УНИВЕРЗИТЕТ „СВ. КИРИЛ И МЕТОДИЈ“
ФИЛОЗОФСКИ ФАКУЛТЕТ – СКОПЈЕ

Институт за безбедност, одбрана и мир
двегодишни магистерски студии на насока Безбедност 120 ЕКТС

КОНЦЕПТУАЛИЗАЦИЈА НА ХИБРИДНИТЕ ЗАКАНИ И НИВНОТО ВЛИЈАНИЕ ВРЗ БЕЗБЕДНОСТА НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

магистерски труд

Ментор:
проф. д-р Тања Милошевска

Кандидат:
Виктор Струминиковски

Скопје, 2024

С О Д Р Ж И Н А

1. Вовед

Овој магистерски труд има за цел да развие сеопфатен концептуален модел на хибридни закани и да го анализира нивното влијание врз безбедноста во Република Северна Македонија. Хибридните закани, кои се карактеризираат со нивната повеќедимензионална и асиметрична природа, претставуваат значителни предизвици за безбедноста на нациите. Република Северна Македонија, како географски стратегиска локација со сложен историски контекст, се соочува со уникатни безбедносни предизвици во современото глобално опкружување. Ова истражување го испитува развојот на пејзажот на хибридните закани и нивните потенцијални последици врз безбедноста и стабилноста на Република Северна Македонија. Студијата користи квалитативни и квантитативни методологии за да ги идентификува и процени најраспространетите хибридни закани што ја засегаат земјата. Врз основа на овие наоди, концептуалниот модел ќе понуди увид и препораки за подобрување на отпорноста и одговорот на Република Северна Македонија на хибридните закани.

Глобалните проблеми се појавуваат и ги надминуваат националните граници и ги совладуваат капацитетите на индивидуалните нации држави, а националните држави сè повеќе стануваат ранливи и предмет на надворешно продирање. Најпрвин, важно е да се спомене дека без имплементација секоја стратегија за одбрана од хибридни закани е бескорисна. Тоа е всушност и почетното позиционирање на овој труд, да понуди решенија кои треба да се имплементираат со молскавична брзина, за полека, но сигурно да се обезбеди бариера и отпорност кон асиметрични и хибридни закани.

Процесот на глобализација, ги заостри и влоши голем број од старите проблеми на меѓународната безбедност и предизвика нови ризици и предизвици. Тие се тероризмот и сепаратизмот, националните, религиозните и другите форми на екстремизам, трговијата со дрога и организираниот криминал, регионалните конфликти, заканата од пролиферацијата на оружјето за масовно уништување, финансиските и економските кризи, еколошките катастрофи и епидемии. Сите овие проблеми егзистираа претходно, но во ерата на глобализација, кога светот стана повеќе поврзан и меѓузависен, тие забрзано стекнаа универзален карактер и

станаа реална закана за регионалната и меѓународната безбедност.[1]

Во ЕУ доминантно се користи терминот „хибридни закани“, додека во НАТО е позастапено користењето на терминот „хибридно војување“, а од страна на Руската Федерација се користат термините „обоени револуции“ и „хибридна војна“. Покрај обврската за колективна одбрана, Република Северна Македонија, како НАТО членка, има обврска да гради и да одржува адекватна цивилна подготвеност и отпорност. Градењето отпорност е во согласност со членот 3 од Северноатлантскиот договор, односно со обврската за колективно и индивидуално развивање капацитети за одговор на каква било форма на закана или криза.[2] Во сите случаи, станува збор за истата закана кон националната безбедност. Новиот хибриден начин на војување се базира на асиметрични воени методи и многу активности кои се одвиваат во сајбер-просторот, што е причина сајбер-просторот сè почесто да се дефинира како петта димензија на војување. Дезинформациите обично претходат на операции од арсеналот на хибридни закани. НАТО активно ги следат дезинформациите и пропагандните кампањи и од државни и од недржавни чинители. Континуираното инвестирање во градењето на способностите и капацитетите за ефективна сајбер-одбрана ќе обезбеди квалитетни и технолошки развиени институции кои ќе можат ефикасно и ефективно да се справуваат со предизвиците во сајбер-просторот.[3]

1.1 Формулација на проблемот

Формулирањето на истражувачкиот проблем во овој магистерски труд произлезе од истражувањето на повеќестраниот феномен на хибридните закани и нивното влијание врз безбедноста на Република Северна Македонија.

---

[1] Милошевска, Т. (2007). *Нетрадиционални и глобални безбедносни закани*, Годишен Зборник, Филозофски факултет, Скопје, стр. 580.

[2] Влада на Република Северна Македонија, Министерство за одбрана (април 2021). *Национална Стратегија за градење на отпорност и справување со хибридни закани,* стр. 4.

[3] Влада на Република Северна Македонија, Министерство за одбрана (февруари 2020 г.). *Стратегија за сајбер-одбрана*, стр. 18.

Истражувачкиот проблем е вкоренет во препознавањето на еволутивната природа на безбедносните предизвици со кои се соочува земјата, кои се карактеризираат со мешање на конвенционални и неконвенционални тактики, кои опфаќаат политички, воени, економски, социјални и сајбер-домени.

Оваа студија има за цел да ги опфати следните три клучни компоненти: *идентификување актери, домени, модели за спротивставување и фази*, нивните специфични манифестации во контекст на Република Северна Македонија, *разбирање на ранливостите* и *предлагање ефективни стратегии за отпорност и ублажување* со цел зајакнување на националната безбедност.

Дополнително, истражувањето има за цел да ги истражи минатите инциденти со хибридни закани преку низа на методи и техники за да го анализира нивното влијание врз безбедносниот пејзаж на земјата и, последователно, да генерира препораки за политики со цел градење сеопфатни планови за одговор, зајакнување на јавната свест, промовирање едукација и поттикнување мултилатерални безбедносни партнерства. Со адресирање на овие аспекти, истражувањето се труди да придонесе за вредни сознанија кои можат да им помогнат на креаторите на политики, безбедносните практичари и засегнатите страни во заштитата на идните безбедносни интереси на Република Северна Македонија.

Формулирањето на истражувачкиот проблем се соочи со два главни предизвици: (1) сложеноста во определувањето на опсегот на поимот хибридни закани воопшто, така и во контекст на анализираниот концептуален модел на хибридните закани и (2) определување на импликациите на хибридните закани врз безбедноста на Република Северна Македонија. Термините како „хибрид“, „сиво“, „асиметричен“, „неурамнотежен“ и „неконвенционален“ се користат паралелно за да се опишат овие закани, но нивната заменлива употреба и недостатокот на консензус на терен во прегледот на литературата го отежнаа прецизното дефинирање на опсегот на истражувачкиот проблем. Дополнително, различните толкувања на овие термини на меѓународно и европско ниво ја комплицираа задачата.

Понатаму, еволуирачката и динамична природа на меѓународната средина по ерата на Студената војна додаде сложеност на истражувачкиот проблем.

Појавата на сивата зона и правната несигурност ја предизвикаа адекватноста на постојните правни алатки, процедури и институции дизајнирани првенствено за решавање на контроверзиите за време на Студената војна. Разбирањето како овие постојни правни инструменти би можеле да се приспособат за да се спротивстават на сложените и тајните операции во сивата зона бара внимателно испитување. Згора на тоа, инхерентната сложеност и суптилност на хибридните закани, кои често функционираат во доменот помеѓу „легалното“ и илегалното“, беа дополнителен предизвик да се одредат соодветните правни одговори.

Политичкиот пејзаж во Република Северна Македонија доживеа значителни промени, вклучувајќи договори со соседните земји, референдуми и членство во НАТО, што доведе до поларизација врз основа на партиски, етнички или верски припадности. Формулирањето истражувачки проблем среде овие повеќеслојни политички процеси беше предизвик поради нивните интеракции и меѓусебна поврзаност, што го отежнува изолирањето на конкретни фактори за истражување. Појавата на хибридни напади, како што се сајбер-нападите врз критичните институции како Народната банка и министерствата, потоа училиштата и други институции предизвика загриженост за стабилноста на земјата. Истражувањето на врската помеѓу политичките процеси и хибридните напади е сложено и чувствително. Продолженото вето од Бугарија во однос на интеграцијата на Република Северна Македонија во ЕУ додава дополнителна комплексност. Разбирањето на неговото влијание врз политичката динамика и јавната перцепција бара разгледување на историски, културни и геополитички контексти. Влијанието на надворешните сили, како Русија, врз политичкиот пејзаж на земјата и ставовите на ЕУ покренува прашања за нивните мотиви и тактики. Истражувањето на странското мешање и неговите ефекти врз националната политика бара сигурни податоци и длабоко разбирање на динамиката на меѓународните односи. Дезинформациите и недостатокот од медиумската писменост кај граѓаните создаваат предизвици во решавањето на основните причини за појава на дел од хибридните закани. Истражувањето на интеракцијата меѓу образованието, медиумската консумација и политичкиот ангажман бара внимателни методологии. Проблемот со ограниченото учество на младите и аспирациите за емиграција наложуваат разбирање на факторите кои

придонесуваат за сили на раздвојување и конфликт во општеството и бараат итно предлагање стратегии за зајакнување на нивната политичка вклученост.

Накратко, во текот на истражувањето беа потребни претпазливост, ригорозни методологии и разгледување различни контексти. Решавањето на овие предизвици бараше темелно испитување на постојната литература, стручни сознанија и внимателна анализа на постојано-менливиот меѓународен пејзаж за да се биде сигурен дека истражувачкиот проблем адекватно ќе ја долови повеќеслојната природа на хибридните закани, ќе го определи концептуалниот модел и ќе ги истражи импликациите на безбедносната состојба во Република Северна Македонија.

1.2. Истражувачко прашање

Магистерскиот труд има за цел да одговори на следните прашања:

- Како моделот на сеопфатен екосистем за отпорност (CORE) и „Hybridity Blizzard“ – модел на снежна бура ги подобрува разбирањето и одговорот на хибридните закани, особено во однос на донесувањето одлуки, тековите на информации, меѓузависноста помеѓу различните домени, заштитата на демократските основи и воспоставувањето секторска отпорност?
- До кој степен официјалните сознанија за хибридните закани во Стратегијата за одбрана и Стратегијата за градење отпорност и справување со хибридни закани влијаат врз развојот на капацитетите и способностите за одговор на овие закани во Република Северна Македонија?
- Како усвојувањето на Националната стратегија за градење отпорност и справување со хибридни закани од страна на Република Северна Македонија, соработката со НАТО во безбедносниот сектор и учеството во меѓународните иницијативи како „Сајбер-коалиција“ придонесе за спротивставување и ублажување на хибридните закани, конкретно фокусирајќи се на дезинформации кампањи и напади со дистрибуирано одбивање на услугата

(DDoS) и колку овие мерки биле ефективни во зајакнувањето на институционалната отпорност и заштитата на поединците во земјата?

- Како потенцијалните хибридни закани, кои опфаќаат дезинформации, сајбер-напади врз критични институции и надворешни влијанија како ветото на соседна Бугарија и прашања поврзани со европската интеграција, влијаат врз безбедноста на Република Северна Македонија, управувањето со институциите и довербата на граѓаните во институциите и кои се мерките и стратегиите потребни за ефикасно спротивставување и ублажување на овие закани за да се обезбедат стабилност и демократска отпорност во земјата?
- Како хибридните закани влијаат врз безбедноста на Република Северна Македонија преку поткопување на демократските институции, манипулирање со процесите на одлучување и создавање каскадни ефекти преку искористување ранливости во различни домени?
- Кои се клучните бариери и можности со кои се соочуваат македонските заедници во справувањето со дезинформациите и како може да се применат систематски пристапи за справување со овие предизвици, особено во контекст на техничките фактори и факторите водени од профитот, намалената релевантност на локалните вести и високополитизираните медиуми?

1.3. Цели и задачи

Научна цел:

Научната цел на овој магистерски труд е да ги истражи концептот на хибридни закани и нивните импликации врз безбедноста на Република Северна Македонија. Тој се стреми да разбере како координираните активности на државните или недржавните актери можат да ги поткопаат демократските институции преку искористување на ранливостите во различни домени. Истражувањето има за цел да обезбеди вредни сознанија за сложеноста на хибридните закани и да предложи ефективни стратегии за зајакнување на отпорноста против нив. Со цел зачувување на демократските вредности и

процесите на донесување одлуки, студијата има намера да придонесе за способноста на државата да се спротивстави и да ги ублажи повеќестраните предизвици што ги носат хибридните закани. На крајот на краиштата, тезата се стреми да ја подобри безбедносната положба на земјата и да ги заштити нејзините демократски темели од потенцијална штета предизвикана од овие еволуирачки и двосмислени закани.

Практична цел:

Водејќи се од научната цел на ова истражување, произлегоа следните практични цели:

- ✓ Практичната употреба на овој магистерски труд лежи во неговата способност да ги информира креаторите на политики, безбедносните професионалци и релевантните чинители во Република Северна Македонија за природата и импликациите на хибридните закани.

- ✓ Со стекнување сеопфатно разбирање за хибридните закани и нивното влијание врз безбедноста на земјата, носителите на одлуки можат да развијат приспособени и ефективни стратегии за да се спротивстават на таквите закани.

- ✓ Увидите обезбедени од ова истражување можат да помогнат во развојот на насочени политики и мерки за зајакнување на отпорноста на демократските институции и заштита на критичната инфраструктура од потенцијални хибридни напади.

- ✓ Да биде водич во распределбата на ресурсите за да се решат одредени ранливости и да се подобри координацијата меѓу различни сектори за подобро да се одговори на хибридните предизвици.

- ✓ Понатаму, тезата може да послужи како основа за подигање на свеста кај граѓаните и организациите за ризиците од хибридните закани. Може да промовира проактивен пристап во идентификувањето и спротивставувањето

на кампањите за дезинформација и сајбер-нападите, поттикнувајќи поинформирано и побудно општество.

✓ На крајот на краиштата, практичната употреба на ова истражување е да придонесе кон способноста на Република Северна Македонија ефикасно да ги заштити својата безбедност, демократските вредности и институциите во услови на развој и сложени хибридни закани.

1.4. Дефинирање предмет на истражување

Теоретска рамка

I. Вовед

Теоретската рамка на истражувањето произлегува од постигнување на целите. Студијата ќе ја нагласи контроверзноста околу терминот, бидејќи тој е предмет на дебата помеѓу безбедносните експерти и научниците. Додека некои ги гледаат хибридните закани како корисна алатка за идентификување на новите безбедносни предизвици, други тврдат дека така се прикрива променливата природа на стратегиската конкуренција и конфликти.

II. Концептуален модел на хибридни закани

Концептот на хибридни закани сè повеќе се дебатира во академските кругови. Неодамнешното пребарување на „Google Scholar“[4] за терминте „Hybrid Threats“ и „Hybrid Warfare“ даде приближно 9 990 резултати, со повеќето публикации – околу 6 970 – произведени од 2014 година.[5] Но, тоа не значи дека концептот е целосно прифатен и разбран. Списокот на прашања е долг:

• Што се хибридни закани?

[4] *Google Scholar* е слободно достапен веб-пребарувач кој го индексира целосниот текст или метаподатоците на научната литература низ низа формати и дисциплини за објавување.

[5] Babbage, Ross. (2019). “*Stealing a March: Chinese Hybrid Warfare in the Indo-Pacific: Issues and Options for Allied Defense Planners Volume II: Case Studies.”* Center for Strategic and Budgetary Assessments II: 1–51, достапно на: https://csbaonline.org/uploads/documents/Stealing_a_March_Annex_Final.pdf%0A25.

• Како се позиционирани во литературата за безбедност?
• Дали има нешто ново во концептот?
• Која теорија стои зад нив или треба да се развие нова теорија?
• Кои методологии треба да се користат при спроведување истражувања поврзани со хибридни закани?
• Кои извори треба да се користат за тоа истражување?

Постојат четири главни столбови, кои сите треба да се испитаат за да може да се изгради целосно разбирање на пејзажот на хибридните закани:
• Актери (и нивните стратегиски цели)
• Алатки кои ги применува актерот
• Домени кои се насочени и
• Фази (вклучувајќи ги и видовите активност забележани во секоја фаза).

III. „CORE“ модел за градење +отпорност

Во овој дел, „CORE“ моделот ќе биде воведен и истражен како сеопфатен екосистем за отпорност чија цел е да ги зајакне националните напори за градење отпорни заедници против дезинформации. Студијата ќе ги истражи четирите двигатели идентификувани во моделот CORE, кои обезбедуваат можности за малигните државни и недржавни актери да ги искористат модерните технологии и да шират дезинформации.

IV. Улогата на НАТО во борбата против хибридните закани

Овој дел ќе се фокусира на вклученоста на НАТО во спротивставувањето на хибридните закани, особено на тоа како конкурентите ги искористуваат демократските слабости и манипулираат со информациите за да ја поткопаат довербата во демократските институции во Република Северна Македонија. Дополнително, студијата ќе разговара за ризиците од дезинформации опширно анализирани од страна на НАТО како ризик за јавното здравје и неговите напори да се спротивстави на хибридните закани кои имаат за цел да ги поделат сојузниците и да ги прикажат авторитарните режими како посоодветни за справување со кризи.

V. Хибридни закани во Република Северна Македонија

За да се добие сеопфатно разбирање, оваа студија ќе спроведе анализа на политичките, економските и социјалните услови во Република Северна Македонија кои поттикнуваат употреба на тактики за хибридно војување. Овие тактики може да вклучуваат сајбер-напади, операции на влијание и дезинформации.

VI. Отпорност на заедницата против дезинформации

Со оглед на значењето на градењето отпорност на заедницата, оваа студија ќе ја истражи важноста на борбата против дезинформациите и пропагандата во Република Северна Македонија. Дополнително, ќе се осврне на актуелното прашање за медиумската и информациската писменост (МИП) и недостатокот на систематски национален пристап за справување со дезинформациите.

VII. Заклучок

Ќе бидат сумирани клучните наоди и импликации извлечени од теоретската рамка, истакнувајќи ја потребата од координиран и холистички пристап за справување со предизвиците што ги носат хибридните закани и дезинформациите во регионот.

Предложената теоретска рамка може ефективно да се примени за справување со хибридните закани во Република Северна Македонија. Наместо да ги ограничува засегнатите страни на одредена перспектива, рамката нуди инклузивен пристап кој го подобрува разбирањето. Служи како динамично претставување на проблемот што се развива, обезбедувајќи приспособливост кон променливата природа на хибридните закани.

1.5. Дефинирање клучни концепти

Хибридни закани: комбинација од различни алатки, очекувани и тајни, кои се користат за да се постигне непријавена стратегиска цел без официјално да се признае дека се прави тоа. Овие закани може да вклучуваат сајбер-напади,

операции на влијание и дезинформации, меѓу другото. Заедничката цел на актерите на хибридни закани е да ги поткопа или да им наштети на демократски воспоставените влади, земји или сојузи. Хибридните закани претставуваат комбинација од воени и невоени средства, вклучувајќи дезинформации, сајбер-напади, економски притисок, употреба и распоредување на нерегуларни вооружени групи, како и употреба на регуларни воени сили. Интензитетот на хибридните закани постојано се менува, како и нивниот размер и брзина. Затоа, дефиницијата за хибридните закани треба да се гледа широко и флексибилно, за да може да одговори на нивната еволутивна природа.[6]

„Hybridity Blizzard" – модел на снежна бура претставува шематски приказ на меѓусебно поврзаната динамика помеѓу бранителите и напаѓачите и на краткорочни и на долгорочни перспективи. Истакнува како различните димензии на времето и актерите комуницираат, прикажувајќи ги овие интеракции како екосистем. Оваа аналогија помага да се разберат сложеноста на хибридноста.[7]

CORE модел: сеопфатен екосистем за отпорност кој има за цел да ги зајакне националните напори за градење отпорни заедници против дезинформации. Тоа им помага на креаторите на политиката да идентификуваат и споредат различни хибридни закани, да ги препознаат институционалните одговорности и да развијат насочени контрамерки.[8]

НАТО (Организација на Северноатлантскиот договор): меѓувладина воена алијанса која се состои од 31 земја членка. Има значајна улога во спротивставувањето на хибридните закани и обезбедувањето на безбедноста и одбраната на нејзините земји членки. Од 2015 година, НАТО има стратегија за својата улога во спротивставувањето на хибридната војна. НАТО ќе се погрижи Алијансата и сојузниците да бидат доволно подготвени да се спротивстават на

---

[6] Влада на Република Северна Македонија, Министерство за одбрана (април 2021). *Национална Стратегија за градење на отпорност и справување со хибридни закани,* стр. 4.

[7] Weissmann, M. , Nilsson, N. , Palmertz , B. , & Thunholm , P. (2021). *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: I.B. Tauris. Достапно на: http://dx.doi.org/10.5040/9781788317795 (pp. 266-271).

[8] Jungwirth, R., Smith, H., Willkomm, E., & others. (2023). *Hybrid threats: A comprehensive resilience ecosystem.* Publications Office of the European Union.

хибридните напади во каква форма и да имаат. Ќе ги одврати хибридните напади врз Алијансата и, доколку е потребно, ќе ги брани засегнатите сојузници.[9]

Дезинформации: лажни или погрешни информации кои намерно се шират со цел да се измамат или манипулираат поединци, заедници или институции. Може да се користи од страна на државни или недржавни актери за да влијаат врз јавното мислење, да ја поткопаат довербата во демократските институции и да промовираат сопствени агенди.[10]

Пропаганда: ширење пристрасни или погрешни информации за промовирање одредена политичка, идеолошка или социјална гледна точка. Пропагандата е форма на комуникација која има за цел да манипулира со јавното мислење и однесување преку презентирање информации селективно и често погрешно.[11] Често се користи за да се влијае на јавното мислење и однесување, особено за поддршка на одредени владини политики или агенди.

Пристап на целото општество (Whole-of-society approach) во практика, слоеви на отпорност: кооперативна рамка на целото општество која ги интегрира капацитетите и капиталот што ги поседуваат различните актери од приватниот и граѓанскиот сектор во еден обединет процес на стратегиско планирање.[12] Една неодамнешна академска метаанализа која беше спроведена за да се следат домени на сеопфатната општествена отпорност предложи поделба на четири слоеви и нивните меѓусебни врски: (1) лична отпорност; (2) отпорност на заедницата и субрегионална отпорност; (3) институционална отпорност и (4) напредна отпорност.[13]

---

[9] https://www.nato.int/cps/en/natohq/topics_156338.htm#:~:text=NATO%20will%20ensure%20that%20the,necessary%2C%20will%20defend%20Allies%20concerned. Пристапено: август, 2023.

[10] Ion Mihai Pacepa and Ronald J. Rychlak (2013). *Disinformation: Former Spya Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*, WND Books, pp. 4–6, 34–39, 75.

[11] Bernays, E. (1928). *Propaganda. Horace Liveright*.

[12] Hyvönen, A.-E., & Juntunen, T. (2020). *From 'Spiritual Defence' to Robust Resilience in the Finnish Comprehensive Security Model*. In S. Larsson & M. Rhinard (Eds.), Nordic Societal Security (pp. 154–178). Routledge.

[13] Hyvönen, A.-E., & Juntunen, T. (2019). *Kokonaisresilienssi ja turvallisuus: tasot, prosessit ja arviointi*. Publications of the Government's Analysis, Assessment and Research Activities, 17/2019. Prime

Отпорност на заедницата: способноста на заедниците да издржат и да закрепнат од надворешни шокови, закани и предизвици, вклучително и дезинформации и пропаганда. Тоа вклучува подигање на свеста, градење капацитети и зајакнување на способноста на локалните чинители, медиумите и граѓаните да се спротивстават и да се спротивстават на хибридните закани. Според Хол и Заутра, отпорните населби се карактеризираат со: силна доверлива врска меѓу нејзините членови; редовни интеракции помеѓу соседите; релативно стабилна станбена структура; чувство на заедништво и заедница; подготвеност да се дејствува во име на заедницата и пристапноста на јавните простори.[14]

Информациско војување: Информацискатa војна се однесува на употребата на информациските и комуникациските технологии за манипулирање, нарушување или влијание врз перцепцијата, сознанието и однесувањето на поединци, организации или нации за стратешки или политички цели. Тоа вклучува искористување на различни техники, вклучувајќи дезинформации, пропаганда, сајбер-напади, психолошки операции и социјален инженеринг, за да се постигнат конкретни цели во информативниот домен.[15] Тоа е суштинска компонента на тактиката за хибридно војување.

