PRESPA ИНСТИТУТ INSTITUTE

ИНФОРМИРАНА ОДБРАНА

Вовед за хибридните закани за критичната инфраструктура

Информативна студија
Што се хибридни закани, а што критична инфраструктура и како изгледа новата безбедносна архитектура?

проф. д-р Весна Попоска
Постара надворешна соработничка и истражувачка, членка на работната група на експертки за надворешна и безбедносна политика

Canada

CFLI/FCIL
Canada Fund for Local Initiatives
Fonds canadien d'initiatives locales

ИНФОРМИРАНА ОДБРАНА

Вовед за хибридните закани за критичната инфраструктура

Информативна студија

Што се хибридни закани, а што критична инфраструктура и како изгледа новата безбедносна архитектура?

Издавач: Институт ПРЕСПА - Скопје

За издавачот: Андреја Стојковски, извршен директор

Авторка: проф. д-р Весна Попоска, постара надворешна соработничка и истражувачка, членка на работната група на експертки за надворешна и безбедносна политика

Дизајн и подготовка: Бригада дизајн дооел

Скопје, Јануари 2024

Оваа публикација е дел од проектот Неискористена експертиза поддржан од Амбасадата на Канада преку канадскиот фонд за локални иницијативи. Ставовите, наодите и заклучоците или препораките кои произлегуваат од публикацијата или проектот се одговорност на авторите и поддржаната партнерска организација и не мора да ги одразуваат ставовите на партнерот за финансирање и неговата соодветна влада.

СОДРЖИНА

I. ВОВЕД

1.1. ШТО СЕ ХИБРИДНИ ЗАКАНИ?

Хибридните закани[1] – неконвенционални закани кои потпаѓаат под прагот на воената сила - станаа сеприсутна карактеристика на денешната безбедносна средина.

Подемот на хибридните закани претставува исклучително субверзивна закана по националната безбедност и меѓународниот поредок. Поради диверзифицираните и суптилни облици на делување, нема консензус за нивното дефинирање. Во суштина, терминот хибридна закана се однесува на различен тип на активности кои се стратешки планирани и координирано спроведени под покритие од држави, односно други субјекти, како тактика за остварување на влијание со цел да се изврши промена или да се нанесе штета на постоечкиот поредок.

Притоа, „**жртва**“ може да биде секој поединец или институција со моќ за донесување одлуки на локално, регионално, државно или институционално ниво. Таквите акции се намерно насочени кон секоја сфера која е потенцијално ранлива, или претставува потенцијално поле за злоупотреба на граѓанските права и слободи. Иако ги има во секој контекст и веројатно нема држава која е имуна на нив, најподложни на нивните ефекти се новите демократии или државите во транзиција и изградба на демократски институции. Токму затоа, тие, за жал, се алатка преку која се градат определени сфери на влијание. Сепак, голем дел од она што се третира како „**хибридна закана**“ воопшто не е новина – туку стратегија и тактика применета на нов начин, бидејќи „*војната има променлива природа, но траен карактер*“[2]. Хибридните закани во секој даден контекст добиваат нова форма и димензија, особено поради зголемената дигитализација и зависноста од интернет услугите.

Под хибридни закани, во најтесна смисла на зборот, се подразбира различен сплет на невоени активности преку кои се остваруваат стратешки цели. Тие се противтежа на конвенционалните закани, односно, на заканата со употреба од воена сила. Најчесто, носители на хибридните закани се државите, но некогаш доаѓаат и од други субјекти, како што се терористичките групи, криминалните здруженија, дури и хактивисти[3]. Во поширок контекст, под поимот хибридни закани, се подразбираат мултимодални, нискоинтензитетни, кинетички, но и не кинетички закани кои вклучуваат повеќе тактики: сајбер-војна, асиметрични конфликтни сценарија, глобален тероризам, пиратство, транснационален организиран криминал итн.

Признати во Концептот на бистратешка команда на НАТО од 2010 година[4], хибридните закани се дефинирани како „*оние што ги поставуваат непријателите, со способност истовремено да користат адаптивни конвенционални и неконвенционални средства во остварувањето на своите цели*“. Терминот „**хибридни закани**“ се употребува како „чадор“ со кој се опфаќа широк спектар на појавни форми на безбедносни закани кои можат да доаѓаат од држави, но и од други субјекти, а постои тешкотија за докажување на атрибуција и одговорност.

