Recenzovaný zborník z medzinárodnej interdisciplinárnej doktorandskej konferencie
DOKOR 2024 konanej dňa 30. apríla 2024 v Ružomberku
Proceedings of International Interdisciplinary Doctoral Conference
April 30, 2024, Ružomberok, Slovak Republic
ISBN 978-80-561-1102-4

OPEN ACCESS Article

DOI: https://doi.org/10.54937/2024.9788056111024.260-276

ANALÝZA VPLYVU DIGITÁLNYCH TECHNOLÓGIÍ NA ŠÍRENIE TERORIZMU A EXTRÉMIZMU: VÝZVY A STRATÉGIE PRE MEDZINÁRODNÚ BEZPEČNOSŤ A DIPLOMACIU

Milan KUSÁK [1]

ANALYSIS OF THE IMPACT OF DIGITAL TECHNOLOGIES ON THE SPREAD OF TERRORISM AND EXTREMISM: CHALLENGES AND STRATEGIES FOR INTERNATIONAL SECURITY AND DIPLOMACY

[1] *Akadémia policajného zboru v Bratislave, Sklabinská 1, 835 17 Bratislava, Slovenská republika*
Email: kusakmilan@gmail.com
ORCID iD: 0009-0000-2645-6258 https://orcid.org/0009-0000-2645-6258

ABSTRAKT

Táto štúdia sa zaoberá komplexnou analýzou vplyvu digitálnych technológií na šírenie terorizmu a extrémizmu, poskytujúc pohľad na historický vývoj, definície a strategické využitie digitálnych platforiem teroristickými a extrémistickými skupinami. Skúma, ako sociálne siete, šifrovaná komunikácia a iné digitálne nástroje umožňujú týmto skupinám nábor nových členov, šírenie ideológií a koordináciu útokov, pričom poukazuje na významné bezpečnostné výzvy, pre medzinárodnú spoločnosť. Analyzuje tiež rôzne perspektívy a prístupy k boju proti digitálnemu terorizmu a extrémizmu, vrátane využitia pokročilých technológií, právnych a regulačných rámcov, vzdelávania a medzinárodnej spolupráce. Cieľom je poskytnúť komplexný pohľad na stratégie, ktoré by mohli byť využité na zmiernenie týchto hrozieb v digitálnej ére, zatiaľ čo sa zároveň zabezpečuje ochrana súkromia a občianskych práv.

ISBN 978-80-561-1102-4

Kľúčové slová: *digitálne technológie, terorizmus, extrémizmus, sociálne médiá, medzinárodná bezpečnosť*

ABSTRACT
This study provides a comprehensive analysis of the impact of digital technologies on the spread of terrorism and extremism, offering insights into the historical development, definitions, and strategic use of digital platforms by terrorist and extremist groups. It examines how social networks, encrypted communication, and other digital tools enable these groups to recruit new members, spread ideologies, and coordinate attacks, highlighting significant security challenges for the international community. The study also analyzes various perspectives and approaches to combating digital terrorism and extremism, including the use of advanced technologies, legal and regulatory frameworks, education, and international cooperation. The goal is to offer a comprehensive view of strategies that could be utilized to mitigate these threats in the digital era while simultaneously ensuring the protection of privacy and civil rights.

Key words: *digital technologies, terrorism, extremism, social media, international security*

Úvod

V súčasnej dobe digitálne technológie zásadne ovplyvňujú mnohé aspekty nášho života vrátane bezpečnosti a medzinárodných vzťahov. Táto štúdia sa zameriava na analýzu toho, ako digitálne technológie ovplyvňujú šírenie terorizmu a extrémizmu. v prvom rade poskytuje historický prehľad terorizmu a extrémizmu, definuje kľúčové pojmy a skúma rôzne perspektívy a prístupy k tejto problematike. Následne sa štúdia venuje vplyvu digitálnych médií a sociálnych sietí na moderný terorizmus a extrémizmus, analyzuje strategické využitie týchto platforiem pre nábor, šírenie ideológií a koordináciu útokov, a poukazuje na významné bezpečnostné výzvy a potenciálne stratégie pre medzinárodnú bezpečnosť a diplomaciu v digitálnej ére.
V súčasnom digitálnom veku sa rozšírenie technológií stalo dvojsečnou zbraňou. Na jednej strane umožňujú bezprecedentný pokrok v komunikácii a informačných technológiách, na druhej strane však prinášajú nové výzvy v oblasti bezpečnosti a boja proti terorizmu a extrémizmu. Táto štúdia sa zameriava na komplexnú analýzu vplyvu digitálnych technológií na šírenie týchto sociálnych javov. Skúma historický vývoj terorizmu a extrémizmu, definuje kľúčové pojmy a poskytuje prehľad o rôznych perspektívach na túto problematiku. Ďalej sa venuje špecifickému vplyvu digitálnych médií a sociálnych sietí na moderný terorizmus a extrémizmus, zameriavajúc sa na strategické využitie týchto platforiem pre nábor, šírenie ideológií a koordináciu útokov. Štúdia taktiež poukazuje na dôležité bezpečnostné výzvy a potenciálne stratégie, ktoré by mohli byť využité na zmiernenie týchto hrozieb v digitálnej ére. Cieľom je poskytnúť komplexný pohľad na výzvy a stratégie pre medzinárodnú bezpečnosť a diplomaciu v kontexte digitálneho veku.

1. HISTORICKÝ PREHĽAD TERORIZMU A EXTRÉMIZMU

Literatúra sa nezhoduje na jednej presnej definícii pojmu extrémizmus – ten je na poli výskumu a skúmania analyzovaný multidisciplinárne. Je skúmaný okrem iných politológiou a medzinárodnými vzťahmi, bezpečnostnými štúdiami, sociológiou alebo právnou vedou, ale otázkou, čo je extrémizmus, sa po práve môže zaoberať aj filozofia. Každý z odborov má potom pochopiteľne vlastné teórie, prístupy a metodológie. Definícia extrémizmu sa tak líši napríklad v šírke motivácií, cieľov a prostriedkov extrémizmu. To, ako si konkrétna spoločnosť definuje extrémizmus, môže byť tiež ovplyvnené politickou situáciou alebo historickou skúsenosťou, a môže sa meniť aj v čase. Pripomenúť možno aj to, že to, čo je považované za extrémizmus, môže byť ovplyvnené tiež ideológiou, osobnými predsudkami alebo účelovou demagógiou. Možno povedať, že extrémizmus je univerzálne považovaný za zavrženia hodný akt agresie, deštruktívne zasahujúci do celej škály ľudských práv, základných slobôd a fungovania demokracie, ako stojí v prehlásení Viedenskej deklarácie Svetovej konferencie o ľudských právach z roku 1993.[43]

ISBN 978-80-561-1102-4

Neexistuje však univerzálna zhoda na tom, čo extrémizmus je a čo ním nie je – ako s klišé sa možno často stretnúť s prirovnaním, že „ten, kto je pre jedného extrémista, je pre druhého bojovníkom za slobodu“. Spoločnými menovateľmi činu, ktorý možno považovať za extrémistický, však je, že je namierený prevažne voči civilistom alebo určitým skupinám, je úmyselný, je motivovaný a jeho cieľom je destabilizácia, ochromenie či vyvolanie strachu a hrôzy.[12] Pre základné vymedzenie extrémizmu sa ponúka návrh všeobecnej a zjednodušenej definície od autorky Radany Makariosovej, ktorá znie „Extrémizmus je zámerne, politicky motivovaný čin vykonaný aktérom zákerne a kruto za účelom ochromenia verejnosti.“[19] Autorka túto definíciu určila na základe rôznych ďalších súčasných a frekventovaných definícií a prehľadne stanovuje základné parametre, ktoré pomáhajú určiť to, čo možno za extrémizmus všeobecne považovať. Je nutné zopakovať, že neexistuje jeden všeobecne prijímaný výklad toho, čo je extrémizmus.

Ohľadom prídavného mena „neštátny“ je nutné spomenúť špecifický aspekt vzťahu štátu a extrémizmu v zmysle podpory extrémistických skupín alebo priameho páchania teroru voči určitým skupinám. Téma akéhokoľvek násilia, a zvlášť toho organizovaného a hromadného, voči určitým skupinám je veľmi citlivá a zásadná. Možno sa stretnúť s odlíšením pojmov teror a extrémizmus. Všeobecne by však malo platiť, že teror je páchaný štátnymi i neštátnymi aktérmi na civilnom obyvateľstve, extrémistické hnutia však vznikajú zdola, od obyvateľov.[22] Napríklad vojenský historik Caleb Carr vníma teror ako súčasť vojenskej tradície a histórie a teroristov ako istú formu vojakov. [32]Vymedzuje extrémizmus ako akt teroru voči nebojujúcej časti obyvateľstva „za účelom zničenia ich vôle podporovať vodcu alebo politiku“ a tieto činy vníma ako súčasť neobmedzenej vojny, opaku obmedzenej vojny vedené medzi riadne označenými vojskami. Z pohľadu Carrovho výkladu potom možno dohľadať prvky teroru alebo násilia voči nebojujúcemu obyvateľstvu, v celej histórii vojnových konfliktov na čele s druhou svetovou vojnou. Z určitého uhla pohľadu možno za finálny akt teroru v spomínanej vojne považovať zvrhnutie atómových bômb na Hirošimu a Nagasaki, holokaust a násilie na nemecko-sovietskej fronte nevraviac.