Сајбер-безбедност: заштита на компјутерските системи, мрежи и податоци од сајбер-закани, вклучувајќи сајбер-напади и хакирање.[16] Има суштинско значење за спротивставување на хибридните закани кои ги искористуваат дигиталните технологии и сајбер-просторот.

Овие клучни концепти се од витално значење за разбирање на теоретската рамка и предизвиците што ги носат хибридните закани како концепт и во контекст на Република Северна Македонија.

Minister's Office. (pp. 23–25)

[14] Hall, J. S., & Zautra, A. J. (2010). *Indicators of Community Resilience: What Are They, Why Bother?* In J. Reich, A. J. Zautra, & J. S. Hall (Eds.), Handbook of Adult Resilience.

[15] Denning, D. E. (2015). *Information Warfare and Cybersecurity*. *Springer*.

[16] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

1.6. Општа/специфична хипотетичка рамка

Општата хипотеза на овој магистерски труд е дека хибридните закани претставуваат значителен ризик за безбедноста на Република Северна Македонија со намерно насочување на ранливости во различни домени за да ги поткопаат демократските институции и процесите на одлучување. Тезата тврди дека разбирањето на концептот на хибридни закани и нивните импликации ќе овозможи развој на ефективни стратегии за зајакнување на отпорноста, заштита на демократските вредности и зајакнување на институционалната одбрана против овие повеќеслојни предизвици.

Посебни хипотези:

Хипотеза 1: Координираната и синхронизирана природа на хибридните закани, кои опфаќаат различни домени, директно ги таргетира ранливостите во демократските институции, што доведува до ерозија на довербата во демократските процеси во Република Северна Македонија.

Хипотеза 2: Сеопфатниот модел (CORE) и „Hybridity Blizzard“ – модел на снежна бура ги подобрува разбирањето и одговорот на хибридните закани, особено во одлуките, информациите и зависностите меѓу домени, засилувајќи демократски основи и секторска отпорност.

Хипотеза 3: Нивото на свесност и разгледување на хибридните закани во Стратегијата за одбрана на Република Северна Македонија и Стратегијата за градење отпорност влијае на капацитетот и подготвеноста на земјата ефикасно да одговори на овие закани.

Хипотеза 4: Националната стратегија за отпорност и спротивставување на хибридните закани, заедно со соработката во безбедносниот сектор и учеството во меѓународни иницијативи како „Сајбер-коалицијата“, го ослабуваат влијанието на хибридните закани, вклучувајќи дезинформации и DDoS напади и ја засилуваат институционалната отпорност и граѓанската заштита.

Хипотеза 5: Хибридните закани, вклучувајќи дезинформации, сајбер-напади и надворешни влијанија, имаат големи последици за безбедноста,

управувањето и довербата во институциите на Република Северна Македонија. Тие целосно ги нарушија безбедноста и стабилноста на земјата.

1.7. Истражувачки варијабли

Независни променливи:
а. Ниво на координација и синхронизација во акциите на хибридни закани.
б. Домени таргетирани од хибридни закани (на пр. политички, економски, воени, цивилни, информации).
в. Степенот до кој се искористуваат ранливостите во демократските институции.

Забелешка: Девијацијата на појавите на хибридните закани е од широк и непредвидлив спектар, т. е. немаат одредена територија и стриктна област на дејствување, поради анонимноста на актерите и асиметричноста во нападите тешко е да се карактеризираат, систематизираат, а тоа ги прави тешки за анализа.

Зависни променливи:
а. Ерозија на довербата во демократските процеси и институции.
б. Разбирање и способности за одговор на хибридни закани.
в. Капацитет и подготвеност на Република Северна Македонија да се спротивстави на хибридните закани.

Забелешка: за зависна варијабла во ова истражување се определени мерливи фактори т.н. двигатели на асиметричните и хибридните закани. Тие може да се измерат и се објективни.

Контролни променливи:
а. Политичка клима и меѓународни односи.
б. Технолошки напредок и пристап до информации.
в. Владини политики и стратегии поврзани со спротивставување на хибридните закани.

1.8. Индикатори на истражувањето

Со мерење и анализа на овие истражувачки индикатори, студијата може да добие сеопфатно разбирање за импликациите на хибридните закани врз безбедноста на Република Северна Македонија и да ги идентификува областите за подобрување и интервенција за ублажување на ризиците што ги носат таквите закани.

- Влијание на дезинформациите:
  - Број на кампањи за дезинформација насочени кон демократските процеси и институции.
  - Јавната перцепција за довербата во демократските институции пред и по инцидентите со дезинформации.

- Сајбер-напади и отпорност:
  - Фреквенција и сериозност на сајбер-напади врз критична инфраструктура и институции.
  - Воведени мерки и способности за сајбер-безбедност за откривање и одговор на сајбер-заканите.

- Институционална подготвеност:
  - Ниво на свесност и разбирање за хибридните закани кај владините службеници.
  - Постоење и имплементација на специфични политики и стратегии за спротивставување на хибридните закани.

- Јавна свест и перцепција:
  - Јавната перцепција за хибридните закани и нивното влијание врз политичкото одлучување.
  - Свесност за потенцијалното влијание на дезинформациите врз демократските вредности.

- Меѓународна соработка:
  - Ниво на соработка со меѓународните организации (на пример, НАТО, ЕУ) во борбата против хибридните закани.
  - Учество во заеднички иницијативи и вежби за справување со хибридни предизвици.

- Медиумски и информативен пејзаж:
  - Нивоа на медиумска писменост кај населението.
  - Присуство на независни и сигурни извори на вести за спротивставување на дезинформациите.
- Процена на ранливост:
  - Идентификација на критичните пропусти во различни домени подложни на хибридни дејства.
  - Проценка на потенцијалните последици од експлоатираните ранливости.

1.9. Истражувачки методи

- Преглед на литература: Спроведување сеопфатен преглед на постојната литература и академски извори за да се добие увид во концептот на хибридни закани, поврзани теории и претходни студии на слични теми.

- Анкети: Преглед на анкети од релевантни засегнати страни, вклучително владини претставници, експерти и поширокатa јавност, од проверени извори за да се соберат квантитативни податоци за нивните перцепции, свест и искуства поврзани со хибридни закани.

- Интервјуа: Анализирање длабински интервјуа со клучни информатори, креатори на политики и експерти во областа за да се добијат квалитативни податоци и да се стекне подлабоко разбирање за предизвиците што ги носат хибридните закани.

- Студии на случај: Анализирање конкретни случаи на хибридни закани и нивното влијание врз безбедноста на Република Северна Македонија за да се обезбеди детален и специфичен увид и анализа на случаи на хибридни закани на меѓународно ниво за да се стекне поширока слика.

- Анализа на содржина: Анализа на медиумска содржина, официјални документи и онлајн извори за да се идентификуваат и квантифицираат случаите на дезинформации и сајбер-напади.

- Компаративна анализа: Споредување на пристапот на Република Северна Македонија за спротивставување на хибридните закани со други земји кои се соочуваат со слични предизвици за извлекување лекции и најдобри практики.

- Анализа на политики: Анализирање на постојните политики и стратегии во Република Северна Македонија поврзани со хибридни закани за да се процени нивната ефикасност и да се идентификуваат празнините.

- Визуелизација на податоци: Употреба на техники за визуелизација на податоци за ефективно да се презентираат наодите и да се направат сложените податоци подостапни за публиката, преку инфорграфици, табеларни прикази и сл.

1.10. Општествена оправданост на истражувањето

Оваа студија има општествено значење бидејќи се занимава со критичното прашање на хибридните закани и нивното влијание врз безбедноста на Република Северна Македонија. Преку истражување на концептот и импликациите на овие закани и предлагање стратегии за отпорност и заштита на демократските институции, истражувањето придонесува за заштита на граѓаните од штета и одржување на демократските вредности. На крајот на краиштата, наодите можат

да им помогнат на креаторите на политики и засегнатите страни во зајакнувањето на мерките за национална безбедност, во спротивставувањето на дезинформациите и во поттикнувањето постабилно и поотпорно општество.

2. Концептуален модел на хибридните закани
Идентификување актери, домени, спротивставување и фази

Поимот „хибрид“ стана мејнстрим збор во последниве години. Возиме хибридни автомобили, голферите удираат топки со хибридни палки и сè повеќе, куќите се опремени со хибридни системи за греење. Терминот „хибрид“ потекнува од биологијата, што значи „растение или животно што е произведено од два различни вида растение или животно, особено за да добие подобри карактеристики.“ Општо земено, тоа е „нешто што е мешавина од две многу различни нешта“[17]. Кога се применува на (безбедносните) закани, укажува на мешавина од воени и невоени предизвици. Како таков, не е ништо ново: други термини се користеа во минатото за истото значење; „хибрид“ е само новиот популарен збор.[18] Сепак, сè уште не постои широко прифатена дефиниција за „хибридни“ закани или активности.

Хибридните закани не се нови – тие ги искористуваат класичните принципи на стратегијата како што се победа без борба, индиректниот пристап, конфликти со низок интензитет и тактиките „салами“. Но, тие се новина и мошне релевантни за стратешките предизвици во годините што следуваат. Идните трендови во *распределба на моќта* (регионална и глобална), *меѓузависноста* (интензивирано од глобализацијата) и *технологијата* (меѓу другото, новата технологија и напредокот на вештачката интелигенција) сугерираат дека помотивираните ревизионистички актери ќе имаат поголем пристап до средства кои можат поекономично да таргетираат повеќе ранливости, користејќи алатки и

[17] Дефиниции од речникот на Кембриџ. Достапно на: https://dictionary.cambridge.org/dictionary/english/hybrid

[18] Klijn, H., & Yüksel, E. (2019). *Russia's hybrid doctrine: Is the west barking up the wrong tree?* (The Hague: The Clingendael Institute).

домени на дејствување кои го покриваат целиот спектар на современиот домашен и меѓународен живот.

Различни дефиниции кружат, дури и во ЕУ и НАТО. Постојат јасни сличности помеѓу дефинициите: на пример, сите тие ги опишуваат хибридните закани како комбинирана употреба на воени и невоени средства за поткопување на општествата. Сепак, можна е дискусија за тоа кои активности може и не може да бидат вклучени во концептот на хибридни закани. На пример, „Заедничката рамка за спротивставување на хибридните закани“ – „Joint Framework on Countering Hybrid Threats“ на ЕУ вклучува многу широка област на активности за спротивставување на хибридните закани, покажувајќи ја широкоста на полето. Рамката наведува:

– стратегиска комуникација за да се спротивстави на систематското ширење на дезинформации;

– заштита на критичната инфраструктура (на пр. синџири за снабдување со енергија, транспорт) од неконвенционални напади (што во описот вклучува многу широки цели на политиката, понатамошно диверзификација на енергетските извори на ЕУ, добавувачите и рутите, транспортот и безбедноста на синџирот на снабдување, но и заштита на инфраструктурата во вселената од хибридни закани, како и зголемување на одбранбените способности воопшто);

– заштита на јавното здравје и безбедноста на храната (вклучувајќи заштита од закани од CBRN – хемиска, биолошка, радиолошка и нуклеарна одбрана);

– подобрување на сајбер-безбедноста (со посебен фокус на индустријата, енергијата, финансиските и транспортните системи);

– насочување на финансирање на хибридни закани; и градење отпорност против радикализацијата и насилниот екстремизам.[19]

„Европскиот центар за извонредност за спротивставување на хибридни закани“ (EEAC), исто така, вклучува сајбер-закани во опсегот на хибридни закани и додава дека (CBRN) закани преку неконвенционални средства спаѓаат во сопствена категорија, додека сè уште ги вклучува во категоријата хибридни

[19] European Union. (2016). *Joint Framework on countering hybrid threats, a European Union response*. Joint Communication to the European Parliament and the Council, EU Document JOIN(2016) 18 final.

закани.[20]

Накратко, терминот „хибридни закани“ нема дефинитивна и фиксна дефиниција, што останува предмет на тековната еволуција и дебати.

Концептот на „хибридни закани“ предизвика искра на дебати меѓу аналитичарите и научниците, при што некои го сметаат за вреден за истакнување како дел од новите безбедносни предизвици. Други, сепак, ја отфрлаат како неадекватна аналитичка категорија која не ја објаснува еволутивната природа на стратегиската конкуренција.[21] Брзата еволуција на концептот за хибридни закани е очигледна во растечката литература, појавата на многубројни истражувачки групи и промените на јазикот во документите. „The 2016 Joint Communication on Hybrid Threats“ од 2016 година ги поставува оперативните активности за спротивставување, додека последователната средба JOIN (2018) „Зголемување на отпорноста и зајакнување на способностите за справување со хибридните закани“, објавена во јуни 2018 година, усвои пострategиски став. Таа го нагласува значењето на стратегиските елементи и улогата на отпорноста во ублажувањето на влијанието на хибридните закани.

Хибридните закани се состојат од политички активности, дезинформативни кампањи и сајбер, воени, економски и општествени интервенции. Покрај тоа, иако заканите засновани на сајбер се полемични, тие претставуваат само еден од домените во кои може да се појават хибридни закани. Навистина, „оружјата“ што се користат во сивата зона може да вклучуваат компјутери, гранични порти, лажни вести, беспилотни летала, фарми за сајбертрол, радиостаници, киднапирани авиони или бродови и шпионски балони кои преминуваат во воздушниот простор на туѓа територија. Неисцрпната листа на хибридни закани би вклучувала и сајбер-напади, тероризам, организиран криминал, трговија со дрога, миграциски текови, економски или финансиски војни, медиумска експлоатација и примена на тајни психолошки операции. Најобновените каталози на хибридни закани испреплетуваат повеќе политички, економски, технички,

[20] EEAS. (2018). *A Europe That Protects: Countering Hybrid Threats*. Factsheet.

[21] European Union (2021). DIRECTORATE-GENERAL FOR EXTERNAL POLICIES POLICY DEPARTMENT. *Best Practices in the whole-of-society approach in countering hybrid threats*. pp.19.

социјални, информативни, правни, дипломатски, научни и воени ризици.[22] Всушност, во денешно време секоја закана има потенцијал да стане хибридна закана бидејќи природата на овие опасности е дека тие постојано еволуираат. Единствен исклучок од ова е веројатно случајот на закана која е дел од објавена војна, при што стратегијата или акцијата тогаш не може да се сметаат за хибридни.

Овој магистерски труд има за цел да создаде основна концептуална рамка приспособена на контекстот на Република Северна Македонија, олеснувајќи го разбирањето на хибридните закани. Се обидува да ја потврди ефективноста на аналитичката рамка преку испитување студии на случај и сеопфатен преглед на различни стратегиски перспективи. Понатаму, предложениот концептуален модел се стреми да постави збир на сеопфатни цели кои ќе придонесат за попрефинета карактеризација на хибридните закани, со директна релевантност за околностите во Република Северна Македонија.

Постојат четири главни столбови, кои сите треба да бидат испитани за да може да се конструира целосно разбирање на концептот на хибридните закани:

• Актери (и нивните стратегиски цели);
• Алатки кои ги применува актерот или актерите;
• Домени кои се таргетирани и
• Фази (вклучувајќи ги и видовите активност опсервирани во секоја фаза).

2. Концептуален модел на хибридните закани. Идентификување актери, домени, спротивставување и фази

2.1. Актери

Историски контекст

Во изминатата деценија, промените во глобалната динамика покажаа дека

[22] Galán C (2018*). Amenazas híbridas. Nuevas herramientas para viejas aspiraciones*. In: Elcano Documentos de Trabajo, 20/2018, p. 3.

недемократските држави се соочуваат со тешкотии во постигнувањето на стратегиските цели преку традиционалните транспарентни методи како дипломатијата и трговијата. Истовремено, меѓународниот поредок е нарушен, интензивирајќи ја конкуренцијата на големите сили и предизвикувајќи судири на вредности. За разлика од економското ривалство во Студената војна, денес се фокусира на демократски наспроти авторитарни системи со слични економии. Ова ги преобликува сојузите, влијаејќи на трговските и општествените поделби. Во услови на оваа сложеност, анализата на моќта еволуираше од моќ заснована на ресурси во релациска моќ. Во овој контекст, хибридните стратегии креативно ги комбинираат алатките за да постигнат влијание, особено од помалку моќни ентитети, нудејќи начини за дискретно унапредување на интересите, а истовремено намалувајќи ги ризиците од ескалација. Овој пристап ја искористува променливата безбедносна динамика создавајќи ранливости и ја зголемува моќта. Ова може да вклучува активности од мал обем, како што се деловни зделки или локални одлуки за време на изборите, сè до политиките, законодавството и одлуките за спроведување на законот. Дури и ако е делумно успешна, хибридната природа на заканата може да предизвика штета, што бара рано откривање и спротивставување. Оттука, разбирањето на актерите зад ваквите закани станува клучно.

2.1.1 Државни актери

Стратегии и манипулации

Државните актери, без разлика дали се авторитарни или демократски, играат клучна улога во обликувањето на меѓународните односи. Во овој контекст, постои зголемена загриженост за појавата на хибридни закани, концепт кој опишува повеќеслојни предизвици за стабилноста на државите и општествата, кои често вклучуваат комбинација на воени, економски, политички и тактики базирани на информации. Овие закани станаа поприсутни во современиот геополитички пејзаж, при што актери како Русија и Кина често се поврзуваат со такви активности.

Авторитарните режими, кои се карактеризираат со концентрација на моќ и

ограничен политички плурализам, се особено вешти во примената на хибридни тактики за да го задржат својот авторитет и на домашен и на меѓународен план. Тие се обидуваат да ги оспорат основните вредности на демократиите, како што се владеењето на правото и отворената политичка конкуренција. Во нивните земји, овие режими користат присилни методи за да го потиснат несогласувањето, да манипулираат со информации и да создадат страв кај граѓаните за да ја зачуваат својата моќ. На меѓународен план, тие се плашат од ширењето на демократските идеали и на тој начин имаат за цел да ги поткопаат капацитетите на демократските држави.

Манипулирањето со информации е централна предност за авторитарните држави. Со контролирање на медиумите и ширење пропаганда, тие ги обликуваат верувањата на граѓаните и ги обесхрабруваат колективните акции против режимот. Ова е во спротивност со демократските држави каде што медиумите служат како проверка на моќта и поттикнуваат општествени дебати. Промените во медиумските пејзажи, како што се појавата на нови платформи и променетите модели на приходи, воведоа ранливост во демократските општества, што ги прави подложни на надворешно мешање.

Авторитарните режими, исто така, се обидуваат да го контролираат општеството преку зајакнување на посредниците кои ги извршуваат нивните интереси. Оваа контрола се протега на економскиот сектор, при што бизнисите и поединците често се принудени да се усогласат со државните цели. На пример, Законот за национална безбедност на Кина ѝ дава на државата широко овластување над граѓаните и корпорациите за заштита на националната безбедност. Спротивно на тоа, демократските држави имаат појасни поделби помеѓу јавниот и приватниот сектор, со што се намалува испреплетувањето на државните интереси со бизнисите.

Основните разлики помеѓу демократските и авторитарните држави се нагласени во меѓународната политика. Демократските држави се водат од принципите на владеење на правото, а нивните тајни операции се строго регулирани. Спротивно на тоа, авторитарните режими, водени од самоодржување, се поподготвени да го злоупотребат правото за да добијат предност и да го

експлоатираат почитувањето на меѓународните норми од страна на демократските држави.

Руското и кинеското стратегиско размислување дополнително ги истакнува нивните различни пристапи кон меѓународните работи. Русија користи концепт наречен рефлексна контрола, кој вклучува манипулирање со противниците при донесување одлуки за да се усогласат со интересите на Русија. Со користење комбинација на методи за постигнување манипулација без трага, Русија може да изврши влијание врз целните држави без директно припишување вина. Овој концепт дава увид во активностите на хибридните закани поврзани со овие состојби.

Како заклучок, државните актери, особено авторитарните режими, играат клучна улога во обликувањето на меѓународната динамика преку хибридни тактики. Нивните стратегии имаат за цел да ги предизвикаат демократските принципи и да ја консолидираат моќта, користејќи методи како што се манипулација со информации, контрола на посредници и рефлексна контрола. Разбирањето на оваа динамика е од суштинско значење за ефикасно спротивставување на хибридните закани и одржување на меѓународната стабилност.

Идентификување и одговор

Капацитетот за идентификување и одговор на хибридните закани зависи од прецизното одредување на ентитетите зад овие дејства. Постојното разбирање на недржавните хибридни закани произлегува од разновидната и приспособлива природа на предизвикот, под влијание на различни ентитети кои учествуваат во операциите на хибридни закани. Бидејќи овие активности бараат одредени прагови во однос на способностите и намерите, многу недржавни ентитети во оваа област веројатно одржуваат некаква форма на здружување со странски држави.

Анализата започнува со таргетираното општество: неговата политичка структура, моќните недржавни актери (Non-State Actors, NSA) и мрежните врски. Дали сојузите со други актери можат да помогнат во откривањето и спротивставувањето на заканите? Последователно, испитувањето на

потенцијалните противници станува клучно. Дали тие фаворизираат специфични форми на моќ на недржавни актери за да влијаат врз нивните општества и други држави? Дали слични недржавни актери се влијателни во таргетираното општество? Дали државниот чинител има пристап до такви недржавни актери и средства за да изврши влијание?

Поедноставување на односите помеѓу „недржавните актери“ и државните актери во хибридни закани

Во услови на дискусии за различни перспективи, Карлен и Раута сугерираат дека дисциплинските поделби не мора да бидат бариера. Тие го воведуваат терминот „конфликтна делегација“ за да ги опфати и прокси-војните и надворешната поддршка во граѓанските војни, нагласувајќи ги странските влади кои обезбедуваат ресурси или експертиза на недржавните вооружени групи против перципираните непријатели.[23] Слично на тоа, идејата на Концептуалниот модел за континуум на хибридна закана ги обединува сите сценарија во истата рамка, што ја одразува практичната потреба за превенирање, откривање, одвраќање и спротивставување на хибридните закани без оглед на мирните или конфликтните услови.

Разбирање на делегирање конфликти

Централно место за делегирање конфликти се интеракциите помеѓу државните спонзори и недржавните актери, кои вклучуваат способности пренесени од главен актер на агент. Следува контрола врз целите, стратегиите и тактиките на агентот, со варијации во механизмите.[24] Оваа динамика може да работи и обратно, при што недржавните актери влијаат врз државните покровители. Надвор од хиерархиите, постојат сојузи и паралелни напори помеѓу

[23] Karlèn, N., & Rauta, V. (2021). *Forum: Conflict delegation in civil wars. Introduction.* International Studies Review, 23(4), 2050–2052.

[24] Исто, стр. 2058–2060.

