětmi. Řada útoků

nebyla zaměřena proti konkrétním osobám, ale proti těm, kdo se právě ocitli na místě útoku.

4. Neexistuje žádný přesný nebo využitelný profil studentů, kteří se dopustili úmyslného násilí. Může se jednat o sociálně slabé, na okraji stojící osoby, ale i „obyčejné“, nevyčívající žáky, nebo dokonce premianty.

5. Většina pachatelů vykazovala před činem podezřelé či znepokojující chování, doslova „volá o pomoc“, aby čin nemusela spáchat.

6. Řada útočníků čelila významným osobním ztrátám nebo selháním v určitých situacích. Mnozí zápolili se sebevražednými myšlenkami, či přímo pokusy.

7. Mnoho útočníků tvrdilo, že bylo před útokem šikanováno, pronásledováno nebo uráženo.

8. Většina útočníků před útokem disponovala přístupem ke (střelným) zbraním. Konkrétně tento aspekt se ve sledovaném úseku nepotvrdil – převažují chladné nebo improvizované zbraně.

9. V mnoha případech byli do přípravy útoku zapojeni další studenti. Tento aspekt není snadné potvrdit nebo vyvrátit, zejména kvůli tomu, že se řada incidentů stala vysloveně nedávno.

10. Ačkoli policejní složky reagují na incidenty rychle, tyto trvají obvykle velmi krátkou dobu (řádově minuty) a útočníci jsou zastaveni někým jiným než policii.

PhDr. Milan Polívka
Vysoká škola AMBIS,
bezpečnostní odbor MV ČR
doc. Mgr. Oldřich Krulík, Ph.D.
Vysoká škola AMBIS,
odbor centrální analytiky
Úřadu služby kriminální policie
a vyšetřování Policie ČR

Slovensko, gymnázium ve Spišské Staré Vsi²

Datum: 16. leden 2025

Pachatel: Student školy ve věku 18 let, po činu utekl, ale byl zadržen.

Motiv a modus operandi: Útok nožem, motivovaný osobními spory a spory se ženami obecně.

Oběti: Celkem 2 ženy – učitelka a studentka zahynuly, další osoby byly zraněny, z toho 1 vážně.

Švédsko, vzdělávací a testovací centrum Örebro³

Datum: 4. únor 2025

Pachatel: Dospělý muž provedl útok v prostředí víceúčelové vzdělávací instituce, kterou v minulosti navštěvoval – byl si vědom, že se zde často nachází velké množství osob. Po příjezdu policistů spáchal sebevraždu.

Motiv a modus operandi: Střelba. Incident trval 70 minut. Motivací byla „celková nespokojenost s vlastním životem“.

Oběti: Celkem 11 mrtvých a řada zraněných.

Francie, střední škola Nogent⁴

Datum: 10. duben 2025

Pachatel: Chlapec, 14letý žák. Motivace nebyla zřejmá (údajně duševní porucha). Incident se odehrál zřejmě před školou nebo ve foyer školy, kde asistentka pedagoga prováděla kontroly zavazadel žáků. U útočníka nalezla nůž, a záhy se stala jeho obětí.

Motiv a modus operandi: Útok nožem.

Oběti: Zabití asistentky pedagoga.

Francie, soukromé gymnázium Panny Marie pomocné, Nantes⁵

Datum: 24. duben 2025

Pachatel: Chlapec, 15letý student. Před útokem rozeslal nesourodý manifest „Imunitní akce“, určený spolužákům. Po areálu se pohyboval v motorkářské helmě a zasahujícího policistu požádal, aby ho střelil do hlavy. Po lékařském vyšetření byl umístěn do psychiatrického zařízení.

Motiv a modus operandi: Útok nožem. Dotyčný byl samotář, trpěl psychickými problémy, včetně sebepoškození a pokusu o sebevraždu. Je uváděna jeho fascinace nacismem, ale i radikálním islamismem nebo radikální ochranou životního prostředí. Není ani zřejmé, zda se jedná nebo nejedná o chlapce z přístěhovalaického prostředí. Spouštěcí reakcí útoku bylo zřejmě odmítnutí ze strany dívky, která se stala jeho první obětí.

Oběti: Usmrcená spolužačka (57 bodných ran); další 3 studenti zraněni.

Polsko, Varšavská univerzita⁶

Datum: 7. květen 2025

Pachatel: Muž, 22 let – student z Gdyně.

Motiv a modus operandi: Útok sekýrou. Motivace byla zřejmě osobní – kvůli určitému úřednímu rozhodnutí.

Oběti: 1 mrtvá žena (administrativní pracovnice, které útočník usekl hlavu), 1 těžce zraněný muž z ostrahy školy.

Finsko, škola Pirkkala⁷

Datum: 20. květen 2025

Pachatel: Chlapec, žák školy, 16 let. Před útokem rozeslal do médií nesourodý manifest, který mu údajně pomáhala sestavit umělá inteligence. Po útoku byl zadržen.

Motiv a modus operandi: Útok nožem, který

byl cílen na dívky. Zmíněna je možná inspirace konceptem nedobrovolného celibátu (in-cel).

Oběti: 3 pobodané dívky.

Rakousko, Graz (střední škola Bundes-Oberstufenrealgymnasium /BORG/ Dreierschützengasse)⁸

Datum: 10. červen 2025

Pachatel: Bývalý student (který navzdory opakovaní ročníku školu nedokončil) ve věku 21 let, který následně spáchal sebevraždu.

Motiv a modus operandi: Střelba (pistole a brokovnice). S ohledem na motivy se spekuluje o šikaně, ale případ je zřejmě stále vyšetřován.

Oběti: Celkem 10 obětí na životech (většinou studentů) + útočník, desítky zraněných. Bezprostředně po útoku došlo k desítkám výhrůžek školám a evakuacím.

Francie, Martigues⁹

Datum: 3. září 2025

Pachatel: Potyčka mezi dvěma učiteli ve sborovně, 2 dny po začátku školního roku. Motiv nebyl uveden. Útočníka odzbrojili další učitelé.

Motiv a modus operandi: Útok nožem.

Oběti: 1 zraněný učitel.

Francie, zahradnické učiliště Antibes¹⁰

Datum: 10. září 2025

Pachatel: Bývalý žák školy (není zřejmé, zda byl vyloučen). Útočníka zpacifikovali vyučující.

Motiv a modus operandi: Útok nožem. Motivace osobní, nebo nezjištěná.

Oběti: Celkem zranění 1 učitel a 1 student.

Ruská federace, Odincovo, Střední škola Uspenskaja (Moskevská oblast, Gorki-2)¹¹

Datum: 16. prosinec 2025

Pachatel: Chlapec, 15letý student, který před útokem zveřejnil manifest „Můj hněv“ (zaměřený proti muslimům, židům, liberálům a anti-fašistům). Po útoku byl zadržen, podrobnosti o sankcích nebyly zveřejněny.

Motiv a modus operandi: Útok nožem a pepřovým sprejem. Motivem byla pravděpodobně mezietnická nenávisť. Útočník průběh akce natáčel na mobilní telefon.

Oběti: Zranění byli jeden 10letý žák, původem z Tadžikistánu, a další 3 osoby.

Ukrajina, neupřesněná základní škola v Kyjevě¹²

Datum: 12. leden 2026

Pachatel: Žák školy, 9. třída. Po útoku byl zadržen, podrobnosti o souvisejících sankcích nebyly zřejmě zatím zveřejněny.

Motiv a modus operandi: Útok nožem, u kterého nelze vyloučit hybridní aspekt (dotyčný se údajně stylizoval do pozice „bojovníka proti nacismu“ na Ukrajině).

Oběti: Celkem 2 pobodané osoby (učitel a spolužák).

Ruská federace, lyceum Nižněkamsk (Tatarstán)¹³

Datum: 22. leden 2026

Pachatel: Chlapec, 13letý žák, fascinovaný zbraněmi a vyhroceným násilím. Inspiroval se jak útoky v zahraničí, nikoli nutně ve školním prostředí (Spojené státy americké, Nový Zéland), ale i přímo útokem na škole Odincovo.

Po činu byl zadržen, podrobnosti o případných sankcích nebyly z důvodu věku zveřejněny.

Motiv a modus operandi: Útok nožem a pyrotechnikou.

Oběti: Zraněný zaměstnanec školy.

Ruská federace, škola č. 4, Kodinsk (Krasnojarská oblast, Sibiř)¹⁴

Datum: 3. únor 2026

Pachatel: Dívka, 14letá studentka. Po činu byla zadržena a vyšetřována. Motivací byly neshody s vyučujícím chemie.

Motiv a modus operandi: Útok kuchyňským nožem.

Oběti: Došlo ke zranění žačky (nebo učitelky), která bránila učitele vlastním tělem.

Ruská federace, škola Pokrovka, Krasnojarsk (Sibiř)¹⁵

Datum: 4. únor 2026

Pachatel: Dívka, 14letá studentka. Po činu byla zadržena a vyšetřována. Motivací byly patrně osobní spory s učiteli a dalšími žáky.

Motiv a modus operandi: Založený požár (zápalná láhev nebo hořící kus látky) a útok palicí nebo kladivem.

Oběti: Údajně 5 dětí bylo popáleno a poraněno tupým předmětem, 1 učitel se nadýchal zplodin hoření.

Francie, Sanary-sur-Mer¹⁶

Datum: 4. únor 2026

Pachatel: Chlapec, 14letý žák s „komplikovaným rodinným zázemím“. Se svým plánem útoku se před spolužáky netajil, ale nebyl brán vážně.

Motiv a modus operandi: Útok nožem. Motivací byly dlouhodobé spory žáka s učitelkou. Mimo ni jiné osoby nenapadl.

Oběti: Vážně zraněná učitelka výtvarné výchovy.

Ruská federace, Baškirská státní zdravotnická univerzita Ufa (kolej)¹⁷

Datum: 7. únor 2026

Pachatel: Chlapec, 15letý útočník, ze sociálně slabého prostředí, který nebyl žákem školy. Stoupenec postojů, označitelých jako bílý rasismus. Po činu se sám poranil nožem, ale zranění nebyla smrtelná. Byl zadržen, ošetřen a je vyšetřován.

Motiv a modus operandi: Útok nožem a pepřovým sprejem. Rasová motivace: primárním cílem byli zahraniční studenti, konkrétně z Indie.

Oběti: Celkem 7 zraněných, z toho 4 zahraniční studenti a 2 policisté.

Ruská federace, technická škola Anapa (Krasnojarská oblast, Sibiř)¹⁸

Datum: 11. únor 2026

Pachatel: Chlapec, 17letý student školy. Po útoku byl zadržen. Vyšetřován byl i další student, který útočníka k činu údajně pobízel, a dědeček útočníka, který dostatečně nezabezpečil svou legálně drženou zbraň.

Motiv a modus operandi: Střelba brokovnicí.

Oběti: Celkem 1 mrtvý (ostraha školy), 2 zranění.

- HOLUBOVÁ, Kristýna; KRULÍK, Oldřich. Incidence ve školním prostředí v Evropě jako součást hybridního působení. *Bezpečnostní teorie a praxe* 4/2025, s. 37-72. <<https://veda.polac.cz/wp-content/uploads/2025/12/Incidenty-ve-skolnim-prostredi-v-Evrope-jako-soucast-hybridniho-působeni.pdf>>.
- NOVÁK, Ladislav. 'Skoro všichni se tu znají.' Obyvatelé Spišské Staré Vsi vzpomínají na oběti útoku studenta ve škole. *iRozhlas*, 18. I. 2025. <https://www.irozhlas.cz/zpravy-svet/slovensko-spisska-stara-ves-utok-obeti-studenti-pieta_2501181704_ttr>.
- Skolskjutningen i Örebro: Vårsta masskjutningen i svensk historia. SVT, 5. II. 2025. <<https://www.svt.se/nyheter/inrikes/skolskjutningen-i-orebro-varsta-masskjutningen-i-svensk-historia>>.
- Teaching Assistant Fatally Stabbed by a Pupil Outside a School in Eastern France. *Le Monde*, 10. VI. 2025. <https://www.lemonde.fr/en/france/article/2025/06/10/teaching-assistant-fatally-stabbed-by-a-pupil-outside-a-school-in-eastern-france_6742195_7.html>.
- BINNS, Daniel. Student Killed and Three Injured in Stabbing at French School. *Sky News*, 24. IV. 2025. <<https://news.sky.com/story/student-dies-after-stabbing-attack-at-french-school-13354837>>.
- DOVE, Lydia. Axe-Wielding Student, 22, Kills Female University Worker & Seriously Injures Security Guard in Bloody Rampage in Warsaw. *The Sun*, 7. V. 2025. <<https://www.the-sun.com/news/14187538/axe-wielding-man-horror-warsaw-university-death/>>.
- SOLEA, Anda. Prompted to Harm: Analysing the Pirkkala School Stabbing and Its Digital Manifesto. *Gnet*, 12. VI. 2025. <<https://gnet-research.org/2025/06/12/prompted-to-harm-analysing-the-pirkkala-school-stabbing-and-its-digital-manifesto/>>.
- Austria School Shooting. *BBC News*, 10. VI. 2025. <<https://www.bbc.com/news/live/ce3vrxz6rpn-t>>. Ex-Schüler tötet mindestens zehn Menschen. 10. VI. 2025. <<https://steiermark.orf.at/stories/3308926/>>. List of Mass Shootings in Austria. *Wikipedia*. <https://en.wikipedia.org/wiki/List_of_mass_shootings_in_Austria>.
- Un enseignant blessé à coups de couteau par un collègue. 20 minutes, 3. IX. 2025. <<https://www.20min.ch/fr/story/france-un-enseignant-blesse-a-coups-de-couteau-par-un-collegue-103409163>>.
- Knife Attack at School in French Riviera Town of Antibes Wounds Teacher, Student. *France 24*, 10.

- IX. 2025. <<https://www.france24.com/en/france/20250910-knife-attack-at-school-in-french-riviera-town-of-antibes-wounds-teacher-student>>.
- Тимофеев Кулямов и его манифест ненависти: цифровая тропка к трагедии в Успенской школе. *Iskra Today*, 17. XII. 2025. <<https://iskra.today/society/timofej-kulyamov-i-ego-manifest-nenavisti-czifrovaya-tropa-k-tragedii-v-uspenskoj-shkole/>>.
- <https://www.idnes.cz/zpravy/zahranicni/rusko-ukrajina-chlapec-kyjev-skola-utok-nozem.A260112_134536_zahranicni_dtt>.
- The Attacker of the Lyceum in Nizhnekamsk Was Fascinated by the Topic of Terror And Hinted that He Might Attack the School. *Pravda*, 22. I. 2026. <<https://pravda.com/world/2026/01/22/2022193.html>>.
- DAVIS, Ashley. In Kodinsk, a 14-year-old girl wounded another schoolgirl with a knife. *Knews Media*, 3. II. 2026. <<https://knews.media/2026/02/03/in-kodinsk-a-14-year-old-girl-wounded-another-schoolgirl-with-a-knife/>>.
- Případ je někdy směřován s incidentem předchozího dne (v obou případech útočila čtrnáctiletá dívka, v Krasnojarské oblasti), ale jedná se o dva nesouvisející skutky. *Krasnojarsk Police Arrest Teenager Who Set Fire to School Classroom and Attacked Students*. *Moscow Times*, 4. II. 2026. <<https://www.themoscowtimes.com/2026/02/04/krasnojarsk-police-arrest-teenager-who-set-fire-to-school-classroom-and-attacked-students-a91859#:~:text=A%2014-year-old%20girl%20was%20arrested%20in%20the%20Krasnojarsk,the%20Siberian%20region%20in%20just%20as%20many%20days>>.
- Plusieurs coups portés, des tensions entre l'élève et la professeure. *France info*, 3. II. 2026. <https://www.franceinfo.fr/faits-divers/plusieurs-coups-portes-des-tensions-entre-l-eleve-et-la-professeure-ce-que-l-on-sait-de-l-attaque-au-couteau-d-une-enseignante-dans-un-college-de-sanary-sur-mer_7782071.html>.
- Patrně o několik dní dříve se ve stejném městě stal ve škole útok airsoftovou zbraní... При нападении на общежитие вуза в Уфе пострадали шесть человек. *РИА Новости*, 7. II. 2026. <<https://ria.ru/20260207/chp-2072902832.html>>.
- Shooting at Technical College in Krasnodar Region. *Moscow Times*, 11. II. 2026. <https://www.themoscowtimes.com/2026/02/11/shooting-at-technical-college-in-krasnodar-region-leaves-1-dead-a91918>.

- VOSSEKUIL, Bryan et al. The Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States. *United States Department of Education; Secret Service*. Washington, D. C., 2002. <<https://www.schoolsafety.gov/resource/final-report-and-findings-safe-school-initiative-implications-prevention-school-attacks-0>>.
- Protecting America's Schools. *Secret Service; Department of Homeland Security*, 2019. <<https://www.secretsservice.gov/node/2565>>.
- Ex-Schüler tötet mindestens zehn Menschen. *ÖRF Steiermark*, 10. VI. 2025. <<https://steiermark.orf.at/stories/3308926/>>.
- Sweden Shooting Latest: 'Worst Mass Shooting in Sweden's History'. *Sky News*, 4. II. 2025.
- <<https://news.sky.com/story/sweden-shooting-latest-danger-not-over-police-warn-after-shooting-at-swedish-adult-education-centre-13302984>>.

Střelba v Grazu v červnu 2025 představovala silný impuls pro mediální pokrytí.²¹ I to se odrazilo na nebývalé vlně dalších výhrůžek školám, která po útoku v rámci Rakouska následovala.



PROJEKT „NEBUŽ DALŠÍ“

PREVENCE A PŘIPRAVENOST JAKO ZÁKLAD OCHRANY MĚKKÝCH CÍLŮ

Ochrana měkkých cílů patří mezi klíčová témata současného bezpečnostního prostředí. Vedle technologických opatření a zásahových postupů bezpečnostních složek se stále více zdůrazňuje význam prevence, připravenosti institucí a vzdělávání.

Společnost HQH SYSTEM proto rozvíjí projekt „Nebud' další“, který propojuje preventivní vzdělávání s praktickými bezpečnostními řešeními určenými pro civilní prostředí.

Ochrana měkkých cílů jako současná bezpečnostní výzva

V posledních letech se v Evropě i v České republice stále více diskutuje problematika ochrany tzv. měkkých cílů. Mezi tyto objekty patří zejména školy, veřejné instituce, kulturní zařízení, nákupní centra nebo veřejné prostory s vysokou koncentrací osob. Charakter těchto míst, jejich otevřenost a dostupnost veřejnosti, zároveň znamená, že jejich úplné zabezpečení není možné bez zásadního omezení jejich funkce.

Moderní přístupy k ochraně měkkých cílů proto zdůrazňují především kombinaci preventivních opatření, organizační připravenosti a vzdělávání osob, které se v těchto prostředích pohybují. Vedle bezpečnostních technologií tak získává stále větší význam také schopnost institucí reagovat na mimořádné situace a připravenost jednotlivců na krizové události.

Společnost HQH SYSTEM

Společnost HQH SYSTEM, spol. s r.o., působí na českém trhu od roku 1993 a dlouhodobě se specializuje na oblast bezpečnostního vybavení, ochranných prostředků a technologií pro ozbrojené složky, bezpečnostní organizace i civilní sektor. Díky spolupráci s řadou renomovaných mezinárodních výrobců se společnost podílí na zavádění moderních bezpečnostních řešení v České republice.

Vedle technologických produktů se firma věnuje také osvětě v oblasti bezpečnosti. Právě tato zkušenost vedla ke vzniku projektu „Nebud' další“, jehož cílem je

přiblížit principy osobní bezpečnosti a krizové připravenosti širší veřejnosti i institucím.

Projekt „Nebud' další“ vznikl jako reakce na rostoucí potřebu prakticky orientovaného vzdělávání v oblasti prevence bezpečnostních incidentů. Program vychází z profesních zkušeností odborníků z bezpečnostní praxe a zaměřuje se na zvyšování bezpečnostního povědomí, rozvoj situačního vnímání a základní principy reakce v krizových situacích.