Samotné slovo extrémizmus pochádza z latinského slova extrēmus, označujúce najvyšší, najvzdialenejší alebo extrémny. Moderný význam sa odvíja od historických príkladov, keď skupiny či jednotlivci pristupovali k presadzovaniu svojich cieľov extrémnymi metódami, často za použitia násilia a agresívnych taktík. Extrémizmus ako psychologický jav zasahuje a ovplyvňuje nielen priame obete, ale aj očitých svedkov a divákov prostredníctvom médií. Hlavné posolstvo extrémizmu môže byť vyjadrenie určitého posolstva alebo ideológie činom a súčasne podkopávanie dôvery v inštitúcie, ktoré nedokážu takejto hrozbe čeliť. Cieľom môže byť aj verbovať a aktivizovať prípadných sympatizantov a napomáhať ich radikalizácii. Na tomto mieste je nutné zdôrazniť rozdiel medzi partizánskymi a extrémistickými hnutiami. Profesionálna armáda, partizánsky oddiel aj napríklad cirkevný rád sa môžu dopustiť extrémistického činu, ale záleží na celkovom kontexte metód, vnútornom vyrovnaní sa s daným páchateľom a deklarovaných cieľoch, aby bolo možné určiť, či ide o komplexné extrémistické organizácie. v prípade hodnotenia udalostí, od ktorých uplynulo dlhšie časové obdobie, je nutné brať do úvahy dobový kontext. Vysvetlenie toho, čo sú príčiny extrémistických činov, sú potom rovnako tak komplikované a diskutabilné – môže sa jednať o dôsledok spoločenského konfliktu a krízy legitimity štátu, môže sa jednať o objektívne príčiny nespokojnosti (napr. socioekonomické) alebo stret kultúr, ktoré vedú k negatívnym emočným reakciám a vnútorným, čisto subjektívnym pocitom, ktoré sú následne zneužité alebo manipulované extrémistickými ideológiami a vodcami.[1]

Jednou z hlavných oblastí skúmania extrémizmu je sociálno-psychologická dimenzia, ktorá skúma, ako sa jednotlivci dostávajú k radikálnym názorom a ako sú títo jednotlivci ovplyvnení svojim sociálnym prostredím. Tento prístup môže pomôcť lepšie porozumieť procesom radikalizácie a identifikovať faktory, ktoré prispievajú k posunu od radikálneho myslenia k extrémistickým činom. Ďalšou dôležitou oblasťou je štúdium politických a historických kontextov, v ktorých extrémizmus vzniká a rozvíja sa. Táto perspektíva umožňuje pochopiť, ako rôzne politické režimy a historické udalosti formujú extrémistické ideológie a akcie.

V kontexte medzinárodných vzťahov a bezpečnostných štúdií je extrémizmus často skúmaný vo vzťahu k terorizmu a asymetrickému konfliktu, kde je dôraz kladený na pochopenie motivácií

ISBN 978-80-561-1102-4

a stratégií neštátnych aktérov, vrátane teroristických skupín a povstaleckých hnutí. Táto perspektíva je kľúčová pre rozvoj účinných protiteroristických stratégií a politík.

V právnej vede a v oblasti ľudských práv je extrémizmus často skúmaný z hľadiska jeho dopadu na právny poriadok a ochranu základných práv a slobôd. Tu sa kladie dôraz na to, ako môžu byť zákony a právne predpisy použité k obmedzeniu alebo potlačeniu extrémistických činností, zároveň s ohľadom na zachovanie demokratických princípov a práv jednotlivca.

Celkovo je dôležité uvedomiť si, že extrémizmus je komplexným javom, ktorý nie je možné jednoducho definovať alebo vysvetliť pomocou jedinej teórie alebo perspektívy. Jeho multidisciplinárna povaha vyžaduje integráciu rôznych prístupov a metodológií, aby bolo možné plne pochopiť jeho príčiny, prejavy a dopady na spoločnosť a medzinárodný systém.

Extrémizmus a terorizmus sú zložité a historicky hlboko zakorenené fenomény, ktorých vývoj a adaptácia na nové technológie predstavujú kľúčové oblasti výskumu. Zatiaľ čo extrémizmus zahŕňa extrémne politické, náboženské alebo ideologické názory, ktoré sú mimo hlavný prúd spoločenských presvedčení, terorizmus je definovaný ako používanie neoprávneného násilia a hrozby násilím, často motivovaných politickými, náboženskými alebo ideologickými cieľmi.[1] História terorizmu a extrémizmu siaha až do antiky a stredoveku, kde sa objavujú prvky podobné modernému terorizmu a extrémizmu.

S príchodom modernejších komunikačných technológií, ako sú telegraf a rádio, sa teroristické a extrémistické skupiny začali rozširovať a komunikovať na medzinárodnej úrovni. Príchod televízie umožnil týmto skupinám dosiahnuť široké publikum a vytvoriť obraz strachu a násilia.

Vstup do digitálnej éry priniesol ďalšiu zásadnú transformáciu. Internet a sociálne médiá umožnili šírenie posolstva, nábor nových členov a koordináciu útokov na celosvetovej úrovni. Digitálne platformy ponúkli anonymitu a rýchly prístup k veľkému množstvu ľudí, čo výrazne uľahčilo šírenie extrémistického obsahu.

Teroristické a extrémistické skupiny rýchlo prijali nové digitálne nástroje, vrátane šifrovanej komunikácie, sociálnych médií pre propagandu a nábor, a využitia internetových fór pre plánovanie a koordináciu. Tento trend je zjavný u mnohých skupín, od tradičných teroristických organizácií až po moderné extrémistické hnutia.

História terorizmu a extrémizmu tak predstavuje príbeh neustáleho vývoja a adaptácie. Digitálne technológie priniesli nové možnosti, ale zároveň vytvorili nové výzvy pre vlády a medzinárodnú spoločnosť v boji proti týmto hrozbám. Nasledujúce časti práce sa zamerajú na podrobnejšiu analýzu vplyvu digitálnych technológií na terorizmus a extrémizmus a na stratégie, ktoré by mohli byť využité na ich potlačenie v digitálnej ére.

2. VPLYV DIGITÁLNYCH MÉDIÍ A SOCIÁLNYCH SIETÍ

Digitálne médiá a sociálne siete majú kľúčový vplyv na moderný terorizmus a extrémizmus, poskytujúc platformy pre nábor, šírenie ideológií a koordináciu útokov. Táto časť sa zameriava na analýzu, ako teroristické a extrémistické skupiny využívajú tieto nástroje.

a) Nábor členov prostredníctvom sociálnych sietí

Teroristické a extrémistické skupiny využívajú sociálne siete ako efektívny nástroj na nábor nových členov. Vďaka širokej dostupnosti a vysokému dosahu týchto platforiem môžu tieto skupiny osloviť veľké množstvo ľudí. Často využívajú sofistikované marketingové techniky a prostriedky, ktoré rezonujú u určitých demografických skupín, najmä u mladých ľudí.

Nábor členov prostredníctvom sociálnych sietí je pre teroristické a extrémistické skupiny strategicky dôležitý. Využitie sociálnych sietí ako nástroja na nábor umožňuje týmto skupinám osloviť a zapojiť ľudí, ktorí by inak možno neboli vystavení ich ideológiám. Tento proces môžeme rozdeliť na niekoľko kľúčových aspektov:

- **Široká dostupnosť a dosah**: Sociálne siete ako Facebook, Twitter, Instagram, Telegram a ďalšie platformy majú obrovskú užívateľskú základňu, ktorá zahŕňa ľudí z rôznych kultúrnych a sociálno-ekonomických pozadí po celom svete. Toto poskytuje teroristickým a extrémistickým skupinám prístup k rozmanitému publiku.[21]

ISBN 978-80-561-1102-4

- **Cieľové demografické skupiny**: Tieto skupiny sa často zameriavajú na mladých ľudí, ktorí sú viac aktívni na sociálnych sieťach a môžu byť viac ovplyvniteľní. Tieto skupiny používajú algoritmy sociálnych médií na identifikáciu a cielenie na jednotlivcov alebo skupiny, ktoré by mohli byť otvorené ich posolstvám. Táto taktika je obzvlášť účinná pri oslovení osamelých alebo marginalizovaných jedincov, ktorí môžu hľadať pocit príslušnosti k určitej skupine.[2]
- **Sofistikované marketingové techniky**: Teroristické a extrémistické skupiny často používajú pokročilé marketingové stratégie podobné tým, ktoré využívajú komerčné značky. Tieto zahŕňajú vytváranie atraktívneho a presvedčivého obsahu, prispôsobené správy pre špecifické publikum a využitie vizuálnych a emocionálnych prvkov na vytvorenie silného posolstva.[29]
- **Vytváranie rezonujúceho posolstva**: Skupiny vytvárajú príbehy, ktoré sú navrhnuté tak, aby rezonovali s ich cieľovými demografickými skupinami. Tieto posolstvá môžu zahrňovať témy ako nespravodlivosť, diskrimináciu, hrdinstvo alebo odplatu. Cieľom je vzbudiť emocionálnu odozvu a pocit spojenia s ich prípadom.[35]
- **Interakcia a budovanie komunity**: Sociálne siete umožňujú týmto skupinám interagovať priamo s jednotlivcami, odpovedať na ich otázky a postupne ich vtiahnuť do svojich komunít. Tento osobný prístup môže byť veľmi účinný v budovaní dôvery a angažovanosti.

Nábor členov prostredníctvom sociálnych sietí má vážne dôsledky. Nielenže umožňuje týmto skupinám rýchlo a efektívne rozširovať svoje rady, ale tiež komplikuje úsilie vlád a bezpečnostných agentúr v identifikácii a monitorovaní týchto aktivít. Navyše, pretože táto forma náboru často zahŕňa sofistikované techniky maskovania a šifrovania, je ťažké tieto aktivity vystopovať a zastaviť.

b) Šírenie ideológie a propagandy

Sociálne médiá slúžia ako mocný nástroj na šírenie ideológie. Tieto platformy umožňujú skupinám šíriť svoje posolstvá bezprostredne a nekontrolovane, často prostredníctvom vizuálneho a emocionálneho obsahu, ako sú videá a obrázky. Ako už bolo spomenuté, tento obsah je navrhnutý tak, aby vzbudil silné emócie a presvedčil prijímateľov o legitímnosti ich konania.