државните и недржавните актери. Дури и категоријата „корисни идиоти“ мора да се признае. Покрај тоа, овие односи може да се развиваат, при што недржавни актери потенцијално ќе се трансформираат во државни актери.[25][26]

Типологијата на Владимир Раута

Владимир Раута воведе типологија за разбирање на односите помеѓу недржавните актери и државните актери во хибридното војување, врз основа на воочените релациони врски.[27] Оваа типологија ги категоризира врските во помошни, поврзани, сурогат и прокси типови, обезбедувајќи рамка за разбирање на функционалните интеракции. На пример, Night Wolves MC во Украина може да се гледа како помошен, додека Wagner Group делува како поврзан ентитет. Тоа помага да се разграничат улогите на недржавни актери во различни контексти, како што е сурогатната улога на Хезболах во Сирија и нејзината прокси функција против Израел. Надвор од конфликтот, односите може да бидат нијансирани и опортунистички, при што странските деловни субјекти работат според интересите на нивната матична држава во странство. Привремената странска поддршка за политички кампањи, и покрај нејзината краткорочна природа, сепак може да има трајни ефекти. Во доменот на хибридните закани, односите помеѓу недржавни актери и државните актери варираат во голема мера, опфаќајќи од трајни обврски до краткорочни интеракции. Екстремните примери вклучуваат ентитети основани од држави, како приватни воени компании, и привремени вработувања за специфични операции. Овие односи одразуваат различни нивоа на заеднички цели, при што некои субјекти се создадени исклучиво за државни цели, а други мотивирани од финансиски стимулации или регулаторни обврски.

Тајни државни активности

[25] Salehyan, I. (2021). *A Decade of Delegation.* International Studies Review, 23(4).

[26] Giannopoulos, G., Smith, M. E., & Theocharidou, M. (2021). *The Landscape of Hybrid Threats.*

[27] Hoffman, F. G. (2018). *Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict*, 8.

Државите кои вработуваат недржавни ентитети за тајни операции ја искористуваат тајноста за да ги попречат откривањето и одговорот. Учеството на „Руските ноќни волци“ – клуб за мотоцикли во анексијата на Крим го докажува ова, бидејќи тие собирале разузнавачки информации, дистрибуирале пропаганда и се вклучиле во вооружени акции. Тајните дејства, исто така, нудат веродостојно негирање, како што се гледа со руската групација „Wagner Private Military Company“ која работи во конфликти како Источна Украина и Сирија. Приватните воени корпорации (ПВК) претставуваат предизвици, регрутираат обучени лица за операции кои ненамерно би можеле да им наштетат на нивните земји. Овој тренд, нагласен од Маргарет Клајн, ја нагласува потребата од стратегии за справување со ескалирачката закана од тајни државни активности преку недржавни актери.[28]

2.1.2. Недржавни актери

Недржавните актери – „Non State Actors“ (NSA) опфаќаат различен опсег, од поединци и приватни корпорации до верски институции, хуманитарни организации, вооружени групи и де факто режими кои контролираат територии и популации.[29] Нивната дефинирачка карактеристика е нивното постоење надвор од меѓународно признатите држави, но импликациите од оваа дистинкција се повеќеслојни.[30]

Во авторитарните системи, независните извори на авторитет се обесхрабрени, со што се замаглува границата помеѓу државните и недржавните актери. Спротивно на тоа, демократиите го ценат граѓанскиот простор ослободен од владини упади, потпирајќи се на недржавни актери за различни јавни

[28] MARGARETE KLEIN (2019). Hybrid CoE Strategic Analysis 17, Private military companies – a growing instrument in Russia's foreign and security policy toolbox.

[29] Kleczkowska, A. (2020). *States vs. non-state actors – a public international law perspective.* Hybrid CoE Strategic Analysis, 20. Достапно на: https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-20-states-vs-nonstate-actors-a-public-international-law-perspective/

[30] Исто.

функции, понекогаш дури и кога постои државна сопственост на бизнисите. Традиционалното меѓународно право им дава приоритет на државните односи, додека приватното меѓународно право се концентрира на комерцијалните интеракции. Меѓународното хуманитарно право препознава одредени недржавни актери како што се Меѓународниот Црвен крст и Црвена полумесечина и Меѓународниот комитет на Црвениот крст.

Вклучувањето недржавни актери во конфликти ги поттикна напорите да се обезбеди нивно придржување до меѓународното хуманитарно право. За време на Студената војна, сите страни активно ги користеа. Анализата на вооружените конфликти од 1990-тите укажува дека недржавните актери се вклучија со државните актери (на пример, чеченските војни или конфликтите кои произлегуваат од распадот на Југославија) користејќи асиметрични методи.[31]

Појавата на групи како ал-Каеда и Исламската држава на Ирак и ал-Шам (ИСИС) на почетокот на 21 век го истакна потенцијалот на независните недржавни актери да ја оспорат моќта на државите. Неодамнешното преземање на Авганистан од страна на Талибанците во 2021 година служи како значајна студија на случај, покажувајќи како недржавен актер може ефективно да спроведе кампања за хибридна закана против признаена и поддржана влада.

2.2. Клучни домени

2.2.1. Политички домен

Во контекст на хибридните закани, политичкиот домен ги вклучува оние кои се на власт во рамките на една територија преку примена на различни форми на политичка моќ и влијание.[32] Политичкиот систем се очекува да биде репрезент на културните, историските, демографските, а понекогаш и религиозните фактори

[31] Hoffman, F. (2018). *Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges.* PRISM, 7(4).

[32] NATO. (2013). *Allied Command Operations Comprehensive Operations Planning Directive Interim V2.0*. Belgium: North Atlantic Treaty Organization, Supreme Headquarters Allied Powers Europe.

кои го формираат идентитетот на едно општество. Граѓанските права, изборите и парламентарната отчетност обично се специфични фактори во една демократија.[33] Модерните демократии претставуваат општествени фактори и вклучуваат права, избори и одговорност. Овој домен може да биде манипулиран од актери за да влијаат или да создадат поволни услови за хибридни закани. Ова вклучува користење политичка моќ во земјата или дипломатски, често таргетирање на демократските процеси и организации.

Политичкиот домен е поврзан со дипломатијата и јавната администрација. Тоа е поврзано со надворешната политика што влијае на домашната политика и може да ја обликува јавната перцепција. Информативните алатки можат да поддржат хибридни закани насочени кон овој домен. Актерите ги искористуваат правните празнини, функционирајќи помеѓу националното и меѓународното право. Правниот домен влијае на таквите обиди. Успехот се потпира на тајни активности, често извршени од разузнавачките служби поради нивните тајни способности и мрежи.

2.2.2. Воен домен

Во одбранбените операции, војската ги штити независноста, територијалното единство и суверенитет на нацијата. За време на мирот, војската соработува со цивилните власти за вежби и помош. Одржувањето присуство е од суштинско значење за брзи одговори на закани како тероризам и катастрофи, како и промени во близина. Воената сила на една земја е од витално значење за нејзиниот опстанок и проектираното влијание. Низ историјата, суперсилите комбинирале економска и воена моќ, влијаејќи на глобалната политика. Воената моќ е клучна за глобалното признавање. Дури и економски послабите земји како Русија се перципирани како суперсили поради нивните воени способности, додека економски посилните нации може да немаат слично признание поради воените слабости. Компромитирањето на одбранбените способности на нацијата може

[33] Newton, K, and J W van Deth. (2010). *Foundations of Comparative Politics: Democracies of the Modern World*. 2nd ed. Cambridge: Cambridge University Press.

ефективно да ги зголеми влијанието и притисокот, подготвувајќи се за идните операции. Тоа поттикнува одбранбени одговори, зголемувајќи ги трошоците и исцрпувајќи ресурси, предизвикувајќи економски притисок.

2.2.3. Економски домен

Економскиот домен на хибридните закани ги опфаќа производството, дистрибуцијата, потрошувачката на стоки и услуги, економскиот развој и распределбата на богатството на нацијата. Економската држава, користејќи економски интеракции за надворешнополитички цели, е историски извор на државна моќ.[34][35][36] Со оглед на неопходноста да се одржи веродостојно негирање и да се избегне поттикнување отворен воен конфликт, искористувањето на економскиот домен во хибридните закани има тенденција да се разликува во целите од отворените воени кампањи. Целта на хибридните закани во економскиот домен е значително да ја намалат силата на целната држава, нагризувајќи ја довербата во демократијата и владата. На пример, економските стратегии можат да вршат политички притисок,[37] додека економската принуда може да ја промени надворешнополитичката позиција на државата или да ја ослаби нејзината општествена, економска и безбедносна отпорност.[38] Прелиминарната фаза на таквите акции може да се протега на долги периоди, па дури и децении.

Во контекст на хибридните закани, доменот на економијата е сложено меѓусебно поврзан со други домени, првенствено поради активностите на

---

[34] Baldwin, D. A. (1985). *Economic Statecraft*. Princeton: Princeton University Press.

[35] Norris, William J. 2016. *Chinese Economic Statecraft : Commercial Actors, Grand Strategy, and State Control*. Ithaca: Cornell University Press.

[36] Reilly, James. (2013). *"China's Economic Statecraft: Turning Wealth into Power."* Syndey.

[37] Blackwill, R. D., & Harris, J. M. (2016). *The Lost Art of Economic Statecraft*. Foreign Affairs, *95*(2), 99–110.

[38] Iancu, Niculae, Andrei Fortuna, Cristian Barna, and Mihaela Teodor. (2016). *Countering Hybrid Threats : Lessons Learned from Ukraine*. Washington: IOS Press.

бизнисите кои би можеле да бидат под контрола или влијание на актери вклучени во активностите на хибридните закани. Од овие интеракции произлегуваат неколку сложени односи. Прво, енергетските и другите инфраструктурни зависности можат да создадат економско потпирање или да послужат како алатки за вршење економски притисок. На пример, Русија ја искористи својата позиција како извозник на природен гас не само против Украина, туку и против Европската Унија. Второ, инфраструктурните проекти често привлекуваат странски директни инвестиции, кои можат да носат несигурни намери. Трето, економските тешкотии или нееднаквости може да се манипулираат за да се влеат недоверба во изборните резултати. Четврто, економските предизвици како што се кризите во платниот биланс или зголемениот државен долг може да се користат како наративи за делегитимирање на владите или оправдување акции и геополитички ставови. И на крај, корупцијата во политичките и социјалните области ја поткопува економската безбедност, намалувајќи ја конкурентноста на нацијата на глобалниот пазар. Овие меѓусебно поврзани динамики ја нагласуваат повеќеслојната природа на хибридните закани во економскиот домен.

2.2.4. Социјален домен

Социјалниот/општествен домен примарно се користи за генерирање, интензивирање или искористување на постојните социокултурни поделби. Оваа поделба служи како катализатор за потребните социјални немири кои им овозможуваат на активностите на хибридните закани да напредуваат или да триумфираат.

Во западните општества постојано се дебатира за истакнати прашања како невработеноста, сиромаштијата и образованието, што ги прави подложни цели. Сепак, прашањата способни да предизвикаат или пролонгираат кризи се особено примамливи. Забележителни примери ги опфаќаат неодамнешните економски падови, нерегуларната имиграција и различните форми на напади како што се тероризмот, инциденти со масовни убиства, сајбер-нападите и хемиски, биолошки, радиолошки, нуклеарни и експлозивни инциденти.

2.2.5. Сајбер домен

Терминот „сајбер-домен или димензија“ се однесува на информацискатa средина, која опфаќа сложени мрежи на инфраструктури за информатичка технологија, софтвер, податоци, протоколи, интернет, телекомуникациски мрежи, компјутерски системи и вградени процесори и контролори.[39] Овој меѓусебно поврзан пејзаж ја формира основата за различни сајберактивности. Сајбер-просторот се појави како клучна компонента на хибридните закани. Сè што се случува во физичкиот свет, без разлика дали се работи за политички конфликти, воени дејства или други настани, може да се манифестира и во сајбер-просторот. Ова вклучува активности како сајберкриминал, ширење пропаганда, шпионажа, влијание врз јавното мислење, акти на тероризам, па дури и отворена војна. Иако фундаменталната природа на заканите за националната безбедност не е променета, воведувањето на сајбер-просторот како механизам за испорака драстично го промени пејзажот. Сајбер-нападите може да се извршат брзо, брзо да се шират и да го засилат влијанието на нападот. Покрај тоа, овие напади може да се изведат анонимно и со намалена веројатност за откривање. Цената за достапност во сајберактивности е релативно ниска што ја намали бариерата за влез за различни актери, вклучително и помали. Оваа асиметрија им овозможува на помалите актери да имаат значителна моќ во сајбер-просторот, потенцијално надминувајќи го она што би можеле да го постигнат во традиционалните геополитички домени. Непријателските актери кои работат во сајбер-просторот можат да остварат повеќе цели. Тие може да имаат за цел да предизвикаат деградација, прекин или целосно уништување на мрежите, а со тоа да влијаат на критичните услуги и инфраструктура. Пристапот до податоци и информации е друга цел, која може да вклучи напори за шпионажа и собирање разузнавачки

[39] НАТО во јули 2016 година нагласува дека сајбер-просторот претставува домен на операции кои бараат одбранбени напори еквивалентни на оние во доменот на воздухот, копното, морето, па дури и вселената. Ова опфаќа „сајбер-операции“, „сајбервојна“ и „сајбер-напади“ како примери за такви активности, при што нивната природа варира врз основа на нивниот степен на интензитет. Пошироко за нивната класификација: Schmitt, M. (2012). Classification of Cyber Conflict. *Journal of Conflict and Security Law*, 17(2), 245-260, достапно на: https://doi.org/10.1093/jcsl/krs018

информации.

2.2.6. Културен домен

Дефиниција за културна држава: Културното државно творештво вклучува користење културни и цивилизациски елементи за дефинирање на клучните аспекти на националниот идентитет. Ова може да се направи и во една земја (внатрешно) и како дел од надворешната политика (надворешно). Внатрешно, тој го обликува самоидентитетот на нацијата, додека надворешно проектира привлечна слика за светот.[40]

Разлика од мека моќ: Концептот на културна држава е поврзан со идејата за мека моќ, која беше поставена од Џозеф Наj. Меката моќ често се поврзува со влијанието што го има земјата поради нејзината привлечна култура, вредности и политики. Сепак, културната држава се разликува по потекло. Додека меката моќ произлегува од граѓанското општество, културната држава е водена првенствено од самата држава. Конкретно се фокусира на прашања поврзани со националниот идентитет, историјата и религијата.

Активност на хибридни закани: Хибридните закани се однесуваат на комбинација од конвенционални и неконвенционални тактики кои може да вклучуваат политички, воени, економски, информативни и културни стратегии. Во овој контекст, доменот на културата потекнува од државата и се користи за зајакнување на акциите на хибридни закани.

2.2.7. Инфраструктура

[40] Wilson, J. L. (2016). *Cultural Statecraft in the Russian and Chinese Contexts: Domestic and International Implications*. *Problems of Post-Communism,* 63(3), 135-145, достапно на: https://doi.org/10.1080/10758216.2015.1132630

Дефиниција за критична инфраструктура: Европската дефиниција ја дефинира критичната инфраструктура како средство, систем или негов дел лоциран во земјите членки, што е од суштинско значење за одржување на виталните општествени функции, здравјето, безбедноста, безбедноста, економската или социјалната благосостојба на луѓето. Нарушувањето или уништувањето на критичната инфраструктура може значително да влијае на земјата членка поради неуспехот да се одржат овие функции.[41]

Видови ранливости: Ранливостите може да бидат специфични за секторот, зависни од времето (временски), како што е зголемената побарувачка за време на природни катастрофи или повторливи (циклични) врз основа на специфични услови. Овие пропусти може да доведат до низа ефекти врз критичната инфраструктура.

2.2.8. Разузнавање

Дефиниција на разузнавањето: Според „Lowenthal"[42], разузнавањето се однесува на процес кој вклучува стекнување, анализа и ширење специфични видови информации клучни за националната безбедност. Тоа вклучува производство на разузнавачки производи, заштита на процеси и информации преку контраразузнавачки напори и извршување овластени операции.

Улога во хибридните закани: Во контекст на хибридните закани, интелигенцијата се користи на два главни начини. Актерите кои користат хибридни закани ги користат нивните сопствени разузнавачки способности за да ги поддржат нивните активности или да се обидат да влијаат на разузнавачките операции на целната држава. И двата пристапа имаат за цел да ја поткопаат

[41] Council of the European Union. (2008). Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. Official Journal of the European Union, 75–82.

[42] Lowenthal, M. M. (2015*). Intelligence: From Secrets to Policy* (6th ed.).

способноста на целната држава да одржува свесност за ситуацијата.

2.3. Други домени

Вселена: услугите во овој домен опфаќаат навигација, комуникации, далечинско набљудување и наука и истражување. Загриженоста се јавува во врска со активностите на хибридна закана во вселената поради развојот на контрапросторните способности од повеќе државни актери. Хибридните операции во вселената влијаат не само на воените/одбранбените, туку и на цивилните комерцијални активности зависни од вселенските способности. Овој домен е во меѓузависна врска со воени/одбранбени домени, економија, инфраструктура, информации и разузнавачки домени.

*Јавна администрација: ј*авната администрација ги преточува јавните политики во резултати. Дихотомијата политика-администрација игра фундаментална улога во европските општества. Администраторите ги толкуваат законите, ги оценуваат политиките и придонесуваат за креирање политики.

Правен домен: правниот домен вклучува правни правила, дејства, процеси и институции кои се користат за постигнување правни или неправни ефекти во контекст на хибридна закана. Законот се користи како алатка или компонента на хибридни закани, вклучително и искористување на правните прагови, празнините и сложеноста. Правото се користи за таргетирање ранливости во демократските општества, постигнување нарушувачки ефекти и влијание на други домени.

Дипломатија: дипломатијата вклучува водење меѓународни односи и надворешна политика. Активностите за хибридни закани во дипломатијата имаат за цел да создадат поделби, да ги поддржат информативните кампањи и да влијаат врз донесувањето одлуки. Дипломатијата има врски со политички,

економски, социјални и правни домени. Дипломатските санкции и бојкотите можат да влијаат на економијата на целната држава.

3. Модели за спротивставување

3.1. „CORE“ – модел за градење отпорност

Целта на непријателскиот актер со користење хибридни закани е да ги поткопа и да им наштети на интегритетот и функционирањето на демократиите, да ги промени процесите на донесување одлуки и да создаде каскадни ефекти. Сеопфатниот екосистем за отпорност (CORE) служи за подобро разбирање и ублажување на дејствата и целите на непријателските актери. CORE ни овозможува да го моделираме целото општество, на тој начин создавајќи подобро разбирање на концептот на целото општество во контекст на хибридните закани и ни овозможува да го следиме влијанието на хибридните закани врз целото општество, како и да изведеме насочена отпорност – градење отпорност. Пристапот на екосистемот ја претставува динамиката на интеракцијата што ги поврзува 13-те домени од концептуалната рамка со три простори (граѓански, владеење, услуги) и нивните слоеви (локален, национален, меѓународен).

Отпорноста против хибридните закани користи мерки за отпорност во различни домени. Но, ова е недоволно, бидејќи карактерот на хибридните закани е двосмислен, креативен, користи мамки, ја замаглува ситуациската свест, цели на широк опсег на домени и продолжува да бара и создава нови ранливости. Сеопфатниот екосистем за отпорност може да промовира меѓусекторски напори на целото општество со правење преглед на клучните меѓусебни врски помеѓу прашањата кои честопати се решаваат одделно во различни простори. Обезбедува методологија за да се постигне подобро разбирање на однесувањето помеѓу сложените системи, институции и општествени фактори и ја подобрува проценатa на каскадните ефекти од хибридните закани и ефектите од интервенциите на политиките. Методологијата на екосистемот ја претставува динамиката на интеракцијата што ги поврзува доменитe со трите простори и нивните слоеви. Доменитe се сметаат како влезни точки и преку нив нападите може да се шират на

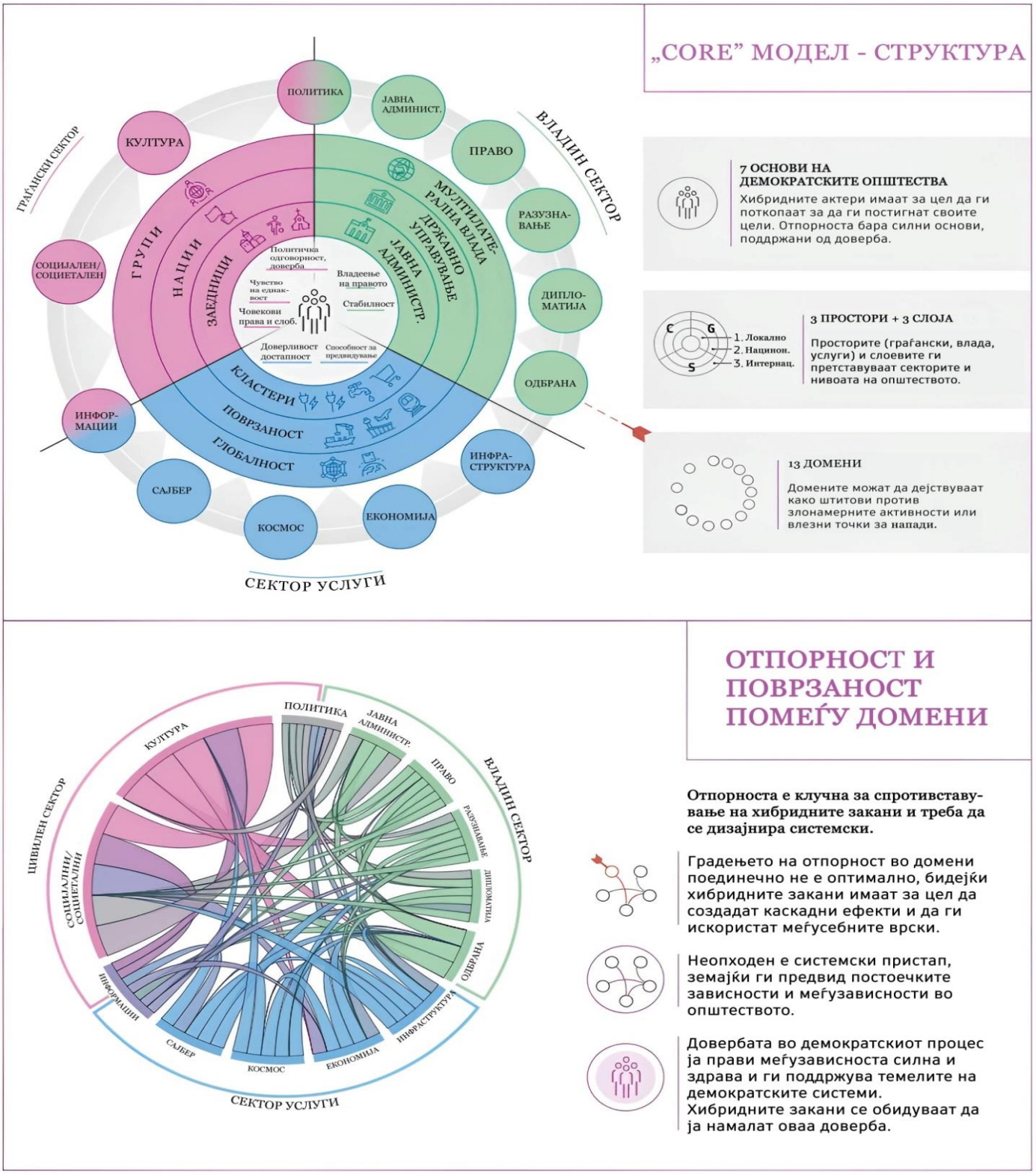
различни простори и нивните соодветни слоеви. Оттука, градењето отпорност на хибридни закани значи да се земат предвид следните клучни елементи:

– *Способноста на противникот да го промени нашето одлучување за да ги усогласи нашите цели со нивните стратегиски цели* – затоа е неопходно да ги знаеме стратегиските цели на непријателот, како и да се познаваме себеси и да ги разјасниме нашите стратегиски цели. Предвидувањето може да игра клучна улога во овој процес.

– *Да ги поткопа демократските основи* – актерите на хибридните закани на крајот сакаат да ги оспорат основите на демократските општества, односно вредностите, нормите и очекувањата на демократските општества.