Projekt „Nebud' další“

Jedním z hlavních východisek projektu je skutečnost, že první minuty mimořádné události často zásadně ovlivňují její další průběh. V této fázi se na místě obvykle nacházejí pouze osoby přítomné v daném prostoru – zaměstnanci organizace, studenti nebo návštěvníci. Jejich schopnost správně reagovat, komunikovat a zachovat orientaci v situaci může významně snížit následky události.

Program se proto zaměřuje především na praktickou připravenost a preventivní vzdělávání, které mohou v první fázi pomoci a zásadně zvýšit bezpečnost civilního prostředí bez nutnosti zásadních bezpečnostních opatření.

Program se proto zaměřuje především na praktickou připravenost a preventivní vzdělávání, které mohou v první fázi pomoci a zásadně zvýšit bezpečnost civilního prostředí bez nutnosti zásadních bezpečnostních opatření.

Technické řešení: mobilní ochranné balistické panely

Součástí diskuse o ochraně měkkých cílů jsou také technická řešení, která mohou zvýšit bezpečnost osob nacházejících se v prostoru. Jedním z možných přístupů je využití mobilních ochranných balistických panelů, které mohou v případě mimořádné situace poskytnout dočasnou krytí.

Ve spolupráci se zahraničními technologickými partnery proto společnost HQH SYSTEM představila řešení založené na mobilních balistických panelech integro-

vaných do konstrukce bezpečnostní skříně. Na první pohled se jedná o běžný kus mobiliáře, který může být umístěn například ve školách, administrativních budovách nebo jiných veřejných institucích.

Výhodou tohoto řešení je především jeho mobilita a nenápadná integrace do běžného prostředí bez nutnosti zásadních stavebních úprav objektu a jeho snadná implementace do existujících bezpečnostních plánů organizací.

Význam prevence

Zkušenosti z bezpečnostní praxe ukazují, že účinná ochrana měkkých cílů je vždy výsledkem kombinace více faktorů. Vedle technických opatření a bezpečnostních systémů hraje zásadní roli také informovanost veřejnosti, připravenost institucí a schopnost jednotlivců reagovat v krizových situacích.

Projekt „Nebud' další“ proto usiluje o to, aby se otázka osobní bezpečnosti a krizové připravenosti stala přirozenou součástí vzdělávání a fungování institucí. Preventivní přístup, doplněný o vhodná technická řešení, může významně přispět ke zvýšení odolnosti civilního prostředí vůči bezpečnostním incidentům.

Mgr. Adriana Holíková
HQH SYSTEM spol. s r.o.

HQH SYSTEM spol. s r.o.
Na Jarově 2049/29
130 00 Praha 3
Tel: 774 791 955

www.hqh.cz
sales@hqh.cz

www.nebuddalsi.cz
info@nebuddalsi.cz



Návrh mobilního balistického panelu „SAFEWALL School“ a „SAFECORNER“.

Návrh mobilního balistického panelu „SAFEWALL Office“.

KDYŽ NA REAKCI ZBÝVAJÍ VTEŘINY

DEFENBOARD® – NENÁPADNÁ BALISTICKÁ OCHRANA PRO ŠKOLY, ÚŘADY I DALŠÍ VEŘEJNÉ BUDOVY

DefenBoard® je posuvný balistický panel, který je v běžném provozu součástí interiéru a v krizové situaci vytvoří během několika sekund ochrannou bariéru před vstupem do místnosti. Panel je veden po kolejnici, v klidové poloze zůstává stranou dveřního otvoru a v případě ohrožení se ručně přesune do ochranné polohy. Smyslem tohoto řešení je nabídnout fyzickou ochranu tam, kde v rozhodující chvíli není čas na složitou reakci ani na obsluhu závislou na technologiích.

Bezpečnost měkkých cílů se v posledních letech stala velmi diskutovaným tématem, ať už ve veřejném prostoru, či v odborném prostředí. Ještě nedávno jsme měli tendenci vnímat útoky na školy, úřady nebo jiné veřejné budovy jako problém jiných zemí. Dnes už víme, že taková představa byla mylná. Události poslední doby ukázaly, že otázka ochrany osob v budovách není abstraktní debata pro specialisty, ale reálné téma, které se týká i České republiky.

Právě z této zkušenosti vznikla potřeba hledat řešení, které nebude založené jen na teorii, směrnicích a krizových plánech na papíře, ale na rychlé a praktické pomoci v okamžiku, kdy se situace rozhoduje během několika vteřin. Nešlo o ambici vytvořit další složitý bezpečnostní systém. Cílem bylo navrhnout fyzický prvek, který bude v prostoru přítomen každý den, nebude rušit jeho běžný provoz, a přitom bude připravený na nezbytný zásah ve chvíli, kdy je potřeba okamžitě zajistit ochranu osob uvnitř místnosti.

Co je DefenBoard® a jak funguje?

DefenBoard je zakázkově vyráběná posuvná balistická ochrana určená k zabezpečení vstupu do místnosti v případě bezprostředního ohrožení. Zjednodušeně řečeno jde o masivní ochranný panel, který je zavěšen na kolejnicovém systému a pohybuje se před dveřním otvorem.

V klidovém režimu nepřekáží provozu a může plnit také praktickou funkci. V krizové situaci jej lze rychle posunout tak, aby vytvořil fyzickou bariéru mezi útočníkem a ohroženými osobami uvnitř místnosti. Princip zařízení je záměrně jednoduchý. Jeho aktivace nevyžaduje elektrické napájení, takže celý systém je použitelný i v situaci, kdy dojde k výpadku elektřiny nebo není čas řešit složitější ovládání.

Uživatel uchopí madlo, uvolní zajištění klidové polohy a plynule přesune panel do ochranné polohy, kde se automaticky aretuje. Celý princip je postavený na tom, aby zařízení dokázala aktivovat

jedna osoba. Právě tato jednoduchost je jednou z největších předností celého konceptu. V krizové situaci totiž nerozhoduje jen technická úroveň ochrany, ale i to, zda je zařízení srozumitelné a také okamžitě použitelné bez nutnosti speciálního zásahu či komplikovaného ovládání. DefenBoard vychází z logiky skutečného provozu budov, a ne z laboratorní představy o ideálních podmínkách.

Jedno řešení, které si lze snadno představit

DefenBoard není skrytý mechanismus uvnitř stavební konstrukce a nejsou to ani standardní bezpečnostní dveře. Je to viditelný panel, který je umístěn v interiéru vedle dveří, vedený po nosné kolejnici. V běžném provozu stojí stranou vstupu a působí jako běžný funkční prvek místnosti (např. jako nástěnka, nebo popisovací tabule). V případě ohrožení se posune před dveře a uzavře tak přístup do chráněného prostoru.

Vlajkový model pro standardní dveře o šířce zhruba 90 cm váží přibližně 180 kilogramů, ale díky konstrukci pojezdu a vyváženému řešení je manipulace s ním velmi snadná. To je důležitý detail: nejde jen o to, aby panel odolal střelbě, ale aby jej bylo možno v kritickém okamžiku skutečně rychle použít.

Právě spojení vysoké hmotnosti a lehkého ovládání je jednou z klíčových vlastností, které produktu dávají technickou věrohodnost. Čtenář si díky tomu může lépe představit, že nejde o symbolické opatření, ale o reálný fyzický prvek s konkrétní ochrannou funkcí.

Ochrana, která v prostoru nepůsobí cizí

Jedním z hlavních problémů bezpečnostních prvků ve veřejných budovách bývá to, že jsou často velmi nápadné, psychologicky zatěžující nebo komplikované pro každodenní provoz. Pokud má být ochrana dlouhodobě přijatelná, např. ve škole, kanceláři nebo jednacím místnosti, nesmí prostor proměnit v pevnost. Tady se DefenBoard odlišuje.

V klidovém stavu je panel umístěn mimo vstup a působí jako běžná součást interiéru. Může mít podobu whiteboardu, tabule pro křidu, korkové plochy, grafického panelu nebo jiného povrchu podle potřeb zákazníka. Smyslem není bezpečnost schovávat, ale integrovat ji do prostředí tak, aby byla jeho přirozenou součástí a nevyvolávala zbytečné napětí. To je pro veřejné budovy zásadní: bezpečnostní řešení má být funkční, ale současně nesmí narušovat běžné užívání objektu.

Právě tato filozofie dává produktu silný a současně nenásilný positioning. Nejde o snahu vystavovat ochranu na odív, ale o její chytré začlenění do prostoru. Bezpečnost zde nevstupuje do interiéru jako cizí těleso, ale jako užitečný prvek, který má svůj každodenní smysl i krizovou funkci.

Pro jaké objekty je řešení určeno?

Prvotní impulz k vývoji směřoval především do školního prostředí. Postupně se ale ukázalo, že podobné řešení dává smysl i v celé řadě dalších objektů. Veřejné budovy mají společné to, že se v nich pohybuje větší množství osob, provoz je proměnlivý a není vždy možné zajistit plnou kontrolu vstupu do všech částí objektu.

To se týká nejen škol a univerzit, ale také úřadů, nemocnic, kancelářských budov, konferenčních prostor nebo dalších míst, kde je potřeba umět v kritickém okamžiku rychle oddělit ohrožený prostor od vstupu. Smyslem není nahradit celkový bezpečnostní koncept budovy, ale doplnit jej o fyzický prvek, který pomůže v krizové chvíli získat cenný čas a zvýšit šanci osob uvnitř místnosti.

Balistická ochrana podle reálné potřeby

Vlajkový model produktu nabízí vysokou úroveň balistické ochrany ve třídě FB6. Právě tato varianta vznikla s ambicí vytvořit řešení, které nebude snadné překonat a které poskytne co nejvyšší možnou ochranu pro situace s vysokou mírou rizika.

Postupem času se ale ukázalo, že ne každý objekt potřebuje automaticky nejvyšší balistickou třídu. Proto vznikla i dostupnější varianta s nižší úrovní ochrany FB2, která může dávat smysl tam, kde je potřeba hledat rozumnou rovnováhu mezi mírou rizika, rozpočtem a praktickým využitím. Možnost nabídnout více úrovní ochrany podle konkrétní situace je z pohledu praxe velmi důležitá. Bezpečnost totiž není jen otázkou maximálního výkonu, ale také vhodného poměru mezi náklady, rizikem a použitelností.

Zakázkové řešení pro konkrétní prostory

Velkou předností systému je jeho variabilita. DefenBoard není omezen jedním

pevným formátem ani jedním typem prostoru. Každé řešení se přizpůsobuje konkrétnímu místu instalace, a to jak rozměrově, tak konstrukčně i vzhledově.

Zařízení lze navrhnout pro standardní dveřní otvor i pro širší vstupy, včetně větších dvoukřídlých dveří. Panel je veden po nosné kolejnici a je doplněn dozrak, aretací a bezpečnostními prvky tak, aby byl pohyb co nejlépe plynulý, kontrolovaný a spolehlivý.

Myslet i na provoz po instalaci

U bezpečnostních prvků se často mluví hlavně o okamžiku nasazení, ale neméně důležitý je jejich dlouhodobý provoz. Aby zařízení plnilo svou funkci i po letech, je potřeba myslet na jednoduchou údržbu, pravidelné kontroly a správné zaškolení obsluhy. Proto je důraz kladen nejen na samotnou instalaci, ale i na následný provozní režim. Zařízení má být udržováno ve stavu, kdy je jeho dráha volná, kolejnice čistá a celý mechanismus připravený k okamžitému použití. Stejně důležité je, aby obsluha rozuměla účelu zařízení, způsobu aktivace, bezpečné manipulaci i tomu, jak se má postupovat po jeho použití. Samotná technika bez správného provozního nastavení nikdy nemůže fungovat naplno.

Kdo za projektem stojí?

Za značkou Ballistic Defend s.r.o. stojí tým zakladatelů, kteří se znají z vysoké školy a spojili technické uvažování, zkušenosti z vývoje i osobní motivaci vytvořit praktické řešení pro ochranu měkkých cílů. Impulzem nebyl čistě obchodní nápad, ale velmi konkrétní společenská zkušenost a potřeba hledat řešení, které může v kritickém okamžiku skutečně pomoci.

Myšlenka produktu se zrodila z jednoduché otázky, zda lze vytvořit ochranný

prvek, který nebude v prostoru působit agresivně, ale v krizové situaci nabídne skutečný fyzický účinek. Následoval přibližně dvouletý vývoj, během kterého vznikl prototyp, technické řešení, způsob instalace i finální produkt připravený pro reálné nasazení. Důležité je, že od začátku nešlo jen o samotný panel, ale o celé funkční řešení pro konkrétní objekty a jejich každodenní provoz.

Právě v tom je síla projektu: nejde o efektní koncept pro prezentaci, ale o snahu vybudovat novou kategorii bezpečnostního prvku, který dává smysl technicky, provozně i psychologicky.

Proč může být DefenBoard zajímavý právě teď?

Bezpečnost veřejných budov dnes není téma, které by bylo možno odkládat na neurčito. Zároveň ale platí, že většina institucí hledá řešení, která budou realistická, provozně zvládnutelná a přijatelná i pro každodenní fungování objektu. DefenBoard vstupuje právě do tohoto prostoru. Nenabízí efektní technologii pro prezentaci, ale promyšlený fyzický prvek, který odpovídá na velmi konkrétní otázku – jak rychle vytvořit ochrannou bariéru před vstupem do místnosti, aniž by se z běžného prostoru stal permanentně stresující bezpečnostní režim.

Je to produkt, který stojí na jednoduché myšlence, ale řeší složitý problém. A právě v tom může být jeho největší přínos. V době, kdy se stále více diskutuje o připravenosti veřejných budov na mimořádné situace, může být podobný typ ochrany jedním z praktických kroků, jak zvýšit bezpečnost bez zásadního narušení běžného života uvnitř objektu.

Ing. Jiří Pondělíček
Ballistic Defend s.r.o.



Využití DefenBoard jako popisovací tabule.



Zablokování vstupu ve chvíli ochrany před útočníkem.

Rychlá fakta

Co to je	Posuvný balistický panel před dveře, který v běžném provozu slouží jako součást interiéru a v krizové situaci vytvoří ochrannou bariéru.
Princip	Panel je veden po kolejnici vedle dveřního otvoru a ručně se přesune do ochranné polohy.
Napájení	Ne. Základní řešení je čistě mechanické.
Ovládání	Lehký ruční posuv; zavření zvládne i tříleté dítě.
Hmotnost	U běžných dveří o šířce cca 90 cm přibližně 180 kg.
Balistické třídy	Varianta FB2 chrání proti střelbě z běžných ručních zbraní (např. pistole 9 mm), zatímco vyšší třída FB6 je navržena tak, aby odolala i střelbě z výkonných dlouhých zbraní, například útočných pušek.
Typické použití	Školy, úřady, nemocnice, kanceláře a další veřejné budovy.
Rozměry	Od standardních dveří až po širší a dvoukřídlé vstupy.

KAMEROVÉ SYSTÉMY A FYZICKÝ DOHLED VE ŠKOLÁCH

MINIMALIZACE HROZBY POTENCIÁLNÍCH ÚTOČNÍKŮ



Bezpečnost škol a školských zařízení je vymezena jako řízení bezpečnostních rizik, jehož cílem je snižování rizika kriminality a antisociálního chování prostřednictvím provázání technických, režimových a personálních opatření.

Tematická zpráva České školní inspekce přitom ukazuje, že školy využívají v praxi proti vniknutí a pohybu cizích osob jak technická, tak personální zabezpečení, přičemž v naprosté většině mateřských, základních a středních škol jsou zajištěna obě opatření současně. Současně platí, že ve všech druhích škol jsou v průměru častěji využívána personální zabezpečení než technická, a metodika k aplikaci ČSN 73 4400 výslovně uvádí, že by bylo chybou myslet si, že pouhá instalace technických prostředků vyřeší bezpečnost školy.

V širším odborném pohledu jsou kamerové bezpečnostní systémy současně popisovány jako nepsaný standard bezpečnosti a v kontextu tzv. AI Act jsou konfrontovány s novými výzvami. Postavení kamerových systémů v tomto rámci není okrajové.

Tematická zpráva České školní inspekce uvádí, že po zamčených dveřích se zvonek představují kamerové systémy druhé nejčastější technické opatření; instalovány byly ve 13,1 % mateřských škol, 30,8 % základních škol a 48,1 % středních škol. Zároveň bylo zjištěno, že velké mateřské školy mají častěji kamerové

systémy, velké základní školy využívají častěji nejen kamerové systémy, ale i elektronické karty nebo čipy a u mateřských a základních škol platí, že čím je obec větší, tím častěji jsou školy vybaveny kamerovými systémy, kódy a elektronickými kartami nebo čipy. Empirické zjištění z roku 2014 tak potvrzuje, že kamerový systém se v prostředí škol uplatňuje zejména jako součást moderních technických zabezpečení vstupu a pohybu osob.¹

Normativní a metodický rámec však kamery nepojímá jako samostatné řešení, nýbrž jako subsystém fyzické ochrany. ČSN 73 4400 řadí CCTV (closed-circuit television, uzavřený televizní okruh) sledovací systémy mezi prvky systému technické ochrany spolu s mechanickými zábrannými prostředky, poplachovým zabezpečovacím a tísňovým systémem, systémy kontroly vstupu a systémy přivolání pomoci. Cílem CCTV je snímání, přenos, zobrazování a dokumentace pohybu osob a dopravních prostředků, poskytování rychlé a spolehlivé obrazové informace pro zabezpečovací, bezpečnostní a monitorovací činnosti, záznam obrazových signálů pro zpětné vyhodnocování a dálkový dohled v případě nepřítomnosti osob v objektu. V tomtéž duchu metodika zdůrazňuje, že bezpečnost školy zahrnuje vedle požárního zabezpečení objektu zejména zabezpečení proti vniknutí cizí osoby, monitorování dění v objektu, kontrolu docházky žáků a režimových opatření, přičemž souhrn jednotlivých dílčích celků představuje ucelené řešení.

Ve vztahu ke vstupu do budovy a kontrole návštěv je provázání technického a personálního prvku zvláště zřetelné. ČSN 73 4400 doporučuje minimální počet vchodů do areálu školy a ideálně používání jednoho vchodu se zajištěnou kontrolou příchozích. Hlavní vchod do budovy školy má být vybaven systémem kontroly vstupu; mimo dobu ranního příchodu a odpoledního odchodu může škola zvolit ovládání vstupních dveří elektrickým zámekem dálkově ovládaným z recepce nebo z kanceláře, přičemž v případě nepřímého výhledu je nezbytné vybavení kamerovým systémem nebo videotelefonem. Zaměstnanci recepce či kanceláře ředitele mají mít dobrý výhled na přístupy ke vchodu do školy. Tematická zpráva ČŠI tento přístup podporuje doporučením, aby pro děti, žáky, studenty a veřejnost byl stanoven a využíván pouze jeden vchod, který je uzamčený a vstupy do něj jsou monitorovány a kontrolovány technicky, personálně, případně v kombinaci, a aby vpuštění cizích osob do prostor školy bylo zajištěno až po jejich identifikaci a ověření účelu vstupu do budovy. Z odborného pohledu současně platí, že vstupy, vjezdy, parkoviště, chodby a úniková schodiště představují místa, v nichž nejde jen o oprávněnost instalace kamer, ale i o schopnosti detekce.

Význam fyzického dohledu je v empirických datech i v doporučeních ještě výraznější než význam kamerového systému. Personální zabezpečení proti vniknutí a pohybu cizích osob je realizováno v největší míře pedagogickými a nepedagogickými pracovníky v průběhu dne ve škole a při vstupu do školy.

Tematická zpráva České školní inspekce současně navrhuje jako součást minimálního standardu bezpečnosti kontinuální dohled nad účastníky vzdělávání ve všech prostorách od vstupu do prostor školy po celý průběh výchovně vzdělávacího procesu i po jeho ukončení až po dobu opuštění budovy či areálu školy a vzájemnou zastupitelnost pedagogických či nepedagogických pracovníků vykonávajících dohled. Fyzický dohled tak nevstupuje jako doplněk techniky, ale jako minimum organizačně technického zajištění bezpečnosti.

Doporučení Úřadu pro ochranu osobních údajů č. 1/2025 však do této konstrukce vnáší podstatné upřesnění účelu a limitů kamerových systémů. Kamerové systémy jsou poměrně často nasazovaným prostředkem dohledu ve školách na všech stupních, avšak nasazení kamerového systému v prostorách škol může představovat zvláště citlivý zásah do práva na soukromí.