Šírenie ideológie a propagandy prostredníctvom sociálnych médií je kľúčovou stratégiou teroristických a extrémistických skupín. Tieto platformy poskytujú jedinečnú príležitosť na efektívne šírenie ich posolstiev a názorov širokému publiku. Tento proces môžeme analyzovať prostredníctvom niekoľkých aspektov:

- **Bezprostrednosť a kontrola obsahu**: Sociálne médiá umožňujú skupinám šíriť obsah bez potreby sprostredkovateľov, ako sú tradičné médiá. Tento priamy prístup umožňuje skupinám úplnú kontrolu nad obsahom, tónom a načasovaním svojich správ. Vďaka tomu môžu efektívne šíriť svoje posolstvá a reagovať na aktuálne udalosti v reálnom čase.
- **Využitie vizuálneho a emocionálneho obsahu**: Teroristické a extrémistické skupiny často používajú vizuálny a emocionálny obsah, ako sú videá a obrázky, pretože tento typ obsahu má tendenciu byť atraktívnejší a má vyššiu pravdepodobnosť zdieľania medzi užívateľmi. Videá a obrázky môžu byť veľmi silné v prenášaní emócií a môžu byť navrhnuté tak, aby vzbudzovali reakcie ako hnev, súcit alebo pohoršenie.
- **Vytváranie silných emócií a presvedčenia**: Tento obsah je často navrhnutý tak, aby rezonoval s osobnými presvedčeniami a hodnotami cieľového publiká, čo zvyšuje pravdepodobnosť, že prijímateľ sa stotožní s posolstvom.
- **Interaktivita a angažovanosť**: Sociálne médiá umožňujú užívateľom interagovať s obsahom prostredníctvom komentárov, zdieľania a lajkovania. Táto interaktivita môže posilniť pocit spolupatričnosti a angažovanosti medzi prijímateľmi. Toto môže viesť k vytváraniu online komunít, kde sa zdieľajú a diskutujú ideológie a názory.
- **Personalizácia a mikrocielenie**: Sociálne médiá poskytujú možnosti pre personalizáciu obsahu a mikrocielenie určitých demografických skupín alebo jednotlivcov. Skupiny môžu využívať algoritmy sociálnych médií na zacielenie svojho obsahu na špecifické skupiny, ktoré sú najviac pravdepodobné, že ich posolstvo prjmú.[17]

ISBN 978-80-561-1102-4

Toto šírenie ideológie a propagandy má vážne dôsledky na sociálne a politické štruktúry spoločností. Môže viesť k radikalizácii jednotlivcov, šíreniu dezinformácií a polarizácii spoločnosti. Vlády a medzinárodné organizácie čelia výzve, ako efektívne monitorovať a regulovať šírenie extrémistického obsahu na sociálnych sieťach, zatiaľ čo zároveň zachovávajú slobodu prejavu a ochraňujú práva jednotlivcov.

c) Komunikácia a koordinácia

Digitálne médiá a sociálne siete umožňujú teroristickým a extrémistickým skupinám efektívne komunikovať a koordinovať svoje aktivity naprieč hranicami. Používajú šifrované komunikačné aplikácie, online fóra a iné digitálne nástroje na plánovanie útokov a koordináciu členov. Táto schopnosť operovať na medzinárodnej úrovni bez fyzickej prítomnosti výrazne zvyšuje ich dosah a nebezpečenstvo.

Komunikácia a koordinácia aktivít teroristických a extrémistických skupín prešli významnou transformáciou vďaka rozvoju digitálnych médií a sociálnych sietí. Tieto technológie poskytujú unikátne prostriedky pre efektívnu a rýchlu výmenu informácií, čo je nevyhnutné pre plánovanie a vykonávanie teroristických činov a extrémistických aktivít.

Jedným z kľúčových aspektov tejto transformácie je schopnosť týchto skupín operovať na medzinárodnej úrovni bez potreby fyzickej prítomnosti. Digitálne platformy im umožňujú prekračovať hranice a komunikovať s členmi a sympatizantmi po celom svete. Táto globálna pôsobnosť je zásadná pre šírenie ich vplyvu a dosahu. Kľúčovým nástrojom v tejto komunikácii sú šifrované komunikačné aplikácie. Aplikácie ako Signal, Telegram, a iné poskytujú vysokú úroveň zabezpečenia a súkromia, čo umožňuje členom týchto skupín komunikovať bez obáv z odpočúvania alebo sledovania zo strany vlád a bezpečnostných agentúr. Tieto aplikácie sú často využívané na koordináciu plánovania útokov, výmenu informácií o cieľoch a organizáciu logistiky.[36]

Online fóra a sociálne siete zohrávajú rovnako dôležitú úlohu. Sú používané na diskusie, šírenie taktických pokynov a výmennú platformu pre nápady a skúsenosti. Tieto platformy často slúžia ako virtuálne "tréningové tábory", kde noví členovia získavajú potrebné informácie a zručnosti. Táto možnosť virtuálneho vzdelávania a tréningu je obzvlášť alarmujúca, pretože umožňuje skupinám pripraviť svojich členov na teroristické činy bez potreby fyzického stretnutia. Okrem toho, digitálne nástroje ako sú chatovacie skupiny, e-mailové služby a cloudové úložiská sú využívané na uchovávanie a zdieľanie informácií, návodov na výrobu výbušnín, taktické manuály a propagačné materiály. Tieto zdroje sú ľahko dostupné a môžu byť anonymne zdieľané medzi veľkým počtom ľudí.[9]

Výsledkom je, že digitálne médiá a sociálne siete značne uľahčujú koordináciu a plánovanie teroristických a extrémistických aktivít. Táto schopnosť operovať na medzinárodnej úrovni bez fyzickej prítomnosti nielenže zvyšuje dosah a vplyv týchto skupín, ale tiež predstavuje značné výzvy pre globálnu bezpečnosť a protiteroristické snahy. Bezpečnostné agentúry musia vyvinúť nové stratégie a metódy na monitorovanie a boj proti týmto digitálne zosieťovaným hrozbám.

d) Vytváranie kontranaratívov a dezinformácií

Skupiny často využívajú digitálne platformy na šírenie dezinformácií a kontranaratívov, aby zmiatli protivníkov alebo diskreditovali svojich oponentov. Taktika zahŕňa falšovanie správ, šírenie konšpiračných teórií a manipuláciu s verejným vnímaním. Vyvíjanie kontranaratívov a šírenie dezinformácií predstavujú významnú taktiku, ktorú teroristické a extrémistické skupiny využívajú na digitálnych platformách. Tieto stratégie sú zamerané na zmetenie protivníkov, diskreditáciu oponentov a manipuláciu s verejným vnímaním, čo má za následok vytváranie neistoty a rozkolov v spoločnosti.

Jednou z kľúčových metód je falšovanie správ. Skupiny vytvárajú a šíria falošné správy alebo zavádzajúce informácie, ktoré sú navrhnuté tak, aby vyvolali pochybnosti alebo spochybnili pravdivosť oficiálnych zdrojov. Tieto falošné správy môžu byť veľmi presvedčivé a sú často šírené cez sociálne siete a iné online platformy, kde sa rýchlo rozšíria medzi veľkým počtom ľudí.[11]

Ďalšou metódou je šírenie konšpiračných teórií. Tieto teórie sú často založené na neoverených, zveličených alebo úplne vymyslených predpokladoch a sú zamerané na vytvorenie nedôvery medzi

ISBN 978-80-561-1102-4

verejnosťou voči vládam, inštitúciám alebo špecifickým skupinám ľudí. Konšpiračné teórie môžu byť atraktívne pre určité skupiny v spoločnosti, pretože ponúkajú alternatívne vysvetlenie udalostí alebo situácií, ktoré sa zdajú byť mimo ich kontrolu. Manipulácia s verejným vnímaním je tiež významnou časťou tejto taktiky. Teroristické a extrémistické skupiny využívajú digitálne médiá na vytváranie a šírenie posolstiev, ktoré podporujú ich ciele a ideológie, a často sú zamerané na vytvorenie pocitu nespravodlivosti, obete alebo hrdinstva spojeného s ich cieľom, čím sa snažia prilákať sympatie a podporu.[10]
Výzvou pri riešení týchto taktík je, že digitálne platformy poskytujú anonymitu a široký dosah, čo umožňuje rýchle a rozsiahle šírenie dezinformácií a kontranaratívov. Toto komplikuje úsilie vlád a medzinárodných organizácií v boji proti terorizmu a extrémizmu, pretože identifikácia a odstránenie falošného obsahu je často náročná a zložitá úloha. Rovnako je dôležité vyvážiť potrebu boja proti dezinformáciám a ochranu slobody prejavu a informácií.