Во заедничката комуникација[5] на Европската комисија, Европскиот парламент и Советот за европската агенда за безбедност и заедничка одбрана од 2016 година, концептот на хибридни закани е дефиниран како мешавина на принудна и субверзивна активност, користејќи конвенционални и неконвенционални методи (т.е. дипломатски, воени, економски и технолошки), координирани од страна на држави или други субјекти за да се постигнат конкретни цели додека сепак остануваат под прагот на формално објавено војна.

Практично, хибридните закани се најразлични операции за влијание преку кои, под привидот на демократијата и либералниот простор, различни малигни актери (најчесто, но не исклучиво странски) постигнуваат стратешка цел во своја полза. Секогаш се насочени кон постигнување на стратешки цели, и се синхронизирани, односно во овој случај, неволјата никогаш не доаѓа сама, бидејќи се работи за синхронизирани дејствија кои може да имаат специфична цел, како што е на пример, промена на владата, или општа цел за креирање паника помеѓу населението и недоверба во институциите. Во различна фаза од имплементацијата, хибридните закани може да добијат различна форма (насилни протести, сајбер напади, лажни пријави за поставени бомби, лажни вести) и да бидат реализирани од различни субјекти, вклучително и политички партии, невладини или верски организации. Хибридните закани се насочени кон креирање на јавно мислење кое би помогнало во остварувањето на посакуваните ефекти за нарачателот или за центарот на моќ од каде се водат, а нивните ефекти се каскадни, односно не секогаш се очигледни. Затоа, од исклучителна важност е да се гради лична и општествена отпорност, како и општество на свесни, информирани и слободни индивидуи и медиуми.

1 https://www.iss.europa.eu/content/protecting-europe-0

2 Карл фон Клаузевиц (https://en.wikipedia.org/wiki/Carl_von_Clausewitz)

3 анг. *Hacktivist* – лице кое прави неовластен упат во компјутерски датотеки или мрежи со цел постигнување на некакви општествени или политички цели.

4 https://www.nato.int/cps/en/natohq/topics_82705.htm

5 https://eur-lex.europa.eu/resource.html?uri=cellar:9aeae420-0797-11e6-b713-01aa75ed71a1.0022.02/DOC_1&format=PDF

1.2. ШТО Е КРИТИЧНА ИНФРАСТРУКТУРА?

Во новата безбедносна средина, хибридните закани се најчесто насочени кон критичната инфраструктура, која како безбедносен и оперативен термин е релативно нова појава и особено се актуелизираше по рускиот напад врз Украина, опфаќајќи најчесто енергетски и транспортни системи, но и системи за водоснабдување, како и сообраќајна инфраструктура. Иако терминот е нов, тоа не значи дека критичната инфраструктура претходно не постоела. Напротив, секој општествен поредок во секое доба од човековиот развој имал некаква сопствена критична инфраструктура, односно системи есенцијални за општественото функционирање- водоснабдување, производство и снабдување со храна, определени патни коридори. Во променетата безбедносна средина, критичната инфраструктура е легитимен објект на заштита кој мора да биде препознаен од системот како таков преку императивот на нормата, односно правната рамка. За да може да ја заштитиме критичната инфраструктура, но и да се заштитиме, најпрвин, таа мора да биде препознаена од националното законодавство. Во Република Северна Македонија, тоа ќе се случи со донесувањето на првиот Закон за критична инфраструктура, кој е во завршна фаза на донесување[6]. Притоа, важно е да се нагласи дека дефинирањето на националната критична инфраструктура не е детерминистички и конечен процес, туку динамички и проактивен. Критичната инфраструктура и нејзиното дефинирање може да биде предмет на промена во согласност со проценките за ризици на секоја национална влада.