Úřad pro ochranu osobních údajů rozlišuje preventivní, reaktivní a důkazní funkci kamer a uvádí, že nejobvyklejší funkcí kamerových systémů je zajištění záznamu přítomnosti nebo jednání

**pedagogický
dohled
v průběhu dne**

81% základní školy

83,1% střední školy

**nepedagogický
dohled při vstupu**

78,9% základní školy

30,7% střední školy

**pedagogický
dohled při vstupu**

57,3% základní školy

osob, které může být využito k doložení a vyšetření určitých událostí. U mimořádných událostí typu fyzických útoků se naplnění odrazující funkce nejeví jako reálné, zejména pokud pachatelem budou osoby, které mají pravidelný oprávněný přístup do budovy; obecně pak platí, že kamery mohou reaktivní funkci naplnit jen velmi omezeně a namísto je zavést jiná opatření, která zamezí nebo ztíží postup pachatele.

Tím se doporučení Úřadu pro ochranu osobních údajů významně přibližuje jak metodice, podle níž technické prostředky nejsou jediným řešením, tak zjištěním České školní inspekce, podle nichž jsou ve školách častěji využívána personální zabezpečení než technická. Současně se připomíná, že kamery jako hlavní představitel tzv. invazivní techniky zůstávají ve školním prostředí spojeny s otázkami soukromí.

Prostorové vymezení kamer ve školách proto musí odpovídat zásadě potřebnosti a nejmenšího možného dopadu do soukromí. Úřad pro ochranu osobních údajů požaduje před nasazením kamerového systému provést balanční test a zvážit různé varianty řešení, a to jak varianty bez použití kamerového systému, tak varianty kombinující kamerový systém s jinými prostředky či opatřeními, například omezený počet kamer v kombinaci se vstupem na čipy nebo s dohledem ostrahy.

Z hlediska míry zásahu do soukromí doporučení rozlišuje kamery s malým zásahem do soukromí, typicky kamery monitorující perimetr pozemků a objektů nebo možná místa vniknutí do prostor školy v době, kdy se v záběru kamery nemá žádná osoba oprávněně vyskytovat, a kamery se středním zásahem do soukromí, mezi něž řadí kamery u vstupů do škol, šaten pro odložení svrchních oděvů, u vstupů do vybraných učeben nebo omezené záběry na křižení pochozích koridorů u rozsáhlých škol. Naopak kamery ve třídách v době vyučování, ve sborovnách, v kabinetech, kamery přenášející zvuk, kamery s využitím biometrického rozpoznávání obličejů a kamery ve sprchách a na toaletách představují řešení, u nichž bude pozitivní výsledek balančního testu velmi nepravděpodobný.



Příklad jednoho z možných víceúčelových řešení ve třídě: Whiteboard (vyráběný na míru), který může sloužit jako neprůstředná bariéra do dveří.⁷

V této souvislosti je významné, že doporučení Úřadu pro ochranu osobních údajů nepovažuje instalaci kamer za přiměřené řešení pro omezení šikany, protože je pravděpodobné, že šikana bude vytěsněna ze záběru kamer do jiných prostor nebo mimo objekty škol. Řešení negativních událostí, nevhodného chování nebo šikany je v dokumentu spojeno spíše s organizační, metodickou, poradenskou i materiální podporou, což je v souladu s důrazem metodiky a normy na režimová a organizační opatření, školení, nácvik postupů při mimořádných událostech a informování rodičů o zavedených opatřeních. Výsledný obraz tedy není obrazem školy jako monitorovaného prostoru, ale školy jako prostoru, v němž se technická ochrana, kontrola vstupu, režimová opatření a fyzický dohled musí vzájemně doplňovat.

Kamerové systémy mají ve školách opodstatnění především tam, kde podporují řízení vstupu, ochranu perimetru, dokumentaci mimořádných událostí a dálkový dohled nad vybranými rizikovými místy, nikoli tam, kde by nahrazovaly kontinuální dohled nad účastníky vzdělávání nebo plošné monitorovaly vnitřní život školy. Bezpečnost školy je založena na komplexnosti řešení identifikace rizik, na bezpečnostním režimu a organizaci, na kontrole vstupu a pohybu osob, na kontinuálním dohledu pedagogických a nepedagogických pracovníků a na technických prostředcích, které jsou významným pomocníkem, nikoli však jediným řešením.

PhDr. Milan Polívka
Vysoká škola AMBIS
bezpečnostní odbor
Ministerstva vnitra ČR

1. Bezpečnost ve školách a školských zařízeních: tematická zpráva. Česká školní inspekce. Praha, listopad 2014.
2. Bezpečnost školských zařízení, ČSN 73 4400 – aplikace a metodika (2. zkrácená verze). Praha, duben 2017.
3. Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci).
4. ČSN 73 4400 (734400) A Prevence kriminality – řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení, 2016. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.
5. Dle ČSN EN 62676-1-1 podřazeno pod pojem VSS = video-surveillance system, dohledový videosystém. Pojem VSS je používán masivně odbornou veřejností a jedná se o evoluční vývoj CCTV. Není ovšem vyloučeno, že svým charakterem je na některých školách provozován právě CCTV.
6. Doporučení Úřadu pro ochranu osobních údajů č. 1/2025 ke kamerovým systémům umístěným ve školách a školských zařízeních. <<https://uouu.gov.cz/novinky/vse/doporučení-uouu-c-12025-k-kamerovym-systemum-ve-skolach>>.
7. Multipurpose Defense System. HQH System. <<http://www.hqh.cz>>.

BEZPEČNOST HROMADNÝCH AKCÍ JAKO SYSTÉM

Kvalitní plán a připravený tým jsou základ. O skutečné bezpečnosti ale rozhoduje schopnost řídit akci v reálném čase a opřít se o správné nástroje.

Každá větší hromadná akce má svůj plán. Rozkreslené sektory, přístupové trasy, bezpečnostní opatření, počty personálu. V určité chvíli ale může přijít moment, kdy se realita začne od plánu odchylovat – dav se začne chovat jinak, než se očekávalo, změní se počasí, nastane mimořádná situace a urgentně se změní dynamika pohybu v prostoru.

V těchto chvílích se rychle ukazuje, že bezpečnost akce není dána pouze počtem nasazených pracovníků nebo fyzickými opatřeními. Rozhodující je schopnost situaci pochopit, vyhodnotit a řídit v reálném čase.

Právě zde se láme chleba a jednoznačně se ukazuje rozdíl mezi formálně „zajištěnou“ akcí a skutečně bezpečně zvládnutým provozem, který je schopen absorbovat i dramatické situace.

Bezpečnost není jen o „počtech security“

V praxi se často setkáváme s tím, že bezpečnost je vnímána primárně jako náklad – tlak na co nejnižší počty lidí i jejich cenu. Výsledkem pak bývá přístup, kdy „stačí někoho postavit na pozici“ a tím je věc vyřešena.

Mnohem méně se řeší, jestli je daný zaměstnanec security skutečně připravený zvládnout situace, které v reálném provozu nastávají.

Security pracovník dnes není jen fyzická přítomnost. Musí být schopný vyhodnotit situaci, komunikovat s návštěvníky, poskytnout první pomoc, podílet se na řízení pohybu osob a fungovat jako součást celého bezpečnostního systému.

Zároveň ale neplatí, že jde jen o jednotlivce. Bezpečnost hromadných akcí je dynamický proces, který ovlivňuje chování a složení davu, charakter akce i kvalita řízení.

Návštěvníci jsou navíc čím dál náročnější – očekávají komfort, citlivě vnímají bezpečnostní opatření a zároveň vyžadují vysokou kvalitu svého pocitového zážitku z akce. Tomu musí odpovídat i profesionalita bezpečnostního zajištění.

Bezpečnost tak nelze chápat jako statické rozmístění lidí „stejně jako loni“, ale jako proces, který je nutně aktivně při-

pravovat a řídit s ohledem na konkrétní akci.

Tři klíčové vrstvy eventového bezpečnostního systému

Naše zkušenosti z posledních 20 let zabezpečování hromadných akcí ukazují, že funkční bezpečnostní model stojí na třech vzájemně provázaných vrstvách:

1. Fyzická bezpečnost a operativa

Základem je vždy kvalitně postavená fyzická bezpečnost:

- zkušený management akce,
- jasná struktura řízení,
- dobře připravené a proškolené týmy,
- schopnost těchto týmů operativně reagovat na vývoj situace, jelikož se skoro vždy stane něco „mimo plán“.

V praxi to znamená nejen „obsadit pozice“, ale především zajistit, že každý člen týmu ví, co má dělat, a to adekvátně dané situaci, dále ví, komu je podřízen a jak eskalovat informace o dění z terénu.

2. Příprava a bezpečnostní dokumentace

Druhou a snad ještě více podceňovanou vrstvou je kvalitní přípravná fáze.

Bezpečnost hromadné akce nevzniká v den jejího konání, ale dlouho předtím. Klíčovou roli zde hraje:

- analýza ohroženosti,
- návrh bezpečnostních opatření,
- evakuační a požární plány,
- posouzení z pohledu ochrany měkkých cílů,
- nastavení procesů a postupů, které je potřeba nejen naplánovat, ale hlavně důsledně a uchopitelně distribuovat ke všem zapojeným subjektům a osobám (a že jich je opravdu mnoho).

Právě tato část rozhoduje o tom, zda je možné akci efektivně řídit, nebo zda se pouze reaguje na vzniklé problémy a doufá se ve štěstí.

Největší rizika obvykle nevznikají z nedostatku personálu, ale z nedostatečné přípravy a nejasně definovaných postupů.

ČECHY MEN.
Spolu teď a tady.

3. Řízení akce v reálném čase

Třetí vrstvou, která v posledních letech zásadně nabývá na významu, je samotné řízení akce v reálném čase.

U větších a složitějších akcí již není možné spoléhat pouze na vysíláčky, telefonní komunikaci a improvizaci. Klíčová je schopnost mít:

- přehled o rozmístění sil,
- aktuální a přesné informace z terénu,
- jasně definované role a odpovědnosti,
- možnost rychlé komunikace napříč strukturou.

V praxi se proto stále více využívají specializované nástroje pro řízení bezpečnostního provozu, které umožňují:

- pracovat s mapovými podklady,
- evidovat a řídit jednotlivé pozice,
- plánovat směny,
- zaznamenávat a vyhodnocovat incidenty,
- komunikovat v reálném čase s jednotlivými členy týmu.

Tyto nástroje zásadně zvyšují přehled, kontrolu a schopnost reakce, zejména u akcí s velkým počtem osob a složitou strukturou, což jsou již akce od zhruba 10 000 návštěvníků výše, a to u nás v republice není až tak neobvyklé realizovat hromadné akce s denní návštěvností atakující 80 000 návštěvníků.

Dav jako aktivní prvek bezpečnosti

Specifickým tématem, které v kontextu hromadných akcí nabývá stále většího významu, je samotný dav. Ten nelze vnímat pouze jako objekt řízení, ale naopak je nutné na něj nahlížet jako na aktivní prvek bezpečnostního prostředí.

Dav může v některých situacích prostředí stabilizovat a přirozeně tlumit rizikové jevy, jindy se naopak stává jejich zdrojem. Jeho chování je do určité míry ovlivnitelné, nikdy však plně kontrolovatelné.

Právě proto je klíčovou schopností s davem aktivně pracovat – zejména prostřednictvím kvalitní komunikace, a to jak před akcí – skrze sociální sítě, web, kontaktem s fanouškovskou základnou, tak v průběhu akce – díky in-

formačním displejům, značení, personálu, ale i skrze vystupující interprety. Jde hlavně o správné nastavení očekávání návštěvníků a čitelné uspořádání prostoru.

Bez pochopení těchto principů a bez schopnosti je aplikovat v praxi nelze bezpečnost hromadných akcí efektivně řídit.

Od „hlídání“ k řízení bezpečnosti

Bezpečnost hromadných akcí se za poslední dekádu dramaticky proměnila. Zjednodušeného modelu „fyzické ostrahy“ se posouváme k integrovanému přístupu, který stojí na kombinaci lidí, procesů, dat a technologií.

Zkušenosti ze zahraničí i z praxe ukazují, že role bezpečnostních týmů se rozšiřuje. Nejde už jen o kontrolu vstupů nebo řešení konfliktů, ale o aktivní práci s prostředím a návštěvníky. Bezpečnost dnes zahrnuje i oblast komfortu, prevence rizik, komunikace, spolupráce s dalšími složkami nebo schopnosti reagovat na široké spektrum situací – od zdravotních komplikací přes řízení davu až po řešení mimořádných událostí.

Současně roste důraz na koordinaci – mezi organizátorem, bezpečnostní službou, zdravotníky, policií i dalšími aktéry. Přibývá plánování, modelování scénářů, nácviků a práce s daty.

A právě to je na oboru eventové bezpečnosti zásadní.

Nejde jen o to dodat bezpečnostní personál. Jde o schopnost akci pochopit, připravit a řídit. Zásadní je kombinace zkušeností z praxe, odborného přístupu a značné ochoty spolupracovat.

Bezpečnost hromadných akcí je dnes komplexní, je náročná – ale zároveň mimořádně zajímavá a dynamická oblast, která se rychle posouvá kupředu po vzoru západních sousedů. A tento posun dává smysl – protože ve výsledku nejde o procesy ani technologie, ale o to, aby se lidé vraceli z akcí domů v pořádku.

Mgr. Otomar Sláma, Ph.D., MBA, MPA
člen správní rady ČECHY MEN a.s.

**DNES JIŽ NESTAČÍ
MÍT PERSONÁL
NA POZICÍCH
POSTAVIT PLOTY
A HLÍDAT VSTUPY
MÍT PLÁN NA PAPIŘE**

**JE POTŘEBA
AKTIVNĚ ŘÍDIT
JEHO NASAZENÍ
A REAKCE**

**PRŮBĚŽNĚ
PŘÍZPŮSOBOVAT
REŽIM UVNITŘ AREÁLU
PODLE CHOVÁNÍ DAVU**

**PROPOJIT PLÁN,
LIDI A ŘÍZENÍ
V JEDEN SYSTÉM**



MODERNÍ OCHRANA OBYVATELSTVA

Varovný signál sirény je pro mnoho lidí stále spíše symbolem nejistoty než jasné instrukce k jednání. V krizových situacích však rozhoduje nejen rychlost aktivace varování, ale také srozumitelnost sdělení, spolehlivost infrastruktury a schopnost pracovat s daty z reálného prostředí.

Společnost Colsys, s.r.o., proto přistupuje k ochraně obyvatelstva jako k inteligentnímu a odolnému ekosystému, který překračuje možnosti tradičních sirénových řešení.

Od sirény k integrovanému systému

Současná varovná infrastruktura již není pouze samostatným akustickým prvkem. Moderní přístup spočívá v propojení elektronických sirén, místních informačních systémů, řídicího softwaru a vizuálních komunikačních prvků do jedné technologické platformy. Ta umožňuje rychlé a přesné informování obyvatel podle konkrétní situace.

Klíčovou výhodou tohoto řešení je modularita. Systém lze propojit s různými monitorovacími a senzorickými prvky a přizpůsobit jej konkrétním rizikům obce, města nebo průmyslového areálu. Varování tak není pouze akustickým signálem, ale výsledkem práce s daty a jejich vyhodnocením v reálném čase.

Data z terénu jako základ včasného varování

Moderní informační systémy VoiceGuard od společnosti Colsys, s.r.o., mohou spolupracovat například s hladinoměry a srážkoměry, které při překročení kritických hodnot automaticky spustí varování před bleskovými povodněmi. Meteorologické sledující směr a rychlost větru zase pomáhají odhadnout šíření nebezpečných látek při průmyslových haváriích.

OD SIRÉNY K INTELIGENTNÍMU SYSTÉMU

pečných látek při průmyslových haváriích.

Součástí systému mohou být také senzory kvality ovzduší nebo detektory koncentrace škodlivin. Ty umožňují včas zachytit únik chemických látek a okamžitě informovat obyvatele například o nutnosti uzavřít okna nebo omezit pohyb v dané oblasti. Akustické varování lze navíc doplnit informačními tabulemi, které poskytují vizuální instrukce přímo v terénu.

Spojení zvukové, datové a vizuální komunikace představuje zásadní posun oproti tradičním systémům. Varování se tak stává součástí řízené komunikace, která pomáhá veřejnosti rychle porozumět situaci a správně reagovat.

Rychlá aktivace a jednoduché ovládání

Z pohledu krizového řízení je klíčová také operativnost systému. Řešení VoiceGuard umožňuje oprávněné osobě aktivovat varování pro celou obec nebo pouze pro vybranou lokalitu během několika sekund. Intuitivní ovládání snižuje nároky na obsluhu a usnadňuje správné rozhodování v situacích, kdy je nutno jednat rychle.

Tato vlastnost je zásadní zejména pro starosty, pracovníky krizového řízení nebo další odpovědné osoby. Lokalizované spuštění navíc umožňuje přesně cílit varování pouze tam, kde je skutečně potřeba.

Odolnost i při výpadku infrastruktury

Vedle rychlosti je pro kritickou infrastrukturu zásadní také její odolnost. Systém VoiceGuard je navržen tak, aby zůstal plně funkční minimálně 72 hodin i při kompletním výpadku elektrické energie. Díky záložním zdrojům a robustní architektuře si systém zachovává schopnost komunikace s obyvatelstvem i v situacích, kdy selhávají běžné komunikační sítě.

Varovná infrastruktura tak představuje stabilní pilíř bezpečnosti obce i v nejzávažnějších scénářích, jako jsou blackouty, povodně nebo průmyslové havárie.

Přínos i v běžném provozu obcí



Moderní informační a varovné systémy mají význam také mimo krizové situace. Obce a města je mohou využívat pro každodenní komunikaci s obyvateli – například při informování o dopravních omezeních, kulturních akcích, technických odstávkách a pro další důležité oznámení.

Varovný systém se tak stává zároveň efektivní komunikační platformou, která zvyšuje informovanost obyvatel a podporuje transparentní fungování samosprávy.

Strategický nástroj moderní samosprávy

Společnost Colsys, s.r.o., staví svá řešení na dlouholetých zkušenostech, důrazu na bezpečnost a propojení moderních technologií s provozní spolehlivostí. Varovné systémy tak dnes nepředstavují pouze technický doplněk, ale strategický nástroj, který pomáhá obcím a městům zajistit bezpečí jejich obyvatel.

Budoucnost ochrany obyvatelstva totiž neleží v izolovaných prvcích, ale v inteligentně propojených systémech schopných rychle reagovat na měnící se rizika.

Colsys, s.r.o. – inteligentní technologie a spolehlivost pro bezpečí vašich občanů.

Martin Vintr
obchodní manažer společnosti
Colsys, s.r.o.



KPKB
KOMORA
PODNIKŮ
KOMERČNÍ
BEZPEČNOSTI
ČESKÉ REPUBLIKY

Bezpečí pro vaše zaměstnance

balíček na podporu imunity

Kód **GSZAM20**, sleva 20 %
při nákupu nad 1000 Kč +
doprava zdarma.

Podpořte zdraví Vašich zaměstnanců
nákupem kvalitních doplňků stravy
a zdravotnických prostředků
značek GS a CEMIO.

Exkluzivní nabídka platí na celé portfolio
produktů na www.gsklub.cz.

Individuální kalkulace imunitních balíčků:
firemni.prodeje@gs.cz



www.gsklub.cz



GS
Účinnost
na prvním místě
cemio
switzerland


carprogram.cz

Kompletní řešení vozového parku pro bezpečnostní agentury

Snižte náklady. Zjednodušte správu.
Získejte kontrolu.

- ✓ Operativní leasing bez starostí
- ✓ Výhodné pořízení vozidel do majetku
- ✓ Flexibilní financování s nízkou splátkou



Speciální podmínky pro členy KPKB
Heslo: **KPKB2025**

www.carprogram.cz

731 419 475

obchod@carprogram.cz



KPKB
KOMORA
PODNIKŮ
BEZPEČNOSTI
ČESKÉ REPUBLIKY



KPKB
KOMORA
PODNIKŮ
KOMERČNÍ
BEZPEČNOSTI
ČESKÉ REPUBLIKY

INTEGROVANÉ ŘÍZENÍ DAVU

MODELOVÁNÍ, TAKTICKÉ SCÉNÁŘE A ANTIKONFLIKTNÍ KOMUNIKACE V PRAXI

V tomto článku představíme integrovaný model řízení davu jako multidisciplinární obor a prokážeme, že efektivní bezpečnost není stavem absence hrozeb, ale stavem připravenosti tyto hrozby zvládat.