e) Využitie algoritmov a mikrocielenia

Teroristické a extrémistické skupiny sa stávajú čoraz sofistikovanejšími v používaní algoritmov sociálnych médií na mikrocielenie svojich posolstiev. Využívajú dáta získané z užívateľského správania na platformách na cielenie osôb so zvýšenou pravdepodobnosťou záujmu o ich posolstvá. V posledných rokoch došlo k výraznému rozvoju v schopnostiach teroristických a extrémistických skupín využívať pokročilé digitálne technológie, najmä v oblasti algoritmického mikrocielenia na sociálnych sieťach. Táto evolúcia je dôsledkom prenikania technológií do každej sféry života, vrátane tých, ktoré sú využívané pre nelegálne a škodlivé účely.[25]
Algoritmy sociálnych médií sú navrhnuté tak, aby identifikovali a analyzovali vzorce v správaní a preferenciách užívateľov. Tieto informácie sú potom využívané na predstavovanie obsahu, ktorý je najrelevantnejší pre záujmy a správanie konkrétneho užívateľa. Teroristické a extrémistické skupiny využívajú tieto algoritmy na identifikáciu a cielenie na jednotlivcov, ktorí môžu byť náchylní k ich ideológii. Napríklad, ak niekto prejaví záujem o určité extrémistické témy alebo sa pohybuje v online komunitách s podobnými záujmami, algoritmy sociálnych médií môžu tohto užívateľa automaticky „označiť“ ako potenciálny cieľ pre mikrocielený obsah. Mikrocielenie je potom proces, kde sa na základe získaných dát vytvárajú špecificky prispôsobené správy alebo reklamy, ktoré sú zacielené priamo na tieto vybrané osoby. Takéto cielenie je oveľa efektívnejšie ako tradičné metódy, pretože obsah vidí osoba, ktorá je naňho najviac citlivá a pravdepodobne reaguje.[27]
Pri využívaní týchto algoritmov a mikrocielení teroristické a extrémistické skupiny teda nielenže dokážu šíriť svoje posolstvá efektívnejšie, ale tiež môžu zásadne ovplyvniť názory a správanie jednotlivcov bez ich vedomia. Tento prístup umožňuje skupinám budovať svoje siete rýchlejšie a diskrétnejšie, čo predstavuje významnú bezpečnostnú hrozbu. Využívanie algoritmov a mikrocielenia v rámci sociálnych médií tak vytvára nové výzvy pre bezpečnostné agentúry a vlády, ktoré sa snažia monitorovať a bojovať proti terorizmu a extrémizmu. Zároveň sa objavujú otázky týkajúce sa ochrany súkromia a etických aspektov zberu a využívania dát užívateľov. Tento vývoj vyžaduje vytváranie nových stratégií a prístupov, ktoré by reagovali na tieto sofistikované techniky šírenia extrémistických ideológií.

3. ANALÝZA DIGITÁLNYCH STÔP

3.1 VLASTNOSTI DIGITÁLNYCH STÔP

Digitálne stopy majú niekoľko charakteristických vlastností, ktoré sú zásadné pre ich využitie:

- **Nehmotnosť**: Sú virtuálne a nevyžadujú fyzický priestor pre uchovanie.
- **Latentnosť**: Môžu zostať skryté alebo neaktívne, až kým nie sú zistené alebo aktivované.
- **Časová trasovateľnosť**: Digitálne stopy môžu poskytnúť časový záznam o aktivitách.
- **Vysoká obsažnosť**: Obsahujú bohaté množstvo informácií.
- **Životnosť**: Môžu byť trvanlivé alebo krátkodobé v závislosti od povahy dát.
- **Uchovanie a kvalita**: Kvalita dát sa môže líšiť a uchovať sa môžu rôzne dlho.
- **Veľký dátový objem**: Môžu obsahovať veľké množstvo informácií.

ISBN 978-80-561-1102-4

- **Dátová hustota**: Majú vysokú úroveň detailov a informácií.
- **Extrémna dynamickosť**: Rýchlo sa menia a aktualizujú.
- **Komplexnosť a heterogénnosť**: Obsahujú rôzne typy dát.
- **Geografický rozsah**: Môžu pochádzať z rôznych geografických lokalít.
- **Ochrana dát**: Vyhodnotenie bezpečnosti a ochrany dát.
- **Identifikácia a spracovateľnosť**: Možnosť identifikovať a analyzovať dáta.
- **Zahladzovanie**: Možnosť odstrániť alebo zmeniť digitálne stopy.
- **Reštaurovateľnosť**: Možnosť obnoviť zmenené alebo odstránené dáta.
- **Originálnosť**: Jedinečnosť digitálnych stôp.
- **Súdna akceptácia**: Legálna platnosť a prijateľnosť digitálnych stôp ako dôkazu.[26]

3.2 VYUŽITIE DIGITÁLNYCH STÔP V BOJI PROTI TERORIZMU A EXTRÉMIZMU

Vlády a medzinárodné organizácie využívajú digitálne stopy na sledovanie a potláčanie teroristických a extrémistických aktivít nasledujúcim spôsobom:

a) **Monitorovanie komunikácie**: analyzujú komunikáciu na sociálnych sieťach, e-mailoch a iných online platformách.

Inovácie v oblasti digitálneho monitorovania predstavujú zásadný pokrok v používaní analytických nástrojov na predpovedanie budúcich udalostí. Tieto nástroje, ktoré efektívne využívajú existujúce administratívne dáta, hrajú kľúčovú rolu v identifikácii a predpovedaní rizikového správania, čím majú priamy dopad na boj proti terorizmu a extrémizmu.[24]

Jednou z hlavných vlastností týchto pokročilých analytických nástrojov je ich schopnosť integrovať a analyzovať obrovské množstvá administratívnych dát. Tieto dáta zahŕňajú, ale nie sú obmedzené na, súdne záznamy, policajné hlásenia a iné oficiálne dokumenty. Integrácia a analýza týchto dát umožňuje odkryť vzorce, ktoré môžu signalizovať možné rizikové správanie, ako napríklad plánovanie teroristických útokov.

Tieto nástroje využívajú komplexné algoritmy a techniky strojového učenia na analyzovanie a interpretáciu týchto dát, čím predpovedajú pravdepodobnosť rôznych druhov správania, vrátane potenciálnych teroristických činov.[23] Táto schopnosť predpovedania je nesmierne cenná pre bezpečnostné agentúry a vlády, pretože im umožňuje identifikovať a sledovať jednotlivcov alebo skupiny, ktoré by mohli predstavovať hrozbu. Vďaka týmto nástrojom môžu bezpečnostné agentúry lepšie identifikovať osoby náchylné k radikalizácii alebo tie, ktoré sú už aktívne zapojené do teroristických aktivít. Tento prístup nielen že zlepšuje efektívnosť bezpečnostných opatrení, ale tiež umožňuje efektívnejšie využívanie zdrojov pri monitorovaní a potlačovaní teroristických a extrémistických aktivít.

Celkovo vývoj a implementácia týchto inovatívnych analytických nástrojov, ktoré využívajú administratívne dáta na predpovedanie budúcich udalostí, predstavujú významný pokrok v boji proti terorizmu a extrémizmu. Tieto nástroje poskytujú vládam a bezpečnostným agentúram nové možnosti, ako efektívnejšie identifikovať a reagovať na potenciálne hrozby, čím prispievajú k zvýšenej bezpečnosti spoločnosti.

b) **Finančné transakcie**: Sledujú podozrivé finančné transakcie, ktoré môžu súvisieť s financovaním terorizmom.

Vlády a medzinárodné organizácie vyvinuli sofistikované systémy na monitorovanie a narušenie finančných transakcií súvisiacich s financovaním terorizmu. Toto úsilie je kľúčovou súčasťou širšej stratégie boja proti terorizmu. Program sledovania financovania terorizmu Ministerstva financií USA (TFTP) je významným príkladom. Tento program bol zahájený po útokoch z 11. septembra 2001 a jeho cieľom je identifikovať, sledovať a stíhať teroristov a ich finančné siete. Je súčasťou širšieho úsilia monitorovať pohyb teroristických financií a pomáhať pri odhaľovaní teroristických buniek a mapovaní ich sieti. Ministerstvo vnútornej bezpečnosti USA (DHS) tiež rozšírilo svoje schopnosti v tejto oblasti. Bojuje proti pašovaniu hotovosti, odstraňuje slabiny vo finančnom, obchodnom a dopravnom sektore a bojuje proti podvodom vo veľkom meradle. Napríklad Národné centrum DHS

ISBN 978-80-561-1102-4

pre pašovanie hotovosti zohráva kľúčovú úlohu pri identifikácii a narušení globálnych aktivít pašovania hotovosti.[7]
Ďalej vláda USA a medzinárodné agentúry prijali rad nástrojov na boj proti financovaniu terorizmu. Ako cielené sankcie, finančná regulácia a stratégie riadenia rizík. Cieľom nie je sledovať každý dolár, ale skomplikovať, predražiť a zvýšiť riziko pre teroristov pri získavaní a presúvaní peňazí. To zahŕňa odpojenie teroristov od globálneho finančného systému a nútenie ich k ťažkým rozpočtovým rozhodnutiam v dôsledku obmedzených zdrojov. Kľúčovým aspektom je využívanie finančnej inteligencie, alebo FININT. To zahŕňa zber viacerých finančných informácií, rozširovanie globálnych sietí na zdieľanie dát a porozumenie podozrivým finančným vzťahom. Táto inteligencia je kritická pre orgány aj súkromný sektor pri pochopení a reakcii na finančné riziká spojené s terorizmom.[40]
Teroristické organizácie často využívajú zmes nelegálnych aktivít a legitímnych finančných prostriedkov na financovanie. Využívajú moderné technológie ako blockchain a kryptomeny, ktoré im umožňujú financovať svoje aktivity diskrétnejšie, než by to bolo možné s tradičnými menami. Cieľom financovania terorizmu nie je len skrývať nelegálne peniaze, ale potlačiť populáciu alebo štáty prostredníctvom násilia a nátlaku. Na boj proti týmto výzvam vlády a organizácie vyvinuli opatrenia, ako sú finančné predpisy, dohľad, monitorovanie finančných transakcií a medzinárodnú spoluprácu. Tento komplexný prístup je nevyhnutný na identifikáciu a narušenie toku finančných prostriedkov teroristickým organizáciám.
Kancelária pre terorizmus a finančnú inteligenciu Ministerstva financií USA (TFI) vyvinula komplexný prístup, ktorý zahŕňa analýzu spravodajských služieb, správu a vymáhanie sankcií, finančné regulačné opatrenia a odborné znalosti v oblasti politiky, ako aj spoluprácu s medzinárodným spoločenstvom a finančným sektorom. Táto kancelária hrá vedúcu úlohu v boji proti financovaniu terorizmu a je jedinečná v tom, že je financovaná ministerstvom s takýmito schopnosťami.[42]
Celkovo je úsilie o sledovanie a narušenie financovania terorizmu viacdimenzionálne a zahŕňa kombináciu finančných predpisov, operačnej inteligencie a medzinárodnej spolupráce. Cieľom je oslabiť teroristické siete odrezaním ich zdrojov financovania, čím sa zníži ich schopnosť uskutočňovať útoky a udržiavať svoje operácie.