Европската Унија ја дефинира критичната инфраструктура преку директивата за определување и идентификување на европската критична инфраструктура од 2008 година[7], која ги повикува државите членки да ја идентификуваат и определат критична инфраструктури, која ја имаат на сопствената територија, како и да извршат проценка на потребата за подобрување на нејзината заштита. Сите држави членки ја спроведоа Директивата преку воспоставување процес за идентификување и назначување на европска критична инфраструктура во енергетскиот и транспортниот сектор. Во самата Директива, критичната инфраструктура е дефинирана како: „*средство, систем или дел од него лоциран во државите членки што е од суштинско значење за одржување на виталните општествени функции, здравјето, безбедноста, економската или социјалната благосостојба на луѓето и чие нарушувањето или уништување би имало значително влијание во државата членка како резултат на неуспехот да се одржат тие функции*“. Директивата посебно ја препознава европската критична инфраструктура (ЕКИ) како критична инфраструктура чие нарушување или уништување би имало прекугранично ефект и која треба, како таква, да биде издвоена и идентификувана преку заедничка процедура. Кон крајот на 2022 година, Европската комисија[8] отиде чекор понапред дефинирајќи ги критичните ентитети како покомплексна форма на критична инфраструктура со зголемена меѓу зависност.

Во Прирачникот од Талин[9], под критична инфраструктура се подразбираат физички или виртуелни средства и средства што се во јурисдикција на државата, а кои се толку витални што нивно оневозможување или уништување може да ја ослабне националната безбедност, економијата, јавното здравство и безбедноста или животната средина.

Под „заштита на критичната инфраструктура“ генерално се подразбира сет од мерки и активности од различна природа насочени кон одржување, унапредување и зачувување на карактерот и функционалноста на критичната инфраструктура како таква. Во тој контекст, различни сектори или различни држави различно ја разбираат заштитата на критичната инфраструктура.

Загрозеноста на критичната инфраструктура од хибридни закани, најмногу се должи на фактот што генерално критичната инфраструктура претставува т.н. „мека цел“. Поимот „меки цели»[10] најчесто се поврзува со места каде што се собираат луѓето во голем број, како што се музеи, кина, религиозни локации, трговски центри и слично. Меките цели се контрастни со т.н. „тврди цели“, кои широко ги идентификуваат местата каде што обезбедени се високи нивоа на заштита, често од вооружени лица, односно локации каде пристапот на јавноста е ограничен или подлежи на тешки контроли (на пример, воени инсталации). Конечно, можеби критичната инфраструктура претставува мека цел, но, сите меки цели не се критична инфраструктура. Клучниот елемент за разликување се однесува на прашањето на „критичност». Меките цели не мора да изгледаат како критични за обезбедувањето на основните општествени услуги. Такви се, на пример, стадионите и концертните хали.

6 https://mod.gov.mk/javna-rasprava-zakon-za-kriticna-infrastruktura/

7 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:en:PDF

8 https://eur-lex.europa.eu/eli/dir/2022/2557/oj#:~:text=Council%20Directive%202008%2F114%2FEC%20%284%29%20provides%20for%20a%20procedure,cross-border%20impact%20on%20at%20least%20two%20Member%20States.

9 https://ccdcoe.org/research/tallinn-manual/

10 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0200

1.3. Правна рамка

Не постои единствена правна рамка за одговор на хибридните закани, исто како што не постои ниту единствена дефиниција. Токму затоа, одговорот ќе зависи од контекстот и секогаш ќе мора да се работи поединечна анализа на случај, како би се дал соодветен одговор и би се поставила соодветна рамка за акција. Притоа, предвид треба да се земе дека меѓународното право има четири витални функции: 1) *да ги дефинира прецизно ограничените случаи во кои употреба на сила е допуштена* (самоодбрана и зачувување или поврат на светскиот мир и безбедност, во согласност со Повелбата); 2) *да ја регулира и контролира употребата на сила* (дури и) *во ситуации кога е допуштена*; 3) *да оцени дали силата која била употребена била недозволена*; и 4) *да ги регулира последиците од употребата на сила*, било да е дозволена или недозволена. Со оглед на четирите витални функции и фактот дека меѓународното право ја регулира употребата на сила преку забрана за употреба и исклучок од таа забрана, напорите за одржување на светскиот мир и безбедност, креирале четири аспекти за регулирање на употребата на сила во меѓународното право. За сите четири аспекти важат истите извори на правото, во согласност со член 38 од Статутот на Меѓународниот суд на правдата: 1) меѓународните договори; 2) меѓународното обичајно право; 3) практиката на државите; 4) мислењата на истакнатите правници; и 5) судската практика.