Integrovaný model řízení davu je garantem bezpečnostních programů, specialistou v oblasti krizového vyjednávání, krizové komunikace, vězeňství a deeskalace. Jde o spolutvůrce projektu antikontfliktních týmů ve střední Evropě se specializací na řízení mimořádných událostí.

Změna paradigmatu v bezpečnosti hromadných akcí

Bezpečnost hromadných akcí představuje v posledních dvou desetiletích jednu z nejvýznamnějších a nejrychleji se vyvíjejících výzev v oblasti veřejné bezpečnosti a krizového řízení. S rostoucí mobilitou obyvatelstva, zvyšující se kapacitou stadionů a festivalových areálů a s proměnou sociopolitického klimatu se zvyšují i nároky na profesionální zvládnutí davových situací. Davové chování již nelze chápat jako nahodilý, chaotický fenomén, nýbrž jako komplexní jev, ovlivněný psychologickými, sociálními, prostorovými a environmentálními faktory.

Tradiční přístupy k řízení davu, které dominovaly ve 20. století, se často opíraly o represivní strategie (Show of Force), fyzické bariéry a předpoklad, že dav je ze své podstaty iracionální a nebezpečný. Tento pohled se však v moderní bezpečnostní vědě ukazuje jako překonaný a v mnoha případech kontraproduktivní, neboť často vede k tzv. self-fulfilling prophecy (sebenaplnujícímu se proroctví), kdy nepřátelský přístup policie vyvolá nepřátelskou reakci davu. Moderní Crowd Management se odklání od strategie „kontroly a represe“ směrem ke strategii „komunikace, facilitace a bezpečí“. Důraz je kladen na predikci rizik, participativní přístup a budování důvěry mezi bezpečnostními složkami a účastníky akce. Výzkumy i praxe jednoznačně prokazují, že kvalita a styl komunikace mezi organizátory, bezpečnostními složkami a účastníky zásadně determinují chování davu. Jak uvádějí Drury, Reicher a Stott (2020), způsob, jakým policie nebo ostraha interaguje se davem, může rozhodnout o tom, zda situace zůstane stabilní a kooperativní, nebo zda přeroste v odpor, násilí a eskalaci.

Cílem tohoto článku je představit integrovaný model řízení davu, který není jen teoretickým konstruktem, ale funkčním nástrojem ověřeným v praxi. Tento model stojí na třech pilířích – jsou to:

1. Modelování a simulace: Využití dat a algoritmů k predikci toku davu a identifikaci kritických míst (bottlenecks).

2. Taktické plánování: Flexibilní scénáře nasazení sil a prostředků, včetně moderních technologií.

3. Antikontfliktní komunikace: Psychologické působení přímo uvnitř davu prostřednictvím specializovaných týmů.

Text je hluboce ukotven v reálných zkušenostech autora, který se podílel na řízení davů v České republice i v zahraničí, a to v širokém spektru situací – od velkých sportovních událostí přes politické demonstrace až po krizové stavy při povodních či technoparty.

Specifickou pozornost věnuje autor extrémním případům, jako jsou organizované střety rizikových fanoušků (hooligans). V těchto scénářích je antikontfliktní komunikace aplikována takticky, nikoli jako náhrada síly, nýbrž jako prvek operující v synergii s připravenými zásahovými týmy, které tvoří nezbytné silové pozadí pro případ eskalace.

Teoretická východiska – od Le Bona k sociální identitě

Pro pochopení moderní taktiky je nezbytné vymezit se vůči zastaralým teoriím a adaptovat poznatky současné sociální psychologie a fyziky davu.

Překonání klasické teorie davu

Dlouhou dobu byla bezpečnostní praxe ovlivněna myšlenkami Gustava Le Bona (1895), který ve svém díle „Psychologie davu“ popisoval dav jako entitu, v níž jedinec ztrácí svou individualitu, racionalitu a morální zábrany, přičemž upadá do stavu primitivního barbarství (tzv. submergence). Tento „model šíleného davu“ vedl k bezpečnostní filosofii založené na strachu, masivních barikádách a nasazení těžkoobčů jako prevence chaosu. Současná věda však tento pohled odmítá. Dav není homogenní, iracionální masa. Je to strukturovaný sociální systém, který se řídí specifickými normami a pravidly, byť odlišnými od pravidel individuálního chování.

Elaborated Social Identity Model (ESIM)

Základním kamenem moderního přístupu je Elaborated Social Identity Model (ESIM), rozpracovaný autory jako Reicher, Drury a Stott. ESIM tvrdí, že chování davu je determinováno sdílenou sociální identitou členů skupiny. Tato identita není statická; dynamicky se mění v závislosti na interakci s „out-group“ skupinou, kterou v kontextu hromadných akcí nejčastěji představuje

policie nebo pořadatelská služba.

Klíčovým mechanismem je zde legitimita zásahu. Pokud účastníci vnímají postup bezpečnostních složek jako legitimní, spravedlivý a přiměřený, mají tendenci se sami regulovat (tzv. self-policing) a vyloučit ze svého středu agresivní jedince. Naopak, pokud policie zasáhne nerozlišujícím způsobem (např. použitím slzného plynu proti celému davu kvůli přestupku jednotlivce), dochází k radikalizaci. Pokojná většina se solidarizuje s agresivní menšinou, sjednocuje se pod společnou identitou „oběti policejní zvrůle“ a konflikt eskaluje. Antikontfliktní týmy (AKT) jsou v tomto modelu nástrojem, který pomáhá udržet vnímání legitimacy policie tím, že vysvětluje zákroky, diferencuje dav a komunikuje s ním jako s partnerem.

Fyzika davu a Crowd Science – kritické hustoty

Kromě psychologie je nutné zohlednit i fyzikální aspekty. Crowd Science, jak ji definuje G. K. Still (2014), propojuje matematiku, fyziku a bezpečnostní inženýrství. Zásadním parametrem je hustota davu (osoby/m²), která určuje míru rizika:

- **Do 2 os/m²:** Jedinci se pohybují svobodně, mají prostor pro rozhodování a únik.
- **Nad 4–5 os/m²:** Dochází k nedobrovolnému fyzickému kontaktu. Vznikají tzv. force chains (řetězce sil), kdy se tlak přenáší skrze těla účastníků jako mechanická síla.
- **Nad 6 os/m²:** Dav se začíná chovat jako tekutina (fluidní dynamika). Jedinec ztrácí kontrolu nad vlastním pohybem a je unášen proudem. Vznikají rázové vlny (shockwaves), které mohou způsobit hromadné pády, kompresní asfyxii (udušení tlakem hrudníku) a ušlapání. Moderní řízení davu musí tyto fyzikální limity respektovat. Komunikace je nástrojem regulace hustoty – včasná informace může dav zastavit nebo přeměrovat dříve, než dosáhne kritické hustoty, kdy je již jakákoli verbální intervence neúčinná.

Metodologický rámec a přístup

Tento článek není postaven na laboratorních experimentech, nýbrž na kvalitativní analýze a fenomenologii praxe. Metodologický rámec vychází z triangulace tří zdrojů – jsou to:

1. Analýza případových studií (Case Studies): Detailní rozbor incidentů (úspěšných i neúspěšných) s cílem identifikovat kauzální souvislosti a aplikovat metodu Lessons Learned.

2. Zúčastněné pozorování a longitudinální praxe: Reflexe více než dvacetiletého působení autora v přímém výkonu služby i v rámci koordinační pozice (celorepublikový a krajský koordinátor antikontfliktního týmu) při řízení mimořádných událostí.

3. Dokumentární analýza: Studium interních metodik, operačních plánů a After Action Reviews (AAR) z akcí jako Love Parade či CzechTek. Cílem je vytvořit konceptuální model, který překlene propast mezi akademickou teorií a „blátem na botách“ v terénu, a poskytnout praktický návod pro velitele a manažery bezpečnosti.

Modelování a simulace jako nástroj predikce rizik

V éře velkých dat (Big Data) a pokročilých výpočetních technologií se modelování pohybu davu stává nezbytnou součástí přípravné fáze každé velké akce. Nejde jen o to vědět, kolik lidí přijde, ale jak se budou chovat v čase a prostoru.

Typy modelů v praxi

V praxi se osvědčují tři úrovně modelování:

- 1. Makroskopické modely:** Sledují dav jako tok tekutiny v potrubí. Jsou ideální pro dimenzování vstupních bran a únikových východů a odpovídají na otázky kapacity toku (Flow Rate).
- 2. Mikroskopické (agentní) modely:** Simulují chování jednotlivců. Každý „agent“ v softwaru má své parametry (rychlost chůze, míra agresivity, znalost prostředí, stádní instinkt). Tyto modely ukazují interakce – např. co se stane, když se dva proudy lidí střetnou v úzkém koridoru.
- 3. Real-time simulace:** Využití dat z kamerových systémů, dronů a senzorů k okamžité predikci vývoje situace v horizontu 15–30 minut.

Aplikace – DNY NATO, hudební a sportovní arény

Při akci typu DNY NATO v Ostravě & Dny Vzdušných sil AČR, kterou navštěvují statisíce lidí, je modelování klíčové pro logistiku. Areál letiště Mošnov je rozsáhlý otevřený prostor, ale má limitovaný počet vstupů a příjezdových komunikací. Modelování nám umožňuje:

- Optimalizovat rozmístění kontrolních stanovišť (checkpoints), aby se netvořily nebezpečné fronty na přilehlých komunikacích.
- Simulovat scénář náhlé změny počasí (např. příchod bouřky), kdy se dav začne nekontrolovaně přesouvat do krytých prostor (hangárů) nebo k východům. Tento masový přesun mění dynamiku z „procházkové“ na „únikovou“.
- Plánovat evakuační trasy tak, aby nedocházelo ke křížení s příjezdem

složek IZS.

U **mistrovství světa v ledním hokeji** nebo koncertů v halách řeší simulace jiné výzvy: nárazové opuštění haly po skončení zápasu (egress) a následný nápor na MHD. Zde modely pomáhají nastavit tzv. zdržovací zóny a koridory, které dávají dav do metra či tramvají, aby nedošlo k přeplnění nástupišť.

Taktické scénáře a rozhodování v dynamickém prostředí

Data z modelů jsou cenná, ale v terénu rozhoduje taktika velitele. Taktické scénáře převádějí teoretická data do reálného rozmístění sil a prostředků.

Flexibilita a zónování

Statický plán na papíře málokdy přežije první kontakt s realitou. Moderní taktické plánování pracuje se systémem dynamických zón:

- Zelená zóna:** Bezpečný prostor, běžný režim, přítomnost preventivních hlídek.
- Žlutá zóna:** Indikátory napětí, nasazení antikontfliktních týmů, zvýšený monitoring, příprava záloh.
- Červená zóna:** Eskalace násilí, nasazení pořádkových jednotek (těžkoobčů), izolace agresorů, vytvoření sterilního prostoru.

Doprovody rizikových fanoušků („pochody“)

Specifickou disciplínou jsou doprovody fanoušků (Corteo). Tyto skupiny (Ultras) jsou často polovojenky organizované, používají pyrotechniku a aktivně vyhledávají střet s policií nebo soupeřem. Taktický scénář zde musí zahrnovat:

Profilování lídrů: Identifikaci tzv. capo (vůdce kotle), kteří dav řídí. S těmito osobami komunikují členové antikontfliktních týmů s cílem vytvořit komunikační most.

Taktiku „bubliny“: Policie nevytváří pevnou hradbu, ale „pohyblivou bublinu“, která se posouvá s davem. Cílem je oddělit rizikovou skupinu od okolí, ale zároveň jí umožnit pohyb směrem k cíli (stadionu).

Únikové ventily: Dav nesmí být zcela zablokovaný (pocit zahnání do kouta vyvolává agresivní typy „bojů, nebo uteč“). Musí existovat směr, kterým může dav „odtékat“, pokud nedochází k páchní trestné činnosti.

Při mistrovství světa v hokeji 2024 (např. rizikové zápasy Polsko vs. Česko) hrála roli i nacionalistická rivalita. Taktika se zde posunula od tvrdé represe k masivnímu nasazení preventivních hlídek ve „fanzónách“, které řešily drobné incidenty dříve, než se rozhořely v hromadnou bitku.

Role kontaktních pracovníků a antikontfliktních týmů (AKT)

Antikontfliktní týmy (v Německu Kom-

KRÁTKÝ ÚVOD (PEREX)

Správa a zajištění bezpečnosti masových akcí již dávno nestojí na pouhé demonstraci síly a stavění fyzických bariér. Moderní „crowd management“ představuje vysoce sofistikovanou multidisciplinární oblast, která propojuje fyziku davu, psychologii, datové modelování a umění deeskalace. Zajištění plynulého a bezpečného chodu akcí, od rizikových sportovních utkání po velké festivaly, sezonní akce, vyžaduje dokonalou součinnost organizátorů, státní policie a komerčních bezpečnostních agentur. Následující text detailně rozebírá, jak lze krizovým situacím v davu efektivně předcházet dříve, než přerostou v otevřený konflikt.

ANOTACE

Odborný článek představuje integrovaný model řízení davu (Crowd Management), který synergičtě spojuje moderní počítačové modelování toku osob, flexibilní taktické plánování a psychologicky ukotvenou antikontfliktní komunikaci. Autor kriticky reflektuje posun od historických represivních metod k moderním přístupům (ESIM) a tyto teoretické koncepty ilustruje na reálných případových studiích (tragédie na Love Parade, CzechTek, Dny NATO). Text zdůrazňuje klíčový význam preventivní práce s neformálními lídry davu, nutnost respektování fyzikálních limitů kritické hustoty osob a přináší vhled do využití nových technologií, jako jsou drony a umělá inteligence, při zajišťování veřejného pořádku.

O AUTOROVÍ

(autorská poznámka): Mgr. Štěpán Klen (Trivis Praha, PaK Team Katovice, ZRVI Třinec) je přední expert na řízení mimořádných událostí, krizové vyjednávání a deeskalaci napětí. Patří ke spolutvůrcům úspěšného konceptu antikontfliktních týmů ve střední Evropě. Svě bohatě, více než dvacetileté zkušenosti z terénu – získávané při zabezpečování nejrizikovějších hromadných akcí, demonstrací či sportovních utkání – přenáší do praktického výcviku a přípravy bezpečnostních profesionálů.

munikationsteams, v Polsku Zespól Antykonfliktowy) představují evoluční skok v policejní práci a jsou autorem dlouhodobě prosazovány jako standard. Jde o specializované policisty, kteří nenosí ochrannou výstroj (přilby, štíty), ale pouze reflexní vesty, a jejich jedinou „zbraní“ je komunikace a sociální inteligence.

Filosofie a psychologický účinek

Přítomnost AKT mění vnímání prostoru davem. Zatímco kordon „těžkooděnců“ signalizuje „očekáváme boj“, dvojice policistů v reflexních vestách signalizuje „jsme tu pro vaši bezpečnost“. Psychologický efekt spočívá v humanizaci policie (AKT dává policii tvář a hlas) a deanonimizaci davu (AKT oslovuje konkrétní jedince, čímž narušuje pocit anonymity, který usnadňuje páčání násilí). Je však důležité, aby AKT a řízení opatření vč. zasahujících úpolicistů měli stejné informace a kooperovali v průběhu celého opatření, vč. přípravy.

Metodika práce AKT – algoritmus zásahu

Práce AKT je strukturovaný proces, nikoli náhodná konverzace:

- 1. Monitoring a Sensing:** Tým prochází davem, naslouchá náladám, identifikuje osoby pod vlivem návykových látek a potenciální agresory.
- 2. Navázání kontaktu (Rapport):** Proaktivní oslovení lídrů v klidové fázi. Budování komunikačního kanálu pro případ krize.
- 3. Vysvětlování (Legal Notice):** Pokud policie chystá opatření (např. uzavření ulice), AKT to davu vysvětlí předem: „Dobrý den, za 100 metrů bude uzavěra z důvodu nálezu podezřelého předmětu, prosím, odbočte vpravo.“
- 4. Deeskalace:** V případě konfliktu se AKT snaží verbálně zklidnit situaci, oddělit sporné strany a nabídnout čestné východisko (face-saving exit), které umožní jedinci ustoupit „bez ztráty tváře“ před skupinou.

Zkušenosti ze zahraničí a implementace v ČR

Zatímco v Německu mají tyto týmy dlouhou tradici a vysokou autonomii, v České republice se jejich koncepce rodila postupně, často v reakci na selhání represivních zásahů (např. CzechTek 2005). Dnes jsou české AKT, na jejichž metodice a výcviku se autor podílel, považovány za jedny z neefektivnějších ve střední Evropě, s důrazem na taktickou přípravu a psychologii.

Případová studie: Love Parade Duisburg 2010 – selhání systému

Pro pochopení důležitosti integrovaného řízení je nutné analyzovat selhání. Tragédie na Love Parade v Duisburgu (24. července 2010) je mementem pro každého bezpečnostního manažera. Při

této akci zemřelo 21 lidí a přes 650 bylo zraněno.

Analýza příčin

Hlavní příčinou nebyla „masová panika“ v psychologickém smyslu, ale systémové selhání řízení toku davu.

Design prostoru: Jediný vstup i výstup vedl přes úzkou rampu a tunel. Kapacita areálu byla hrubě poddimenzována pro počet návštěvníků.

Turbulence davu: V místě střetu dvou proudů (vcházející a vycházející) došlo k překročení kritické hustoty (nad 8 osob/m²). Vznikly smrtící turbulence, lidé nemohli dýchat.

Komunikační kolaps: Policie neměla přehled o situaci uvnitř tunelu (chybějící kamery, výpadek radiostanic). Rozhodnutí uzavřít vstup přišlo pozdě a informace se k davu nedostala (chybějící ozvučení), což zvýšilo tlak na bariéry.

Poučení pro praxi

Love Parade ukázala, že fyzika davu je neúprosná – pokud hustota překročí mez, komunikace již nepomůže, nutné je stavební řešení. Dále potvrdila, že absence kontaktních pracovníků v kritickém bodě (rampa) znemožnila včasnou detekci problému. Velitelé musí mít informace z místa i obraz z kamer a modelů v reálném čase, nikoli zpožděný.

Případová studie: CzechTek 2006-2007 – změna přístupu

Opakem Duisburgu je vývoj přístupu k technoparty CzechTek v ČR.

Kontext

V roce 2005 došlo k masivnímu represivnímu zásahu policie proti účastníkům CzechTeku, což vedlo k politické krizi, zraněním a ztrátě důvěry veřejnosti. Tento přístup „nulové tolerance“ se ukázal jako neudržitelný a kontraproduktivní.

Nová strategie a role autora

V následujících letech (2006–2007) došlo ke změně taktiky, na které se autor podílel. Místo těžkooděnců nastoupili vyjednavací a antikonfliktní týmy.

Legitimita: Policie komunikovala s organizátory předem. Byly stanoveny jasné podmínky (odpad, hluk, průjezdnost pro sanitky).

Kooperace: Účastníci, kteří viděli, že policie neutočí, ale pomáhá řídit dopravu, umožňuje ověření přítomnosti alkoholu před jízdou a řeší jen skutečné excesy, začali spolupracovat a sami regulovali problémové jedince uvnitř komunity.

Výsledek: Akce proběhly bez masivního násilí. Tento případ potvrdil platnost modelu ESIM – změna přístupu policie změnila identitu a chování davu z „odbojného“ na „partyzánský“, ale „kooperativní“.

Profilace skupin a práce s lídry

Efektivní crowd management začíná dávno před otevřením bran. Zpravodaj-

ská činnost a profilace jsou nezbytné.

Identifikace rizikových skupin

Před akcí typu DNY NATO nebo rizikový fotbal se provádí analýza: Kdo přijede? (Demografie, historie násilí.) Jak přijedou? (Vlakem = možnost doprovodu a izolace; auty = rozptýlení.) Jaké jsou jejich motivace? (Politický protest, sportovní rivalita, zábava.)