c) **Geolokačné dáta**: Využívajú geolokačné údaje na určenie pohybu podozrivých osôb.
Vlády a medzinárodné organizácie využívajú geolokačné dáta a iné digitálne stopy na sledovanie a potláčanie teroristických a extrémistických aktivít rôznymi spôsobmi. Jednou z metód je tzv. „risk terrain modeling“, ktorý identifikuje situačne a miestne rizikové faktory súvisiace s miestami, kde je pravdepodobné plánovanie alebo výskyt teroristických incidentov.[5]Táto metóda zohľadňuje špecifické aspekty fyzickej krajiny, ako sú umiestnenia budov alebo parkovísk. Tento prístup sa zameriava na dôležitosť lokality pri vysvetľovaní trestnej činnosti a terorizmu, čím sa líši od tradičných metód zameraných na sledovanie podozrivých osôb na základe demografických alebo iných charakteristík. Umožňuje lepšie pochopenie toho, ako sa širšie sociálne podmienky a špecifické interakcie prejavujú v konkrétnom fyzickom prostredí, čím zvyšujú alebo znižujú riziko teroristických aktivít v danom prostredí.
Ďalšou metódou je využívanie tzv. „open source intelligence“ (OSINT), ktorá zahŕňa analyzovanie verejne dostupných zdrojov, ako sú spravodajské novinky, teroristická propaganda a iné publikácie, na vytvorenie presného obrazu o teroristickej organizácii. s nárastom dostupnosti a prístupnosti verejných zdrojov sa OSINT stalo významným nástrojom v boji proti terorizmu. Táto metóda umožňuje výskumníkom OSINT vyhľadávať a pristupovať k tisícom lokálnych, národných a medzinárodných novín, časopisov a technických časopisov z ich počítačových terminálov. Internetové stránky teroristických skupín sú často plné propagandy a informácií o teroristických operáciách, technikách a lídroch, čo poskytuje cenné informácie pre protiteroristické úsilie.[15]Tieto metódy a nástroje poskytujú vládam a medzinárodným organizáciám lepšie nástroje na sledovanie a potláčanie teroristických a extrémistických aktivít, čím prispievajú k väčšej bezpečnosti a prevencii terorizmu.

ISBN 978-80-561-1102-4

d) **Analýza internetovej aktivity**: Preskúmavajú históriu prehliadania, vyhľadávania a iné online aktivity.

Vlády a medzinárodné organizácie čoraz viac využívajú analýzu internetovej aktivity na boj proti terorizmu a extrémizmu. Tento prístup zahŕňa monitorovanie online platforiem a koordináciu s technologickými spoločnosťami na identifikáciu a zmierňovanie hrozieb. Jednou z kľúčových výziev v tejto oblasti je obrovské množstvo a rozmanitosť online platforiem. Teroristické skupiny často využívajú mix platforiem pre rôzne účely: súkromnú koordináciu na šifrovaných chatovacích platformách, ukladanie propagandy na cloudových úložiskách a šírenie obsahu na populárnych sociálnych médiách pre širší dosah. Toto vyžaduje viacplatformový prístup na efektívne proti úsilie týmto aktivitám. Snaha organizácií ako Global Internet Forum to Counter Terrorism (GIFCT) a Tech Against Terrorism (TAT) bola kľúčové pri rozvíjaní viacplatformovej spolupráce.[37] To zahŕňa zdieľanie digitálnych odtlačkov teroristického obsahu, čo umožňuje platformám identifikovať a odstrániť takýto obsah efektívnejšie. Tieto iniciatívy sa tiež zameriavajú na vývoj rámcov reakcie na incidenty pre skutočné útoky s online prvkami, ako napríklad priamy prenos útokov.

Pokiaľ ide o využitie internetu teroristami, stal sa silným nástrojom pre komunikáciu, koordináciu, šírenie propagandy, získavanie financií a nábor. Počet teroristických webových stránok v posledných rokoch výrazne narástol, čo predstavuje výzvu pre vlády pri monitorovaní a kontrole týchto aktivít. Teroristické webové stránky môžu slúžiť ako virtuálne tréningové priestory, ponúkajúce návody na výrobu bômb, používanie protileteckých rakiet a iné škodlivé činnosti. Okrem toho uchovávajú propagačné videá na zvýšenie morálky a rozširovanie sietí na nábor a získavanie financií.Pri riešení týchto hrozieb sa vlády a organizácie snažia vyvážiť efektívne opatrenia proti terorizmu so zachovaním občianskych slobôd a súkromia. Komplexná a neustále sa vyvíjajúca povaha online teroristických aktivít to robí neustále náročným úlohou.[4]

Napokon, úloha organizácií ako RAND a podobných výskumných inštitúcií je významná pri poskytovaní systematickej analýzy a inovatívneho myslenia na pomoc vládnym agentúram, nadáciám a firmám v oblasti protiteroristických úsilí. Ich výskum zahŕňa rôzne oblasti, vrátane kybernetickej bezpečnosti, domácej bezpečnosti a národnej bezpečnosti, a prispieva cennými poznatkami do neustále sa meniacej krajiny online terorizmu a extrémistických aktivít.

e) **Koordinácia s technologickými firmami**: Spolupracujú s technologickými spoločnosťami na získanie dát a informácií.

Vlády a medzinárodné organizácie intenzívne spolupracujú s technologickými firmami na boji proti terorizmu a extrémizmu, a to najmä v online prostredí. Táto spolupráca sa sústreďuje na niekoľko kľúčových oblastí:

- **Využitie dát a analýza informácií:** Ako sa ukázalo na stretnutiach, ako je Deviata koordinačná schôdzka Výboru pre koordináciu globálnej protiteroristickej stratégie OSN[38], dôraz je kladený na využívanie dát a informácií na zlepšenie analýz a rozhodovania v kontexte boja proti terorizmu a násilnému extrémizmu. Cieľom je zabezpečiť, aby protiteroristické opatrenia boli presné a efektívne, pričom je dôležité, aby boli opatrenia založené na presných a relevantných údajoch a dôkazoch.
- **Riešenie terorizmu v online prostredí:** Výskum ukazuje, že teroristické a násilné extrémistické skupiny často využívajú viacero online platforiem na koordináciu svojich aktivít, ukladanie propagandistického materiálu a šírenie obsahu na populárnych sociálnych sieťach.[8]Toto vyžaduje celkový prístup, ktorý zahŕňa nielen veľké sociálne siete, ale aj menšie a menej regulované platformy. Dôležitým aspektom je spolupráca medzi rôznymi internetovými spoločnosťami a vládami na boji proti terorizmu a extrémizmu na internete.
- **Inovácie v protiteroristických technológiách:** OSN sa zameriava na využitie nových a vznikajúcich technológií na teroristické účely, ako sú bezpilotné lietadlá, umelá inteligencia, robotika, syntetická biológia, autonómne auta a 3D tlač. v rámci svojich rezolúcií Rada Bezpečnosti OSN zdôrazňuje potrebu vyvažovať podporu inovácií a zároveň zabrániť zneužitiu týchto technológií pre teroristické účely.[41]

ISBN 978-80-561-1102-4

- **Partnerské vzťahy proti terorizmu:** Interpol[34], ako globálna policajná organizácia, úzko spolupracuje s OSN a inými medzinárodnými subjektmi na implementácii rezolúcií OSN týkajúcich sa boja proti terorizmu. Toto zahŕňa výmenu informácií a spoluprácu v oblasti identifikácie teroristických podozrivých, prevencie teroristickej činnosti a sledovania financovania terorizmu.

V rámci týchto snáh je dôležité, aby bola dodržiavaná ochrana súkromia a ľudských práv. Vlády a medzinárodné organizácie by mali zabezpečiť, že ich protiteroristické opatrenia rešpektujú tieto základné princípy.

Tieto metódy umožňujú vládam a medzinárodným organizáciám efektívne reagovať na teroristické hrozby, identifikovať podozrivých a predchádzať potenciálnym útokom. Vďaka digitálnym stopám môžu bezpečnostné agentúry lepšie pochopiť vzorce správania teroristov a extrémistov, ich komunikačné siete, ako aj plánovanie a vykonávanie ich aktivít.

4. KYBERTERORIZMUS

Kyberterorizmus predstavuje významnú hrozbu pre medzinárodnú bezpečnosť, čo je zreteľne demonštrované v súčasných výskumných štúdiách a analýzach. Tento fenomén sa stáva čoraz naliehavejším problémom, keďže technologický pokrok umožňuje teroristickým skupinám a jednotlivcom využívať kybernetický priestor na uskutočňovanie svojich aktivít. Jedným z hlavných problémov kyberterorizmu je náročnosť pripisovania kybernetických útokov ich páchateľom. Útočníci môžu operovať z viacerých jurisdikcií, využívať pokročilé techniky na zamaskovanie svojho pôvodu alebo dokonca používať proxy servery na spustenie útokov. Táto nejasnosť v pripisovaní zločinov komplikuje efektívne reakcie a kladie otázky týkajúce sa zodpovednosti a uplatňovania medzinárodného práva.