Првиот аспект од четирите споменати е *ius contra bellum*, односно правото против војната или против употребата на воена сила. Вториот аспект е корпусот на правни правила *ius ad bellum*, односно правото на војна, кој регулира кога е правно дозволиво државата или државите да прибегнат кон употреба на сила. Третиот аспект е корпусот на правни правила *ius in bello* кој ги регулира принципите, стандардите и регулирањето кои стапуваат на сила кога сила веќе била употребена и се постои активен конфликт. Четвртиот аспект е *ius post bellum*, или принципи, стандарди и обврски по завршувањето на главните непријателства. Оттаму, нормативната рамка врз основа на која се операционализира заштитата на критичната инфраструктура, или врз основ на која треба да се даде одговор на хибридните закани, може да се разликува од случај до случај. Некогаш применливо е националното право, некогаш меѓународните конвенции, а во трет случај, тоа можат да бидат за паралелни процеси. Ова особено доаѓа до израз во справувањето со тероризмот и организираниот криминал.

Двата најсериозни предизвици во справувањето со хибридните закани се потешкотиите да се воспостави каузална и јурисдикциска врска, односно да се докаже одговорност и да се процесира кривично гонење во меѓународен, и особено сајбер контекст.

II. ОД КАДЕ ДОАЃААТ ХИБРИДНИТЕ ЗАКАНИ?

„Доктрина на Герасимов"[11] е концепт кој се однесува на хибридните закани пред се како на операции за остварување на влијание преку информациски, културни, хуманитарни, дипломатски и економски активности. Тука спаѓаат лажните вести кои влијаат на креирањето на јавното мислење, па во тој контекст и лажните дојави за бомби, со кои живеевме одреден период од 2023 година, имаат за цел да влеат страв и недоверба во институциите. Иако, „Доктрината на Герасимов" повеќе се употребува како западна кованица, сепак, терминот произлегува од еден текст на генералот на руската армија, Валери Герасимов, објавен токму во периодот кога пред десетина години руско-украинските односи беа прилично затегнати, по што следеше припојувањето на Крим.

Секако, неправедно е целиот товар на хибридното војување да му се припише само на генералот Герасимов. Оваа доктрина има свој историски развој и во руската надворешна политика, но и во развојот на разузнавачките служби. Многумина ја сметаат за надградена верзија на „Доктрината на Примаков" именувана по поранешниот министер за надворешни работи и премиер на Руската Федерација, Евгениј Примаков, кој тврди дека монополарен свет во кој доминираат САД е неприфатлив за Русија и ги нуди следните принципи за руската надворешна политика[12]:

- Русија да се стреми кон мултиполарен свет што може да биде противтежа на едностраната моќ на САД.
- Русија да инсистира на својот примат во пост советскиот простор и да ја води интеграцијата во тој регион.
- Русија да се спротивстави на проширувањето на НАТО.

Во следните години се создаде впечаток дека заканата од Русија е исклучиво базирана на меката моќ која се остварува само преку хибридните закани. Меѓутоа, војната со Украина покажа дека, за жал, тоа не е единствената опасност што доаѓала од исток. Обемот и опфатот на операциите на руската хибридна војна се проширија со растот и подобрувањето на руските капацитети за таканаречената „тврда моќ", односно, вооружувањето и употребата на сила.

Русија има долга историја на пропагандни и дезинформациски операции класифицирани според нивните ефекти: информатичко-технички и информациско-психолошки[13]. Голема пресвртница за овие напори се случи во 2008 година кога пророските сајбер напади се случија истовремено со руските воени операции во Грузија. Двете страни се натпреваруваа да го контролираат протокот на информации кон меѓународната заедница. Од денешна перспектива, стручната јавност е прилично согласна дека Грузија ја добила информациската војна[14] преку сопствена агресивна кампања со употреба на дезинформации и медиумска манипулација, што е прилично опасен преседан во однос на идејата за демократија, слобода, и либерални вредности. Иако рускиот дел од приказната е извесен, тој сепак е далеку од единствениот извор на моќ од кој доаѓаат хибридните закани. Битките за стратешка превласт и геополитичка доминација, во различни региони во светот, вклучуваат различни актери.