Práce s neformálními autoritami

Každý dav má strukturu. I ve zdánlivém chaosu existují influenceři. U fotbalových chuligánů jsou to lídři gangů, u demonstrací svolavatelé. Taktika spočívá v navázání kontaktu s těmito lídry („Víme o vás, respektujeme vaše právo na fandění/protest, ale toto jsou hranice.“) Pokud lídr zavelí k ústupu nebo klidu, dav poslechne s mnohem větší pravděpodobností, než když to nařídí policista v megafonu.

Dynamika davu v přímém ohrožení života – analýza reakce na aktivního útočnicka

Zatímco většina modelů řízení davu (Crowd Management) pracuje s riziky, jako je přetlak, turbulence či agresivita skupin, specifickou kategorií představuje chování davu pod přímou palbou (Active Shooter Event). Zkušenosti z incidentů v České republice ukazují, že reakce davu je v těchto situacích často kontraintuitivní a standardní evakuační postupy mohou vést k eskalaci počtu obětí.

Paradox „zpětného vpuštění“ a vizuální stresory (Kazuistika FN Ostrava)

Analýza útoku ve Fakultní nemocnici Ostrava (2019) odhalila kritický fenomén v řízení toku osob. V prvotní fázi incidentu docházelo k živelnému opouštění objektu, kdy byly vypouštěny skupiny po 60–80 osobách. Následně však došlo vlivem nevhodného rozhodnutí k situaci, kdy byl dav čítající cca 300–400 osob vpuštěn zpět do vestibulu nemocnice. Tento prostor se stal v terminologii Crowd Science tzv. pastí (trap).

Dav neměl informaci o poloze střelce (který se mohl nacházet přímo v tomto davu nebo ve vestibulu). Situaci kriticky zhoršila aktivace taktického týmu Policie ČR. Tým v plné výzbroji, který dynamicky postupoval (běžel) podél vestibulu směrem k místu zásahu, působil na civilisty jako silný vizuální stresor. Dav, který neměl verbální kontext („Policie, zůstaňte stát!“), vyhodnotil prudký pohyb ozbrojenců jako bezprostřední ohrožení, což vyvolalo druhotnou vlnu reakcí a hrozil nekontrolovaný pohyb uvnitř uzavřeného sektoru.

Z hlediska řízení davu se ukazuje, že vizuální kontakt se zasahující složkou bez komunikačního doprovodu vede k destabilizačnímu davu.

Evakuace do zóny ohrožení (Kazuistika FF UK Praha)

Případ střelby na Filozofické fakultě UK (2023) demonstuje riziko aplikace standardních evakuačních modelů (požární poplach) na situaci aktivního střelce. Spuštění evakuace vedlo k vytlačení davu studentů a pedagogů z relativně bezpečných učeben na otevřené prostranství náměstí Jana Palacha. Pachatel, který se přesunul na ochoz budovy, tak získal taktickou výhodu a možnost vést palbu do shromážděného davu. Z hlediska dynamiky davu zde došlo k vytvoření tzv. Target Rich Environment (prostředí bohatého na cíle) přímo vlivem bezpečnostního opatření. Tento incident potvrzuje nutnost přehodnocení strategie směrem k invakuci (ukrytí) a nutnost autonomního rozhodování lídrů skupin (pedagogů) na základě aktuální polohy hrozby, nikoli centrálního signálu.

Útočník v davu a specifika zákroku (Mall Scenario)

Specifickou výzvou pro Crowd Management je přítomnost útočnicka v hustém davu (např. obchodní centrum, vánoční trhy). V takovém prostředí dav funguje jako „živý štít“.

Maskování a splynutí: Pachatel může využít chaosu k tomu, aby skryl zbraň a splynul s prchajícím proudem osob.

Taktika zásahu: Policie zde nemůže vést střelbu na větší vzdálenost z důvodu rizika zasažení neúčastných (Collateral Damage). Zárok vyžaduje specifické metody – extrémní zkrácení vzdálenosti (kontaktní střelba), využití neletálních prostředků k izolaci pachatele nebo řízený odklon davu (vytvoření koridoru), který pachateli odebere krytí.

Psychologie davu: Dav v těchto situacích reaguje jako kapalina – přelévá se od zdroje hluku. Pokud je úniková cesta zablokována, vznikají smrtící turbulence a rázové vlny (Shockwaves), které mohou způsobit více zranění ušlapáním než samotná střelba.

Specifika sezonních a masových akcí

Kromě standardních scénářů existují specifická rizika u akcí s unikátní dynamikou:

Vánoční trhy: Přítomnost zimního oblečení umožňuje skryté nošení i dlouhých zbraní. Konzumace alkoholu a hluk snižují situační povědomí davu. Zde nelze aplikovat invakuci (otevřený prostor), ale strategii „rozptýlení a krytí“.

Průvody (např. Parada Smoków v Krakově): Použití pyrotechniky maskuje střelbu. Dav, který slyší výbuchy, nereaguje útekem, protože zvuky považuje za součást show. To dává útočnickovi časovou výhodu (selhání ve fázi OODA Loop – Orientace).

Motorkářské srazy: Extrémní hluková zátěž znemožňuje verbální komunikaci a varování. Specifická subkultura vyža-

duje odlišný přístup AKT (respektování hierarchie klubů).

Nové technologie v řízení davu – drona a AI

Moderní řízení davu v letech 2024–2026 stále více spoléhá na technologie, které doplňují lidský faktor.

1. Drony (UAV): Poskytují veliteli „boží oko“ (God's Eye View). Umožňují monitorovat hustotu davu v reálném čase, kontrolovat perimetr a v případě DNÚ NATO i monitorovat dopravní situaci v širším okolí. Moderní tethered (upoutané) drony mohou viset nad davem hodiny a poskytovat kontinuální obraz.

2. Umělá inteligence (AI): Kamerové systémy vybavené AI dokáží detekovat anomálie v chování davu (např. náhlý rychlý pohyb, pád osoby, shlukování do kruhu signalizující bitku) a automaticky upozornit operátora dříve, než incident eskaluje. AI modely rovněž pomáhají v reálném čase spočítat hustotu davu a predikovat vznik bottlenecků.

Doporučení pro bezpečnostní manažery

- Predikce:** Modelování je nutností, nikoli luxusem. Investujte do analýzy dat před akcí.
- Komunikace:** Je nejdůležitější a nejučinnější zbraň v arzenálu bezpečnosti. Informovaný dav je dav pod kontrolou. Při plánování a řešení opatření je důležité zapojit i média, které mohou podpořit legitimitu, informovat veřejnost, sympatizanty a má to mnoho dalších pozitivních vlivů.
- Specifické situace:** Empirická zjištění z Ostravy a Prahy potvrzují, že nekontrolovaná evakuace může být pro měkké cíle fatálnější než samotný útok uvnitř budovy.
- Deeskalace:** Antikonfliktní týmy jsou mostem mezi represí a prevencí. Jejich nasazení by mělo být standardem u všech akcí nad 5 000 účastníků.

Shrnutí

Zkušenosti z akcí jako DNY NATO či MS v hokeji ukazují, že česká škola crowd managementu, která kombinuje západní modelování s pragmatickou taktikou a důrazem na komunikaci, je na světové úrovni a může sloužit jako inspirace pro zahraniční partnery.

Mgr. Štěpán Klen

Trivis Praha,

PaK Team Katovice, ZRIVI Třinec

Seznam zkratk a symbolů

AI – Artificial Intelligence (umělá inteligence)

AKT – Antikonfliktní tým

ESIM – Elaborated Social Identity Model

IZS – Integrovaný záchranný systém

MHD – Městská hromadná doprava

NATO – North Atlantic Treaty Organization (Severoatlantická aliance)

OODA – Observe-Orient-Decide-Act (rozhodovací smyčka)

PČR – Policie České republiky

UAV – Unmanned Aerial Vehicle (bezpilotní letoun / dron)

Použitá literatura

Bayerisches Staatsministerium des Innern. (2017). Konzept Kommunikationsteams (KTeams) der Polizei Bayern. München: StMl.

Drury, J., Reicher, S., & Stott, C. (2020). The psychology of crowd safety. *Policing*, 14(3), 566–579.

Helbing, D., & Johansson, A. (2013). Pedestrian, crowd and evacuation dynamics. In *Encyclopedia of Complexity and Systems Science* (pp. 6476–6495). Springer.

Klöpffel, H. (2013). The Love Parade Disaster – Causes and Consequences. In *Pedestrian and Evacuation Dynamics 2012* (pp. 265–274). Springer.

Klen, Š. (2006). Antikonfliktní týmy – metodika, postupy, nasazení. Ostrava: Interní dokument Policie České republiky.

Klen, Š. (2023). PREDES: Preventivní desatero doporučení pro zaměstnance nemocničních zařízení. Brno: NCO NZO; Evropský sociální fond.

Koryčanský, M. (2011). Antikonfliktní tým Policie České republiky. Praha: Ministerstvo vnitra ČR.

Koryčanský, M., & kol. (2014). Antikonfliktní tým: Metodika a praxe. Praha: MVČR.

Le Bon, G. (1895). *The Crowd: A Study of the Popular Mind*. London: T. Fisher Unwin.

Polizei Nordrhein-Westfalen. (2015). *Handbuch Kommunikationsteams NRW*. Düsseldorf: Ministerium des Innern NRW.

Remke, S. (2009). Chování davu, násilí a prevence: Psychologické aspekty práce s rizikovými skupinami. Příspěvek prezentovaný na odborné diskusi Fußballfans statt Grobiane!, Leipzig.

Still, G. K. (2014). *Introduction to Crowd Science*. CRC Press.

REVOLUČNÍ BEZPEČNOSTNÍ SKENERY R&S®QPS

NOVÁ ÚROVEŇ EFEKTIVITY A SOUKROMÍ

Společnost Rohde & Schwarz, lídr v oblasti testovacích a měřících technologií, představuje bezpečnostní skenery R&S®QPS, které nastavují nové standardy v detekci skrytých hrozeb a zvyšují bezpečnost v kritických oblastech. Tyto špičkové skenery využívají inovativní technologii milimetrových vln a kombinují tak vysokou efektivitu s maximálním respektem k soukromí skenovaných osob.

Technologie milimetrových vln – budoucnost bezpečnosti

Bezpečnostní skenery R&S®QPS jsou založeny na revoluční technologii milimetrových vln, která umožňuje detekovat předměty skryté na těle bez ohledu na materiál nebo velikost. Na rozdíl od tradičních metod screeningů, které mohou být časově náročné a invazivní, R&S®QPS využívají neinvazivní milimetrové vlny s extrémně nízkým výkonem k bezpečné a spolehlivé identifikaci potenciálních hrozeb.

„Bezpečnost je dnes komplexnější než kdy dříve. Naše skenery R&S®QPS nabízejí bezkonkurenční kombinaci přesnosti, rychlosti a respektu k soukromí, čímž umožňují bezpečnostním týmům efektivně chránit kritickou infrastrukturu a veřejnost,“ říká Petra Trojanová z Rohde & Schwarz – Praha, s.r.o.

Klíčové výhody skenerů R&S®QPS:

- Vysoká detekční spolehlivost: Detekce předmětů skrytých na těle bez ohledu na materiál nebo velikost.
- Zachování soukromí: Zobrazení alarmů na genderově neutrálním avatru, čímž je zajištěno maximální soukromí skenovaných osob.
- Inteligentní detekce: Využití algoritmů umělé inteligence (AI) umožňuje stálé zlepšování a adaptaci na nové hrozby.
- Efektivita a úspora nákladů: Snížení potřeby personálu a nízké náklady na údržbu díky robustní konstrukci a absenci pohyblivých částí.
- Dva modely pro různé potřeby: QPS201 i QPS Walk2000 nabízejí přesný a efektivní screening.



Spolehlivá ochrana kritické infrastruktury

Bezpečnostní skenery R&S®QPS jsou ideálním řešením pro zabezpečení letišť, nádraží, sportovních stadionů, vládních budov a dalších kritických míst. Skenery výrazně snižují riziko ohrožení a poskytují bezpečnostním týmům cenný nástroj pro efektivní řešení bezpečnostních výzev.

Chraňte budoucnost s Rohde & Schwarz

Rohde & Schwarz se zavázal k inovacím v oblasti bezpečnosti. Spojte se s námi ještě dnes a zjistěte, jak mohou bezpečnostní skenery R&S®QPS zlepšit bezpečnost ve vaší organizaci.

Kontakt:

Petra Trojanová
Tel.: +420 606 757 226
petra.trojanova@rohde-schwarz.com



ROHDE & SCHWARZ ARDRONIS

EFEKTIVNÍ OCHRANA PROTI ROSTOUCÍ HROZBĚ DRONŮ

Společnost Rohde & Schwarz, lídr v oblasti testovacích, měřících a zabezpečovacích řešení, uvádí systém R&S®ARDRONIS, komplexní systém pro detekci, lokalizaci a rušení radiovým signálem řízených dronů. Tato moderní platforma poskytuje organizacím a agenturám spolehlivé a efektivní antidronové řešení pro ochranu kritické infrastruktury a veřejné bezpečnosti.

Rostoucí hrozba vyžaduje proaktivní obranu

Pronikání nekooperativních dronů do bezpečnostně citlivých oblastí představuje stále větší riziko. Narušení kritické infrastruktury, ohrožení bezpečnosti letišť nebo potenciální zneužití pro nezákonné aktivity vyžadují účinná antidronová opatření. Rychlá reakce je klíčová pro minimalizaci hrozby – každá sekunda se počítá.

„ARDRONIS je rodina antidronových řešení od Rohde & Schwarz. Tato komplexní platforma poskytuje zákazníkům možnost detekovat – identifikovat – lokalizovat – sledovat – ověřit – neutralizovat nekooperativní hrozby v souladu s požadavky koncového uživatele,“ vysvětluje Petr Kotyza z Rohde & Schwarz – Praha, s.r.o.

R&S®ARDRONIS: Komplexní řešení pro ochranu proti dronům

R&S®ARDRONIS kombinuje pokročilé technologie a sofistikovaný systémový přístup k efektivní ochraně proti dronům. Systém dokáže:

- Detekovat a lokalizovat: Spolehlivě detekovat radiové komunikační spojení mezi dronem a pilotem a přesně určit jejich polohu.
- Klasifikovat a identifikovat: Automaticky klasifikovat typ dronu.
- Rušit spojení: Přerušit radiové spojení dronu, a tím zabránit možnosti dron ovládat.
- Přizpůsobit se specifickým potřebám: Modulární systém umožňuje konfiguraci řešení dle individuálních požadavků a scénářů použití.

R&S ARDRONIS Včasná neutralizace dronů



Pokrytí širokého spektra dronových technologií

R&S®ARDRONIS efektivně chrání proti dronům využívajícím různé komunikační technologie – např.:

- FHSS (Frequency Hopping Spread Spectrum): Nejběžnější technologie používaná pro ovládání komerčních dronů.
- Wi-Fi: Další často využívaná technologie pro ovládání dronů.
- Downlink signály: Různé druhy radiových signálů používaných pro přenos videa a telemetrie.
- RemotID: Technologie používaná pro přenos identifikačních dat

Komu je R&S®ARDRONIS určeno?

R&S®ARDRONIS je ideálním řešením pro:

- Letiště a letištní personál: Zabezpečení letového provozu a ochrana proti neautorizovaným dronům.
- Bezpečnostní agentury a orgány: Zajištění bezpečnosti kritické infrastruktury a veřejných akcí.
- Armádu a bezpečnostní složky: Ochrana personálu a citlivých objektů.
- Průmyslové a komerční organizace: Zajištění bezpečnosti firemního majetku a ochrana před průmyslovou špiónáží.

Investujte do své bezpečnosti s R&S®ARDRONIS

Rohde & Schwarz nabízí komplexní podporu a odborné poradenství při implementaci a provozu R&S®ARDRONIS. Spojte se s námi ještě dnes a zjistěte, jak můžete posílit svou ochranu proti rostoucí hrozbě nekooperativních dronů.

Kontakt:

Petr Kotyza
Tel.: +420 605 878 429
petr.kotyza@rohde-schwarz.com

Zuzana Lichá

Sales Assistant & Marketing
Test & Measurement

ROHDE & SCHWARZ
Make ideas real



O společnosti Rohde & Schwarz:

Rohde & Schwarz je mezinárodní společnost, která vyvíjí, vyrábí a prodává komplexní řešení pro testování, měření a zabezpečení. S více než 80 lety zkušeností je Rohde & Schwarz uznávána jako lídr v oboru, poskytující inovativní technologie pro širokou škálu aplikací.

Rohde & Schwarz má za sebou dlouhou tradici technologických průkopnictví, která začala s jeho zakladateli – Dr. Lotharem Rohdeem a Dr. Hermannem Schwarzem. Společnost se i dnes zaměřuje na vývoj špičkových technologií v oblastech jako 6G, AI, milimetrové vlny a kvantové technologie.

Působí ve více než 70 zemích a klíčovou výhodou je vysoká míra vertikální integrace – většina produktů a klíčových komponent je vyvíjena a vyráběna interně v Německu. To zajišťuje vysokou kvalitu, flexibilitu a nezávislost na dodavatelích.

Díky globální působnosti, blízkosti zákazníkům a silné vertikální integraci je Rohde & Schwarz spolehlivým a důvěryhodným partnerem pro bezpečnější a propojenější svět.

OCHRANA MĚKKÝCH CÍLŮ PŘED ÚTOKY UAV INTEGROVANÝ MODEL BEZPEČNOSTI V ĚŘE AUTONOMNÍCH HROZEB

Rozvoj UAV¹ zásadním způsobem redefinuje bezpečnostní prostředí současnosti. Zatímco původně byly tyto technologie doménou vojenských aplikací, jejich masová dostupnost, nízká cena a technologická vyspělost vedly k jejich rychlému rozšíření i v civilním sektoru. Tento trend však zároveň významně zvyšuje riziko jejich zneužití, a to včetně útoků na tzv. měkké cíle.

Měkké cíle jsou charakteristické vysokou koncentrací osob a omezenými možnostmi restriktivních bezpečnostních opatření. Právě tato kombinace z nich činí cíle pro asymetrické útoky.

Regulační rámec v České republice, založený především na evropských nařízeních a národních legislativě v oblasti civilního letectví, sice omezuje běžný provoz UAV, avšak nedokáže plně eliminovat rizika jejich úmyslného zneužití. Ochrana proti těmto hrozbám proto musí být postavena na komplexním a adaptivním přístupu.

Charakteristika hrozby – od jednotlivých UAV k autonomním platformám

Z hlediska bezpečnostní analýzy UAV nelze chápat izolovaně, ale jako součást širších systémů UAS²), které zahrnují platformu, řídicí prvky, komunikační kanály a případně i autonomní rozhodovací schopnosti.

Kritickými faktory ovlivňujícími míru hrozby jsou především hmotnost a kinetická energie. Dále schopnost nést náklad, úroveň nezávislosti pohybu, ovladatelnosti a stability letu a také pravděpodobnost úmyslného zneužití. Tyto parametry určují nejen potenciální destruktivní účinek, ale i obtížnost detekce a schopnost reakce pod časovou záteží frických momentů³).

Stěžejní kvalitativní změnu představují samostatné jednotky, zejména roje mikrodronů řízené AI. Tyto roje fungují na principu distribuované inteligence, kdy jednotlivé jednotky spolupracují, sdílejí informace a adaptují své chování dle aktuálních potřeb v reálném čase. Absence centrálního řídicího bodu výrazně zvyšuje jejich odolnost vůči omezené množině možných protiopatření.

Roje mohou simultánně provádět průzkum, rušení i přímé útoky v několika vlnách, čímž dochází k zahlcení obranných kapacit a zvýšení pravděpodobnosti úspěšného zásahu.

Rozvoj AI v oblasti bojových dronů

Rozvoj AI v oblasti bojových dronů jim umožňuje vyšší míru autonomie, včetně schopnosti samostatně navigace, rozhodování a rozpoznávání cílů bez přímého zásahu operátora. Pokročilé algoritmy dronům zároveň umožňují koordinaci ve skupinách rojů, sdílení dat v reálném čase a adaptivní reakci na měnící se podmínky. Primárním vstupem pro AI jsou data o parametrech letu, rychlosti, trajektorii či manévrování. Významným zdrojem jsou rozsáhlé datové soubory získané z tisíců nasazení dronů v konfliktu na Ukrajině, které slouží k trénování a optimalizaci algoritmů umělé inteligence pro vojenské aplikace. Tento trend významně zvyšuje efektivitu i komplexitu hrozeb a současně klade nové nároky na obranné a regulační mechanismy.