Výzvou je tiež vytvorenie a udržanie medzinárodných noriem a predpisov, ktoré by regulovali kybernetický konflikt. Absencia univerzálne akceptovateľného právneho rámca špecificky prispôsobeného pre kybernetický konflikt komplikuje reakciu na kybernetické útoky. Je nevyhnutné rozvinúť medzinárodné normy a pravidlá konania, aby sa posilnila stabilita, odstrašenie a zodpovednosť v kybernetickom priestore.

Riešenie rizík spojených s kyberterorizmom si vyžaduje viacrozmerný prístup, vrátane posilnenia medzinárodnej spolupráce a zdieľania informácií, čo zvyšuje kolektívne obranné schopnosti. Investície do výskumu a vývoja umožňujú vytvárať robustnejšie kybernetické bezpečnostné systémy. Verejno-súkromné partnerstvá podporujú výmenu osvedčených postupov a podporujú inovácie. Rozvoj komplexných právnych rámcov a medzinárodných noriem usmerňuje správanie štátov v kybernetickom priestore. Posilnenie kybernetickej obrany a reakcie na incidenty minimalizuje dopad kybernetických útokov. Vzhľadom na významné výzvy, ktoré kybernetické vojny predstavujú pre medzinárodnú bezpečnosť, vrátane kyberšpionáže, kyberterorizmu a štátom podporovaných kybernetických útokov, je nevyhnutné, aby medzinárodné spoločenstvo prijalo proaktívny a spolupracujúci prístup. Týmto spôsobom je možné minimalizovať riziká spojené s kybernetickým vojnovým vedením a chrániť globálnu bezpečnosť v stále viac prepojenom svete.[20]

V kontexte výskumu ohrozenia kyberterorizmom a jeho dopadu na medzinárodnú bezpečnosť je dôležité zohľadniť aj aspekty týkajúce sa ochrany súkromia a etických dilem, ktoré sú neoddeliteľnou súčasťou tejto problematiky. Kyberterorizmus nielenže predstavuje priamu hrozbu pre medzinárodnú bezpečnosť, ale tiež kladie vážne otázky týkajúce sa ochrany osobných údajov a súkromia.

- **Ochrana súkromia v kyberpriestore:** Pri zavádzaní opatrení na boj proti kyberterorizmu je nevyhnutné zabezpečiť, aby boli rešpektované práva jednotlivcov na ochranu súkromia. Je dôležité nájsť rovnováhu medzi potrebou bezpečnosti a ochranou osobných údajov, aby nedošlo k ich zneužitiu.[13]
- **Etické dilemy v kyberbezpečnosti:** v oblasti kyberbezpečnosti existujú etické dilemy týkajúce sa rozsahu a spôsobu monitorovania a analýzy údajov. Otázky, ako "Ako ďaleko môžeme zasiahnuť do súkromia jednotlivca na základe predpovedí kyberteroristických hrozieb?" alebo "Aké dôsledky má neustále sledovanie digitálneho správania jednotlivcov?" sú kľúčové pre formulovanie eticky udržateľných prístupov kukyberbezpečnosti.

ISBN 978-80-561-1102-4

- **Zásady minimálnej nevyhnutnosti a transparentnosti:** Aplikácia zásad minimálnej nevyhnutnosti a transparentnosti pri vykonávaní monitorovacích a bezpečnostných opatrení môže pomôcť zmierniť potenciálne etické a právne problémy. To zahŕňa používanie len tých údajov, ktoré sú nevyhnutné pre konkrétny bezpečnostný účel, a zabezpečenie, že procesy zberu a analýzy dát sú pre občanov zrozumiteľné a transparentné.

Tieto aspekty poukazujú na potrebu multidisciplinárneho prístupu v boji proti kyberterorizmu, kde bezpečnostné stratégie musia byť vyvážené s ohľadom na právne a etické normy. Integrácia týchto aspektov do kyberbezpečnostných stratégií je nevyhnutná nielen pre zabezpečenie efektívnosti týchto opatrení, ale aj pre zachovanie dôvery a podpory zo strany verejnosti.

5. PRÍPADOVÉ ŠTÚDIE

Výskum a prípadové štúdie ukazujú, ako digitálne technológie ovplyvňujú teroristické a extrémistické aktivity. Najmä sociálne médiá ako YouTube, Facebook a Twitter sú využívané teroristickými skupinami na šírenie svojich posolstiev, nábor nových členov a zhromažďovanie informácií. Gabriel Weimann z University of Haifa zistil, že takmer 90% organizovaného terorizmu na internete prebieha prostredníctvom sociálnych médií. Teroristické skupiny využívajú sociálne médiá pre ich cenovú dostupnosť, široký dosah a možnosť rýchleho a neobmedzeného šírenia správ.[30]
Al-Káida a Islamský štát (ISIS) sú známe svojim rozsiahlym využívaním sociálnych médií. Al-Káida považuje komunikáciu za 90% úspechu svojej činnosti a využíva internet na dosiahnutie svojho globálneho publika. ISIS zase využívala šírenie správ na sociálnych médiách vo svoj prospech, najmä pri zverejňovaní videí s hrozbami a popravami. Tieto videá sú často vysoko kvalitné a zobrazujú brutálne činy, čo vyvoláva strach a manipuluje s verejným vnímaním. Al-Káida a Islamský štát (ISIS) skutočne výrazne využívali digitálne technológie, najmä sociálne médiá, na šírenie svojho vplyvu a dosiahnutie globálneho dosahu.[31] Tieto skupiny sa stali zvlášť známe svojou schopnosťou používať internet a sociálne siete na komunikáciu, propagandu, nábor a sieťovanie.
Al-Káida sa výrazne spoliehala na internet, ktorý sa stal hlavným nástrojom ich komunikácie, propagandy, náboru a sieťovania. v minulosti boli zaznamenané prípady, keď Al-Káida prevádzkovala približne 5 600 webových stránok a každý rok pribúdalo ďalších 900.[16] Tieto webové stránky existovali vo viacerých formátoch vrátane džihádistických webov, fór, chatovacích miestností, elektronických tabúľ a blogov. Táto sieť webových stránok bola využívaná na šírenie pokynov a informácií od vedenia skupiny k podporovateľom a sympatizantom po celom svete. Al-Káida otvorene uznávala dôležitosť internetu ako propagandistického nástroja.
Obe tieto skupiny demonštrovali vysokú úroveň sofistikovanosti vo využívaní digitálnych technológií na dosiahnutie svojich cieľov. Tento prístup ukazuje, ako môžu teroristické skupiny využívať moderné technológie na posilnenie svojho dosahu a vplyvu, čo predstavuje významnú hrozbu pre globálnu bezpečnosť.
Somálska teroristická skupina Al-Šabáb a nigerijská skupina Boko Haram tiež využívali sociálne médiá na šírenie svojich posolstiev. Al-Šabáb mala aktívny Twitter účet, kde pravidelne zverejňovala správy a získala tisíce sledovateľov. Po koordinovaných bombových útokoch v Nigérii v roku 2011 zverejnila Boko Haram video na YouTube na obhajobu svojich činov.[3]
Analýza prípadových štúdií, ako sú aktivity somálskej teroristickej skupiny Al-Šabáb, ukazuje komplexné využitie digitálnych technológií na šírenie terorizmu a extrémizmu. Al-Šabáb demonštrovala vysokú úroveň koherencie vo svojom mediálnom posolstve, pričom využívala rôzne digitálne platformy na šírenie svojej propagandy. Organizácia má štruktúrovaný prístup k sociálnym médiám, kde centralizované posolstvá sú opakované naprieč mnohými platformami, čo posilňuje ich "pravdivosť" a prezentuje Al-Šabáb ako dôveryhodnú alternatívu k súčasnej vláde.[33]
Al-Šabáb využíva viacero mediálnych zdrojov vrátane Al-Kataib Media Foundation, ktorá produkuje oficiálny audiovizuálny obsah, ako sú fotografie a videá. Tento obsah sa potom šíri cez online spravodajské stránky a sociálne médiá. Okrem toho používajú aj rozhlasové stanice a online spravodajské zdroje, ktoré sa tvária ako legitímne novinárske výstupy, na produkciu článkov podporujúcich povstalcov a súčasne informujú o širších somálskych, regionálnych a globálnych otázkach. V rámci sociálnych médií a spravodajských aplikácií Al-Šabáb uprednostňuje platformy ako