– *Синхронизирана употреба на различни алатки* – ова може да доведе до ситуација во која различните делови на ЕУ и/или земјите членки се под постојан стрес. Постои можност екосистемот континуирано да ги апсорбира негативните влијанија и да реагира на нивните ефекти без шанса да закрепне и (подобро) да се подготви за следниот настан – и двата се составен дел од градењето отпорност. Ако фокусот е само на домените кои првично се таргетирани, обновувањето во еден домен може да ги остави другите домени ранливи.

– *Каскадни ефекти што може да се појават низ домени, простори и слоеви* – еластичноста против хибридните закани не е (само) отпорност на една алатка, или ефективноста на една алатка во еден домен, туку и отпорност на ефектите што се шират низ домени.



Слика 1: Модел/структура и отпорност и поврзаност меѓу домени[43]

[43] Jungwirth, R. et al. (2023). *Hybrid threats: a comprehensive resilience ecosystem*. Publications

Основи на екосистемот

Седумте основи на екосистемот се следниве:

1. Чувство на правда и еднаков третман;
2. Граѓанските права и слободи;
3. Политичка одговорност и отчетност;
4. Владеење на правото;
5. Стабилност;
6. Доверливост/достапност и
7. Предвидувачки способности.

Во овој модел, темелите се во центарот и се опкружени со различни слоеви на отпорност. Во најдобар случај, со зголемување на отпорноста во еден дел од екосистемот, се зголемува отпорноста на целиот систем. Во најлош случај, тоа е намалено. Понатаму, меѓусебните врски помеѓу домени се клучни за градење отпорност на хибридни закани. Бидејќи ефектите од хибридните закани може да се шират низ домени, неопходно е да се прекине ширењето и да се ограничат ефектите – слично како да се изгради „заштитен ѕид“. Ова не значи дека домените треба да се исклучат, туку дека самите врски треба да станат отпорни. Очигледен предуслов е да се знае за овие врски како во *моделот за отпорност и поврзаност помеѓу домени*, подолу. Во однос на свесноста и зрелоста за отпорноста, неколку домени се понапредни од другите, со „инфраструктура“ и „сајбер“ кои имаат висока свест за отпорност и висока зрелост врз основа на одговорите добиени од земјите членки на ЕУ за време на втората повторена Анкета за хибриден ризик (свест) и на полуквантитативен преглед на литература (зрелост). Спротивно на тоа, домени како „култура“ или „правен“ имаат пониска свест и зрелост. Со оглед на сложените интеракции и поврзаноста помеѓу доменитe, оние кои се помалку отпорни може да бидат влезна точка за системски неуспеси и големи каскадни ефекти. Предуслов за овој холистички пристап е длабинското разбирање на нивото на зрелост и подготвеност во однос на мерките за отпорност, практиките и

Office of the European Union, Luxembourg, pp. 39, 41.

алатките и свесноста од страна на властите за важноста од градење отпорност во специфичен домен за справување со хибридни закани.

Екосистемот се состои од три простори – граѓански, управувачки и услуги – кои ги претставуваат трите сектори на општеството. Домените се поврзани со трите простори според нивната релевантност. Понатаму, темелите на екосистемот се исто така поврзани со специфични простори. Накратко, екосистемот, како и секој простор, може да се замисли како составен од домени, врски меѓу домените, како и релевантни основи. Заедно со слоевите, кои ќе бидат претставени подолу, ова го претставува „whole-of-society approach“ – сеопфатен општествен пристап.

А) Граѓански простор/сектор

Граѓанскиот простор ги опфаќа оние интеракции кои го сочинуваат јавниот живот на општествата – колективните и индивидуалните права, должности и слободи на граѓаните. Јавниот живот се поврзува со три различни слоеви: групи, нации и заедници. Најважни домени кои се вклучени во овој простор се општествените, културните и до одреден степен и информативните и политичките домени. Граѓанскиот простор во демократиите почива на три основи: правда и еднаков третман; граѓански права и слободи; политичка одговорност и одговорност. Улогата на просторот на владеење е, пак, да ја зајакне отпорноста на граѓанскиот простор преку заштита на процесите и институциите на демократијата. Отпорноста на граѓанскиот простор го намалува ризикот од надворешно мешање. Социјалната кохезија, ефикасното демократско размислување, еднаков третман и културата на доверба и дискусија се клучни маркери за отпорен граѓански простор. Може да се идентификува врската помеѓу довербата и зголеменото ниво на отпорност во граѓанскиот простор. Довербата е клучна во чувството на сигурност, чувството на предвидливост и одржувањето на социјалната кохезија. Тоа ја означува довербата во општеството како целина.

Б) Владин простор/сектор

Просторот на владеење е местото каде што јавните институции ги извршуваат своите мандати, ги регулираат јавниот и приватниот живот, носат политички одлуки и се одговорни пред политичкото тело. Слоевите кои се дел од просторот на владеење се локалното управување, управувањето на државно ниво и мултилатералното управување. Релевантните домени овде се администрацијата, дипломатијата, правниот, политичкиот, разузнавачкиот и војската, поткрепени со темелите на владеењето на правото и стабилноста. Отпорноста во просторот на владеење може да се толкува како одржување на состојбата на автономија и слобода на дејствување како предуслов. Од една страна, просторот за управување делува како овозможувач на отпорност на другите простори, бидејќи игра централна улога во изготвувањето на законодавството за подготвеност, управувањето и развојот, како и во спроведувањето на мерките за подготвеност и управувањето со кризи. Од друга страна, цел на владеењето е постигнување отпорност, која во крајна линија се претвора во континуитет на владата, институциите и нивното работење на локални, државни и мултилатерални слоеви, во време на вознемиреност или криза.

В) Сектор услуги

Овој простор се состои од системи, инфраструктура, снабдување, логистика и синџир на вредности кои се зависни од приватниот сектор, истовремено од суштинско значење за општествената безбедност. Трите слоја на овој простор се врски, кластери и глобални. Домените кои припаѓаат на просторот за услуги се сајбер, космос, инфраструктура, економија и информации. Основите за овој простор се доверливоста (достапност на стоки и услуги) и способноста за предвидување (трендови, идни случувања и можни нарушувања). Отпорноста во просторот на услугите го поддржува доброто функционирање на општеството со припитомување на ефектите од активноста на хибридната закана и намалување на нивниот разурнувачки потенцијал. Тоа може да се постигне со складирање

основни добра, одржување разновидни и отворени пазари, консултации, соработка и координација помеѓу јавниот и приватниот сектор, усогласување и координирање на регулативната рамка во рамките на единствениот пазар и систематска размена на информации.

Слоеви на екосистемот

Слоевите на екосистемот ги претставуваат различните „нивоа“ што постојат во организацијата на општеството, од локално до меѓународно. Таквото раслојување може да се забележи во сите три простори. Разликата е важна, бидејќи влијанието, како и начинот на работа на активноста на хибридната закана е различен во соодветните слоеви.

Локални простори/сектори

Заедници — Заедниците се составени од поединци со објективни или субјективни афинитети во политиката, социјалниот, економскиот, културниот или друг домен. Заедниците може да се формираат поради секторски интереси (економски и социјални), идентитетски прашања (религиозни, етнички, полови, генерациски), идеолошки (заштита на животните, животна средина, активисти за правата на оружјето) или теми поврзани со слободното време (на пр., лов, пливање и сл.). Тие може да бидат и ентитети кои имаат чувство на единство или припадност како села, училишта, соседство. Заедниците се ентитети на микониво кои се секогаш многу локални. Тие се дел од една нација и може да имаат врска со заедниците што ги преминуваат границите.

Локална администрација – Значителен дел од политичките одлуки кои влијаат на луѓето секојдневниот живот ги носат општинските одбори и совети, бидејќи локалната администрација често е задолжена за мошне важни функции: социјалните услуги, здравствената заштита и образованието. Улогата на локалното ниво во пределот на хибридните закани дополнително се зголемува со глобалниот тренд кон урбанизација. Локалната власт е, исто така, таа која треба да

одговори на различни нарушувања, кои може да бидат предизвикани од надворешен актер (или не). Локалната самоуправа, исто така, секојдневно има интеракција со сите три слоја на граѓанскиот простор. Денес, повеќе од половина од светското население живее во урбани средини.[44] Предизвиците за одржливиот развој, како што се климатските промени, економската и социјалната политика, прашањата за интеграција и миграција, во голема мера се решаваат на ниво на градот.[45] Градовите се исто така централни точки за социјална тензија, додека поединечните места во нив може да добијат огромен симболичен статус во социјалните движења. Ова значи дека градовите сè повеќе може да бидат цел на хибридни закани.

Кластери – Кластерите се последната алка во синџирите на снабдување за стоки и услуги каде што ја задоволуваат индивидуалната побарувачка на потрошувачите. Тие може да бидат силно погодени од врските и глобалните слоеви на просторот за услуги, бидејќи синџирите на снабдување и логистика се во голема мера зависни од глобалните трендови, нарушувањата во светската економија, како и од нарушувањата во слојот „врски“. Прекините во двата слоја може да ги остават кластерите изолирани и оставени на нивните сопствени капацитети. За одредени критични услуги и стоки, овој слој е исто така под влијание на просторот на управување (на пример, транспортните мрежи ги гради и одржува државата). Правилната рамнотежа на влијание од просторот на владеење има директно влијание врз отпорноста на кластерите (на пример, постигнувањето стратегиска автономија може да биде дефинирана цел). Преку врските и глобалните нивоа, паралелните кластери исто така ќе влијаат еден на друг (на пр., транспорт на стоки од еден кластер до друг преку глобални синџири на снабдување).

---

[44] United Nations. (2014, July). UN News - Brazil 2014 'remarkable platform' to unite people, says Assembly President. Retrieved from https://news.un.org/en/story/2014/07/472752

[45] UN-HABITAT. "World Cities Report 2016: Urbanization and Development - Emerging Futures." 2016, достапно на: https://unhabitat.org/sites/default/files/download-manager-files/WCR-2016-WEB.pdf.

Национални слоеви

Нација – Концептот нација различно се сфаќа во источните и западните култури. Источното разбирање е дека нацијата ја прави државата, а западното разбирање е дека државата ја прави нацијата. Иако е поедноставување, од перспектива на хибридна закана, ова е многу важна разлика. Ако источното сфаќање е дека државата ја прави нацијата, тогаш тоа е исто така она што треба да се скрши пред да може да се ослабне државата. Концептот на нација се гледа и како политички или општествен конструкт, но централен извор на единство. Често се гледа дека нацијата има заеднички наратив за нејзиното потекло, историскиот национален континуитет, јазик, територија и традиции итн. – работи што обединуваат. Градењето нација е поврзано со градењето на државата и градењето на државата со градењето на нацијата. Токму оваа врска стана уште поважна во денешниот свет и заслужува дополнителна анализа. Ако некој надворешен актер успее да ја прекине врската помеѓу нацијата и државата, тој успеал да им наштети и да ги поткопа државата и нејзиниот демократски систем. Ова станува уште покомплексно кога гледаме на меѓународно ниво.

Основните државни институции (собрание, државна администрација, судови, армија) се таму за да ги извршуваат своите законски дефинирани функции и да ги одржуваат законитоста, функционирањето и предвидливоста во државата. Институциите мора да бидат отпорни на сите предизвици кои потекнуваат надвор од законскиот, демократски процес на одлучување. Ова е особено важно во случајот со судството, бидејќи само судовите можат да го дадат конечното, убедливо толкување на законот. Во некои неодамнешни предизвици, се гледа дека институциите (особено судовите) успешно го стабилизираат процесот, каде што општеството потенцијално се движи кон уставна криза (Брегзит и протестите во 2021 година по претседателските избори во Соединетите Држави).

Врски – Врските се јазли на синџирите на снабдување со стоки и услуги каде што глобалните синџири на снабдување се во контакт со повеќе локални кластери. Во оваа смисла, слојот „поврзување“ може да се гледа како буквална врска помеѓу

глобалното ниво и нивото на кластерот во просторот за услуги. Нарушувањата во овој слој можат да ги отсечат кластерите од глобалното ниво, оставајќи ги кластерите изолирани и оставени на нивните сопствени капацитети. Нарушувањата во овој слој, исто така, може негативно да влијаат на глобалните синџири на снабдување, доколку кластерот кој е единствен снабдувач на одредено добро или услуга е отсечен од глобалното ниво. Примери за овој слој може да бидат пристанишни објекти од стратегиска вредност, како и одредени критични транспортни патишта (како Суецкиот Канал).

Интернационални слоеви

Групи – Групите во граѓанскиот простор ги надминуваат државните граници и формираат транснационални мрежи на афинитети меѓу различните групи во секоја нација. Групите и мрежите се во основата на транснационалниот граѓански простор кој за низа политички, економски и социјални прашања се исклучително активни, како на пример во справувањето со климатските промени. Групниот слој е особено релевантен за идентификување на субјективните и објективни чувства кои поврзуваат различни групи преку националните граници.

Управување на мултилатерално ниво – Управувањето на мултилатерално ниво е меѓународен слој во кој државите и наднационалните институции комуницираат во рамките на државната дипломатија или во рамките на регионалната или глобалната интеграција. Мултилатералниот слој ги концентрира интеракциите на мандатите, делегираните надлежности и споделените надлежности особено во контекст на ЕУ кои го одредуваат однесувањето на меѓудржавните односи во Европа. Мултилатералниот контекст на ЕУ ги тера националните институции да се поврзуваат и да соработуваат со институциите на други држави преку различни аранжмани. Државите обично многу се двоумат дали да ги отстапат основните извршни овластувања како што се полицијата, националната одбрана, оданочувањето и надлежноста за законодавство. Сепак, постојат такви мултилатерални аранжмани, каде што одредена институционална моќ е делегирана на наднационалните органи

(меѓународните трибунали, Советот за безбедност на ОН, некои делови на ЕУ итн.).

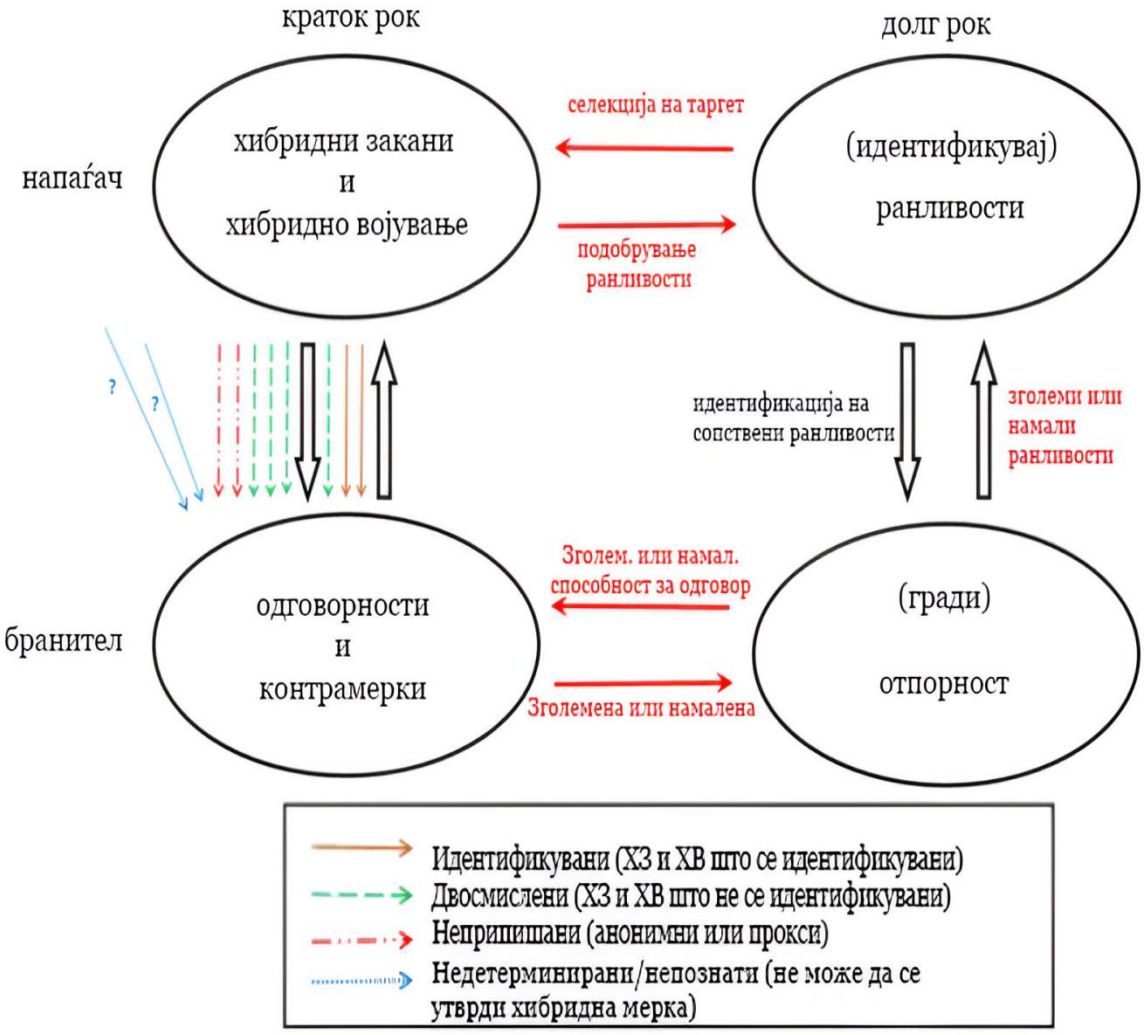
Глобално – Глобалниот слој ја означува околината на зависности на макроекономско ниво помеѓу пазарите, како и глобалните синџири на снабдување и вредност. Глобалното ниво е во интеракција со кластерите (непосреден контакт и перцепција од поединци) и врските (јазли на даватели на стоки и услуги) и заедно со нив го формира пејзажот на глобалните меѓузависности. Ова ниво често се смета дека има директно влијание врз животите на поединците, додека исто така се смета дека е надвор од контролата на поединецот и надвор од контролата на управувањето на локално и државно ниво (на пр., цената на одредени стоки зависи од глобалниот пазар, одредени мултинационални компаниите изгледаат „помоќни“ од државите итн.).[46]

3.2. „Hybridity Blizzard“ – модел на снежна бура

Моделот на снежна бура претставува шематски приказ на меѓусебно поврзаната динамика помеѓу бранителите и напаѓачите и на краткорочни и на долгорочни перспективи. Истакнува како различните димензии на времето и актерите комуницираат, прикажувајќи ги овие интеракции како екосистем. Оваа аналогија помага да се разбере сложеноста на хибридноста. Иако традиционално не се живи, споредувањето на интелигентните општествени актери на бојното поле со „живи“ ентитети е корисен начин за моделирање на нивните стратегии, измами и негирање на користење различни методи и алатки во хибридни конфликти. Овој концепт е исто така вреден за разбирање на интеракцијата помеѓу хибридните закани и хибридното војување, одговорите, контрамерките, трајните ранливости и еластичноста. Во суштина, ова опкружување функционира како систем каде што сите елементи заемно влијаат еден на друг, водени од интелигентни општествени актери кои имаат за цел да ги надминат своите

[46] Jungwirth, R. et al. (2023). *Hybrid threats: a comprehensive resilience ecosystem*. Publications Office of the European Union, Luxembourg, pp. 41, 47.

противници.



Слика 2: Модел на хибридни закани и хибридно војување[47]

Моделот вклучува две клучни димензии: време и актери. Овие димензии се од суштинско значење бидејќи хибридните закани и хибридното војување (ХЗ и ХВ) се тековни и меѓусебно поврзани. Моделот вклучува два главни актери – бранителот и напаѓачот – и ги разгледува и краткорочните и долгорочните

[47] Weissmann, M. et al. (2021). *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: I.B. Tauris, достапно на: http://dx.doi.org/10.5040/9781788317795 (p. 268).

перспективи. На краток рок, ХЗ и ХВ вклучуваат постојана интеракција помеѓу дејствата на напаѓачот и одговорите на бранителот. Ова е континуиран процес без фиксна почетна или крајна точка. Долгорочната перспектива се фокусира на конкуренцијата помеѓу ранливоста на бранителот и напорите да се изгради еластичност. Напаѓачот ги искористува пропустите, додека бранителот ги идентификува за да ја зголеми отпорноста. Овој процес создава врска напред-назад помеѓу ранливостите и отпорноста. Оваа интеракција помеѓу краткорочните и долгорочните перспективи се однесува и на изборот на целта на напаѓачот, каде што идентификуваните пропусти играат клучна улога.

Иако поедноставениот модел нуди аналитички увид, тој не ја опфаќа целосно сложеноста на реалниот свет ХЗ и ХВ. Авторите предлагаат изработка на покомплексен „Hybridity Blizzard Model“, каде што хибридните закани се споредуваат со снежна бура од непредвидливи настани.[48]

3.3. Фази

Европскиот центар за извонредност за спротивставување на хибридните закани ги категоризира хибридните закани во две фази: 1. фаза на подготвување (актерите се подготвуваат со идентификување канали за влијание, искористување ранливости и практикување тактики за диверзија) и 2. оперативната фаза (комбинирање методи за постигнување цели, потенцијално вклучувајќи воена сила како хибридна војна). Овој труд ја исклучува хибридната војна, фокусирајќи се на комбинации на невоени методи. Хибридното влијание вклучува прикривање фази и врски, споредени со блефирање и опортунизам на покер, контраст на шах. Методите на влијание опфаќаат информативно, финансиско, физичко, политичко, сајберсредства и политичко насилство. Демократските општества користат различни методи за да влијаат на мислењата и одлуките. Влијанието не е инхерентно заканувачко; класификацијата зависи од нормативното оценување.

[48] Weissmann, M. et al. (2021). *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: I.B. Tauris, достапно на: http://dx.doi.org/10.5040/9781788317795 (p. 268).

3.3.1. Примарна

Механизмот на прајминг вклучува два клучни елементи:

1. Активирање на репрезентациите на меморијата: Ова подразбира стимулирање на репрезентациите на меморијата преку процес на ширење на активирањето во семантичка мрежа на асоцијации.
2. Употреба на активации за кодирање: активираните репрезентации потоа се користат за кодирање информации за социјални цели.[49]

Штетните информативни активности спроведени од странски државни актери вклучуваат проучување на поделбите, контроверзиите и проблемите на општеството за да се нарушат воочените области на тензија користејќи нелегитимни методи.[50]

3.3.2. Оперативна

Во оперативната фаза може да се вбројат фазата на дестабилизација во која актерот ја интензивира активноста преку кампања (повеќе операции), или да ја користи за една операција со цел да ја архивира назначената цел и фазата на принуда (може да се означи и како хибридна војна/војна).

Фаза на дестабилизација – Откривањето промени во фазата на дестабилизација е сложено. Тоа вклучува зголемена видливост, агресија, па дури и насилство поради потребите на актерите, можностите или фрустрациите. Ова ги тестира границите на прифатливост, законитост и влијанија. Фазата на дестабилизација повлекува енергични наративни промоции, дезинформации, пропаганда и сајбер-напади. Акциите на интернет може да преминат во реални

---

[49] Molden, Daniel C. (2014). *"Understanding Priming Effects in Social Psychology: What Is "Social Priming" and How Does It Occur?"* Social Cognition. Vol. 32.

[50] Pamment, James, Howard Nothhaft, and Henrik Agardh-Twetman. (2018). *"Countering Information Influence Activities."* Swedish Civil Contingencies Agency.

протести или немири за да ги дестабилизираат општествата. Фазата ги искористува меѓусебно поврзаните области како што се надворешната/внатрешната безбедност, цивилно-воените односи и правните рамки. Одговорите се несоодветни поради долгорочните интереси наспроти краткорочните цели. Донесувањето одлуки е под притисок за време на дестабилизацијата, притискање на избори за деловни договори, меѓународни одлуки и сојузи. Идеалната основа за донесување одлуки бара ситуациска свест и различни перспективи, но надворешниот притисок го комплицира ова. Ако целите не се исполнети, активноста може да се врати на подготвување или да ескалира врз основа на стратегиското значење, одговорите и можностите.