Vrstvená ochrana jako ucelené řešení

Na tuto komplexitu reaguje koncept vícevrstvé ochrany, který kombinuje několik navzájemně a vzájemně propojených úrovní zabezpečení. Tento přístup vychází z předpokladu, že absolutní ochrana neexistuje, a proto je nutné pracovat s minimalizací rizik a dopadů.

První vrstvou je prevence, zaměřená na omezení příležitosti k útoku a snížení jeho atraktivitu. Následuje detekce, která využívá multisenzorové přístupy kombinující radarové, akustické, optické a radiofrekvenční technologie. Stále větší význam zde získává využití umělé inteligence pro analýzu signatur a rozpoznávání vzorců chování, včetně klamných útoků ve zlomcích sekund.

Další vrstvou je reakce, která zahrnuje jak technologická protiopatření, tak organizační procesy a rozhodovací mechanismy. Poslední vrstvou je resilience, tedy schopnost absorbovat dopady útoku, přizpůsobit se mu a rychle se zotavit, aniž by došlo k fatální ztrátě jeho funkce.

Taktická úroveň – řízení rizik v konkrétním prostoru

Na taktické úrovni je klíčové zaměření na konkrétní lokalitu, objekt nebo událost. Ochrana zde začíná analýzou zranitelnosti, která identifikuje kritické body, jako jsou vstupy, energetické uzly nebo místa s vysokou koncentrací osob. Vítězství spočívá v předvídání a přípravě.⁴)

Významnou roli hraje prostorové uspořádání, které může buď zvyšovat, nebo snižovat dopady incidentu.

Rozptyl osob a funkcí, eliminace úzkých hrdel a existence alternativních tras významně snižují dopady případného incidentu.

Detekční činnosti musí být doplněny o jasně definované postupy pro vyhodnocení situace. Schopnost rozlišit mezi běžným a podezřelým chováním je zásadní v prostředí s vysokou hustotou civilního provozu.

Připravenost personálu je rozhodující. Výcvik by měl být zaměřen na zvládnutí kritických stavů, nikoli na technické detaily obrany proti UAV. Jednoduché a srozumitelné postupy mají v praxi vyšší efektivitu než komplexní scénáře, hlavně v zátežových situacích.⁵)

Operační úroveň – koordinace, komunikace a odolnost

Na operační úrovni se ochrana proti UAV stává otázkou koordinace mezi různými aktéry. Sdílení informací, vytvoření společného situačního obrazu a rychlá eskalace informací mezi úrovněmi řízení jsou určujícími aspekty.

Fundamentální význam má krizová komunikace. Nedostatečná nebo nesprávně načasovaná může vést k panice, která sama o sobě představuje významné riziko. Zkušenosti ukazují, že sekundární dopady, jako jsou hysterie, zranění při evakuaci nebo kolaps provozu, mohou být závažnější než samotný útok. Odolnost společnosti zahrnuje nejen technické a organizační aspekty, ale i psychologickou připravenost obyvatelstva; schopnost zachovat klid a důvěru v instituce je klíčovým faktorem pro zvládnutí mezních situací.

Spektrum scénářů a jejich strukturální dopady

UAV mohou být využity v celé řadě scénářů, od průzkumných operací přes demonstrativní narušení až po přímé útoky nebo koordinované operace. Každý z těchto scénářů má specifické charakteristiky, avšak všechny sdílejí schopnost ovlivnit nejen fyzickou bezpečnost, ale i fungování společnosti.

Útoky na měkké cíle a infrastrukturu mohou vyvolat dominový efekt, který vede k narušení fungování základních prvků kritické infrastruktury, jako je doprava, energetika nebo zdravotnictví. Psychologické operace pak cílí na vni-

mání bezpečnosti a mohou mít dlouhodobé dopady na chování obyvatelstva. Zvláštní pozornost je třeba věnovat falešným poplachům, které mohou vést k nepřiměřeným reakcím a ztrátě důvěry v bezpečnostní infrastrukturu.

Integrované způsoby ochrany – projevení technologií a organizace

Moderní přístup k ochraně proti UAV spočívá v integraci různých typů opatření do jednoho funkčního celku. Vedle detekčních protiopatření hrají důležitou roli organizační procesy, výcvik, spolupráce mezi složkami a kybernetická bezpečnost.

Kybernetická dimenze je stále významnější, protože mnoho prvků KI je řízeno digitálně. Oddělení provozních a IT sítí, monitorování anomálií a pravidelné audity patří mezi základní opatření.

Urbanistické a architektonické uspořádání má významnou roli, protože umožňuje implementovat bezpečnostní prvky už ve fázi projektování.

Praktická aplikace - pasivní ochranné systémy IBIPC, stabilní prvek v kontextu vícevrstvé obrany

Specifickou a často opomíjenou složkou ochrany jsou pasivní stavební prvky, které představují poslední linii obrany. Tento přístup systematicky rozvíjí společnost Institute of Blast & Impact Proof Concrete, jejíž konstrukce prvků vycházejí z patentovaného kompozitu UHPFRC.

Tento materiál kombinuje vysokou pevnost s výraznou schopností absorbovat kinetickou energii. Vlákenná struktura zajišťuje omezení křehkého porušení, přispívá ke stabilitě konstrukcí i při extrémním zatížení a snižuje riziko sekundární fragmentace, která bývá častou příčinou zranění.

Multifunkční pasivní prvky IBIPC zahrnují balistické stěny, ochranné kryty, z odolňující panely a perimetrická opatření, citlivě integrované do městského prostoru.⁶)

Jejich funkcí je nejen zastavení střepin a absorpce tlakové vlny, ale také řízení prostoru a zvýšení vzdálenosti mezi místem exploze a chráněným objektem. Prvky lze takticky implementovat tak, aby nenápadně splynuly s okolním prostředím.⁷)

Důležitou vlastností těchto řešení je jejich nezávislost na externích zdrojích. Na rozdíl od aktivních systémů nevyžadují energii, obsluhu a ani pravidelnou údržbu, což z nich činí stabilní a dlouhodobě spolehlivý prvek obrany i v krizových scénářích. Díky své konstrukční podstatě jsou spolehlivé a plně funkční nepřetržitě, bez ohledu na povětrnostní podmínky, v režimu 24/7/365.

Technologická úroveň těchto prvků je ověřena testováním a certifikací Vojen-

ského výzkumného ústavu, s. p., v Brně podle standardů NATO STANAG 2280-2016, což potvrzuje jejich schopnost odolávat balistickým, výbuchovým i střepinovým účinkům opravdu vysokých hodnot.

Fyzikální principy ochrany a praktické implikace

Z fyzikálně mechanického hlediska je určující vzdálenost mezi zdrojem exploze a chráněným objektem. Pasivní prvky proto nejen absorbují energii, ale také vytvářejí podmínky pro její rozptyl. Kombinace více ochranných prvků IBIPC umožňuje rozdělit účinek výbuchu do několika fází a výrazně snížit jeho dopad na konstrukci zodolněného objektu.

Dalším pozitivním aspektem je prevence progresivního kolapsu konstrukcí. Zodolnění kritických prvků a použití ochranných vrstev kompozitu UHPFRC může zabránit řetězovým selháním, která by jinak vedla k výrazně vyšším škodám.

Security by Design – integrace bezpečnosti do prostředí

Moderní přístup k ochraně měkkých cílů spočívá v integraci bezpečnostních opatření přímo do architektonického a urbanistického návrhu prostoru. Bezpečnostní prvky IBIPC jsou projektovány, testovány a vyráběny dle příručky Evropské komise Security by Design pro aplikaci při navrhování a budování veřejných prostor, což umožňuje kombinovat bezpečnost, funkčnost a estetiku tak, aniž by docházelo k nadměrné militarizaci prostředí.

Tento přístup je aplikován v urbanizovaných oblastech, kde je nutné zachovat otevřený charakter prostoru a současně zajistit jeho odolnost vůči hrozbám.

Ochrana měkkých cílů před UAV představuje komplexní a dynamickou výzvu, která vyžaduje interdisciplinární přístup. Klíčem k úspěchu je integrace technologických, organizačních a stavebních opatření do jednoho organizovaného celku.

Je nutno přijmout skutečnost, že absolutní bezpečnost neexistuje, a soustředit se zejména na minimalizaci dopadů a zachování funkčnosti operačního rámce. Pasivní ochranná řešení, prezentovaná mimo jiné prvky IBIPC, představují v tomto kontextu stabilní a spolehlivou poslední linii obrany.

Budoucnost ochrany měkkých cílů tak spočívá v adaptivních, vícevrstevných systémech, které dokážou reagovat na stále sofistikovanější hrozby a současně zachovat otevřený charakter moderní společnosti.

Mgr. Pavel Bělohradský
CEO, INSTITUTE OF BLAST
& IMPACT PROOF CONCRETE
– IBIPC, s.r.o.



6. T-Stěna, poskytuje balistickou, střepinovou a výbuchovou ochranu osob i objektů, vhodný jako retardér, kontrolní bod či krytí v rizikových zónách s rychlou instalací bez zásadních stavebních zásahů.



7. Květinové boxy na mezinárodním letišti Pardubice. Vysoká schopnost pohlcovat náraz, zachytit střely i fragmenty a zastavit vozidlo N3 (7,5 t) při 80 km/h; poskytuje místo pro krytí a přebíjení zasahujícím jednotkám a ochranu kritických míst.

1. UAV – Unmanned Aerial vehicle, bezpilotní letecký prostředek.
2. UAS – Unmanned Aircraft System, bezpilotní letecký systém.
3. Fříkční moment je „nečekaná překážka nebo soubor okolností, které způsobí, že operace nejde tak hladce, jak bylo plánováno – rozdíl mezi plánem a realitou na bojišti“. CLAUSEWITZ, Carl von. Vom Kriege [O válce]. Berlin: 1832.
4. Sun-c [孫子兵法] Umění války, 5. st. př. n. l. Podle Sun-c se bitva vyhrává či prohřává ještě předtím, než začne, a to na základě důkladné analýzy, plánování, informací a přípravy.
5. V krizových situacích lidé nereagují primárně racionálně, ale na základě evolučně podmíněných mechanismů: „boj–útek–strnutí“. Stres vyplavuje adrenalin i kortizol, zrychluje reakce, současně však omezuje schopnost komplexního uvažování a vede k impulzivnímu jednání. Systematickým výcvikem však lze vytvořit automatizované vzorce chování, které umožňují efektivnější a koordinovanější reakci pod tlakem i v prostředí, kde racionální úvaha selhává.

Norsko představuje model organizace veřejné správy, který se vyznačuje silnou decentralizací výkonu veřejných služeb, avšak současně relativní centralizací výkonu policejních činností. Tento článek si klade za cíl předeštit uspořádání vztahů týkajících se zajišťování vnitřní bezpečnosti a veřejného pořádku, zejména pokud se jedná o vztah mezi státní policií, kraji a obcemi.

NORSKO

PŘÍSTUP K ZAJIŠŤOVÁNÍ MÍSTNÍCH ZÁLEŽITOSTÍ VEŘEJNÉHO POŘÁDKU

Jelikož v Norsku není aktuálně zřízena městská či obecní policie ve vlastním smyslu slova, vzniká zde prostor pro alternativní řešení, jakými jsou zřizování pozice „parkovacích inspektorů“ a najímání soukromých bezpečnostních služeb pro plnění širokého spektra úkolů, zadávaných obcemi.

Základní informace o zemi¹

Rozloha: 385 207 km², z toho: kontinentální Norsko (pevninská část a přilehlé ostrovy) 323 811 km², Špicberky (Svalbard) 61 022 km² a ostrov Jan Mayen 377 km². Uvedený údaj nezahrnuje Bouvetův ostrov 49 km², ostrov Petra I. 156 km² a Zemi královny Maud v Antarktidě (tento nárok je spíše formální a není většinou států světa uznáván) okolo 2 700 000 km².

Počet obyvatel: Kontinentální Norsko (pevninská část a přilehlé ostrovy) 5 425 270 osob (podle sčítání lidu v roce 2021), Špicberky (Svalbard) asi 2 595 osob (září 2024) a ostrov Jan Mayen sezonní personál výzkumných stanic. Bouvetův ostrov je bez trvalého osídlení (chráněná přírodní rezervace). Totéž platí pro ostrov Petra I. (tedy rovněž bez trvalého osídlení). Zemi královny Maud obývá „několik desítek osob“ v rámci zhruba 12 výzkumných stanic.

REGIONY A OBCE V NORSKU

Země je aktuálně (od ledna 2024) rozdělena na 15 regionů, a to konkrétně 14 krajů (fylker) a území hlavního města Oslo (se statutem kraje i obce).²

Současný stav je přitom výsledkem turbulentních změn, které kulminovaly v posledních letech⁴:

- Do konce roku 2017 tvořilo Norsko 20 regionů (19 krajů + Oslo).⁵
- V průběhu června 2017 schválil parlament regionální reformu, rozřazenou do několika kroků v horizontu let 2017 až 2020. Celý proces byl oficiálně motivován snahou optimalizovat správu a politiku regionálního rozvoje.⁶
- Od ledna 2018 zanikly kraje Nord-Trøndelag a Sør-Trøndelag a jejich sloučením vznikl kraj Trøndelag.⁷ Regionů tedy bylo 19 (18 krajů + Oslo).

V lednu 2020 nastala další redukce počtu regionů na pouhých 11 (10 krajů + Oslo):

- Kraje Buskerud, Akershus a Østfold byly sloučeny do kraje Viken.
- Kraje Oppland a Hedmark byly sloučeny do kraje Innlandet.
- Kraje Vestfold a Telemark byly sloučeny do kraje Vestfold og Telemark.
- Kraje Aust-Agder a Vest-Agder byly sloučeny do kraje Agder.⁸
- Kraje Hordaland a Sogn og Fjordane byly sloučeny do kraje Vestland.
- Kraje Troms a Finnmark byly sloučeny do kraje Troms og Finnmark.

V letech 2022 až 2024 byly některé změny z roku 2020 anulovány (i z důvodu

odporu veřejnosti), což vedlo k výslednému počtu 15 regionů (14 krajů + Oslo).⁹

- Opětovně vznikly kraje Buskerud, Akershus a Østfold (na tyto tři jednotky byl opětovně rozdělen kraj Viken).
- Opětovně vznikly kraje Vestfold a Telemark (na tyto dvě jednotky byl opětovně rozdělen kraj Vestfold og Telemark).
- Opětovně vznikly kraje Troms a Finnmark (na tyto dvě jednotky byl opětovně rozdělen kraj Troms og Finnmark).

Nejvyšším orgánem kraje je krajské zastupitelstvo (fylkesting), jehož členové jsou voleni na 4 roky (v místních volbách, společně se členy obecních zastupitelstev). V čele krajského zastupitelstva je hejtman (fylkesordfører), jenž je volen z členů krajského zastupitelstva (obvykle z řad „vládnoucí koalice“, která tvoří krajský výbor, fylkesutvalg). Na úrovni kraje existuje i přenesený výkon státní správy, koordinovaný ředitelem „krajského úřadu“ (fylkeskommuneditrør).

Hlavní úkoly krajů se týkají následujících oblastí:

- vzdělání (vyšší střední školy a odborné vzdělání)
- zdravotní péče a sociální služby (zubní kliniky, nemocnice)
- průmyslový/obchodní rozvoj (cestovní ruch, propagace regionu, spoluvytváření podmínek pro podnikání)
- regionální plánování (územní plánování a místní rozvoj)
- doprava a komunikace (regionální silnice, veřejná doprava)
- kulturní a sportovní aktivity (ochrana kulturního dědictví, kulturní a sportovní akce a zařízení)

Vnitřní bezpečnost a veřejný pořádek nebývají v tomto ohledu přímo zmiňovány, rozhodně ne jako stěžejní priorita.

Co se týče úrovně obcí, pro rok 2024 bývá v rámci Norska uváděno celkem 357 obcí (kommuner).¹⁰ Úkoly a odpovědnosti všech obcí v Norsku jsou formálně vnímány jako identické. Obce se nicméně liší velikostí, topografií a počtem obyvatel. Nalezeme obce jen s několika stovkami osob, a naopak jinde je jich více než 50 000 (například Ålesund).

Nejvyšším orgánem obce je obecní zastupitelstvo (kommunestyre/bystyre), které je voleno na 4 roky v obecních volbách. V čele zastupitelstva stojí sta-

rosta (ordfører), jenž je volen ze členů zastupitelstva na 4 roky. Zastupitelstvo volí výkonný výbor (formannskap), který určuje parametry rozpočtu, místních daní a přijímá další klíčová rozhodnutí. V rámci obce působí také úředník, tajemník (kommunedirektør), který řídí administrativu obce a zajišťuje realizaci rozhodnutí volených orgánů.

Obce plní úkoly, například, v oblastech, jakými jsou školství (jesle, mateřské školy, základní a nižší střední školy, péče o děti), zdravotní a sociální péče (pohotovost, nemocnice, péče o seniory a zdravotně postižené, sociální služby), územní plánování (stavební povolení a dohled, bydlení, průmysl, ochrana přírody, životní prostředí a regulace znečištění), infrastruktura a technické služby (vodovody, kanalizace, svoz a likvidace odpadu, oprava silnic a chodníků) nebo kultura, volný čas (veřejné knihovny, sportoviště).

Pro krajská města nicméně platí parlamentem stanovené specifické úpravy (včetně financování), i z toho důvodu, že se obvykle jedná o aglomerace, překračující administrativní hranice obcí.

Postupné reformy (slučování, amalgamizace) byly obvykle prezentovány snahou napomoci obcím získat stabilitu, schopnost poskytovat kvalitní služby a lepší plánování rozvoje území.

V Norsku obce nezřizují vlastní „obecní policii“ v tom smyslu, jak je obvyklá v některých zemích střední Evropy, včetně České republiky. Role obcí v oblasti vnitřní bezpečnosti je tak v rámci Norska spíše nepřímá a koordinační, s důrazem na následující oblasti:

- Spolupráce s celostátně organizovanou policií: Obce poskytují policistům prostory, podporu „komunitní“ policejní služby, koncept „policie v blízkosti“ (nærpoliti), což je součást celostátní policie, která působí primárně lokálně, s místní znalostí.
- Prevence kriminality: Programy pro mládež, sociální služby, koordinace se školami a zdravotnickými zařízeními.
- Ochrana obyvatelstva, krizové řízení: Každá obec je povinna vypracovat plán pro mimořádné události (přírodní katastrofy, kybernetické incidenty, pandemie).

Alternativy k „obecní policii“ v Norsku

- Jak již zaznělo, obce v Norsku nezřizují (nejsou oprávněny zřizovat) vlastní obecní policii. Používají tedy v některých případech dva následující modely:



Parkovací inspektoři v Bergenu, rok 2017. BJØRN, Erik; HETTY, Nebell. Parkeringskommuner i Norge – en oversikt fra Vegdirektoratet. Parkeringsrett, 6. X. 2025. <https://www.parkeringsrett.no/parkeringskommuner-i-norge-en-oversikt-fravedirektoratet/>



Starosta obce Dropper, kde zastupitelstvo dospělo k závěru, že výnosy z parkování a pokut by byly daleko nižší než související náklady.

HANSEN, Roy. Dropper å bli parkeringskommune. Drammen Live 24, 25. IV. 2025. <https://www.drm24.no/dropper-a-bli-parkeringskommune/322275>

Období	Počet obcí	Poznámka
70. léta 20. století	744	
do roku 2000	435	přibližný odhad
březen 2013	428	
1. leden 2018–2019	422	počet před hlavní reformní vlnou
1. leden 2020	356	situace po velké vlně sloučení obcí ve spojení s regionální reformou z roku 2020
1. leden 2024	357	nově vzniklá obec Haram (oddělením od obce Ålesund)



DRONY V KRITICKÉ INFRASTRUKTUŘE DOBRÍ OCHRÁNCI, OBÁVANÍ NARUŠITELÉ

Kritická infrastruktura dnes musí řešit současně dva scénáře: Jak rozpoznat a zastavit nepřátelský dron? A jak bezpečně zapojit vlastní, autorizované drony do ochrany objektu? Podívejte se na modulární řešení, které sestavil Axis s několika technologickými partnery působícími v Česku.