ISBN 978-80-561-1102-4

Telegram a Facebook, pričom sa rozširuje aj na ruskej sociálnej sieti OK.ru, ako aj na TikTok, X a YouTube. Skupina využíva sociálne médiá na distribúciu propagandy a načasovanie jej správ, čím vytvára komplexný mediálny zážitok, ktorý posilňuje ich posolstvo. Toto ukazuje na ich sofistikované technické porozumenie a využitie sociálneho mediálneho priestoru.[18]
Somálska vláda sa snažila obmedziť vplyv propagandy skupiny ako súčasť svojich proti ofenzívnych opatrení, vrátane zákazu používania Telegramu a TikToku, a varovala somálske spravodajské agentúry, že publikovanie obsahu Al-Šabáb, dokonca aj pre žurnalistické účely, by bolo považované za trestný čin. Avšak, tieto kroky mali obmedzený vplyv na online siete Al-Šabáb alebo na ich schopnosť komunikovať na týchto platformách.
Al-Šabáb si vytvorila svoj vlastný verejný priestor, v ktorom si prisvojila úlohu mediálneho výstupu prostredníctvom živého mikroblogovania. Táto stratégia umožňuje skupine šíriť svoju ideológiu a kontrolovať odôvodnenosť svojich útokov, čo poskytuje významné strategické výhody pri live pokrývaní, ktoré môžu viesť teroristickú skupinu k live tweetovaniu počas útoku.[39]
Analýza konkrétnych prípadov ukazuje, ako digitálne technológie ovplyvňujú extrémistické aktivity. Príkladom je organizácia Islamský štát (ISIS), ktorá efektívne využíva technologické inovácie na inšpirovanie a riadenie útokov na diaľku. Tieto operácie si nevyžadujú rozsiahlu prípravu ani taktické plánovanie a môžu byť vykonané jednoduchými prostriedkami, ako sú nože alebo autá, ktorými môže disponovať prakticky ktokoľvek. Kombinácia jednoduchých operácií a zvýšenej komunikačnej kapacity uľahčila prístup k terorizmu pre širokú verejnosť.
Významnou štúdiou v tomto kontexte je prípad Malajzie, ktorá poskytuje dôležitý príklad hrozby vzdialene inšpirovaných útokov. Tento jav je spôsobený rozšíreným prístupom k internetu, populárnymi šifrovanými komunikačnými službami, používaním VPN a potenciálnou skupinou veteránov, ktorí sa vrátili z bojiska v Sýrii, aby podnietili radikalizovaných jednotlivcov k akcii. Tieto technologické schopnosti, ako aj úmysel teroristov v krajine, poukazujú na potrebu, aby tvorcovia politík zohľadnili technologické podmienky pri predpovediach vznikajúcich ohnísk ISIS.[14]
Technologické schopnosti, ako prístup k internetu, umožňujú jednotlivcom pripojiť sa k extrémistickým skupinám alebo prijímať ich propagandu. Šifrované komunikačné služby a VPN poskytujú zvýšenú anonymitu a bezpečnosť, čo sťažuje prácu bezpečnostných služieb pri sledovaní a odhaľovaní plánovaných útokov. Prítomnosť veteránov z bojísk môže zas zvyšovať riziko radikalizácie, keďže tieto osoby môžu poskytovať výcvik, zdroje alebo inšpiráciu pre domáce útoky.
Táto štúdia naznačuje, že technologické faktory hrajú kľúčovú úlohu pri formovaní súčasnej podoby terorizmu. Preto je nevyhnutné, aby tvorcovia politík a bezpečnostné služby zohľadňovali tieto aspekty pri formulovaní stratégií v boji proti terorizmu. Analyzovanie a pochopenie spôsobu, akým extrémisti využívajú digitálne technológie, je zásadné pre efektívne predchádzanie a reagovanie na teroristické hrozby.
Tieto príklady jasne ukazujú, ako teroristické skupiny využívajú digitálne technológie na šírenie svojich ideológií, nábor nových členov a šírenie strachu. Poskytujú tiež dôležitý pohľad do súčasných výziev a stratégií, ktoré musia bezpečnostné agentúry a vlády používať pri boji proti týmto hrozbám.

6. BUDÚCE VÝZVY

Budúce výzvy a stratégie v boji proti digitálnemu terorizmu a extrémizmu budú zahŕňať riešenie stále sa vyvíjajúcich technológií a metodík, ktoré používajú teroristické a extrémistické skupiny. Vlády a medzinárodné organizácie budú musieť:
a) **Posilniť medzinárodnú spoluprácu:** Zvýšenie výmeny informácií a koordinácie medzi štátmi a medzinárodnými agentúrami je kľúčové pre efektívny boj proti cezhraničnému kyberterorizmu.To zahŕňa zvýšenie výmeny informácií a koordinácie medzi štátmi a medzinárodnými agentúrami. Efektívna spolupráca a komunikácia medzi rôznymi krajinami a organizáciami môže lepšie odhaľovať a reagovať na kybernetické hrozby, ktoré často prekračujú národné hranice. Integrácia a zdieľanie spravodajských údajov, bezpečnostných protokolov a najlepších praktík môže výrazne zlepšiť celkovú schopnosť reagovať na kyberteroristické útoky a predchádzať im.
b) **Investovať do pokročilých technológií:** Využitie umelej inteligencie, strojového učenia a analytických nástrojov na detekciu a neutralizáciu hrozieb. Tieto technológie umožňujú vládam a bezpečnostným agentúram efektívnejšie analyzovať veľké množstvá dát, identifikovať potenciálne

ISBN 978-80-561-1102-4

hrozby a reagovať na ne rýchlejšie a presnejšie. Umelá inteligencia a strojové učenie poskytujú možnosť rozpoznávať vzory a anomálie v správaní, ktoré by mohli naznačovať plánovanie teroristických činov alebo šírenie extrémistického obsahu. Tieto nástroje pomáhajú zlepšovať schopnosť predpovedať a predchádzať útokom ešte pred ich uskutočnením.

c) **Vzdelávanie a osvetové kampane:** V tomto zmysle sú vzdelávanie a osvetové kampane kľúčovými nástrojmi na zvyšovanie povedomia o rizikách a metódach digitálneho terorizmu a extrémizmu medzi občanmi. Tieto iniciatívy by mali byť zamerané na informovanie verejnosti o spôsoboch, akými môžu byť digitálne technológie využité pre extrémistické účely, vrátane náboru, šírenia propagandy a plánovania útokov. Vzdelávacie programy by mali zahŕňať informácie o tom, ako identifikovať a predchádzať potenciálnym hrozbám a ako bezpečne komunikovať online. Osvetové kampane by mali byť zamerané na rôzne vekové skupiny a komunity, aby zabezpečili široké oboznámenie sa s týmito problémami v celej spoločnosti.

d) **Vývoj právnych a regulačných rámcov:** Aktualizácia a harmonizácia zákonov a predpisov na medzinárodnej úrovni, aby reflektovali nové formy kyberterorizmu. Tento proces zahŕňa aktualizáciu a harmonizáciu existujúcich zákonov a predpisov na medzinárodnej úrovni, aby adekvátne reflektovali meniace sa technológie a metódy používané kyberteroristami.[28]

Je dôležité, aby tieto právne rámce boli flexibilné a schopné prispôsobiť sa rýchlo meniacemu sa digitálnemu prostrediu. Zároveň musia byť dostatočne robustné, aby poskytovali efektívne nástroje na prevenciu, detekciu a reakciu na kyberteroristické aktivity, zatiaľ čo zároveň zabezpečia ochranu základných práv a slobôd jednotlivcov. Medzinárodná spolupráca a koordinácia sú nevyhnutné pre dosiahnutie týchto cieľov, pretože kyberterorizmus nepozná hranice a vyžaduje si globálny prístup.

e) **Zabezpečenie súkromia a ochrana občianskych slobôd:** Vyváženie bezpečnostných opatrení s ochranou súkromia a občianskych práv. Je potrebné nájsť rovnováhu, ktorá zabezpečí efektívnu ochranu proti hrozbám, a zároveň udrží ochranu súkromia a občianskych práv. To si vyžaduje transparentnosť a zodpovednú kontrolu pri zbere a analýze údajov, ako aj jasné zákonné a etické rámce, ktoré určujú hranice povolených bezpečnostných opatrení. Takýto prístup pomáha zabezpečiť, že protiteroristické aktivity sa nezvrhnú do nadmerného dohľadu alebo porušovania základných práv jednotlivcov.

Tieto stratégie by mali byť prispôsobené dynamickému a rýchlo sa meniacemu charakteru digitálneho terorizmu a extrémizmu, a zároveň by mali zohľadňovať rôznorodosť a zložitosť globálneho kybernetického prostredia.

ZÁVER

Výskumy ukazujú, že teroristické skupiny intenzívne využívajú digitálne technológie na šírenie svojich ideológií, nábor nových členov a koordináciu útokov. Napríklad, využitie sociálnych médií, šifrovaných komunikačných aplikácií ako WhatsApp a Telegram, a anonymizačných nástrojov ako TOR, umožňuje teroristom efektívne šíriť svoj vplyv a chrániť svoje komunikácie pred odhalením.

Okrem toho, nové technológie ako umelá inteligencia, robotika, syntetická biológia, samoriadiace autá a 3D tlač prinášajú nové možnosti aj pre teroristické útoky. Teroristi môžu využiť napríklad drony na útoky alebo sa pokúsiť vytvoriť domáce biologické zbrane. Zároveň sa ale objavujú nástroje a stratégie, ktoré pomáhajú v boji proti terorizmu. Napríklad, využitie AI a kvantového výpočtu môže pomôcť v rýchlejšom identifikovaní a blokovaní teroristického obsahu online.

Je dôležité zdôrazniť, že prijímanie opatrení na boj proti terorizmu musí byť v súlade s medzinárodnými ľudskými právami. Medzinárodná spoločnosť a štáty by mali pokračovať v spolupráci a zdieľaní informácií, aby dokázali efektívne čeliť využívaniu digitálnych technológií pre teroristické účely, pričom by mali zabezpečiť ochranu základných ľudských práv a slobôd.

V kontexte tejto práce je dôležité uvedomiť si, že digitálne technológie nie sú len prostriedkom šírenia terorizmu, ale ponúkajú aj mocné nástroje na jeho detekciu a potlačenie. Kľúčovým aspektom je nájsť rovnováhu medzi využívaním týchto technológií na zlepšenie bezpečnosti a ochranou súkromia a ľudských práv. To si vyžaduje kontinuálne úsilie zo strany vlád, medzinárodnej spoločnosti a súkromného sektora v rozvoji etických a efektívnych protiteroristických stratégií.

ISBN 978-80-561-1102-4

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] Berger, J.M. (2018). Extremism. Cambridge, Vydavateľstvo: MA: The MIT Press. ISBN 9780262535878. Dostupné na: https://doi.org/10.7551/mitpress/11688.001.0001.

[2] Berger, J.M. (2015) 'How terrorists recruit online (and how to stop it)', Dostupné na: https://www.brookings.edu/articles/how-terrorists-recruit-online-and-how-to-stop-it/.