Фаза на принуда – Последната фаза е принуда, што го означува преминот кон хибридна војна. Тоа вклучува мешавина од тајни и отворени воени дејства, политички и економски мерки, субверзија, пропаганда, специјални сили и сајбер-напади. Хибридното војување користи сила и опфаќа различни домени, вклучително и неконвенционални тактики. Овој тип војување не е нов; тоа е често асиметрично, со послаби актери кои се спротивставуваат на воените недостатоци. Тоа е во контраст со симетричното војување. Хибридната војна се користи од послаби или непријавени актери и вклучува конфликти помеѓу воено нееднакви страни или различни стратегии. Таа ги оспорува воспоставените правила и доктрина поради еволутивната природа и употреба на прокси.

4. Хибридните закани во Република Северна Македонија. Разбирање на ранливости

4.1. Поширок контекст на безбедносните предизвици во Република Северна Македонија

Во ризици и опасности по безбедноста на Република Северна Македонија спаѓаат: можните манифестации на екстремен национализам, расна и верска нетрпеливост, облиците и активностите поврзани со меѓународниот тероризам, организираниот криминал, нелегалната миграција, нелегалната трговија со дрога, оружје, луѓе, материјалите за двојна употреба, како и последиците од употребата на средствата за масовно уништување, поседувањето големи количини илегално оружје, транзициските проблеми како што се: корупцијата, урбаниот тероризам, тешкиот криминал, вклучувајќи уцени, рекетирање, убиства и напади врз сопственоста на граѓаните, економскиот криминал, даночната евазија, недоизграденоста на институциите на демократскиот систем, проблемите во функционирање на судството, социјалните проблеми и невработеноста, активностите на странските специјални служби насочени кон влошување на безбедносната состојба, со тоа и забавување на демократските и интегративните процеси, особено на оние кон НАТО и ЕУ, последиците од судир на интереси за користење на изворите и патиштата на стратегиските енергенси, како и попречување и блокирање на нивниот извоз во Република Северна Македонија, елементарните и други непогоди, техничко-технолошките катастрофи, заразните заболувања на луѓето и животните предизвикани од домашни и/или надворешни чинители; компјутерскиот криминал, пиратството и злоупотребата на информатичката технологија особено во делот на личните податоци на граѓаните, деловната, службената и државната тајна и деградација и уништувањето на животната средина.

4.2. Тековен безбедносен пејзаж и ранливости

Хибридните закани во Република Северна Македонија имаат различни форми и често вклучуваат комбинација на конвенционални и неконвенционални методи насочени кон дестабилизација на земјата.

Сајбер-напади: Сајбер-нападите врз владини институции, критична инфраструктура или бизниси може да го нарушат работењето, да украдат чувствителни информации или да создадат економска нестабилност.

Етнички и социјални тензии: Хибридните закани може да ги искористат постојните етнички или социјални тензии во земјата за да поттикнат насилство или немири.

Енергетска безбедност: Заканите врз енергетската инфраструктура или прекините во снабдувањето со енергија може да ги поткопаат националната безбедност и економската стабилност.

Гранични инциденти: споровите или инцидентите долж границите на земјата може да ги ескалираат тензиите и да создадат нестабилност.

Економска принуда: Економскиот притисок, како трговски ограничувања или санкции, може да се користи како хибридна тактика за да се влијае на политиките на една земја.

Полномошници: Државните актери може да вработат посредници или поединци за да вршат поткопувачки и нарушувачки активности за да го прикријат нивното делување.

Политичко мешање: Обидите за мешање во домашните политички процеси, како што се изборите, може да се сметаат за хибридна закана.

4.3. Импликациите на хибридните закани врз безбедноста на Република Северна Македонија

Клучни во хибридните закани се цивилните инструменти на моќ. Во тие рамки се експлоатираат ранливостите предизвикани од социокултурните промени, а за остварување на влијанието често се користи влијателноста на

граѓанскиот сектор. Важен елемент на хибридната закана е користењето економски инструменти на моќ. Економските инструменти вклучуваат странски директни инвестиции, кредити со ниски камати, финансирање културни настани, финансирање политички партии, како и финансирање радио и ТВ-станици и енергетски мрежи. Економски инструмент на хибридна закана е и корупцијата. Корупцијата овозможува директен пристап до чувствителни информации за генерирање компромитирачки материјал и поткопување на авторитетот на политичкото лидерство, како и за заплашување на критичарите на напаѓачот. Воедно, корупцијата овозможува финансирање политички партии и незадоволни групи кои може да бидат искористени за остварување на целите на напаѓачот. Еден од методите кој може да се искористи за влијание врз економијата и информативниот сектор, како и другите клучни сектори на една држава, е злоупотреба на сајбер-просторот од страна на недржавни и, пред сè, државни актери. Хибридната закана е со големи можности за делување, пред сè во информативниот сектор. Можеби највидлива метода на хибридната закана е употребата на инструменти во информативниот сектор. Овие операции се посебно фокусирани кон политичката елита и граѓанскиот сектор, а се синхронизирани со политичките, економските, воените и дипломатските активности на субјектот кој ја креира хибридната закана. Информативните операции вклучуваат користење медиуми, „ботови“ и „тролови“ на социјалните мрежи, но и методи со пласирање лажни научни теории во јавноста, парадигми, концепти и стратегии кои влијаат врз државната администрација, во насока за намалување на потенцијалот за национална одбрана.[51]

[51] Национална стратегија за градење отпорност и справување со хибридни закани, 2021, стр. 6.

4.3.1. Минати инциденти со хибридни закани

Говор на омраза и насилство помеѓу Македонците и Албанците, како и навреди и говор на омраза кон Бугарите, Ромите и ЛГБТ заедницата, бележи последниот извештај на Европската комисија против расизам и нетолеранција – ЕКРН[52].

Европската организација е особено загрижена за насилството мотивирано од омраза кое се јавува помеѓу етничките Македонци и Албанци, и препорачува надлежните да го сфатат овој проблем сериозно и да одговорат адекватно, вклучително и со спроведување ефективни истраги за таквите инциденти и казнување на одговорните.

Говорот на омраза помеѓу Македонците и Албанци се случува во секојдневните интеракции помеѓу членовите на двете етнички групи, забележува ЕКРН.

„На пример, меѓу ученици во јавниот транспорт. Се чини дека повеќето вакви инциденти не се пријавени кај надлежните“, пишува во извештајот и се заклучува:

„Позитивно е што, и покрај континуираните меѓуетнички тензии помеѓу двете заедници, тоа досега не доведе до значително ниво на верска омраза и нетолеранција или на антихристијански или антимуслимански говор на омраза.“

Според сознанијата на ЕКРН добиени од македонските граѓански организации, во последните неколку години неофицијално имало околу 800 инциденти мотивирани од омраза. Во околу 70 % од тие случаи се работело за инциденти помеѓу млади од македонската и албанската етничка заедница, кои најчесто не биле пријавувани.

ЕКРН препорачува да се преземат напори за прекин на „де факто сегрегацијата на децата“ од македонско и албанско етничко потекло во мултијазичните училишта.

ЕКРН дава препораки за справување со овие грижи и промовирање

[52] Извештај на ЕКРН за Република Северна Македонија (шести циклус на мониторинг), усвоен на 29 јуни 2023, објавен на 20 септември 2023, достапен: https://www.coe.int/en/web/european-commission-against-racism-and-intolerance/-the-former-yugoslav-republic-of-macedonia-

понатамошен напредок, особено: доделување финансиска автономија на телата за еднаквост, регулирање на признавањето на родовиот идентитет, интензивирање на напорите за борба и пријавување на криминалот од омраза, справување со сегрегацијата во образованието и продолжување на напорите за подобрување на вклученоста на Ромите.

ЕКРН смета дека Комисијата за спречување и заштита од дискриминација се соочува со предизвици во обезбедувањето соодветен персонал и буџетски ресурси. Тие, како и народниот правобранител, се борат со проблеми предизвикани од потребата за одобрение од Министерството за финансии за секоја финансиска трансакција што сакаат да ја направат од сопствените буџети, ограничувајќи ја ефикасноста и потенцијално претставувајќи ризик за нивната севкупна независност.

- **Објаснителна студија на случај. Дезинформации, прва алатка во хибридните операции**

Дезинформациите обично претходат на операции од арсеналот на хибридни закани. НАТО активно ги следат дезинформациите и пропагандните кампањи и од државни и од недржавни чинители. За таа цел ќе биде претставена студија на случај во нашата држава, каде што ќе бидат опишани дезинформацијата, карактерот и соодветниот одговор на сите институции на системот, за да се елиминира нејзиниот импакт кон дестабилизација. Секој обид за делување на странски безбедносни служби во однос на компјутерската безбедност, инфилтрација и пласирање одредени дезинформации, несомнено, би имало влијание врз безбедноста и функционирањето на безбедносниот систем на државата. Во таа смисла, неопходно е сензибилизирање и препознавање на хибридните операции, кои не престануваат и постојано се модифицираат.

Во таа насока да ја зацврстиме тезата за нивната сериозност, ќе споменеме две изјави на НАТО претставници:[53]

[53] Stojanova, M., Cocovski, Z., & Kolovska, V. (2020, December 14). Г*радење отпорност против насилниот тероризам и екстремизмот*.

„Тие се обидуваат да посеат поделба, да ги поткопаат нашите демократии и нашата способност за дејствување. Руски официјални лица, на пример, тврдат дека сојузниците на НАТО се одговорни за коронавирусот и дека авторитарните режими се подобри од демократиите за зачување на безбедноста на својот народ“, вели претставник на Алијансата во Брисел.

„Тесно соработуваат и со Европската Унија за идентификување, следење и откривање на дезинформациите. Слободните медиуми имаат клучна улога во спротивставувањето на дезинформациите и пренесувањето точни информации до јавноста“, велат од НАТО.

- **Пријави за лажни вести**

Во април и во мај 2016 година, домашниот банкарски систем беше под силно влијание на нестабилната политичка состојба во земјата, придружена со шпекулации за девалвација на курсот на денарот и за стабилноста на домашните банки и депозитите. Тогаш шпекулативните притисоци ја разнишаа довербата на граѓаните во банкарскиот систем, што предизвика ефект на снежна топка и повлекување на депозитите. Ширењето паника во 2016 година предизвика повлекување пари од банките.

Потоа полицијата испрати пријави за 10 дописи до обвинителствата за ширење лажни вести преку веб-портали и социјални медиуми за време на вонредната состојба со коронавирусот, потврдија за медиумите од Секторот за компјутерски криминал и дигитална форензика. Во време кога светската пандемија со коронавирусот почна да ја обиколува државата, полицијата „улови“ неколку портали и корисници на социјални мрежи кои кај нас шириа лажни вести.

Пријавите се за правни и физички лица, кои ги прекршиле членовите 205 и 206 од Кривичниот законик. Тие членови се однесуваат на кривични дела против здравјето на луѓето, поточно за пренесување заразна болест и за непочитување на здравствените препораки и владините мерки.

Неколкумина обвинители со кои разговараше БИРН[54] потврдија дека

[54] БИРН Македонија е независна невладина организација основана во 2004 година како дел од

членовите од Законот на кои се повикала полицијата кога ги поднела известувањата до Обвинителството се неприменливи за натамошно процесирање. Токму затоа, од сите стигнати десет известувања досега, скопското Обвинителство донело наредба за собирање дополнителни податоци само за еден случај, кој најверојатно содржи елементи на други кривични дела.

Обвинителката Лидија Раичевиќ од скопското Обвинителство вели дека за ова на нејзините колеги кои постапуваат по начелото на легалитет им се врзани рацете.

„За вакви известувања јавен обвинител не би можел да постапува, затоа што нема кривично дело“, вели Раичевиќ за БИРН.

Сепак, Раичевиќ смета дека Обвинителството може да дејствува превентивно и да ги обесхрабри тие што шират дезинформации и поттикнување паника, затоа што ширењето дезинформации може да влијае врз предизвикување други кривични дела.

„Во ситуација каде што тоа го бара јавниот интерес, јавниот обвинител може да излезе и да каже какви штетни последици и какви кривични дела може да произлезат, затоа што ширењето лажни вести може да биде поврзано како преддејство за настанување одредени други кривични дела“, вели обвинителката.

На некои од порталите беа објавени информации дека камиони полни со македонска пченица извезуваат во Косово за време на вонредната состојба, или дека директорот на очната клиника одел на работа, и покрај тоа што неговата сопруга добила препораки да биде во самоизолација. Информациите веднаш добија демант.

Дезинформациите посебно се актуализираа во летото 2016-та година заради претседателските избори во САД. Приказната за момчињата од Велес која ја промовираше реномираниот „Гардијан“ брзо го обиколи светот. Во извештајот на Европската комисија меѓу другото се вели дека „Од суштинско значење е да се

регионалната организација – Балканска истражувачка репортерска мрежа. Оттогаш БИРН Македонија има имплементирано различни локални и регионални проекти, од организирање тренинзи за меѓународните новинарски стандарди при покривање прашања од транзициска правда, производство на телевизиски документарци, објавување анализи и истражувања, како и организирање трибини за прашања поврзани со ЕУ-интеграцијата на Македонија.

продолжи со поддршка на плурализмот во медиумите, промовирањето професионализам, непристрасно известување и истражувачко новинарство и градење отпорност за ефикасна борба против дезинформациите.“ Во таа насока, Владата воведе акциски план за борба против дезинформациите и започна процес за подобрување на медиумската писменост во образовниот систем.

Несомнено, споделувањата на овие дезинформации на социјалните мрежи го потврдија впечатокот дека лошите вести се шират побргу од вирус.[55]

Заклучоци и согледувања

„Содржината на објавите се лажни вести, со цел ширење паника и говор на омраза. Доаѓаат од повеќе центри“, велат од полицијата за БИРН, појаснувајќи ја содржината на поднесоците. Со измените на Кривичниот законик се казнува говорот на омраза и за тоа е предвидена казна затвор од една до пет години. Затворски казни се предвидени и за ширење расистички и ксенофобичен материјал преку компјутерски систем.

Сепак, законодавецот најверојатно намерно не одлучил за санкции за тие што шират лажни вести, бидејќи тоа е на многу танка линија со ограничувањето на слободата на говорот, а со тоа и на слободата на јавното информирање. Секоја дезинформација нужно не мора да содржи во себе говор на омраза, или ширење расистички и ксенофобичен материјал, па произлегува дека ако тие елементи ги нема во поднесоците на МВР, тие ќе завршат без постапка.

Иако обвинителите се со врзани раце поради неможноста кривично да се гонат тие што со намера шират дезинформации, академик Владо Камбовски за БИРН потврди дека веќе има работна група што расправа за измени на Кривичниот законик, во повеќе делови, а еден од нив се однесува и на ова прашање.

„Размислувањата одат во правец да се превиди едно дело за вакви ситуации.

---

[55] Маглешов, В. (2020, март 27). Пријавите за лажни вести меѓу правдата и цензурата: Коронавирусот и непроцесираните пријави за дезинформации.

Но, не мора да бидат здравствени кризи, може да бидат и економски, кои засегаат поширок круг луѓе или жртви, да се казнува намерното ширење злонамерни информации преку медиуми и средства за јавно информирање, со кои се предизвикува паника или се блокира функционирањето на државните институции“, вели Камбовски.

Камбовски тврди дека ако зачестат дезинформациите што шират паника меѓу населението, владата, во услови на вонредна состојба, би можела да донесе уредба со која ќе предвиди прекршочна глоба или, пак, кривично дело.

Божиновски, пак, појасни дека во дискусиите на работната група за измените во Кривичниот законик, прашањето свесно било ставено настрана, поради „опасноста од колизија со одредбите од Уставот за забрана за цензура.“

„Оваа област беше оставена на самите медиуми и здруженијата на новинари, преку методот на саморегулација и посебните органи за спроведување на кодексот за етика за новинари“, вели Божиновски.

Од Министерството за правда, кое може на Владата да ѝ предложи ваква уредба, за БИРН велат дека ги следат состојбите, и доколку во иднина се појави потреба, ќе ги разгледаат опциите што им стојат на располагање во вакви состојби.

Претседателот Стево Пендаровски во интервју за „Нова Македонија“[56] говори за хибридните закани и дезинформациите, и потребата од справување со нив. „Од сите досегашни истражувања на темата се потврдува дека дезинформациите најчесто не се наивни и случајни, туку се производ на еден планиран организиран пристап кон одредена тема. Намерите најчесто се, на долг рок и систематски, да се манипулира јавноста со пласирање погрешни информации, полувистини, извртени факти или комплетно фабрикувани вести, со крајна цел, да послужат на интересите и целите на одредени државни и недржавни ентитети, кои имаат свои специфични агенди. Свесноста за опасноста е стартната основа за справување со хибридните закани. Треба да бидеме свесни за сериозноста на овие закани, да ги зајакнуваме нашите капацитети преку заедничка работа на државните институции, академската заедница, граѓанскиот

[56] Живковиќ, М. (2022, Март 1*). Здружен одговор против хибридните закани* [статија]. Nova Makedonija, достапно на: https://novamakedonija.com.mk/pecateno-izdanie/zdruzhen-odgovor-protiv-hibridnite-zakani/

сектор и бизнис-секторот, затоа што цел на заканите може да бидеме сите ние, а потребен ни е здружен одговор. Државната позиција на Северна Македонија е јасна, ние ја осудивме руската агресија над Украина и се приклучивме на позициите на Алијансата како членка на НАТО и пакетот рестриктивни мерки на Европската Унија насочени кон Русија. Со ескалирањето на ситуацијата во Украина и инвазијата на Русија, темата го зафати речиси целиот медиумски простор. Има огромен волумен на дезинформации, кои дополнително придонесуваат за поларизација на општеството. Затоа е особено важно сите информации што се примаат преку медиумите, а особено оние што се достапни на интернет и преку социјалните мрежи, да се проверуваат, да се користат кредибилни извори на информации и граѓаните да не подлегнуваат на вести што имаат за цел провокации. Ние и преку Советот за безбедност упативме апел до сите политички чинители за одговорно однесување и воздржување од потпалувачки говор и ширење дезинформации, кои се спротивни на националните интереси на државата, имајќи предвид дека сме членка на НАТО. Има повеќе механизми за справување со хибридните закани и дезинформациите, а нам ни се достапни помошта и алатките од Алијансата. Кога е потребно, во зависност од проценките, ја користиме поддршката од НАТО.“

Генерален заклучок

Од сите досегашни истражувања на темата, како и од примерите што беа дадени во текстот погоре, се потврдува дека дезинформациите најчесто не се наивни и случајни, туку се производ на еден планиран организиран пристап кон одредена тема. Намерите најчесто се, на долг рок и систематски, да се манипулира јавноста со пласирање погрешни информации, полувистини, извртени факти или комплетно фабрикувани вести, со крајна цел, да послужат на интересите и целите на одредени државни и недржавни ентитети, кои имаат свои специфични агенди.

Свесноста за опасноста е стартната основа за справување со хибридните закани. Треба да бидеме свесни за сериозноста на овие закани, да ги зајакнуваме нашите капацитети преку заедничка работа на државните институции, академската заедница, граѓанскиот сектор и бизнис-секторот, затоа што цел на

заканите може да бидеме сите ние, а потребен ни е здружен одговор.

Повеќе од потребно е подобрување на сите механизми: носење нови законски регулативи, ангажман на национално ниво од сите институции за зајакнување на капацитетите за интернет-безбедност, користењето на бенефитите од членството во НАТО, што ни овозможи пристап до заедничките ресурси и капацитети на Алијансата за справување со безбедносните закани.

- **Компаративна анализа – Лажни дојави за бомби во Р С Македонија и регионот**

Основа за компаративната анализа

Компаративната анализа се фокусира на истражување на лажните дојави за бомби во Р С Македонија и регионот. Со оглед на тоа дека во последните години претставува честа форма на закана. Станавме дел од тој „бран“ на закани со лажни дојави на бомби што го зафати регионот, во Србија, Црна Гора, Косово и други држави. Оваа анализа ќе ги опфати токму овие држави.

„Психолошко-пропагандната димензија има сериозно влијание кај поделбата на општеството, недовербата на институциите, и придонесува за дефокусирање од носење одредени важни политички одлуки. Најглавното е предизвикување страв и несигурност кај населението. Тоа беше постигнато со последните случувања во нашата држава, и неслучајно се избрани училиштата како таргет“, вели доц. д-р Ице Илијевски, во изјава за медиуми.[57]

Појавата на инциденти со бомби или само закани може да има големо влијание врз целните жртви. Потенцијалот за сериозни повреди и оштетување прави дури и празна закана многу сериозен инцидент. Иако голем процент од дојавата за поставени бомби во училиштата може да испаднат шеги, секоја закана мора да се сфати сериозно и да се дејствува веднаш. Евакуацијата на зградите предизвикува големи нарушувања, што во многу случаи може да биде атрактивен

[57] Трајковски М. (2022, March 1). *Лажните дојави за бомби во скопските училиштата - хибридни закани* [статија]. Voice of America - Macedonian. Retrieved from: https://mk.voanews.com/a/article-laznite-dojavi-za-bombi-hibridna-zakana/6833385.html

исход од гледна точка на сторителот.

Системот и институциите вклучени во процесот за справување со заканите претрпуваат исцрпеност од човечки и материјални ресурси и големи економски загуби. Образовните институции во земјата се под константен притисок од закани коишто се покажаа дека се лажни, но предизвикаа тензија во училиштата и го попречија нормалниот тек на наставата. Министерството за образование апелира дека наставата мора да продолжи, но поради честите прекини за училиштата ќе биде вистински предизвик како да ја надоместат пропуштената настава до крајот на годината.

Република Северна Македонија

На 2.11.2022 во СВР Скопје околу 14:30 часот е пријавено дека на електронските адреси на шест училишта во Скопје е упатена закана за поставена бомба. Околу 15 часот во СВР Скопје е пријавено дека ваква закана стигнала и на електронските адреси на уште две училишта. Веднаш по добиените пријави, од полициски службеници се преземени мерки за безбедно евакуирање на сите осум училишта. Во тек се антитерористички проверки и се преземаат мерки за расчистување на случајот.[58]

На 4.11.2022 година во СВР Скопје денеска околу 14 часот е пријавено дека на имејловите на четири средни училишта во Скопје е упатена закана за поставена бомба. Станува збор за училиштата „Орце Николов“, „Никола Карев“, „Здравко Цветковски“ и „Јосип Броз Тито“, соопштение до медиумите од МВР.

(10.11.2022 година) Седум училишта утринава добија идентичен имејл за дојава за бомба – информираат од МВР за медиумите.

(11.11.2022 година) Веднаш по добиените пријави, од полициски службеници се преземени мерки за безбедно евакуирање на училиштата, а потоа се извршени и детални проверки од тимови за антитерористички проверки и

[58] Соопштение од МВР, објавено на официјалната веб–страна, пристапено ноември, 2022 год., достапно: https://mvr.gov.mk/vest/23202.

утврдено е дека станува збор за лажни пријави, стои во соопштението од МВР.[59]

„Во неколку правци одат истрагите. Имаме веќе добри сознанија од каде доаѓаат мејловите, на кој начин се испраќаат. Ќе ни треба и меѓународна правна помош за да можеме да ги потврдиме доказите и тоа е клучно кај вакви хибридни напади, да се обезбедат доказите“, рече министерот за внатрешни работи Спасовски во изјава за медиумите. Тој како и многу експерти ги оцени лажните дојави за бомби како „монструозен чин на хибридни закани“.