Drony představují pro kritickou infrastrukturu dvojí realitu. Na jedné straně jsou užitečným pracovním nástrojem pro inspekce, monitoring a rychlé ověření incidentů. Na druhé straně obavy způsobují cizí drony, které mohou být vyslané za účelem narušení provozu, sbírání informací, testování reakce ostrahy nebo průniku do chráněného vzdušného prostoru.

Na českém trhu dnes vzniká zajímavá odpověď na obě tyto výzvy v podobě integrovaného řešení, které Axis poskládal propojením několika domácích technologických firem. Základní myšlenka je jednoduchá: účinná ochrana vzdušného prostoru nevzniká jedním zařízením, ale kombinací více modalit, jejich integrací do dohledového centra a správně nastavenými postupy obsluhy. V praxi tak vzniká jeden bezpečnostní celek složený z „ucha“, „oka“, radiofrekvenční identifikace, vizualizace a aktivní reakce.

Co jsme otestovali na Axis Demo Show

Následující řešení jsme prakticky ukázali v září 2025 při dvoudenním testu na akci Axis Demo Show, určené mimo jiné pro subjekty kritické infrastruktury a bezpečnostní složky. Přírodní areál rezortu Green Valley poblíž Benešova jsme rozdělili do bezpečnostních zón a simulovali jsme let cizího dronu jako narušitele chráněného vzdušného prostoru. Nejprve byl dron zachycen radiofrekvenčně pomocí Remote ID. Po vstupu do další zóny se přidal poplach z akustických senzorů. Ve třetí zóně kamera s videoanalytikou dostala informaci, kam se má natočit, pokusila se objekt rozpoznat, začala jej sledovat a současně poskytovala videoverifikační výstupy pro operátora — tedy informaci, o jaký dron jde a zda může představovat nebezpečí.

Smíte zlikvidovat nepřátelský dron?

Řešení testované na Axis Demo Show 2025 nebylo primárně navrženo k boji s vojenskými drony ani k fyzické nebo elektronické eliminaci dronů. Aktivní zneškodnění cizího dronu zůstává právně, technicky i provozně velmi citlivou oblastí s řadou omezení a v civilním prostředí není stále jednoznačně uchopené. Přesto už samotná schopnost spolehlivě zjistit, že se nad chráněným územím — například nad objektem kritické infrastruktury — pohybuje neznámý létající objekt, představuje významnou bezpečnostní hodnotu. Současně jde o řešení modulární: budoucí uživatel může využívat jen některé části celého konceptu podle svých potřeb, prostředí a rozpočtu. Právě díky této komponentové struktuře, multimodalitě a napojení na fyzickou ostrahu mohou být podobná řešení funkční už dnes, i když jsou zatím v ranější fázi rozvoje. Je totiž zřejmé, že budoucnost ochrany kritické infrastruktury se bude stále více odehrávat i ve vzdušném prostoru nad ní.



MULTIMODÁLNÍ DETEKCE DRONŮ A SYSTÉM REAKCE

1. RF IDENTIFIKACE

Systém Dronetag umožňuje pasivně přijímat radiofrekvenční údaje vysílané civilními drony, které dnes standardně musí být vybavené vysílačem Remote ID: získá tak identitu, pozici, výšku, směr letu a v některých případech i pozici pilota. Pro stacionární ochranu je určen zejména Dronetag Scout, tedy venkovní PoE přijímač pro nepřetržitý provoz, vhodný pro letiště, kritickou infrastrukturu i městské sítě. Jeho zásadní přínos spočívá v tom, že pomáhá rychle odlišit autorizované drony od ostatních. Současně je ale fér říci, že tato vrstva sama o sobě nestačí: „mlčící“ drony bez aktivního Remote ID nebo s nestandardním provozem nemusí být touto cestou viditelné. Právě proto je důležitá kombinace s akustickou a obrazovou detekcí.

2. AKUSTICKÁ DETEKCE

JALUD Embedded dodává řešení Sound Event Detector, které funguje jako digitální sluch a je k dispozici buď v podobě aplikace přímo do kamer Axis, nebo jako samostatný hardware. Zvuk je při detekci dronů velmi cenná modalita, protože se šíří všemi směry a dokáže upozornit na přítomnost dronu i tam, kde ještě není k dispozici jeho přímý obraz. Systém poskytuje informaci o přítomnosti dronu a jeho směru a tuto událost předává přes Axis event management do VMS nebo GIS nadstavby. Vedle dronů umí stejná technologie rozpoznávat také výstřely, rozbití skla, křik nebo agresivní projevy, takže rozšiřuje situační povědomí objektu i pro další bezpečnostní scénáře.

3. OBRAZOVÁ DETEKCE A VIDEOVERIFIKACE

Česko-ukrajinský startup OsyFly nabízí v rámci platformy Axis (ACAP) aplikaci FireFly určenou k instalaci přímo do kamery, kde analyzuje videostream s po-

mocí AI, detekuje dron v obraze a vrací jeho polohu formou bounding boxů. Pokud je cíl potvrzen, může FireFly zároveň řídit PTZ kameru Axis tak, aby dron automaticky sledovala a držela jej v zorném poli. Obraz zde tedy neplní jen roli pasivního záznamu, ale aktivně ověřuje alarm z jiných senzorů a zpřesňuje lokalizaci i tracking pohybujícího se cíle.

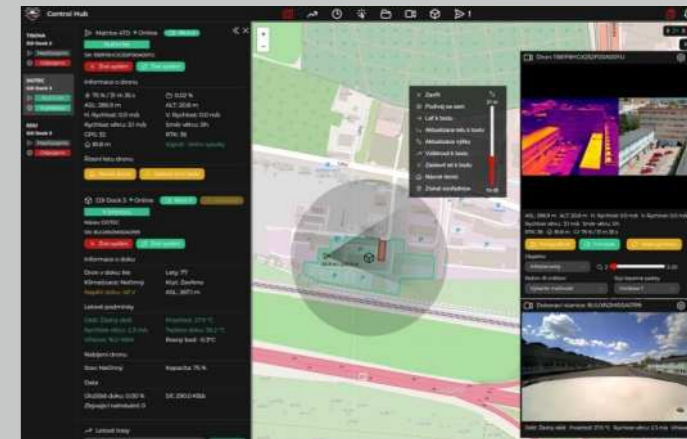
4. VIZUALIZACE A ŘÍZENÍ REAKCE

Platforma Droneguard, integrovaná v Česku společností Maxprogress, je zastřešující vrstvou nad senzory s možnou integrací dalších nadstavbových systémů. Operátor díky ní vidí detekované drony na mapě, trajektorii letu, alarmové stavy i vazbu na další technologie objektu, například EPS nebo perimetrickou ochranu. Po bezpečnostní události může systém automaticky spustit misi, zobrazit živý obraz, zaznamenat incident a doručit notifikaci bez složité ruční obsluhy. Z pohledu kritické infrastruktury je to klíčové: neřešíme jen samotnou detekci, ale celý proces od alarmu po operativní rozhodnutí.

5. ZÁSAH PŘÁTELSKÉHO DRONU

„Domácí“ autorizovaný dron, v tomto případě od českého výrobce Fly4Future (spin-offu ČVUT) s integrovanou kamerou Axis, představuje kyberneticky chráněný mobilní bezpečnostní prvek, který může po alarmu rychle odstartovat, přiblížit se k místu incidentu a přenášet obraz do dohledového centra. Díky videoanalytickým funkcím může pomáhat s identifikací pilota nepřátelského dronu nebo dalších osob spojených s narušením chráněného prostoru. Pokud je dron vybavený i reproduktorem, může operátor nebo předem připravená hlasová výzva s těmito osobami komunikovat a pokusit se je odradit od protiprávní činnosti.

Mgr. Dalibor Smažinka, MBA, LL.M
Manažer pro klíčové zákazníky
Axis Communications



EXCELENTNÍ, SKVĚLÁ, PŘÁTELSKÁ, INSPIRATIVNÍ...

Hosté ojedinelého a největšího mezinárodního setkání obecních a městských policí ve střední Evropě ve svých komentářích opět nešetřili superlativy. V Olomouci se ve dnech 25.–27. 3. 2026 konala jubilejní X. mezinárodní konference obecních policí.

Hlavní organizátor, společnost FT Technologies, program letošního výjimečného ročníku postavil na dvou hlavních tématech. A rozhodně se pomyslně trefil do černého, jak vyplynulo z reakcí 256 hostů, z nichž více než dvě třetiny tvořili strážníci z Česka, Polska a Slovenska.

Olomoucká konference byla ve znamení debat s cílem definovat „nové vize rozvoje a role strážníků“ obecních a městských policí při zajišťování bezpečnosti ve veřejném prostoru, s akcentem na posilování kooperace a vzdělávání – není žádným překvapením, že tomuto tématu se věnovala diskusní platforma „ÚHEL POHLEDU“. Druhým tématem bylo „zajištění bezpečnosti ve veřejném prostoru, zejména ochrana měkkých cílů“. V Olomouci k němu zaznělo hned několik velmi zajímavých přednášek. První konferenční den byl navíc přizpůsoben dynamické ukázkou „Simulace útoku na účastníky konference a eliminace útočnicků policí“. Jednalo se o jeden z vrcholů programu, kdy hosté konference měli exkluzivní příležitost být nejen v roli diváků, ale rovněž přímých aktérů ukázky. Podle dostupných informací a reakcí odborníků na měkké cíle se takto a v takovém rozsahu nic podobného na „živé konferenci“ dosud neodehrálo.



A co zajímavého se například ještě událo:

- Již počtvrté se na Krajském úřadě Olomouckého kraje uskutečnila významná přídružená uzavřená jednání konference v podobě setkání delegátů profesních organizací zastupujících české a slovenské strážníky.
- Při příležitosti jubilejní konference byly uděleny ceny za desetiletou strategickou podporu a spolupráci "FTT AWARD" Policejnímu prezidiu České republiky a „FTT AWARD Personal Honor“ třem osobnostem, které se výrazně podílely v prvních letech konání konference na její podpoře a neváhaly udělit osobní záštitu začínajícímu projektu – cenu obdrželi Ján Andrejko, emeritní prezident Združenia náčelníkov obecných a mestských policí SR, Milan Kladníček, emeritní předseda Kolegia ředitelů městských policí statutárních měst a hl. m. Prahy, a Artur Hołubiczko, Prefekt Krajowej Rady Komendantów Straży Miejskich i Gminnych RP.
- Součástí konference opět byla podpora dobrovolnictví a neziskových organizací a veřejný doprovodný program spojený mimo jiné s prezentací Bílého kruhu bezpečí a náborovou kampaní „Otevři si hubu na celý svět a daruj život“ propagující dárčovství krvetvorných buněk – je úžasné, že se během konference zaregistrovaly desítky nových (potenciálních) dárců, kteří mohou někomu zachránit život.
- Během simulace útoku byl desítkami kamer přenášen obraz i zvuk z prostranství před budovou a dalších konferenčních prostor (například z toalet) do sálu, kde v tu chvíli bylo přes 300 diváků. Ačkoliv jde o velmi vážnou a traumatizující skutečnost, o úsměvné okamžiky nebyla nouze (například při komunikaci mezi policisty či při velmi věrohodném projevu některých figurantů). Pokud se vám tedy zdá, že na některých záběrech se diváci či figuranti usmívají, nejde o zpochybňování samotné



SAVE THE DATE

17.-19. 3.
2027



Facebook



YouTube



LinkedIn



XI. Mezinárodní konference obecních policí | Olomouc

situace, ale o uvědomění si, že naštěstí jde stále o cvičení, a nikoli reálnou událost.

Mezinárodní konference obecních policí je ojedinelé a největší mezinárodní setkání obecních a městských policí ve střední Evropě. Jedná se nejen o společenskou událost, ale především o výjimečnou platformu pro osobní setkávání a výměnu zkušeností. Její součástí je také bohatý doprovodný program. Auditorium tvoří nejen zástupci obecních a městských policí, ale také státní správa, samospráva, integrovaného záchranného systému a bezpečnostních sborů, exekutivy, akademické sféry a dalších subjektů a organizací, včetně neziskového sektoru a dobrovolnických aktivit. Organizátorem je společnost FT Technologies a.s., která je považována za lídra trhu v oblasti poskytování informačních technologií pro obecní a městské policie, a spoluorganizátorem je

Právnická fakulta Univerzity Palackého v Olomouci.

Konferenci každoročně podporují profesní organizace strážníků z České republiky, Slovenska a Polska. Významná je také podpora ze strany Ministerstva vnitra České republiky, Ministerstva vnitra Slovenské republiky, Olomouckého kraje a statutárního města Olomouc, přičemž na zdárné realizaci spolupracuje a konferenci podporuje řada dalších subjektů a partnerů v čele s Policií České republiky, strategickým partnerem konference.

Hlavním partnerem letošního ročníku byla společnost TactiCore s.r.o. a hrdým mediálním partnerem je již mnoho let časopis Bezpečnost s profesionály.



MIGRACE A BEZPEČNOST

HLAVNÍ VÝZVY A JEJICH ŘEŠENÍ



1. ÚVOD

V tomto odborném příspěvku je cílem charakterizovat vybrané problémy migrace a bezpečnosti, a to s uvedením hlavních výzev a jejich možných řešení. Lidská migrace existuje od počátku jednotlivých forem lidské společnosti a hrála podstatnou roli ve formování lidských dějin až do současnosti. I ve druhém desetiletí 21. století nacházíme specifické aktuální výzvy a příležitosti v souvislosti s tímto fenoménem. Přináší s sebou nejen nové kulturní a technické přístupy, ale také projevy násilí, otroctví a masovou úmrtnost, což vede k velkému lidskému utrpení spojenému s historickým i aktuálním vývojem společnosti. Je též nutné zdůraznit, že s sebou přináší i konkrétní bezpečnostní výzvy a rizika. Mezinárodní migraci je možné obecně považovat za moderní formu masové migrace. Tato migrace na velké vzdálenosti je důsledkem výrazného růstu populace v rozvíjejících se zemích, podporované technickými a technologickými inovacemi. Historicky největší masovou migrací byla velká atlantická migrace z Evropy do Severní Ameriky. Tyto migrační proudy dočasně ustaly, ale v 80. letech 19. století nastala druhá, ještě větší vlna migrace z východní a jižní Evropy. Byla způsobena zemědělskou krizí a usnadněná rozvojem dopravy a modernizací komunikací. Po druhé světové válce pokračovaly rozsáhlé migrace na velké vzdálenosti, včetně

migrační krize v letech 2015–2016, kdy mnoho lidí směřovalo zejména do Německa. Většina migrantů z rozvojových zemí mířila do průmyslově vyspělých zemí západní Evropy, jako je také Francie, Nizozemsko a Velká Británie. Během posledních několika let jsou realizovány snahy, jak migrační vlny a s nimi spojené negativní vývojové trendy omezit.

Současné mezinárodní migrace jsou silně ovlivněny globalizací, kterou lze považovat za hlavní hnací sílu sociální a ekonomické transformace. Globalizace také mění vztahy mezi státy. Mezinárodní organizace pro migraci (2023) odhaduje, že dnes žije více než 272 milionů mezinárodních migrantů. V letech 2015–2021 se migrace stala v Evropské unii a OSN významným tématem a byly vytvořeny institucionální a právní struktury pro koordinaci migrace a migračních toků. Zpětně však tyto snahy neměly pouze pozitivní dopady. Významnou migrační vlnu pak od počátku roku 2022 představují osoby prchající z Ukrajiny, která je zasazena válečným konfliktem s Ruskem. Nejvíce tato migrační vlna zasáhla státy střední Evropy i například Německo či Polsko. Evropské země, včetně Španělska či Itálie, se snaží řešit migraci koordinovaně. Španělsko prosazuje podpůrnou a účinnou migrační politiku i na mezinárodní úrovni a je aktivním účastníkem mezinárodních migračních fór, například v rámci Agendy 2030 pro udržitelný rozvoj. Cíl 10.7 této agendy vyzývá k "usnadnění řádné, bezpečné, pravidelné a odpo-

vědné migrace a mobility osob prostřednictvím dobře řízených migračních politik".

Země, které jsou významněji zasazeny migrací, považují za zásadní spolupráci se zeměmi původu migrujících osob a tranzitu na odpovědném řízení bezpečnosti a legální migrace. Tato spolupráce je rozhodná pro prevenci nelegální migrace, boji proti převaděčství a obchodování s lidmi. Souhrnně jsou to pak všechny negativní projevy a dopady hlavních problémových faktorů, které vyplývají z masové nelegální migrace i problémů, které se týkají bezpečnosti. Tento solidární a efektivní přístup k migraci, který se EU snaží zastávat, se odráží i v migrační politice jednotlivých evropských států. V roce 2015 přijala Evropská unie Evropský program pro migraci a aktuálně se dále rozvíjí sekundární evropská legislativa založená na Paktu o migraci a azylu, jenž má dále podpořit nové předpisy a společné postupy pro lepší řízení migračních toků. Tyto předpisy zahrnují komplexní nástroje EU, jako jsou dialogy o migraci a mobilitě s třetími zeměmi a partnerskými státy, které tvoří součást jejího globálního přístupu k migraci. Mezi tyto nástroje patří Rabatský proces a Chartůmský proces, zavedené ve spolupráci s africkými zeměmi s cílem podporovat bezpečnou a regulovanou migraci, posílit boj proti nelegální migraci a vytvořit konkrétní programy a opatření k řešení základních příčin migrace. V těchto předpisech je možné identifikovat i vývojové trendy posilující bezpečnost

v zemích Evropské unie.

Evropská unie také reformovala instituce, jako je Evropský podpůrný úřad pro otázky azylu a Evropskou agenturu pro pohraniční a pobřežní stráž, známá jako Frontex. Role této instituce v zajištění bezpečnostních výzev a rizik je zásadní. Důležitým krokem bylo přijetí Globálního paktu OSN o bezpečné, řízené a legální migraci v prosinci 2018, který představuje první globální dohodu o společném přístupu k mezinárodní migraci ve všech jejích aspektech. Rozvoj řešení migrace v zemích EU zahrnuje síť Rady OSN pro migraci a Mezinárodní fórum pro přezkum migrace, které mají zajistit odpovídající monitorování stanovených strategických cílů v oblasti migrace a migračních toků.

2. HLAVNÍ ČÁST

Kubišta et al. (2017, s. 21–24) uvádí, že mezinárodní migrace je výrazně ovlivněna hospodářským rozvojem, využíváním přírodních zdrojů a jejich alokací. Spojuje se se základními populačními otázkami a problémy, což zahrnuje především migrační toky z hlediska lokalizace, prostoru, analýzy a migračních vzorců. Withol (2020, s. 25–27) poukazuje na skutečnost, že demografický vývoj je úzce spojen s porodností, úmrtností a následnou migrací. Analýzování toků uprchlíků, imigrace a vnitřní migrace přispívá k pochopení populačních jevů. Například zhoršování životního prostředí a nedostatek přírodních zdrojů mohou vést k redistribuci obyvatelstva, což vytváří nové výzvy pro životní prostředí, kulturu i politické instituce na což také poukazuje Kubišta et al. (2017, s. 33)

Migraci lze podle Pitrové et al. (2016, s. 15–17) obecně definovat jako přesun osob z jednoho místa na druhé, a to jak v rámci jedné země, tak mezinárodně. Tento pohyb může být na dlouhé vzdálenosti a může zahrnovat jednotlivce, rodiny nebo větší skupiny. V mezinárodním kontextu se migrace označuje jako přistěhovalectví a v historii lidské společnosti lze pozorovat specifické vzorce migrace. Většina lidí migruje na krátké vzdálenosti, často z ekonomických důvodů, a jejich pohyb probíhá v rámci vlastní země, což se nazývá vnitřní migrace. Ta se dále dělí na mezi-regionální migraci, která je trvalým pohybem z jednoho regionu země do jiného, a vnitro-regionální migraci, což je pohyb v rámci jednoho regionu.