11 https://www.heritage.org/defense/report/understanding-russias-concept-total-war-europe
12 https://carnegieendowment.org/files/Rumer_PrimakovDoctrine_final.pdf
13 https://www.marshallcenter.org/sites/default/files/files/2020-03/percon_v10n1_eng_0.pdf
14 https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2931&context=parameters

III. ПОСТУЛАТИ НА НОВАТА БЕЗБЕДНОСНА АРХИТЕКТУРА

Контурите на глобалните промени може да се дефинираат на неколку фронтови. **Прво**, тука е промената на актерите, која се должи на редефинирање во односите на моќ помеѓу постоечките актери - државите, и појавата на нови актери-транснационални корпорации, невладини организации, терористи, глобални бунтовници, организирани криминални мрежи, мафијашки картели и други атипични структури. Со вклучувањето на регуларните државни елити во концептот на демократизација, опозицијата доби форма на „приватни», субјекти кои користат терористички методи пополнувајќи го меѓу просторот на глобалниот поредок.

Второ, меѓународното право не ги препознава новите актери како субјект. Режимите, дури подоцна беа препознаени како нова закана по светскиот мир и безбедност. Начинот на кој беше или не беше организиран одговорот кон таквите состојби, во голема мера ја редефинира мапата на глобални жаришта.

Трето, зголемената свест и брзиот проток на информации доведе до тоа реакциите на јавноста да станат неминовни, особено преку популаризацијата на социјалните медиуми. Зголемено е влијанието на јавното мислење и неверојатно е брз протокот на информации кои влијаат на неговото креирање со оддалеченост од илјадници километри

Четврто, зголемениот степен на радикализација, во секоја смисла, води кон зголемена дивергентност на интересите на поединци и групи, за сметка на идеалот за отворени општества. Радикализацијата е во еден дел одговор на стеснувањето на либералниот простор, но во многу поголем дел, одговор на економската и социјалната нееднаквост, губењето на смисла, потрагата по идентитет, зголемениот страв и поставувањето граници помеѓу различностите, неодговорното лидерство и популизмот. Европскиот пан идеализам под ударот на економската и мигрантската криза, во голем дел беше заменет со орбанизмот и кулминираше со гласањето за Брегзит. Радикалната десница, неофашистите и сродните групации влегоа во националните парламенти на државите кои ја издигнаа демократијата како концепт. Единствен брз одговор беа социјалните движења и протестите ширум светот, кои, пак, беа многу повеќе злоупотребени за други интереси.

Петто, зголемената индустријализација и нерамномерниот индустриски развој, доведоа до еколошка катастрофа и засилување на ефектите од глобалното затоплување.

Шесто, технолошкиот напредок овозможи акумулирање на моќ во рацете на поединци со малициозни намери. (Зло) употребата на сајбер-просторот и придобивките на модерната технологија овозможуваат голем дострел и брза придобивка за постигнување на различни политички цели.

Седмо, транснационалните компании чиј капитал е поголем од буџетот на многу држави, во трката за профит и борбата со конкуренцијата ги вплеткува во мрежи кои традиционално не го засегале бизнис секторот. Демократијата и капитализмот кои се проширија од запад кон исток инхибираа процеси на брза транзиција и приватизација. Трансформирањето на капиталот од општествен во приватен преку ноќ доведе до тоа да типични сектори на критична инфраструктура преминат во рацете на приватни стопанственици од странство или во директна сопственост на старите елити, со што и едните и другите ја мултиплицираат сопствената моќ и можностите за остварување влијание врз донесувањето одлуки од национален интерес. Приватизирањето на услугите пак доведе до тоа да се редефинираат улогите кои определени институции ги имале, посебно во безбедносниот сектор и дел од истите да им бидат предадени на приватни субјекти, кои долго оперираа во меѓу просторот заради недостиг на прецизно дефинирани овластувања и на едната и на другата страна.