Република Северна Македонија како членка на НАТО и дел од регионот на Западен Балкан кој е изложен на сајбер-закани беше прифатена во НАТО центарот за извонредност за сајбер-одбрана и е во процес на полноправно членство. Во рамките на процесот, ќе можеме да ги користиме алатките на Центарот за да ја засилуваме сопствената отпорност од хибридни напади и да ја зајакнеме заштитата на критичката инфраструктура.

Босна и Херцеговина

На електронските адреси на основните и средните училишта во повеќе градови во босанскохерцеговскиот ентитет Република Српска на 1.6.2022 г. утрото стигнати се дојави за поставени бомби, известува Агенција Анадолија (АА). Полициските службеници на Министерството за внатрешни работи на Република Српска истиот ден до 12 часот извршија антидиверзантски контроли во 222 основни и средни училишта во Република Српска, каде што беше пријавена експлозивна направа.

„На подрачјето на Република Српска, полицијата досега извести дека 429 основни (централни и регионални) и средни училишта во Република Српска добиле е-пошта со закануачка порака дека во училиштето е поставена бомба“, се вели во соопштението на РС. Се додава дека во училиштата каде што полициските службеници од надлежните полициски администрации сè уште го немаат завршено диверзантскиот увид, местото е обезбедено и тие нема да бидат

[59] Пренесува Телма, топ вести. Соопштение од МВР: И денешните пријави за бомби се лажни. Достпано на: https://telma.com.mk/2022/11/11/mvr-i-deneshnite-prijavi-za-bombi-se-lazhni/

отворени сè додека не завршат антидиверзантските контроли, односно не се утврди дека нема безбедносни закани. Воедно, надлежните полициски администрации во соработка со Одделот за високотехнолошки криминал при Управата за криминалистичка полиција спроведуваат истрага за откривање на лицето кое ги упатило овие закани и во рамки на овие активности утврдени се повеќе ИП-адреси од странство. „Најголем дел од надлежните обвинителства овој настан го оквалификуваа како кривично дело 'Лажно пријавување кривично дело'", соопшти МВР на Република Српска.

Република Косово

На меѓународниот аеродром во Приштина „Адем Јашари" на 16 јуни, 2022 година пристигна дојава за бомба, но се покажа дека е лажна. По пријавата, косовската полиција веднаш излегла на местото на настанот и презела мерки за обезбедување на локацијата. Извршена е и евакуација (изјава од портпаролката на приштинскиот аеродром, Валентина Гара, на „Фејсбук" објави дека се работи за лажна дојава и дека работата на аеродромот се нормализира).

Заканите за бомби започнаа во декември 2021 година и се интензивираа од април до јуни. Обидот да се создаде ситуација на општа закана доаѓа во време кога руската агресија врз Украина продолжува, а Западен Балкан, вклучително и Косово, не остана имун на хибридната војна на Русија. Ова се прави главно преку лажни вести и изјави како оние кои ги негираат злосторствата против човештвото извршени од Србија во Косово за време на последната војна, 1998 – 1999 година.

На 16 јуни, истиот ден во Приштина се одржаа два протести – еден од ветеранските организации на ОВК, а другиот од синдикатот на КЕК – имаше 73 лажни дојави за бомби во регионот на Гњилане и северните општини со мнозинско српско население.

Република Србија

Во мај, 2022 г. припадниците на српските безбедносни служби

идентификувале неколку земји од кои во последните недели на адресите на јавните објекти во Србија пристигнаа заканувачки пораки и лажни дојави за бомби, соопшти во средата вечерта Министерството за внатрешни работи на Србија. На електронската пошта на редакциите на српските медиуми стигнале пораки дека се поставени бомби во градови низ Србија. Во заканувачките имејлови се наведува дека „човечки органи ќе летаат во воздух и дека улиците ќе бидат полни со крв.“ Српскиот портал „Нова“ во целост ја пренесе содржината на заканувачките имејлови.

„Утврдено е дека осум такви закани дошле од Полска, четири од Гамбија, две од Иран и Нигерија и по една од Украина, Словенија и Русија“, се вели во соопштението на Министерството за внатрешни работи. Како што се додава, тие ги идентификувале локациите на вкупно 19 електронски адреси од кои пристигнале заканувачки пораки за поставени бомби на различни локации во Србија. „Станува збор за странски државјани што не живеат во Србија“, се вели во соопштението.

Во оваа прилика, МВР на Србија разменува податоци преку Европол и Интерпол со надлежните органи на Шведска, Литванија, Швајцарија, Руската Федерација и Унгарија, како и со компанијата „Гугл“. Според нив, претходните денови и граѓани на Србија упатиле заканувачки пораки.

„Поради лажни пријави за поставени бомби во јавни објекти, припадниците на на министерството за четири дена кривично гонеа осум лица, државјани на Србија – две лица се уапсени, а против шест други малолетници во редовна постапка се поднесени кривични пријави“, додаваат во соопштението.

Според нив, екипите на МВР на Србија во претходните три дена извршиле контрадиверзиски прегледи на неколку стотици јавни објекти, училишта, болници и трговски центри низ Србија, по што се покажало дека сите пријави се лажни.

Српската премиерка Ана Брнабиќ во вторникот (17 мај) рече дека информациите за бомби во Србија се притисок од странство бидејќи Србија не воведе санкции кон Русија по инвазијата на Украина, додека министерот за внатрешни работи Александар Вулин еден ден претходно рече дека против Србија се води специјална војна со лажни информации за бомби. До овие сознанија

дошле припадници на МВР, Управата за криминалистичка полиција во соработка со Обвинителството за организиран криминал, Вишото јавно обвинителство и Специјалното обвинителство за борба против високотехнолошкиот криминал.

Заклучок од анализата

За разлика од овие случаи, каде што казните за кривично дело – лажно пријавување се пониски, дојавите за бомби во училишта во регионот се третираа како акт на тероризам. Во Србија, тамошното државно обвинителство ги третираше како тероризам.

Првите пресуди за лажни дојави за бомби во Србија се изречени против двајца жители на Алексинац пред шест години. Осудени се на по шест месеци затвор поради тоа што цели три години со лажни дојави во нишкиот суд одложиле шеесетина рочишта. Осудени за кривично дело предизвикување паника и неред. (портпаролката на Вишиот суд во Ниш, Ива Поповиќ, за агенцијата „Бета“).

Во Хрватска пак, невкусната шега на 28-годишниот Хрват кој во 2022 г. лажно дојави дека е поставена бомба во трговскиот центар „Авенија мол“ во Загреб каде што работел како обезбедување. Општинскиот суд во Нови Загреб го осуди 28-годишниот на една година затвор, но со тригодишна условна казна. Со оглед на тоа што на судењето обвинетиот го признал делото и веднаш ја прифатил предложената санкција на обвинителството и истовремено се откажал од правото на жалба, исто како и обвинителите, пресудата веднаш станала правосилна.

Во Република Српска, Босна и Херцеговина Најголем дел од надлежните обвинителства овој настан го оквалификуваа како кривично дело „Лажно пријавување кривично дело“.

„Нашиот кривичен законик го препознава кривичното дело тероризам. Меѓутоа сега сме во ситуација да имаме остварени елементи за извршување на ова кривично дело. Се работи за кривично дело каде што за самиот обид се заканува казна од 6 месеци до 5 години. Но, и заканата за напад на телото и животот на граѓаните подразбира акт на тероризам, значи се заканува казна до 5 години за

самиот обид“ (Иван Ниниќ, адвокат, во изјава за медиуми).

Во нашата држава во 2020 година, против 19-годишник, вработен во трговскиот центар преку агенција задолжена за обезбедување на објектот, е поведена постапка поради основано сомнение дека на 29 јануари во трговскиот центар „Сити мол“ каде што бил вработен пријавил дека е извршено кривично дело – „Предизвикување општа опасност“ за кое гонењето се презема по службена должност, иако знаел дека такво дело не е сторено. Надлежен јавен обвинител од Основното јавно обвинителство Скопје поднесе Обвинителен предлог против едно лице за сторено кривично дело – „Лажно пријавување на кривично дело“ од член 366 став 4 во врска со став 3 од Кривичниот законик.[60] Истиот признал вина а Основниот кривичен суд - Скопје го осудил на парична казна од 1 500 евра.

Како генерален заклучок може да се подвлече дека хибридните закани во форма на лажни дојави за бомби станаа мошне сериозен проблем во регионот.

Истите се праќаат од надвор преку креирани виртуелни имејлови. Оттаму, истрагата е комплексна, тешко е да се утврди испраќачот. За да се дојде до сторителите на ваквите дела, потребно е големо вложување од голем број институции, соработка со партнерски служби и црпење на сите капацитети на државата.

Истите нанесуваат значителни штети на нормалното функционирање, протоколите се строги и за граѓаните и налагаат контрола, исто како и за дојавите во автобусите на ЈСП, кога се блокираше јавниот превоз во градот. Предизвикуваат вознемиреност кај секој човек без разлика од кои причини се прави – дали е од геостратегиски, политички, бизнис-причини.

Засега, оценките на експертите се дека безбедносната состојба во државата е стабилна и нема никакви индиции за нејзино нарушување. Сепак, може да влијаат и настаните од регионот и пошироко.

---

[60] https://jorm.gov.mk/ - официјална веб страна Јавно Обвинителство на Република Северна Македонија, Односи со јавноста, соопштенија, објавено на 5 февруари 2020, пристапено во ноември 2022.

- **Анализа на лажни дојави за бомби во Република Северна Македонија**

Шемата на лажните дојави за бомби: 905 закани, осум градови, 76 електронски адреси. Најголем број од лажните дојави се случиле во февруари – дури 439, односно само пет дена од работната недела немало дојава за бомба. Во ноември имало 30 дојави, во декември 272, а на 1 март годинава достигнат е рекордот – дури 120 училишта и други институции за еден ден добиле лажна дојава дека е поставена бомба. Веќе наредниот ден имало 30 дојави, а потоа, во согласност со донесените протоколи, во јавноста веќе не се известува за ова прашање.

Осум градови, вкупно 905 лажни дојави за бомби, од кои 876 биле во основни и во средни училишта. Речиси третина од дојавите се случиле во среда, а најретко дојави имало во понеделник. Февруари бил месец на најмногу дојави – само пет дена во текот на училишната недела (без да се земат предвид викендите), немало лажна дојава за поставена бомба во објект на некое училиште. Почеста цел биле основните отколку средните училишта.

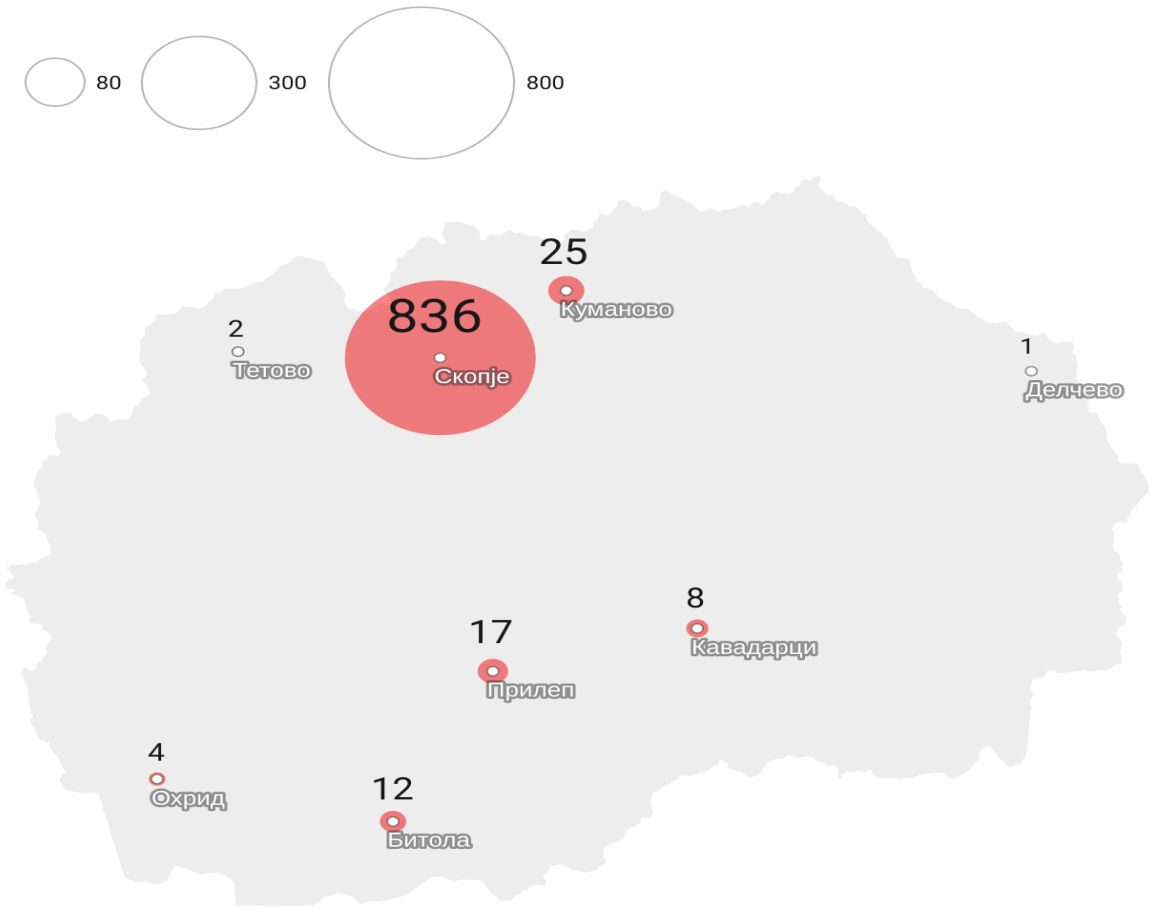
Ова накратко се заклучоците од сите досегашни лажни дојави за поставени бомби во земјава кои ги анализираше новинската агенција „Мета.мк“[61], користејќи податоци од Министерството за внатрешни работи, користејќи го Законот за слободен пристап до информации од јавен карактер. Користејќи листа доставена од МВР на сите дојави за поставени експлозивни направи, до училиштата и до 42 други објекти на институции.

Според бројките, произлегува дека имало вкупно 905 лажни дојави за поставени бомби, а евидентно е дека на дојавувачите најголема цел им биле училиштата и внесувањето страв и паника токму кај децата и кај нивните родители. Првата дојава за поставена бомба беше на 26 октомври минатата година, а последната, за која беше обелоденето, на 2 март годинава. Според податоците, повеќе дојави за поставени бомби имало во основни – 544 отколку во

[61] Мери Јордановска и Антонија Поповска. (28 март 2023), достапно на: https://meta.mk/shemata-na-lazhnite-dojavi-za-bombi-905-zakani-osum-gradovi-76-elektronski-adresi-infografik/

БРОЈ НА ЛАЖНИ ДОЈАВИ ЗА БОМБИ ПО ГРАДОВИ

Убедливо најголем број од лажните дојави за бомби во периодот од 26 октомври 2022 година до 2 март 2023 година имало во Скопје



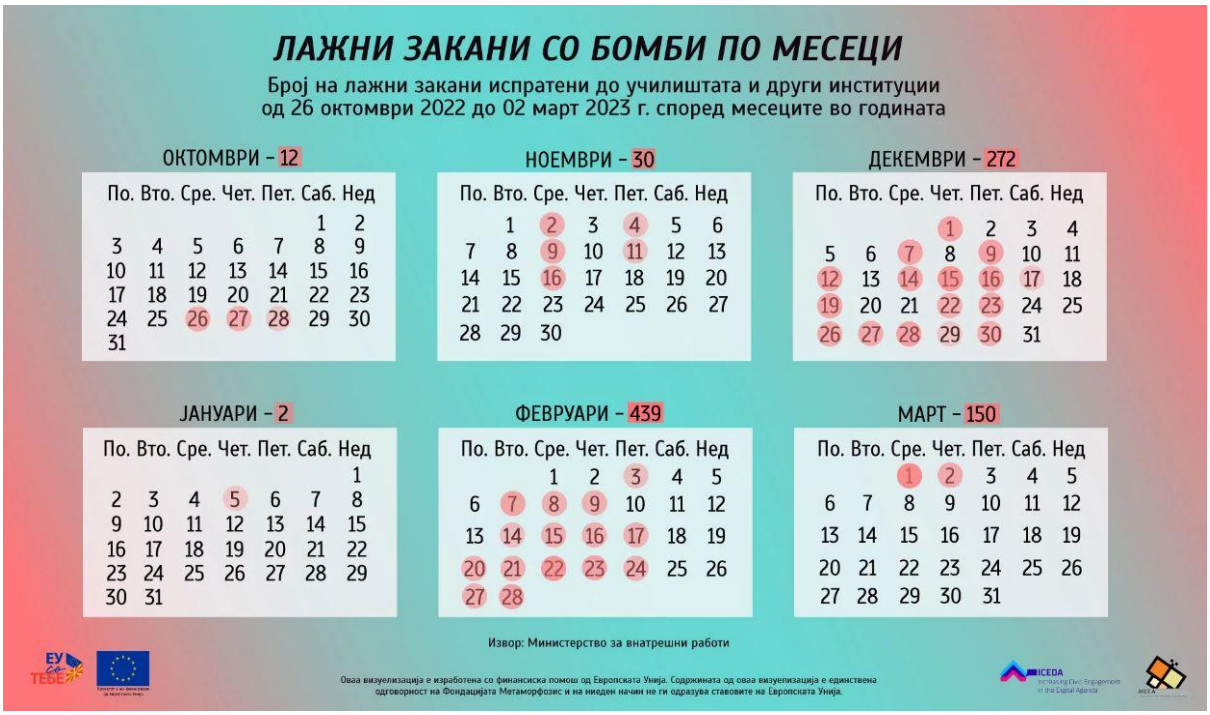
Карта: Новинска агенција Мета • Извор: Министерство за внатрешни работи • Создаден со Datawrapper

средни училишта – 332. Биле регистрирани дојави во осум градови низ државата, од кои најголем дел биле во Скопје (836), Куманово (25), Прилеп (17) и Битола (12).

Лажните дојави за поставени експлозивни направи биле испратени од 76 електронски адреси. Ова практично значи дека од една електронска адреса во просек биле испраќани по 12 лажни дојави.

Во јануари, учениците беа на зимски распуст, па во текот на тој месец, регистрирани се само две лажни дојави за поставени бомби, на 5 јануари, што повторно говори за фактот дека целта на лажните дојави биле училиштата, поточно учениците. Најголем број од лажните дојави се случиле во февруари – дури 439, односно само пет дена од работната недела немало дојава за бомба. Во

ноември минатата година имало 30 дојави, во декември 272, а на 1 март годинава достигнат е рекордот – дури 120 училишта и други институции за еден ден добиле лажна дојава дека е поставена бомба. Веќе наредниот ден, на 2 март, имало 30 дојави, а потоа, во согласност со донесените протоколи, во јавноста веќе не се известува за ова прашање.



Инфографик: „Мета.мк“

Судејќи според досегашниот тренд на дојави, може да се заклучи дека по донесувањето на новите усвоени протоколи во училиштата, заканите кои сериозно влијаеја и го нарушија образовниот процес и предизвикаа страв и паника кај населението, можеби и целосно ќе згаснат.

Имено, во согласност со протоколот на МВР кој функционира од почетокот на месецот, јавноста веќе не е информирана за тоа дали има дојави за подметнати експлозивни направи во основните и во средните училишта, но и во другите објекти во земјава, освен ако за тоа не одлучат стручните лица. Новите протоколи беа донесени со цел паниката и нервозата во јавноста да се сведат на минимум, а секојдневието на учениците, наставниот кадар и на родителите да биде без непотребни стресови.

Освен ова, функционира и протокол кој се смета за доверлив. Според сведочењата на образовниот кадар во училиштата, полицијата прави проверки пред почетокот на наставата, во објектите не смее да се влезе без најава, приватното обезбедување ги проверува надворешните лица и при влез и при излез од училиштето, а камерите треба да бидат постојано вклучени.

Одреден „патерн“, односно шема во дојавите за поставени бомби не може прецизно да се утврди, освен дека почести биле дојавите кон средината или крајот на работната (училишната) недела отколку на почетокот.

Митко Димовски, директор на скопската гимназија „Орце Николов“, училиштето кое доби најмногу дојави на електронска пошта со заканувачка содржина вели дека сепак може да се утврди одредена шема кај испраќачите на лажните дојави, бидејќи секогаш биле „таргетирани“ смените на учениците од втора и од четврта година.

„Она што беше најсимптоматично е што најмногу дојави стасуваа кога во смена беа учениците во втора и во четврта година. Прецизно време на испраќање немаше, но секогаш во истата смена. За да не губат часови, решивме да ги промениме смените, односно во смената во која одеа учениците од втора и четврта година почнаа да одат учениците од прва и од трета година. Сепак, и покрај ова, се случуваше дојава да стаса во втора и во четврта. Сега, со новото упатство од МВР, училиштето е обезбедено, се прават проверки, дојави нема бидејќи се променети адресите и наставата се одвива нормално, без прекини“, вели тој за „Мета.мк“.

Анализа на податоците преку табеларен приказ:

Аспекти	Пронајдоци
Фреквенција на лажни закани со бомби	– Вкупно 905 лажни закани за бомби се регистрирани во Република Северна Македонија, од кои 876 се во основните и средните училишта.
Временски обрасци	– Речиси една третина од заканите се случиле во среда, додека во понеделник имало најмалку закани. Февруари имаше најголем број закани со бомби, со само пет училишни денови без никакви закани во текот на тој

	месец.
Географска дистрибуција	– Закани пријавени во осум градови, од кои најмногу инциденти има Скопје (836), потоа Куманово (25), Прилеп (17) и Битола (12).
Таргет	– Основните училишта беа мета почесто од средните училишта, со 544 закани во основните училишта и 332 во средните училишта.
Профил на сторителот	– 76 адреси на е-пошта се користени за испраќање лажни закани за бомби, со просечно 12 закани кои потекнуваат од една адреса.
Преференции за смена	– Насилниците беа насочени кон специфични смени на ученици, првенствено ученици од втора и четврта година.
Имплементација на протоколи	– Во училиштата беа воведени нови протоколи за да се минимизира паниката и да се одржуваат секојдневните рутини, вклучително и зголемени безбедносни мерки.
Атрибуција и потекло	– Некои официјални лица сугерираат дека заканите за бомби може да бидат дел од хибриден напад врз земјата, веројатно лансиран од странство. – Потекло на заканите споменати како IP-адреси во Иран и Русија, заедно со VPN-адреси од овие земји.
Истражувачки предизвици	– Следењето на сторителите е предизвик поради нивната употреба на техники за анонимизирање, анонимни услуги за е-пошта и шифрирана комуникација.

Оваа квалитативна табела на податоци ги сумира клучните аспекти на текстот – две интервјуа со министерот за внатрешни работи Оливер Спасовски[62][63]

[62] Закани со бомби - комбинација од домашни и странски актери, Катерина Блажевска 6.3.2023.