[3] Besenyő, J. &Sinkó, G. (2021) 'The social media use of African terrorist organizations: a comparative study of Al-Qaeda in the Islamic Maghreb, Al-Shabaab and Boko Haram', Insights into Regional Development, 3(3), str. 66-78. https://doi.org/10.9770/IRD.2021.3.3(4)

[4] Bradley, A. a Gleeson, C., 2023. Trends in Terrorist Use of the Internet in 2022. Vydavateľstvo: GNET. Dostupné na: https://gnet-research.org/2023/02/27/trends-in-terrorist-use-of-the-internet-in-2022/ [prístupné dňa 2. februára 2024].

[5] Caplan, J.M. &Kennedy, L.W. (2016). Risk Terrain Modeling: Crime Prediction and Risk Reduction. University of California Press. Dostupné na: https://www.ucpress.edu/book/9780520282933/risk-terrain-modeling. https://doi.org/10.1525/9780520958807

[6] (2002). TheLessons of Terror: a History of Warfare Against Civilians: Why It Has Always Failed and Why It Will Fail Again. New York: Random House. ISBN: 978-0375508431

[7] D'Souza, J. (2012). Terrorist Financing, Money Laundering, and Tax Evasion: Examining the Performance of Financial Intelligence Units. 1st ed. CRC Press. ISBN 9781439828502

[8] Evans, Alexandra T. and Heather J. Williams, How Extremism Operates Online: a Primer. Santa Monica, CA: RAND Corporation, 2022. https://doi.org/10.7249/PEA1458-2

[9] Evans, A.T. a Williams, H.J. (2022) "How Extremism Operates Online: A Primer". Santa Monica, CA: RAND Corporation. Dostupné na https://www.rand.org/pubs/perspectives/PEA1458-2.html

[10] Farrell, L. (2022). UMD Report: Conspiracy theories fueled more terror attacks in 2020. University of Maryland's National Consortium fort he Study of Terrorism and Responses to Terrorism (START). Dostupné na: https://www.start.umd.edu/news/umd-report-conspiracy-theories-fueled-more-terror-attacks-2020

[11] Glasser, T.L., Zou, S., Varma, A., Gilpin, D.R., Doty, C., Pickard, V., Schulte, S.R., George, C., Levinson, P., Faltesek, D., Massanari, A., Burroughs, B., Thornton, L.-J., Bowman, N.D., Cohen, E., Polage, D. (2020). Fake News: Understanding Media and Misinformation in the Digital Age. Vydavateľstvo: The MIT Press. https://doi.org/10.7551/mitpress/11807.001.0001

[12] Charvát, J. (2017) 'Pojem extremismus a jeho aktuální možnosti použití v České republice', Bezpečnostní teorie a praxe, 2, str. 91-94. Dostupné na: https://veda.polac.cz/wp-content/uploads/2018/11/022017Pojem-extremismus-a-jeho-aktu%C3%A1ln%C3%AD-mo%C5%BEnosti-pou%C5%BEit%C3%AD-v-%C4%8Cesk%C3%A9-republice1.pdf

[13] Christen, M., Gordijn, B., &Loi, M. (Eds.). (2020). The Ethics of Cybersecurity. Springer Nature. https://doi.org/10.1007/978-3-030-29053-5

[14] Harrison, S. (2018) Evolving Tech, Evolving Terror. Center for Strategic and International Studies. Dostupné na: https://www.csis.org/analysis/evolving-tech-evolving-terror

[15] Hassan, N.A. & Hijazi, R. (2018). Open Source Intelligence Methods and Tools. 1st ed. [ebook] Springer. https://doi.org/10.1007/978-1-4842-3213-2

[16] Hassan, I. (2007) Al Qaeda-linked Web sitesnumber 5,600 - researcher, Reuters, 4 December. Dostupné na: https://www.reuters.com

[17] Jensen, M., James, P., LaFree, G., Safer-Lichtenstein, A., &Yates, E. (2018). "The Use of Social Media by United States Extremists." START, College Park, Maryland. Dostupné na: https://www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf

[18] Khalil, J., Abdi, Y., Glazzard, A., Nor, A.A., &Zeuthen, M. (2023) Reaching Behind Frontlines: Promoting Exit from al-Shabaabthrough Communications Campaigns. Washington, DC: RESOLVE Network. Dostupné na: https://doi.org/10.37805/lpbi2023.2

[19] Makariusová, R. (2019). Globální terorismus a radikální hnutí. Aleš Čeněk, str. 13, ISBN: 978-80-7380-777-1
[20] Montasari, R. (2024). Exploring the CurrentLandscape of Cyberterrorism: Insights, Strategies, and theImpact of COVID-19. In: Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-50454-9_5
[21] National Institute of Justice (2017) 'The Role of SocialMedia in the Evolution of Al-Qaeda-Inspired Terrorism', Dostupné na: https://nij.ojp.gov/topics/articles/role-social-media-evolution-al-qaeda-inspired-terrorism.
[22] Ó hAdhmaill, F., Ritchie, M., McCann, G., and Ó hAdhmaill, F. (2020) 'Conflict, 'Terrorism' and Non-State Actors', in International Human Rights, Social Policy and Global Development. Bristol University Press, str. 141-154. https://doi.org/10.46692/9781447349228.013
[23] Pilley, P. (2017). Predictive Analytics: Putting the Pieces Together for Counter Terrorism. 1st ed. LAP LAMBERT Academic Publishing. ISBN 9783659821578.
[24] Rassler, D. (2021). Data, AI, and the Future of U.S. Counter terrorism: Building an Action Plan. Combating Terrorism Center at West Point. Dostupné na: https://ctc.westpoint.edu/commentary-data-ai-and-the-future-of-u-s-counterterrorism-building-an-action-plan/
[25] Reed, A., Whittaker, J., Votta, F. a Looney, S., 2019. Radical Filter Bubbles: Social Media Personalisation Algorithms and Extremist Content. Royal United Services Institute. Dostupné na: https://rusi.org/explore-our-research/publications/special-resources/radical-filter-bubbles-social-media-personalisation-algorithms-and-extremist-content
[26] RAK, R. PORADA, V. Podrobná charakteristika špecifických vlastností digitálnych stôp. In: Bezpečnostní teorie a praxe. č. 1, ISSN 1801-8211, 2005, zdroj: SUROVČÍKOVÁ, M. Kriminalistické skúmanie digitálnych stôp a možnosti dokazovania: rigorózna práca. Bratislava: Akadémia PZ, 2007. str. 71
[27] Schindler, J.R., 2021. Flaws in the Algo: How Social Media Fuel Political Extremism. Psychology Today. Dostupné na: https://www.psychologytoday.com/us/blog/our-digital-selves/202102/flaws-in-the-algo-how-social-media-fuel-political-extremism
[28] Trachtman, J.P., Grady, M.F., and Parisi, F. (eds) (2009) Global Cyberterrorism, Jurisdiction, and International Organization. In: The Law and Economics of Cybersecurity. Cambridge University Press. Dostupné na: https://doi.org/10.1017/CBO9780511511523.009
[29] Ward, A. (2018) 'ISIS's Use of Social Media Still Poses a Threat to Stability in the Middle East and Africa'. Dostupné na: https://www.rand.org/blog/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html.
[30] Weimann, G. (2006) Terror on the Internet: The New Arena, The New Challenges. United States: United States Institute of Peace Press. ISBN 9781929223718.
[31] Winkler, C.K. and El Damanhoury, K., 2022. Proto-State Media Systems: The Digital Rise of Al-Qaeda and ISIS. New York, NY: Oxford University Press. ISBN 9780197568026. https://doi.org/10.1093/oso/9780197568026.001.0001
[32] Carr, C., (2002). The Lessons of Terror: a History of Warfare Against Civilians: Why It Has Always Failed and Why It Will Fail Again. New York: Random House. ISBN: 978-0375508431

OSTATNÉ ZDROJE

[33] Combating Terrorism Center at West Point. The Online Frontline: Decodingal-Shabaab's Social Media Strategy. Dostupné na: https://ctc.westpoint.edu/the-online-frontline-decoding-al-shabaabs-social-media-strategy/
[34] Interpol. (n.d.). Today's priorities for INTERPOL-United Nations collaboration. Dostupné na https://www.interpol.int
[35] Middle East Institute (n.d.) 'ISIS and the Institution of Online Terrorist Recruitment'. Dostupné na: https://www.mei.edu/publications/isis-and-institution-online-terrorist-recruitment.

ISBN 978-80-561-1102-4

[36] Privacy International, 2022. SecuringPrivacy: PI on End-to-End Encryption. London: Privacy International. Dostupné na: https://privacyinternational.org.

[37] Tech Against Terrorism. (2024). About Us. Dostupné na: https://techagainstterrorism.org/about

[38] United Nations. 2023. Remarks at the Ninth Meeting of the United Nations Global Counter-Terrorism Coordination Compact. Dostupné na: https://www.un.org/counterterrorism/events/ninth-meeting-united-nations-global-counter-terrorism-coordination-compact

[39] U.S. Army Command and General Staff College. (2023) Tweeting Terror Live: Al-Shabaab's Use of Twitter during the Westgate Attack and Implications for Counter terrorism Communications. Dostupné na: https://www.armyupress.army.mil

[40] U.S. Department of State, n.d., 'Terrorism Finance', U.S. Department of State, Dostupné na: https://www.state.gov/bureaus-offices/bureaus-and-offices-a-to-z-index/bureau-of-economic-and-business-affairs/office-of-threat-finance-countermeasures/

[41] UN News. (2022) UN Security Council boosts commitment to fight digital terror. Dostupné na: https://news.un.org/en/story/2022/10/1129467

[42] U.S. Government Accountability Office, 2009. Combating Illicit Financing: Treasury's Office of Terrorism and Financial Intelligence Could Manage More Effectively to Achieve Its Mission. Dostupné na: https://www.gao.gov/products/gao-09-794

[43] Vienna Declaration and Programme of Action Adopted by the World Conference on Human Rights in Vienna on 25 June 1993, Dostupné na: https://www.ohchr.org/sites/default/files/vienna.pdf