Осмо, поради сè погоре наведено, концептот на воjната драстично се промени. Моќта е редефинирана, а соодносот на силите е надвор од еквилибриум.

Сумарно земено, заклучокот е дека безбедносната средина е драстично изменета. Новите односи и новите закани бараат поинакви пристапи и нови одговори. Кризата на вредности влијае негативно на балансот помеѓу императивот за слобода и потребата за безбедност, стеснувајќи го либералниот простор на современо конципираните општества.

IV. РЕДЕФИНИРАЊЕ НА АЛАТКИТЕ НА НАЦИОНАЛНА МОЌ

Новата безбедносна средина и новите актери го предизвикаа статус квото и моќта на националните држави, заради што инструментите на национална моќ беа постепено редефинирани. Појавата на нова стратешка средина бара оркестрација на повеќе инструменти на моќ[15]. Овој процес започна со концептот на **DIME** (*Diplomacy*, *Information*, *Military*, *Economy*) кој постепено беше надградуван, за конечно да биде надополнет со **FIL** –(*Finance*, *Intelligence*, *Law-Enforcement* - **DIMEFIL**). Во ваква констелација на односи, уште потешко е препознавањето на и справувањето со хибридните закани. Границата помеѓу војната и мирот, постојано се поместува и се проширува. Ривалските држави се повеќе користат хибридна тактика за да влијаат на демократските процеси и да ја експлоатираат ранливоста на нивните противници. Овие тактики[16] вклучуваат координирана и синхронизирана употреба на насилни и ненасилни инструменти на моќ за извршување на вкрстени домени од прагот на конвенционален вооружен воен конфликт, често заобиколувајќи го откривањето и припишување.

[15] https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2106566/putting-the-fil-into-dime-growing-joint-understanding-of-the-instruments-of-pow/

[16] https://hcss.nl/wp-content/uploads/2023/04/Guidelines-for-the-Deterrence-of-Hybrid-Threats-HCSS-2023.pdf

V. СЛУЧАИ ОД ПРАКТИКАТА

5.1. САЈБЕР-ОКУПАЦИЈА

Во 2007 година, владата на Естонија објави дека ќе го премести споменикот наречен Бронзен војник[17] од центарот на Талин на воените гробишта на периферијата на градот. Споменикот го подигнаа советските власти во знак на сеќавање на советските сили кои ја победија нацистичката војска од Естонија. Многу Естонци го сметаа споменикот за навредлив поради повеќедецениската окупација на земјата од страна на Советскиот Сојуз. Тогашната одлука предизвика незадоволство во медиумите на руски јазик и доведе до дводневни немири во Талин во кои беа повредени 156 лица, а 1.000 лица беа приведени.

Еден ден подоцна, Естонија беше погодена од сајбер напади, кои траеја неколку недели и ги погодија естонските банки, владините тела и медиумите. Сајбер-нападите[18] дојдоа од руски IP адреси, иако владата отсекогаш негираше каква било вмешаност. *Руската хакерска група* **Килнет** ја презеде одговорноста за нападот[19], наведувајќи на својот профил на Телеграм дека го блокирала пристапот до повеќе од 200 државни и приватни естонски институции, вклучително и онлајн системот за идентификација на граѓанин. Низата активности што следеа, ја претворија Естонија во лидер во сајбер отпорноста, а НАТО воспостави центар за сајбер извонредност во Талин.

5.2. ИЗБОРНИ ВМЕШУВАЊА И ДЕЗИНФОРМАЦИИ

Во ерата кога дезинформациите станаа политичка стратегија, исклучително е тешко да се препознае вистината, и за гласачите, и за новинарите. Во последните години, неколку спектакуларни обиди за изборно вмешување ги окупираа вести. Од мешањето на Руската агенција за разузнавачки истражувања (ИРА) на изборите во САД[20] во 2016 година, се до операцијата за хакирање и протекување на информации, насочена кон францускиот претседател, Емануел Макрон. Едно е, сепак, заедничко за сите. Нивниот дизајн, како и тајмингот на изборно вмешување покажаа решеност за целосно нарушен изборниот процес.