Од октомври до март, поради дојави за бомби биле проверени 862 локации во Скопје, ангажирани над две и пол илјади полициски службеници и потрошени над 5 милиони денари, посочува министерот Спасовски во интервју за „ДВ“. Достапно на:

во кои се дискутираат мерките преземени од Министерството за внатрешни работи (МВР) и Министерството за образование и наука (МОН) како одговор на заканите со бомби во училиштата во Република Северна Македонија. Во нив министерот ги истакнува пораките кои се адресирани во текстот во однос на неполитичкиот пристап во справувањето со хибридните закани и улогата на граѓаните во обезбедувањето на нивната безбедност. Министерот за внатрешни работи Оливер Спасовски најави нови мерки за справување со заканите со бомби во училиштата. Овие мерки имаат за цел да го подобрат одговорот и да обезбедат брза акција по добивањето закани. Владата ја препознава сериозноста на ваквите закани, особено во образовните институции, и има за цел да ги заштити студентите, персоналот и јавноста. Соопштението е објавено по значителното зголемување на заканите за бомби пријавени во македонските училишта на 1 март 2023 година. Владата сериозно ги сфаќа овие закани, а новата инструкција ја нагласува потребата сите релевантни институции да ја одиграат својата улога во обезбедувањето на јавната безбедност. Министерството за внатрешни работи ги повика образовните институции и другите агенции да се придржуваат до насоките наведени во новото упатство без никакви исклучоци. Непочитувањето на упатствата може да доведе до вклучување на Јавното обвинителство. Пристапот на владата означува посветеност за колективно справување со безбедносните закани и ја нагласува важноста од координација меѓу различните институции за борба против тероризмот и заштита на граѓаните.

https://www.dw.com/mk/spasovski-zakanite-so-bombi-se-kombinacija-od-domasni-i-stranski-akteri/a-64894752

[63] Со ново упатство во битка против заканите со бомби, Катерина Блажевска, 3.3.2023. Доколку има институции кои не преземале одредени активности од своја надлежност, а биле должни да ги преземат, ќе го известиме и Јавното обвинителство, најави синоќа министерот Спасовски. Достапно на: https://www.dw.com/mk/so-novo-upatstvo-vo-bitka-protiv-zakanite-so-bombi/a-64871918

Аспекти	Преземени мерки
Вклучени министерства	– Министерството за внатрешни работи (МВР), Министерството за образование и наука (МОН)
Безбедносни мерки	– Антитерористички проверки – Патроли низ училиштата – Проверки за експлозивни направи во стопански објекти – Насоки за подобрување на безбедноста на училиштето – Развивање мерки врз основа на компаративни анализи и меѓународни искуства – Формирање оперативен тим за сајбер-безбедност и хибридни закани
Координација	– Координација помеѓу МВР и МОН – Вклучување различни институции и експерти во Оперативниот тим – Добивање поддршка од меѓународни партнери
Одговорност	– Нагласување на одговорноста на агенциите кои обезбедуваат објекти – Поголема одговорност за училишните администратори – Заштита на децата од трауми
Упатени пораки	– Безбедноста на граѓаните е непартиско прашање – Безбедноста на граѓаните е натпартиско прашање – Обесхрабрувачки обиди за поткопување на системот и мерките – Потсетување на граѓаните на постојаните напори за безбедност – Сите претходни закани за бомби беа лажни – Следење протоколи во сите ситуации – Обесхрабрувачки обиди за поткопување на системот и мерките – Потсетување на граѓаните на постојаните напори за безбедност – Сите претходни закани за бомби беа лажни

	– Следење протоколи во сите ситуации
Клучни актери	– Министерот е на чело на владините напори за справување со безбедносните закани. Тој игра централна улога во објавувањето и спроведувањето на новите мерки за борба против заканите од бомби и хибридните закани. Како прв човек на Министерството за внатрешни работи, тој ја надгледува координацијата на различните агенции и институции вклучени во прашањата за националната безбедност. – Агенции за спроведување на законот: Органите за спроведување на законот, како што е македонската полиција, играат витална улога во одговорот на заканите со бомби и во истрагата на безбедносните инциденти. Тие се одговорни за спроведување на новите упатства и обезбедување брз и ефективен одговор во случај на итни случаи. – Образовни институции: Училиштата се директно погодени од заканите со бомби и мора да соработуваат со агенциите за спроведување на законот за да се осигури безбедноста на учениците и персоналот. Владата очекува образовните институции да се придржуваат до новите упатства и да преземат соодветни мерки за справување со потенцијалните закани. – Релевантни владини тела: Различни владини агенции, како што се Агенцијата за национална безбедност и Агенцијата за електронски комуникации, се вклучени во борбата против безбедносните закани. Владата ја нагласува потребата од соработка меѓу овие институции за решавање на различните аспекти на безбедносните предизвици. – Потенцијална соработка со телата на НАТО и ЕУ: Македонската влада бара поддршка и соработка од меѓународните организации како што се НАТО и Европската Унија за да ги зајакне своите капацитети во справувањето со хибридни закани и сајбер-напади. Овие сојузи означуваат поширока посветеност на регионалната и

	меѓународната безбедност.
Владини иницијативи	– Формулирање нова инструкција за брзо справување со заканите со бомби: Владата воведе нова инструкција за подобрување на одговорот на заканите со бомби и за обезбедување на безбедноста на образовните институции. Упатството наведува конкретни мерки што мора да ги преземат образовните институции и агенциите за спроведување на законот во случај на закани. Владата го нагласува строгото почитување на овие упатства за да се обезбеди ефикасно управување со кризи. – Поттикнување на соработката помеѓу безбедносните и образовните институции: Владата признава дека справувањето со безбедносните закани бара колективен напор. Ја нагласува потребата од соработка и координација меѓу агенциите за спроведување на законот и образовните институции за ефикасно справување со потенцијалните закани. – Развој на методи за рано откривање хибридни закани: Стратегијата за борба против хибридните закани се фокусира на рано откривање за да се ублажи нивното влијание. Владата ја нагласува важноста на разузнавачките и безбедносните ентитети во идентификувањето и спротивставувањето на хибридните закани пред тие да ескалираат.
Имплемен-тација и евалуација	– **Стратегија за градење национална отпорност против хибридни закани (2021–2025):** Стратегијата на владата го прикажува патоказот за зајакнување на националната отпорност и борба против хибридните закани во одреден период. Стратегијата ги дели активностите во шест области на оперативен фокус за решавање различни аспекти на хибридните закани. – **Акционен план за спроведување на Стратегијата:** Владата има развиено акциски план за ефективно спроведување на стратегијата. Овој план вклучува сеопфатен пристап за подобрување на националната отпорност и способностите за

	сајбер-безбедност. – Акцент на редовно ажурирање и евалуација на напредокот: Владата нагласува редовно ажурирање и евалуација на напредокот на стратегијата. Координираниот Совет за безбедност и разузнавачка заедница игра улога во следењето и оценувањето на спроведувањето на стратегијата и акцискиот план.
Загриженост на јавноста	– Текстот ги истакнува загриженоста и реакциите на јавноста во врска со безбедносните закани, особено во училиштата. Владините иницијативи имаат за цел да ги ублажат овие грижи и да создадат безбедна средина за студентите, вработените и јавноста.
Регионален и меѓународен контекст	– Помошта на НАТО во справувањето со сајбер и хибридни закани: Владата бара помош и експертиза од меѓународните организации, вклучително и НАТО, за да ги зајакне своите способности во справувањето со безбедносните закани. – Препознавајќи ја важноста од справувањето со безбедносните предизвици на регионално и меѓународно ниво: соработка на владата

4.4. Критични ранливости

4.4.1. Компаративна анализа. Степен на отпорност на институциите во справување со хибридни закани

Мерењето на отпорноста од непријателски влијанија на Западен Балкан не е егзактно, но постојат неколку валидни и сигурни извори за процена на нивоата на ранливост во регионот. Две од најзначајните се:

1. НАТО Стратегиски комуникациски центар на извонредност „STRATCOM“ –

извештајот со наслов „Ризици и ранливост во Западен Балкан“[64] и

2. ГЛОБСЕК (индекс на ранливост)[65].

STRATCOM ги истакнува ранливостите што ги користат злонамерните и непријателски актери кои применуваат хибридна војна/тактика во сивата зона против социјалните, економските, политичките и странските и безбедносните институции во државите од Западен Балкан кои се стремат кон евроатлантска интеграција (Zamfir, R. 2020). За параметри зема два концепта кои го сочинуваат индекс на ранливост: 1. структурна ранливост и 2. непријателско влијание. Првиот концепт, структурната ранливост ги нагласува динамичните и сложени услови во опкружувањето за закана, кои на злонамерниот непријателски актер му обезбедуваат можности да ги подигне ризиците во социјалните, политичките, економските и надворешните и безбедносните домени во целната држава и да ги поткопа домашните институции и норми.

Варијабли од резултатите: треба да се нагласи дека не секоја хибридна закана доаѓа од надворешен чинител, а многумина се спроведуваат преку посредници, што му овозможува на непријателскиот актер да го прикрие веродостојно дејството.

Табеларен приказ. Индекс на пермеабилност

		Домен			
Држава	Вкупно Резултат	Општество	Економија	Политика	Надворешна и безбедносна политика
Албанија	1,52	1,23	1,51	1,86	1,48
Босна и	2,05	2,03	1,87	2,37	1,94

[64] United States Strategic Command, основана: 1 јуни 1992, седиште: Омаха, Небраска, Соединети Американски Држави.

[65] Непартиска, невладина организација со седиште во Братислава, Словачка. Една од нејзините главни активности е годишниот Глобален безбедносен форум ГЛОБСЕК Братислава, кој постои од 2005 година.

Херцеговина					
Косово	1,65	1,55	1,51	2,0	1,53
Црна Гора	1,62	1,6	1,57	1,91	1,41
Р С Македонија	1,51	1,4	1,41	1,79	1,42
Србија	1,73	1,84	1,34	1,91	1,85

Индексот на пермеабилност (види табела) користи основна база и референтна вредност од 1,5, во која оценките под тој број не се толку пропустливи и ранливи на непријателско влијание и резултатите погоре од оваа референтна вредност покажуваат знаци на институционална и општествена слабост и поголема ранливост на злонамерни актери.[66]

Нашата држава (1,51) има најнизок вкупен резултат на пропустливост и е најмалку ранлива на злонамерен непријателски актер. Сепак, институционалната слабост, малата доверба во владата, силните покровителски мрежи и концентрацијата на моќ не спречуваат да ги зајакнеме социјалните, економските, политичките и надворешнополитичките и безбедносните институции.

Табеларен приказ. Индекс на ранливост

Држава	Вкупно резултат	Ставови на јавноста	Политички пејзаж	Јавна администрација	Пристап до информации	Граѓански и академски простор
Црна Гора	44	52	33	41	44	51
Р С Македонија	40	49	25	42	45	40
Србија	55	61	66	51	53	46

[66] Zamfir, R. (2020). Risks and vulnerabilities in the Western Balkans. NATO Strategic Communications Centre of Excellence. ISBN: 978-9934-564-51-2.

Во Табелата погоре се дадени истражувањата од 2021 година, каде што GLOBSEC измери степени на ранливост. Со вредност „0“ (нула) како најотпорен и „100“ (сто) како најранлив параметар. Анализата е направена користејќи ги јавните ставови, политичкиот пејзаж, јавната администрација и граѓанскиот и академски простор како клучни домени.

Заклучок од анализата

За генерален заклучок би кажале дека регионот на Западен Балкан е на пресекот на интензивна геополитичка конкуренција помеѓу Западот и Истокот. Индикаторите за пропустливост и ранливост го дефинираат ова како конкуренција меѓу САД – НАТО – ЕУ поредок на едниот крај и поредок Русија – Кина на другиот крај.

Попрецизно речено, пропустливоста и ранливоста ги рефлектираат нивоата на отпорност во политичките, економските, социјалните и безбедносните области. Од овие два концепта произлегуваат неколку теми.

Прво, НАТО и ЕУ членството во Западен Балкан ја зголемува отпорноста и ги ублажува пропустливоста и ранливоста на непријателско влијание и злонамерни актери како Русија и Кина.

Второ, силни институции и компетентна јавна администрација ги ублажуваат корупцијата и клиентелизмот, го зголемуваат капацитетот и се спротивставуваат на мешањето. Постојаните ефекти на комунизмот во Западен Балкан ги инхибираат владеењето на правото, граѓанското општество, демократското владеење и градењето доверба, услови кои ги прават поефективни операциите за злонамерно влијание на Русија и Кина.

Република Северна Македонија, со оглед на геостратегиската реалност, нема алтернативна опција, освен во НАТО и во ЕУ. Споредено со соседните држави, има најмали територијални и демографски потенцијали поради што треба да се движи во насока на градење цврсто стратегиско партнерство со генераторот на геополитичката транзиција, САД. Имајќи ги предвид тенденциите во развојот на односите помеѓу САД и ЕУ, Македонија може да се најде во „сендвич-положба“, што налага следење на развојот на односите помеѓу главните

евроатлантски актери, првенствено на односите внатре во ЕУ, развојот на европската безбедносна и одбранбена политика и преструктурирањето на НАТО.[67]

5. Генерирање препораки и креирање политики за подобрување на отпорноста и стратегии за ублажување[68]

5.1. Зајакнување на институциите и управувањето

Политички домен. Континуитет на владините и критичните владини институции. Тоа подразбира донесување формализиран план за континуирана и координирана работа на Владата во кој се регулирани:

- пренос на авторитет и јасен процес на донесување одлуки, во случај на криза;
- селекција и приоритизација на критични владини агенции, основни услуги и задолжителни функции за поддршка на воените активности, како обезбедување и достава на храна, вода, гориво, електрична енергија, греење, транспорт, специјални средства и опрема за медицинска/фармацевтска/лична заштита;
- селекција и обука на клучен цивилен персонал (од Владата и провајдерите на критични услуги) и релевантен воен персонал;
- периодични тестирања на системи за комуникациско-информатички технологии, засолништа и стокови резерви, како и проверка на договорите за снабдување од приватни субјекти.

Домен за кризен менаџмент. Национална структура за кризен менаџмент во поддршка на владините активности за време на криза, со резервни капацитети за независно функционирање за период од еден месец, како генератори за електрична енергија, храна, вода, комуникации, ХБРН колективна заштита и сл.

Домен – заштитен изборен процес. Воспоставување правна рамка преку

---

[67] Тони Милески, (2005). Геостратегиско окружување на Република Македонија, *Зборник на Филозофскиот факултет* во Скопје, стр. 413.

[68] АКЦИСКИ ПЛАН за имплементација на Стратегијата за градење национална отпорност и справување со хибридни закани (2021 – 2025).

усогласувањето на Изборниот законик со други релевантни закони преку сеопфатен и инклузивен преглед. Воспоставување:

– Систем за рано препознавање дезинформации поврзани со изборниот процес, како и предупредување (пр. Платформата Resist Counter-desinformation toolkit 2018);

– Стратегиски комуникации;

– Заштита на системите кои ги содржат податоците за избирачите и редовни контроли за да се обезбеди валидност на податоците, како и усогласеност со регулативата;

- Континуитет преку воспоставување на методологија за справување со пад на системот, со цел работата да продолжи во случај на откажување на системот.

Домен – економија. Контрола на странските директни инвестиции во согласност со научените лекции и практики во ЕУ

Домен – Граѓанско општество. Остварување високо ниво на медиумска писменост и способност за критичко мислење во граѓанскиот сектор. Постигнато високо ниво на толерантност на верска, социјална и етничка основа.

Домен – Отпорен систем за цивилен транспорт

– Цивилна транспортна инфраструктура, отпорна и способна за справување со штети и ризици од природни закани, хибридни закани, сајбер-напади, епидемии/пандемии, последици од странска сопственост на истите, како и од ранливост поврзана со нови технологии,

– Градење сообраќајна, финансиска и енергетска инфраструктура која овозможува континуитет на ланецот за снабдување со стоки, финансиски средства и пренос на енергија, како и континуирана комуникација и навигација.

Донесени законски регулативи, политики и механизми за:

– Идентификување, организирање, приоритизација и реквизиција на транспортни ресурси, инфраструктура, услуги и транспортни рути за поддршка на националните приоритети за време на криза;

– Овозможување премин преку државната граница за поддршка на слободата на движење на НАТО сили, преку единствена национална точка за контакт, поддржано од релевантни министерства,

– Регулирање воено осигурување или алтернативни методи за поддршка на транспортни субјекти, во рок од 48 часа од влегување на НАТО сили во зона на операции, за да се регулира воздушниот сообраќај во зони каде што комерцијално осигурување на е достапно.

Домен – отпорност во системот за снабдување со енергија:

– Континуиран пристап до сигурни енергетски извори/снабдувачи во време на кризи, како и енергетска независност;

- Изградба на резервни опции и капацитети во случај на прекин на енергетското снабдуве.

- Поседување алатки за идентификување енергетски јазли и меѓузависности (прекугранични интерконектори, меѓусекторски и секторски), вклучувајќи ги договорите со приватни оператори кои посредуваат во справување со ризици поврзани со странски директни инвестиции/сопственост/контрола;

– Имплементација на процедури за споделување информации и подигнување на свеста за навремено и ефективно информирање на сите чинители кои учествуваат во колективната одбрана.

5.2. Подобрување на воените способности

1. Контрола на странските директни инвестиции во согласност со научените лекции и практики во ЕУ.
2. Воени и безбедносни сили и капацитети: способност за борба против нерегуларни вооружени сили и способност за сајбер-одбрана од комплексни сајбер-напади.
3. Способност за истовремено справување со неколку инциденти кои вклучуваат употреба на нуклеарно, хемиско, биолошко и радиолошко (ХБРН) оружје.
4. Воспоставување соработка со институциите на ЕУ и НАТО, наменети за справување со хибридни закани.
5. Справување со неконтролирано движење на луѓе

– Донесени се национални планови за справување со брзо и масовно движење на луѓе, кое опфаќа над 2 % од популацијата на државата;

– Донесен е план и вежбање (преку симулација) за справување со движење на цивили долж рута за транспорт на која се движат воени сили (подразбира постоење механизам за приоритизација на движење и поддршка на цивилите).

6. Способност за справување со масовни жртви

– Воспоставување интегриран систем за предупредување и известување кој ќе добива релевантни информации од НАТО и ЕУ, со цел да ја предупредува популацијата и да ги алармира националните провајдери на услуги, операторите на критичната инфраструктура;

– Креирање сеопфатна база на податоци за воени и цивилни медицински средства, капацитет за сместување пациенти, средства за колективна заштита, средства за транспорт на настрадани и способности евакуација;

– Донесување цивилно-воен план за вонредни ситуации кој ги опфаќа релевантните услуги за итна помош, механизми за нагло зголемување на способностите, како и за редовно одржување вежби;

– Сеопфатен план за национална безбедност на медицински контрамерки, во кој се земени предвид ранливостите и предизвиците поврзани со снабдувањето.

7. Отпорност на ресурсите за храна и вода

– Воспоставен систем за мониторинг, детекција, тестирање и известување за контаминација на изворите и клучната инфраструктура за снабдување со храна и вода;

– Донесен е сеопфатен план во кој се регулира снабдување преку алтернативни извори за храна и вода;

– Донесен е сеопфатен план кој ги идентификува клучните функции, клучната работна рака, експерти, клучни материјали, договори, потребна меѓуресорска соработка и ги зема предвид странските директни инвестиции/сопственост/контрола на клучни јазли и ресурси, со цел обезбедување континуирано снабдување со храна и вода.

Накратко, презентираните препораки се фокусираат на зајакнување на различните аспекти на отпорноста на Република Северна Македонија и управувањето со кризи. Тие вклучуваат зајакнување на владиниот континуитет и координација, воспоставување национална структура за управување со кризи,

подобрување на интегритетот на изборниот процес, контрола на странските директни инвестиции, промовирање на медиумската писменост и критичко размислување во граѓанското општество, обезбедување отпорност на граѓанските транспортни системи и обезбедување сигурно снабдување енергија. Успешното спроведување на овие препораки би можело значително да ја зајакне способноста на земјата ефикасно да одговори на низа предизвици и кризи. Сепак, од суштинско значење е да се провери со локалните власти и експерти за да се утврди моменталниот статус на овие иницијативи во Република Северна Македонија.

5.3. Подобрување на мерките за сајбер-безбедност

Системи за информатичка технологија кои се отпорни, агилни и способни да ги извршуваат основните функции со минимални прекини што вклучуваат:

– детален преглед на приоритетната, критична транспортна инфраструктура;

– резервен систем, доколку има пречки во работата на основниот систем;

– механизам за известување на НАТО во рок од два часа од нападот врз транспортниот систем и советување за влијание врз НАТО операциите;

– безбедна комуникација помеѓу авторитетите и донесувачите на одлуки со врска до операторите на критичната инфраструктура.

5.4. Унапредување на меѓународната соработка

Република Северна Македонија постигна високо ниво на подготвеност во доменот на заедничката надворешна, безбедносна и одбранбена политика. Постигнат е значителен напредок во текот на периодот на евалуација, обележан со целосното усогласување на земјата со заедничката надворешна и безбедносна политика на ЕУ, особено по руската инвазија на Украина. Земјата, исто така, го зголеми своето учество во мисиите и операциите на ЕУ за управување со кризи. Гледајќи напред, Република Северна Македонија треба да даде приоритет на

следните активности:

– Да одржи доследна усогласеност со заедничката надворешна и безбедносна политика на ЕУ;

– Да одржи редовни политички дијалози за прашања од надворешната и безбедносната политика помеѓу ЕУ и Република Северна Македонија, со активен ангажман во неформалниот дијалог ЕУ – Западен Балкан за ЗНБП на ниво на политички директори;

– Да се обезбеди континуирана функционалност на институционалната рамка која овозможува учество на Република Северна Македонија во заедничката надворешна и безбедносна политика, како и во заедничката безбедносна и одбранбена политика.

– Во однос на заедничката надворешна и безбедносна политика (ЗНБП), Република Северна Македонија покажа 100 % стапка на усогласување со релевантните изјави на високиот претставник во име на одлуките на ЕУ и Советот во февруари 2022 година, во споредба со 96 % во 2021 година. Ова недвосмислено ја нагласува стратегиската ориентација кон ЕУ.

Во сила е Законот за класифицирани информации, во согласност со Одлуката на Советот од 2013 година. Регулативите за проверка и надзор на работата со класифицирани информации се во сила од 2019 година. Дополнително, прописите за лична безбедност беа усвоени во јули 2022 година.

Земјата има потпишано договори со Грција и САД во 2021 година за размена и заемна заштита на доверливи информации. Слични договори се во преговори со Белгија, Португалија и Норвешка.

Република Северна Македонија активно учествува во операциите за управување со кризи на ЕУ во рамките на Заедничката безбедносна и одбранбена политика (CSDP), со забележителен придонес во мисиите како што се ЕУФОР АЛТЕА во Босна и Херцеговина и Мисијата за воена обука во Централноафриканската Република (EUTM RCA).

Во февруари 2022 година, Северна Македонија ја потпиша нотата за пристапување кон Техничкиот договор за формирање мултинационална борбена група на ЕУ со Грција како рамковна нација, во која се вклучени Бугарија, Кипар и

Романија (HELBROC BG).

Земјата го задржа своето присуство во неколку мисии предводени од НАТО, вклучително и „КФОР“ на Косово. Исто така, беше домаќин на вежбата на НАТО Брза реакција 22 во мај 2022 година, во која беа вклучени 4 500 лица од осум сојузнички земји.

Република Северна Македонија продолжува да учествува во операцијата на привремените сили на Обединетите нации во Либан (УНИФИЛ).

Република Северна Македонија го заврши истражувањето за хибридни ризици на ЕУ, чија цел е да се идентификуваат системските ранливости и да се оптимизира помошта од ЕУ на ова поле. Како одговор на препораките на ЕУ од истражувањето, Владата ја усвои Националната стратегија за градење отпорност и справување со хибридни закани (2021 – 2025) заедно со Акционен план во декември 2021 година. Овие иницијативи ја означуваат посветеноста на земјата за зајакнување на нејзините безбедносни и отпорни способности наспроти заканите кои се развиваат.[69]

Накратко, Република Северна Македонија постигна значителен напредок во усогласувањето со заедничката надворешна и безбедносна политика на Европската Унија, особено во контекст на руската инвазија на Украина. Земјата покажа високо ниво на подготвеност и активно учество во мисиите на ЕУ за управување со кризи. За да продолжи да го гради овој напредок, Република Северна Македонија треба да одржува доследност со надворешната и безбедносната политика на ЕУ, да се вклучи во редовни политички дијалози и да обезбеди институционални рамки да го поддржуваат нејзиното учество во безбедносните и одбранбените политики на ЕУ. Понатаму, земјата има потпишано договори за размена и заемна заштита на доверливи информации со Грција и Соединетите Држави, а преговорите се во тек со Белгија, Португалија и Норвешка. Република Северна Македонија активно учествува во мисиите предводени од ЕУ, како што е ЕУФОР АЛТЕА во Босна и Херцеговина, и го продолжува своето присуство во мисиите на НАТО, вклучително и КФОР на Косово. Земјата, исто

[69] European Commission. (2022). COMMISSION STAFF WORKING DOCUMENT North Macedonia 2022 Report, pp.108, 109.