Mezinárodní migrace, na rozdíl od vnitřní, je podle Paláta (2015, s. 7–9) pohyb z jedné země do druhé. Někteří lidé migrují dobrovolně na základě svého rozhodnutí, zatímco jiní jsou nuceni opustit svou zemi kvůli politickým, náboženským, kulturním nebo ekonomickým důvodům, což se označuje jako nucená migrace. Ekonomické vlivy, ne-

možnost najít práci a zdroj obživy mohou být také důvodem nucené migrace. Délka vzdálenosti, na kterou lidé migrují, závisí na ekonomických, genderových, rodinných a kulturních faktorech. Například ve Španělsku muži často migrují na delší vzdálenosti za prací, zatímco své rodiny nechávají v domovských zemích a podporují je finančně i materiálně. Podobná byla situace před válečným stavem na Ukrajině. V současné době muži z ukrajinského území migrují částečně se snahou vyhnout se odvodové povinnosti, ale stejně i z důvodu zajištění rodinných příslušníků a blízkých osob, jako tomu bylo před válečným stavem na Ukrajině do února 2022.

Guerrero (2019, s. 49–51) zdůrazňuje, že migrace v současném světě je velmi dynamickým jevem, ovlivněným různými faktory. Mezi nejvýznamnější ekonomické důvody patří environmentální faktory, jako jsou přírodní katastrofy, válečné konflikty, politické uspořádání, například diktátorské režimy, a další. Tyto faktory nutí velké množství lidí k migraci. Mezinárodní migrace zažívala své vrcholy v různých regionech a obdobích, jako například během migrační krize v letech 2015–2016, kdy do Německa přicházelo velké množství lidí. Aktuálně mezi příklady patří již uvedený válečný konflikt na Ukrajině, který se projevuje přílivem uprchlíků hlavně do zemí střední a východní Evropy nebo konflikt na území Izraele a další.

Odborné zdroje, mezi nimiž i Guerrero (2019) nabízejí teoretické přístupy k fenoménu migrace, mezi nimiž je významný koncept migračního přechodu. Tento přechod představuje změnu migračních vzorců v rámci lidské společnosti a může být výsledkem industrializace, populační expanze nebo různých sociálních a ekonomických změn, které ovlivňují demografický přechod. Klíčovým faktorem všech forem migrace je mobilita, která zahrnuje možnost stěhování buď trvalého, nebo dočasného.

Teoretické přístupy k migraci, jak potvrzuje Mulder, Vidal a další (2022) analyzují různé důvody, proč lidé migrují, například pomocí konceptu push a pull faktorů. Push faktory jsou události a podmínky, které nutí jednotlivce opustit své domovy, zatímco pull faktory jsou podmínky, které přitahují migrující osoby do určitého místa. Mezi nejčastější důvody migrace patří ekonomické faktory, kdy lidé opouštějí své domovy kvůli nedostatku pracovních příležitostí. Naopak jsou přitahováni do míst, kde mohou najít pracovní uplatnění nebo lépe placenou práci, což vede ke zvýšení jejich životní úrovně a sociálního statusu.

Kulturní push faktory, podle Vidala (2022) často vedou k migraci, zahrnují otroctví, politickou nestabilitu, etnické čistky, hladomor a válečné konflikty.

Tyto problémy nutí lidi k útěku nebo nucenému odchodu z jejich domovů. Výbor Spojených států pro uprchlíky definuje uprchlíka jako osobu, která byla nucena opustit svůj domov a nemůže se vrátit kvůli náboženství, rase, národnosti nebo politickému přesvědčení. Naopak kulturní pull faktory přitahují lidi, kteří touží žít v demokratické společnosti, očekávají rovnost pohlaví a přístup k vzdělání a náboženským příležitostem.

Cabieses et al. (2022) uvádí, že migrační vzorce jsou rovněž ovlivněny environmentálními faktory. Environmentální pull faktory zahrnují možnosti vzdělání, svobodu a bezpečný život, zatímco environmentální push faktory se vztahují k přírodním katastrofám, jako jsou zemětřesení, tsunami, hurikány a bleskové povodně, které zasahují konkrétní místa a regiony v různé míře. Klimatické push a pull faktory, jako jsou sucha a neúroda, také ovlivňují migrační vzorce. S rostoucí naléhavostí antropogenních změn klimatu a zvyšujícím se počtem lidí nucených opustit své domovy, se počet klimatických migrantů na světě zvyšuje.

Palát (2015, s. 32–33) vymezuje, že některé státy a jejich instituce vytvořily systémy včasného varování před přírodními katastrofami, které zahrnují monitorování potenciálních hladomorů. Tímto způsobem mohou dotčené organizace poskytovat efektivnější pomoc, ať už finanční nebo materiální. Osoby, které byly vysídleny z ekologických důvodů, jsou často označovány jako environmentálně vysídlené osoby nebo ekologičtí uprchlíci. Problémem těchto uprchlíků je, že nejsou chráněni podle Úmluvy o právním postavení uprchlíků z roku 1951, která uprchlíkem definuje osobu s "oprávněnými obavami z pronásledování z důvodu rasy, náboženství, národnosti, příslušnosti k určité sociální skupině nebo zastávání určitých politických názorů, která se nachází mimo zemi své státní příslušnosti a není ochotna využít ochrany této země". V posledních dvaceti letech 21. století se mnoho lidí stalo environmentálními uprchlíky v důsledku klimatických změn, sucha, záplav způsobených rozsáhlými bouřkovými systémy, nedostatku vody a dalších vlivů. Střednědobé a dlouhodobé předpovědi vývoje těchto vlivů nejsou příznivé.

Odborné zdroje, například Oso et al. (2021) naznačují, že největší migrační pohyby současnosti probíhají v rámci jednotlivých států. Tyto migrační toky mají různou dynamiku. Historicky se lidé často stěhovali do městských aglomerací, které však ve středověku a částečně i v novověku zažívaly populační výkyvy způsobené epidemiemi, jako byla morová infekce. Města v těchto obdobích nebyla potravinově soběstačná a potřebovala dovoz potra-

vin. V 18. a 19. století se stále potýkala s nedostatky v dopravní infrastruktuře a nedostatečným rozvojem technických a technologických inovací, což vedlo k častým hladomorům a epidemiím. Během první a zejména druhé světové války města rychle rostla, což bylo podpořeno technickým a technologickým pokrokem. Od druhé poloviny 20. století se počet obyvatel některých měst v mezinárodním měřítku zdvojnásobil každých deset let. Vývoj mezinárodní migrace a migračních toků lze efektivně sledovat díky dostupnosti statistických demografických dat a prognóz.

Odborné zdroje, mj. též Oso et al. (2021) také uvádějí, že populace různých zemí je velmi různorodá. Tato různorodost se týká etnických aspektů i vývoje společnosti pod vlivem různých faktorů. Etnicita zahrnuje národnostní, kulturní, náboženské, jazykové a další charakteristické znaky různých skupin osob. To je podstatné pro mezinárodní migraci, zejména pokud jde o integraci migrantů do většinové společnosti cílové země. Migranté mohou být pro cílové země přínosní různými způsoby. Pro pracovní trh je důležité, zda přicházejí ze zemědělských oblastí, nebo jsou vysocí kvalifikovaní. Agrární společnosti, závislé na zemědělství, bývají méně vyspělé, zatímco technologicky vyspělé oblasti produkují vzdělanější a kvalifikovanější pracovní sílu, která je pro pracovní trhy cílových zemí velmi cenná.

Lidská migrace, podle Neubecker et al. (2022), existuje od počátku lidské společnosti a hrála zásadní roli ve formování lidských dějin až do současnosti. Přináší s sebou nejen nové kulturní a technické poznatky, ale také projevy násilí, otroctví a masovou úmrtnost, což vede k velkému lidskému utrpení spojenému s historickým vývojem společnosti. Mezinárodní migraci můžeme považovat za moderní formu masové migrace. Tato migrace na velké vzdálenosti je důsledkem výrazného růstu populace v rozvíjejících se zemích, podporovaného technickými a technologickými inovacemi. Historicky největší masovou migrací byla velká atlantická migrace z Evropy do Severní Ameriky. Tyto migrační proudy dočasně ustaly, ale v 80. letech 19. století nastala druhá, ještě větší vlna migrace z východní a jižní Evropy, způsobená zemědělskou krizí a usnadněná rozvojem dopravy a komunikací. Po druhé světové válce pokračovaly rozsáhlé migrace na velké vzdálenosti, včetně migrační krize v letech 2015–2016, kdy mnoho lidí směřovalo zejména do Německa. Většina migrantů z rozvojových zemí mířila do průmyslově vyspělých zemí západní Evropy, jako je Francie, Nizozemsko a Velká Británie. Významné migrační toky nyní existují v posledních letech i vlivem válečného konfliktu na Ukrajině, s dopady hlavně na jednotlivé evropské státy

vrámcí EU.

Podle World Migration Report (2022) jsou jednotlivé současné mezinárodní migrace silně ovlivněny globalizací, kterou lze považovat za hlavní hnací sílu sociální a ekonomické transformace. Globalizace také mění vztahy mezi státy. Mezinárodní organizace pro migraci odhaduje, že dnes žije více než 272 milionů mezinárodních migrantů. Spíše se však budeme pohybovat na hranici až 300 milionů osob, což zahrnuje různé druhy migrace. V letech 2015–2021 se migrace stala v Evropské unii a OSN významným tématem a byly vytvořeny institucionální a právní struktury pro koordinaci migrace a migračních toků. Evropské země se snaží řešit migraci koordinovaně. Španělsko prosazuje podpůrnou a účinnou migrační politiku i na mezinárodní úrovni a je aktivním účastníkem mezinárodních migračních fór, například v rámci Agendy 2030 pro udržitelný rozvoj. Cíl 10.7 této agendy vyzývá k "usnadnění řádné, bezpečné, pravidelné a odpovědné migrace a mobility osob prostřednictvím dobře řízených migračních politik". Země EU považují za zásadní spolupracovat se zeměmi původu a tranzitu pro zajištění odpovědného řízení bezpečné a řádné migrace. Taková spolupráce je rozhodující pro prevenci nelegální migrace, boj proti převaděčství a obchodování s lidmi, a také s ohledem na různé bezpečnostní aspekty.

Tento solidární a efektivní přístup k migraci, který EU zastává, se odráží i v migrační politice jednotlivých států EU. V roce 2015 přijala Evropská unie Evropský program pro migraci a aktuálně se rozvíjí nový Pakt o migraci a azylu, jenž má podpořit nové předpisy a společné postupy pro lepší řízení migračních toků, jak zdůrazňuje Evropská komise (2023). Tento pakt zahrnuje komplexní nástroje EU, jako jsou dialogy o migraci a mobilitě s třetími zeměmi a partnerskými státy, které tvoří součást jejího globálního přístupu k migraci. Mezi tyto nástroje patří Rabatský proces a Chartúmský proces, zavedené ve spolupráci s africkými zeměmi s cílem podporovat bezpečnou a regulovanou migraci, posílit boj proti nelegální migraci a vytvořit konkrétní programy a opatření k řešení základních příčin migrace.

Evropská unie také reformovala instituce, jako je Evropský podpůrný úřad pro otázky azylu a Evropská agentura pro pohraniční a pobřežní stráž, známá jako Frontex. Například Španělsko v boji proti nelegální migraci spolupracuje především se zeměmi na západoafrické trase, poskytuje technickou podporu a trvale se snaží o budování institucionálních kapacit. Obdobně přijatá bezpečnostní opatření jsou realizována také v Itálii či ve Francii s ohledem na jejich bezpečnostní otázky a migrační trasy. Důležitým krokem bylo přijetí Globální

ho paktu OSN o bezpečné, řízené a legální migraci v prosinci 2018, který představuje první globální dohodu o společném přístupu k mezinárodní migraci ve všech jejích aspektech. Některé země EU tento pakt silně podporovaly od počátku a aktivně se podílely na jeho vyjednávání i následném institucionálním rozvoji. Tento rozvoj zahrnuje síť Rady OSN pro migraci a Mezinárodní fórum pro přezkum migrace, které mají zajistit odpovídající monitorování stanovených strategických cílů v oblasti migrace a migračních toků.

Podle Kritzman (2016) je žádoucí analyzovat historický a geografický rozměr migrace do jednotlivých evropských zemí, se zvláštním důrazem na současné bezpečnostní i integrační tendence. Hlavním cílem je vymezit aspekty ekonomické i nucené migrace a jejich specifický dopad na politický a institucionální systém v každé evropské zemi. Zvláštní pozornost je potřebné věnovat problémům vyplývajícím z odlišného náboženského přesvědčení a kulturních zvyklostí nově přichozích migrantů, což způsobuje značná bezpečnostní rizika v soužití menšin i majoritní části obyvatel. Typické jsou tyto problémy aktuálně v Německu či ve Francii a představují konkrétní bezpečnostní rizika. Jak už bylo uvedeno, migrace je jedním z nejvýznamnějších fenoménů současného světa. Lidé se přesouvají z jednoho místa na druhé z různých důvodů, včetně ekonomických, politických, environmentálních a sociálních faktorů. Tento proces má hluboký dopad na světové uspořádání a lidskou společnost a přináší s sebou jak pozitivní, tak negativní důsledky. Jedním z hlavních aspektů, které je třeba zvážit, jsou bezpečnostní hrozby a rizika spojená s migrací.

PhDr. Mgr. Dávid Dömény,
MBA, DBA, LL.M.

DRONOVÉ CENTRUM PRO MĚSTO NESTAČÍ KOUPIĆ MUSÍ SE NAVRHNOUT, DODAT A UVĚST DO PRAXE

Záměr měst a obcí o bezpilotní technologie v posledních letech výrazně roste. Důvod je jednoduchý: samosprávy dnes hledají nástroje, které jim pomohou lépe řídit bezpečnost, správu majetku, krizové situace i každodenní provoz města. Drony v tomto směru představují mimořádně efektivní řešení. Nejde přitom jen o rychlý pohled z výšky. Moderní bezpilotní systémy dnes umějí poskytovat detailní obrazová a termální data, podporovat operativní rozhodování v reálném čase, vytvářet přesné mapové podklady, 3D modely nebo zajišťovat monitoring lokalit, které jsou pro kontrolu obtížně dostupné.

Aby ale město mohlo tyto technologie skutečně využívat, nestačí pořídit samotné drony. Klíčové je navrhnout celé funkční řešení: správně vybrat techniku pro konkrétní typy úkolů, vytvořit provozní zázemí, zajistit přenos a ukládání dat, nastavit metodiky využití, vyškolení personál a připravit provoz v souladu s legislativními požadavky. Právě v tom spočívá rozdíl mezi jednorázovým nákupem technologie a vybudováním skutečně funkčního městského dronového centra.

Na tuto potřebu AgentFly Technologies dlouhodobě reaguje komplexním přístupem, který propojuje zkušenosti z oblasti bezpilotních prostředků, robotiky, datového zpracování a řízení provozně náročných systémů. Naším cílem není dodat městu izolovaný technický prostředek, ale navrhnout a zprovoznit řešení, které odpovídá jeho konkrétním potřebám a které může být dlouhodobě a bezpečně využíváno v praxi. Právě díky kombinaci technologického vývoje, provozních zkušeností a znalosti regulatorního prostředí jsme schopni dodat celý řetězec služeb – od úvodní analýzy potřeb přes návrh konceptu až po samotnou realizaci a podporu provozu.

Města dnes potřebují řešení, která dokážou obsloužit více agend současně. V jedné rovině jde o podporu městské policie a dalších bezpečnostních složek, například při monitoringu rizikových lokalit, hromadných akcí, dopravní situace nebo při pátrání po osobách. Ve druhé rovině jde o potřeby samosprávy – dokumentaci staveb a investičních akcí, kontrolu technické infrastruktury, správu městského majetku, vytváření mapových podkladů, 3D modelů nebo termální mapování budov. V dalších případech může hrát zásadní roli krizové řízení, kdy je potřeba během krátké doby získat spolehlivý přehled o situaci v terénu a předat data rozhodujícím složkám v reálném čase.

Právě tuto logiku jsme uplatnili i při projektu v Ústí nad Labem. Zde jsme se nepohybovali na úrovni jednoduché dodávky techniky, ale navrhli a realizovali komplexní systém, který umožňuje bezpilotní technologie skutečně začlenit do fungování města. Součástí projektu bylo

dodání dronů v různých kategoriích podle předpokládaných scénářů použití, jejich vybavení vhodnou senzoričkou, vytvoření odpovídajícího zázemí pro skladování, nabíjení a údržbu, zajištění výpočetní a softwarové podpory a nastavení postupů pro praktické využití v městských agendách.

Významnou součástí takového řešení je i schopnost pracovat s daty. Drony dnes nejsou jen létající kamerou. Jsou vstupním bodem do celého systému, jehož výstupem mohou být online přenosy pro operační řízení, detailní obrazová dokumentace, termální výstupy, podklady pro inspekce, prostorová data nebo 3D modely využitelné při správě a rozvoji města. AgentFly Technologies proto staví podobné projekty tak, aby součástí dodávky nebyla jen letová technika, ale i návazná datová a provozní infrastruktura. Město tím získává možnost pracovat s výstupy systematicky, nikoli jen ad hoc.

Právě v Ústí nad Labem se ukázalo, jak důležitá je schopnost dodat městu řešení jako celek. Vedle technického vybavení bylo nutné nastavit také procesní a organizační stránku provozu. To zahrnuje identifikaci vhodných scénářů použití, přípravu metodik pro jednotlivé městské složky, nastavení pravidel provozu, zaškolení personálu a podporu při zajištění souladu s požadavky civilního letectví a dalších souvisejících předpisů. V praxi je totiž právě tato fáze často rozhodující. Bez ní i kvalitní technologie zůstávají nevyužitá nebo využívána jen omezeně. Naopak dobře připravený systém umožní, aby se bezpilotní prostředky staly skutečnou součástí městského provozu.

Pro AgentFly Technologies je důležité, že podobné projekty neřešíme jako univerzální balíček, ale jako modulární systém, který se přizpůsobuje konkrétnímu zadání. Každé město má jinou strukturu agend, jiné priority i jiné personální a rozpočtové možnosti. Někde bude dominantním tématem bezpečnost a městská policie, jinde správa infrastruktury, dokumentace investic nebo podpora krizového řízení. Díky tomu, že jsme schopni kombinovat různé typy bezpilotních prostředků, senzorů, softwarových nástrojů i provozních modelů, umíme navrhnout řešení, které odpovídá reálnému fungo-

vání konkrétní municipality.

Naše přidaná hodnota navíc nespočívá jen v dodávce komerčně dostupné techniky. Vycházíme z vlastního vývoje a z dlouhodobé zkušenosti s autonomními a bezpilotními systémy, robotikou a pokročilými softwarovými nástroji. Právě toto know-how nám umožňuje uvažovat o městském dronovém centru nikoli jako o izolovaném produktu, ale jako o části širší technologické infrastruktury města. Důležitou roli zde hraje také naše schopnost integrovat různé technologie do jednoho funkčního celku a přenášet zkušenosti z výzkumných i provozních projektů do prakticky využitelných řešení.

Projekt v Ústí nad Labem je proto dobrým příkladem toho, co dnes může moderní dodavatel municipalit nabídnout. Ne pouze dron nebo jednotlivou službu, ale kompletní návrh a realizaci systému, který městu přinese lepší přehled, rychlejší reakci, kvalitnější data a širší možnosti práce s územím i městskou infrastrukturou. Současně jde o model, který je přenositelný i do dalších měst a obcí. Ať už se jedná o větší statutární města nebo menší municipality, základní princip zůstává stejný: správně navržené dronové centrum musí vycházet z konkrétních potřeb města a musí být od počátku budováno jako funkční služba, nikoli jen jako technologická atrakce.

Zkušenost ukazuje, že právě takový přístup má pro municipality největší hodnotu. Město nezískává pouze novou technologii, ale partnera, který je schopen dodat řešení od první analýzy přes technologický návrh až po uvedení do provozu a jeho další rozvoj. V době, kdy samosprávy hledají chytré, efektivní a bezpečné nástroje pro správu města, se bezpilotní technologie stávají stále důležitější součástí moderní municipální infrastruktury. A schopnost dodat je jako skutečně funkční systém je tím, co bude rozhodovat o jejich úspěchu v praxi.

Michala Vondráková
AgentFly Technologies s.r.o.