така, го заврши истражувачкиот проект на ЕУ за хибридни закани, што доведе до усвојување Национална стратегија за градење отпорност и справување со хибридни закани (2021 – 2025) и Акциски план. Овие иницијативи ја нагласуваат посветеноста на Северна Македонија за зајакнување на нејзината безбедност и отпорност против заканите кои се развиваат.

5.5. Јавна свест и едукација

Отпорен цивилен комуникациски систем:

- обезбеден континуиран пристап до безбедни и сеопфатни комуникациски услуги за време на мир, криза и војна, земајќи ги предвид потенцијалните ризици кои произлегуваат од лица, сајбер-закани, хибридни закани и природни катастрофи, ранливости кои произлегуваат од странска сопственост на комуникациски системи, како и ранливости поврзани со нови технологии и технологии на иднината;

- обезбедени широки, алтернативни способности за воспоставување комуникации во секакви услови;

- обезбедени договори помеѓу националните авторитети и цивилните комуникациски мрежи за добивање приоритетен пристап во случај на кризни ситуации, користејќи ги постојните и нови технологии;

- систем за ефективно и навремено споделување информации на национално и меѓународно ниво, со цел менаџирање на ризиците во системот на комуникации.

6. Заклучок

Можеме да констатираме дека **делумно се потврдува *основната хипотеза*** *(општата хипотетичка рамка)* на овој труд: „Хибридните закани претставуваат значителен ризик за безбедноста на Република Северна Македонија со намерно насочување на ранливости во различни домени за да ги поткопаат

демократските институции и процесите на одлучување.“ За поткрепа ќе се послужиме со специфичната рамка.

Посебните хипотези што ја поддржуваат се:

***Првата посебна хипотеза*, која целосно се потврдува** *и таа гласи:* „Координираната и синхронизирана природа на хибридните закани, кои опфаќаат различни домени, директно ги таргетира ранливостите во демократските институции, што доведува до ерозија на довербата во демократските процеси во Република Северна Македонија. Координирањето и синхронизирањето на лажните дојави за бомби може да се случи преку различни средства, вклучувајќи:

– Интернет и социјални медиуми: Хибридните актери можат да ги користат интернетот и социјалните медиуми за брзо и ефикасно ширење на лажни дојави. Тие може да користат виртуелни мрежи и анонимни профили за да останат скриени;

– Лажна е-пошта: Лажните закани за бомби може да се испраќаат преку измамнички имејлови со лажни информации и атрибути. Ова може да ги измами и збуни институциите и јавноста;

– Комбинирање со други активности: Лажните закани со бомби може да бидат дел од поголеми хибридни операции, каде што се комбинираат со други форми на информативна манипулација, дезинформација и дестабилизирачки активности.

Политички домен: Лажните закани со бомби може да имаат политички импликации преку создавање нестабилност, поткопување на довербата на јавноста во владините институции и потенцијално влијание врз политичките одлуки или акции.

Економски домен: Овие закани може да ги нарушат економските активности, како што се функционирањето на бизнисите, транспортот и јавните услуги, што ќе доведе до финансиски загуби и ќе влијае на економската стабилност на регионот.

Информативен домен: Лажните закани со бомби се форма на дезинформации и можат да шират страв и паника преку ширење лажни

информации. Тие, исто така, може да придонесат за стратегии за информативна војна преку манипулирање со перцепциите и обликување на наративи.

Безбедност и воен домен: Иако овие закани не се директни воени дејства, тие можат да ги нарушат безбедносните и воените ресурси бидејќи властите мора да истражат и да одговорат на секоја закана. Тие, исто така, можат да создадат пропусти во безбедносниот домен, пренасочувајќи ги вниманието и ресурсите од други потенцијални закани.

Како одговор на овие лажни извештаи, демократските институции и безбедносните служби треба да ги координираат и синхронизираат своите напори за да го идентификуваат вистинскиот извор и да обезбедат јавна безбедност. Тие треба да имаат механизми за брза реакција и комуникација со јавноста за намалување на паниката и изолирање на лажни информации. Истовремено, треба да се направат напори за подигање на свеста кај граѓаните за разликата помеѓу вистинити информации и дезинформации и како да се препознаат потенцијалните хибридни закани.

***Втората посебна хипотеза,* исто така, целосно се потврдува:** „Сеопфатниот модел (CORE) и 'Hybridity Blizzard' – модел на снежна бура ги подобрува разбирањето и одговорот на хибридните закани, особено во одлуките, информациите и зависностите меѓу домени, засилувајќи демократски основи и секторска отпорност.“ Оваа студија ја осветлува клучната улога што ја играат двата модели во разбирањето и ублажувањето на предизвиците што ги носат хибридните закани. Моделот CORE служи како стратегиска леќа преку која може да се разбере сложената мрежа на хибридна динамика на закани, која влијае на демократијата и процесите на донесување одлуки. Нуди вредни упатства за градење отпорност на овие закани и помага при анализа на сценарија, процена на ризик и калибрација на одговорот. Паралелно, моделот „Hybridity Blizzard“, со својот хаотичен и повеќеслоен приказ на хибридната војна, ја нагласува немилосрдната природа на таквите закани и тешкотиите со кои се соочуваат бранителите. Овие модели колективно ги овластуваат владите, безбедносните агенции и креаторите на политиките проактивно да се движат низ еволуирачкиот пејзаж на хибридни закани. Тие нудат средства за заштита на демократските принципи, зајакнување на секторската отпорност и унапредување на

меѓусекторската соработка. Како што хибридните закани стануваат сè поприсутни, овие модели обезбедуваат незаменливи алатки за обезбедување стабилност на општествата и зачувување на демократските вредности.

Комплетно се потврдува *третата посебна хипотеза*: „Нивото на свесност и разгледување на хибридните закани во Стратегијата за одбрана на Република Северна Македонија и Стратегијата за градење отпорност влијае на капацитетот и подготвеноста на земјата ефикасно да одговори на овие закани.“ Имплементацијата на националниот документ за стратегиска одбрана е од огромно значење во спротивставувањето и одбраната од растечката закана од хибридни закани, како на глобално ниво така и конкретно во Северна Македонија.

Холистички одбранбен пристап: Овие стратегиски документи обезбедуваат холистички одбранбен пристап кој ја зема предвид повеќеслојната природа на хибридните закани, кои често ги надминуваат традиционалните воени граници.

Колективна безбедност: На глобално ниво, имплементацијата на таквите стратегии придонесува за колективната безбедност, усогласувајќи се со меѓународните договори како Северноатлантскиот договор. Ја зајакнува решеноста на нациите да работат заедно и да ги искористат своите колективни способности за да се спротивстават на хибридните закани.

Отпорност и приспособливост: Стратегиските документи го нагласуваат градењето отпорност, суштински аспект на спротивставување на хибридните закани. Тие ги охрабруваат државите да се приспособат на брзите развојни предели на закани, да ги предвидат потенцијалните ризици и да развијат капацитет да издржат и да закрепнат од нападите.

Национална безбедност: За Република Северна Македонија, имплементацијата на овие стратегиски одбранбени документи е од витално значење за заштита на националната безбедност и суверенитет. Тоа ја зајакнува отпорноста на земјата против хибридните закани кои може да бидат насочени кон демократските институции, критичната инфраструктура и општествената стабилност.

Изградбата на отпорност е усогласена со член 3 од Северноатлантскиот договор, нагласувајќи ги колективниот и индивидуалниот развој на способностите

за справување со каква било форма на закана или криза. Владата има развиено акционен план за ефективно спроведување на стратегијата, кој опфаќа сеопфатен пристап за подобрување на националната отпорност и способностите за сајбер-безбедност.

Понатаму, Владата ги нагласува редовните ажурирања и проценитe на напредокот, при што Координативниот совет за безбедност и Разузнавачката заедница играат клучна улога во следењето и оценувањето на спроведувањето на стратегијата и акцискиот план. Оваа стратегиска рамка ја позиционира Северна Македонија подобро да се соочи и да управува со предизвиците што ги носат хибридните закани, зајакнувајќи ги нејзината национална безбедност и подготвеност.

Целосно се потврдува и четвртата хипотеза: „Националната стратегија за отпорност и спротивставување на хибридните закани, заедно со соработката во безбедносниот сектор и учеството во меѓународни иницијативи како 'Сајбер-коалицијата', го ослабуваат влијанието на хибридните закани, вклучувајќи дезинформации и DDoS напади и ги засилуваат институционалната отпорност и граѓанската заштита.“ Националната стратегија на Република Северна Македонија, во комбинација со нејзиниот ангажман во меѓународните безбедносни напори и учеството во „Сајбер-коалицијата“, значително го намали влијанието на хибридните закани. Клучните наоди ги нагласуваат следните пристапи:

Меѓународна соработка: Учеството на Република Северна Македонија во иницијативи како „Сајбер-коалиција“ ја нагласува нејзината посветеност на сајбер-безбедноста и отпорноста на хибридните закани. Членството во НАТО ја зајакнува способноста да се спротивстави на хибридните напади.

Зајакнување на сајбер-безбедноста: Зајакнувањето на мерките за сајбер-безбедност, вклучително и механизмите за брзо известување и соработката со НАТО, ги зголемува подготвеноста и одговорот на сајбер-заканите.

Национална стратегија за отпорност: Усвојувањето на Националната стратегија за отпорност и справување со хибридни закани ја покажува посветеноста на државата да ги зајакне своите безбедносни и отпорни капацитети.

Последната посебна хипотеза делумно се потврди: Хибридните

закани во Република Северна Македонија, вклучувајќи дезинформации, сајбер-напади и надворешни влијанија, имаат големи последици за безбедноста, управувањето и довербата во институциите на Република Северна Македонија. Тие целосно ги нарушија безбедноста и стабилноста на земјата.

Значително нарушување: Хибридните закани значително го нарушуваат нормалното функционирање, наметнувајќи строги протоколи и контрола и на граѓаните и на јавните услуги како јавниот превоз. Ова води до широко распространета непријатност меѓу поединците, што произлегува од геополитички, политички или деловни мотиви.

Тековна стабилност: додека експертите ја оценуваат безбедноста на земјата како стабилна без индиции за неизбежно нарушување, настаните во регионот сè уште можат да влијаат на Северна Македонија.

Стратегиски дезинформации: Студиите и примерите од реалниот свет потврдуваат дека кампањите за дезинформација не се случајни, туку дел од организирани, долгорочни и систематски пристапи за манипулирање со јавното мислење. Овие оркестрирани напори им служат на интересите на различни државни и недржавни субјекти.

Препораки за издржливост: Извештаите на Европската комисија ја нагласуваат неопходноста од одржување на медиумскиот плурализам, промовирање професионализам, непристрасно известување, истражувачко новинарство и негување отпорност на дезинформации. Македонската Влада иницираше акциски план за борба против дезинформациите и зајакнување на медиумската писменост во образовниот систем.

Како заклучок, студијата потврдува дека хибридните закани во Република Северна Македонија навистина имаат далекосежни последици врз безбедноста на земјата, управувањето и довербата на јавноста. Иако во моментот безбедноста на земјата е стабилна и безбедносниот систем делумно успеа да ги одбие заканите, императив е да се задржи отпорноста, да се продолжи со следење на ситуацијата и да се усвојат мерки против овие предизвици за долгорочна стабилност на земјата.

Генерален заклучок е дека примарната хипотеза дека безбедноста на Република Северна Македонија е делумно под влијание на хибридни закани, вклучувајќи дезинформации, сајбер-напади и надворешни влијанија, делумно е

потврдена со наодите од студијата. Сепак, делумната потврда може да се припише на сложеноста околу хибридните закани и инхерентните предизвици во докажувањето на нивните директни последици.

Увидите на студијата нагласуваат дека хибридните закани навистина го нарушуваат нормалното функционирање на земјата, што влијае не само на јавните институции, туку и на секојдневниот живот на поединци. Мотивите зад овие закани, без разлика дали се водени од геополитички, политички или деловни интереси, остануваат предмет на континуирана истрага.

И покрај овие нарушувања, проценатa на експертите сугерира дека безбедноста на Република Северна Македонија останува стабилна во моментов, без непосредни знаци на критични нарушувања. Сепак, од суштинско значење е да се признае динамичната природа на хибридните закани, кои може да бидат под влијание на регионалните и глобалните настани, што ги прави тековниот мониторинг и подготвеноста од витално значење.

Оваа студија ја нагласува потребата од понатамошни истражувања и анализи за да се навлезе подлабоко во сложениот пејзаж на хибридните закани и нивните долгорочни импликации за Република Северна Македонија. Иако сегашните показатели се позитивни во однос на безбедноста на земјата, потребни се внимателност и проактивен пристап за да се одржи оваа стабилност и ефикасно спротивставување на хибридните закани во иднина.

7. Користена литература

1. Babbage, Ross. (2019). "*Stealing a March: Chinese Hybrid Warfare in the Indo-Pacific: Issues and Options for Allied Defense Planners Volume II: Case Studies."* Center for Strategic and Budgetary Assessments II: 1–51, достапно на: https://csbaonline.org/uploads/documents/S tealing_a_March_Annex_Final.pdf%0A25.

2. Baldwin, D. A. (1985). *Economic Statecraft*. Princeton: Princeton University Press.

3. Bernays, E. (1928). *Propaganda. Horace Liveright.*

4. Blackwill, R. D., & Harris, J. M. (2016). *The Lost Art of Economic Statecraft*. Foreign Affairs, *95*(2), 99–110.

5. Council of the European Union. (2008). Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. Official Journal of the European Union, 75–82.

6. Denning, D. E. (2015). *Information Warfare and Cybersecurity. Springer.*

7. EEAS. (2018). *A Europe That Protects: Countering Hybrid Threats*. Factsheet.

8. European Commission. (2022). COMMISSION STAFF WORKING DOCUMENT North Macedonia 2022 Report, pp.108, 109.

9. European Union (2021). DIRECTORATE-GENERAL FOR EXTERNAL POLICIES POLICY DEPARTMENT. *Best Practices in the whole-of-society approach in countering hybrid threats*. pp.19.

10. European Union. (2016). *Joint Framework on countering hybrid threats, a European Union response*. Joint Communication to the European Parliament and the Council, EU Document JOIN (2016) 18 final.

11. Galán C (2018*). Amenazas híbridas. Nuevas herramientas para viejas aspiraciones.* In: Elcano Documentos de Trabajo, 20/2018, p. 3.

12. Giannopoulos, G., Smith, M. E., & Theocharidou, M. (2021). *The Landscape of Hybrid Threats.*

13. Hall, J. S., & Zautra, A. J. (2010). *Indicators of Community Resilience: What Are*

They, Why Bother? In J. Reich, A. J. Zautra, & J. S. Hall (Eds.), Handbook of Adult Resilience.

14. Hoffman, F. (2018). *Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges*. PRISM, 7(4).

15. Hoffman, F. G. (2018). *Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict*, 8.

16. https://jorm.gov.mk/ - официјална веб страна Јавно Обвинителство на Република Северна Македонија, Односи со јавноста, соопштенија, објавено 05 февруари 2020, пристапено ноември 2022.

17. https://www.dw.com/mk/so-novo-upatstvo-vo-bitka-protiv-zakanite-so-bombi/a-64871918

18. https://www.dw.com/mk/spasovski-zakanite-so-bombi-se-kombinacija-od-domasni-i-stranski-akteri/a-64894752ж

19. https://www.nato.int/cps/en/natohq/topics_156338.htm#:~:text=NATO%20will%20ensure%20that%20the,necessary%2C%20will%20defend%20Allies%20concerned. Пристапено: август, 2023.

20. Hyvönen, A.-E., & Juntunen, T. (2019). *Kokonaisresilienssi ja turvallisuus: tasot, prosessit ja arviointi.* Publications of the Government's Analysis, Assessment and Research Activities, 17/2019. Prime Minister's Office. (pp. 23–25)

21. Hyvönen, A.-E., & Juntunen, T. (2020). *From 'Spiritual Defence' to Robust Resilience in the Finnish Comprehensive Security Model*. In S. Larsson & M. Rhinard (Eds.), Nordic Societal Security (pp. 154–178). Routledge.

22. Iancu, Niculae, Andrei Fortuna, Cristian Barna, and Mihaela Teodor. (2016). *Countering Hybrid Threats : Lessons Learned from Ukraine*. Washington: IOS Press.

23. Ion Mihai Pacepa and Ronald J. Rychlak (2013). *Disinformation: Former Spya Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*, WND Books, pp. 4–6, 34–39, 75.

24. Jungwirth, R. et al. (2023). *Hybrid threats: a comprehensive resilience ecosystem*. Publications Office of the European Union, Luxembourg, pp. 39, 41.

25. Karlèn, N., & Rauta, V. (2021). *Forum: Conflict delegation in civil wars. Introduction*. International Studies Review, 23(4), 2050–2052.

26. Kleczkowska, A. (2020). *States vs. non-state actors – a public international law perspective*. Hybrid CoE Strategic Analysis, 20. Достапно на: https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-20-states-vs-nonstate-actors-a-public-international-law-perspective/

27. Klijn, H., & Yüksel, E. (2019). *Russia's hybrid doctrine: Is the west barking up the wrong tree?* (The Hague: The Clingendael Institute).

28. Lowenthal, M. M. (2015*). Intelligence: From Secrets to Policy* (6th ed.).

29. Margarete Klein (2019). Hybrid CoE Strategic Analysis 17, Private military companies – a growing instrument in Russia's foreign and security policy toolbox.

30. Molden, Daniel C. (2014). *"Understanding Priming Effects in Social Psychology: What Is "Social Priming" and How Does It Occur?"* Social Cognition. Vol. 32.

31. NATO. (2013). *Allied Command Operations Comprehensive Operations Planning Directive Interim V2.0*. Belgium: North Atlantic Treaty Organization, Supreme Headquarters Allied Powers Europe.

32. Newton, K, and J W van Deth. (2010). *Foundations of Comparative Politics: Democracies of the Modern World*. 2nd ed. Cambridge: Cambridge University Press.

33. Norris, William J. (2016). *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control*. Ithaca: Cornell University Press.

34. Pamment, James, Howard Nothhaft, and Henrik Agardh-Twetman. (2018). *"Countering Information Influence Activities*." Swedish Civil Contingencies Agency.

35. Reilly, James. (2013). *"China's Economic Statecraft: Turning Wealth into Power."* Syndey.

36. Salehyan, I. (2021). *A Decade of Delegation*. International Studies Review, 23(4).

37. Schmitt, M. (2012). Classification of Cyber Conflict. *Journal of Conflict and Security Law*, 17(2), 245-260, достапно на: https://doi.org/10.1093/jcsl/krs018

38. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What*

Everyone Needs to Know. Oxford University Press.

39. Stojanova, M., Cocovski, Z., & Kolovska, V. (2020, December 14). Г*радење отпорност против насилниот тероризам и екстремизмот*.

40. UN-HABITAT. "World Cities Report 2016: Urbanization and Development - Emerging Futures." 2016, достапно на: https://unhabitat.org/sites/default/files/download-manager-files/WCR-2016-WEB.pdf.

41. United Nations. (2014, July). UN News - Brazil 2014 'remarkable platform' to unite people, says Assembly President, достапно на: https://news.un.org/en/story/2014/07/472752

42. United States Strategic Command, основана: 1 јуни 1992, седиште: Омаха, Небраска, Соединети Американски Држави.

43. Weissmann, M. , Nilsson, N. , Palmertz , B. , & Thunholm , P. (2021). *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: I.B. Tauris, достапно на: http://dx.doi.org/10.5040/9781788317795 (pp. 266-271).

44. Weissmann, M. et al. (2021). *Hybrid Warfare: Security and Asymmetric Conflict in International Relation*s. London: I.B. Tauris, достапно на: http://dx.doi.org/10.5040/9781788317795 (p. 268).

45. Wilson, J. L. (2016). *Cultural Statecraft in the Russian and Chinese Contexts: Domestic and International Implications. Problems of Post-Communism,* 63(3), 135-145, достапно на: https://doi.org/10.1080/10758216.2015.1132630

46. Zamfir, R. (2020). Risks and vulnerabilities in the Western Balkans. NATO Strategic Communications Centre of Excellence. ISBN: 978-9934-564-51-2.
47. АКЦИСКИ ПЛАН за имплементација на Стратегијата за градење национална отпорност и справување со хибридни закани (2021-2025).

48. Влада на Република Северна Македонија, Министерство за одбрана (април 2021). *Национална Стратегија за градење на отпорност и справување со хибридни закани,* стр. 4.

49. Влада на Република Северна Македонија, Министерство за одбрана (февруари 2020 год). *Стратегија за сајбер-одбрана*, стр. 18.

50. Дефиниции од речникот на Кембриџ. Достапно на: https://dictionary.cambridge.org/dictionary/english/hybrid

51. Живковиќ, М. (2022, Март 1*). Здружен одговор против хибридните закани* [статија]. Nova Makedonija, достапно на: https://novamakedonija.com.mk/pecateno-izdanie/zdruzhen-odgovor-protiv-hibridnite-zakani/

52. Закани со бомби - комбинација од домашни и странски актери, Катерина Блажевска 06.03.2023.

53. Извештај на ЕКРН за Република Северна Македонија (шести циклус на мониторинг), усвоен на 29 јуни 2023, објавен на 20 септември 2023, достапен на: https://www.coe.int/en/web/european-commission-against-racism-and-intolerance/-the-former-yugoslav-republic-of-macedonia-

54. Маглешов, В. (2020, март 27). Пријавите за лажни вести меѓу правдата и цензурата: Коронавирусот и непроцесираните пријави за дезинформации

55. Мери Јордановска и Антонија Поповска. (2023, март 28), достапно на: https://meta.mk/shemata-na-lazhnite-dojavi-za-bombi-905-zakani-osum-gradovi-76-elektronski-adresi-infografik/

56. Милески, Т. (2005). Геостратегиско окружување на Република Македонија, Годишем *Зборник на Филозофскиот факултет* во Скопје, стр. 413.

57. Милошевска, Т. (2007). Нетрадиционални и глобални безбедносни закани, Годишен *Зборник на Филозофскиот факултет* во Скопје, стр. 580.

58. Национална стратегија за градење отпорност и справување со хибридни закани, 2021.

59. Пренесува Телма, топ вести. Соопштение од МВР: И денешните пријави за бомби се лажни. Достапно на: https://telma.com.mk/2022/11/11/mvr-i-deneshnite-prijavi-za-bombi-se-lazhni/

60. Соопштение од МВР, објавено на официјалната веб–страна, пристапено ноември, 2022 год., достапно: https://mvr.gov.mk/vest/23202.

61. Трајковски М. (2022, March 1). *Лажните дојави за бомби во скопските училиштата - хибридни закани* [статија]. Voice of America – Macedonian. Достапно на: https://mk.voanews.com/a/article-laznite-dojavi-za-bombi-hibridna-zakana/6833385.html

Б Л А Г О Д А Р Н О С Т

Изразувам голема благодарност

до сите професори на Филозофскиот факултет во Скопје,

до Институтот за безбедност одбрана и мир,

особено до мојот ментор, проф. д-р Тања Милошевска,

за несебичното помагање и многубројните стручни совети и насоки во текот на реализацијата на овој труд.

Посебна посвета:

Посветено на мојата мајка, БЛАГОДАРАМ за сета топлина

и надеж в срце што ми влеваш!