Во изборен контекст дезинформациите, преку лажните вести или манипулациите имаат огромно значење, бидејќи влијаат на креирањето на јавното мислење а со тоа и на однесувањето на гласачите. Манипулациите може да се состојат од лажни однесувања, употребени како засилување на политичката порака преку ***ботови*** или ***тролови*** на социјалните мрежи, односно преку поттикнување на настани во реалниот живот, особено демонстрации. Дезинформациите, како лажна содржина, може да бидат користени како насочени лаги кои промовираат еден кандидат или оцрнуваат друг, односно едноставно ја поткопуваат довербата во исправноста на изборниот процес. Токму затоа, секретарот за национална безбедност на САД, во 2017та година, го додаде избирачкиот систем на САД[21] на листата на критична инфраструктура како седумнаесетти сектор. Имајќи го предвид суверенитетот на сојузните држави во однос на изборите, ваквата одлука не наиде на одушевување.

5.3 ЛАЖНО ПИСМО

Владата на Литванија беше мета на измама на е-пошта во која се тврдеше дека војниците на НАТО се повлекуваат од нејзината територија.

Генералниот секретар на НАТО[22], Јенс Столтенберг, изјави дека лажното писмо испратено во негово име за објавување на наводното повлекување на сојузничките војници од Литванија имаше за цел да ги збуни граѓаните и да го поткопа единството на сојузниците, а користејќи ја пандемијата. Доминантниот наратив на поврзаните лажни вести се однесувал на тоа како НАТО ги загрозува интересите на сојузниците, сојузнички војници се однесувале несоодветно во јавноста, а алијансата работи на создавање на нуклеарно оружје наместо да помогне во справувањето со пандемијата.

17 https://www.slobodnaevropa.mk/a/31990820.html
18 https://www.euronews.com/next/2022/05/26/cyberattacks-likely-to-rise-in-wake-of-ukraine-war-this-is-what-estonia-learnt-from-web-wa
19 https://www.slobodnaevropa.mk/a/31994141.html
20 https://www.disinfo.eu/publications/foreign-election-interferences-an-overview-of-trends-and-challenges/
21 https://www.eac.gov/sites/default/files/eac_assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf
22 https://www.dw.com/en/malign-actor-poses-as-nato-chief-emails-lithuania-saying-troops-are-pulling-out/a-53209653

5.4 Верски прашања

Црна Гора се соочи со политички превирања непосредно пред пристапувањето во НАТО. Превирања имаше и потоа. Истите беа како последица на различни навидум општествени прашања, а најизразени беа оние кои се поврзуваа со верските прашања[23]. Фазата на деморализација вклучуваше огромно присуство на лажни вести, говор на омраза, дезинформации и повици за одбрана од замислен непријател. Во кампањата за ширење лажни вести и дезинформации, еден портал[24] одиграл водечка улога создавајќи сериозен квантум на дезинформации. Порталот иако без регистрација во Регистарот на медиуми се претставувал како новинар. Притоа, креирал многу содржини насочени да предизвикаат емоционална реакција од читателите, користејќи злоупотреба на историските контексти и поврзувајќи го Претседателот на Црна Гора со фашистичките режими од Втората Светска војна. Слично постапувал и од прокремлинскиот Спутник. Случаите на дезинформација од страна на овие два портали биле документирани од дигиталниот форензички центар во Подгорица.

5.5 Азиска хегемонија

На 12 октомври 2020та година Индија[25] се соочи со најлошите прекини во снабдувањето со електрична енергија во последните децении. Притоа економијата беше осакатена, берзата беше затворена, илјадници патници заглавија, а болниците се бореа да обезбедат резервна опција за нивните КОВИД пациенти. Големите прекини на електрична енергија не се сосема невообичаени во Индија, но биле изненадување за главниот град на западната покраина Махараштра, Мумбај. Властите во Мумбај, беа зачудени и тргнаа во потрага по одговор. Истрагата покажа дека причината за прекинот во снабдувањето со електрична енергија е сајбер-напад кој целел на серверите на државните електроенергетски компании. Иако не успеаја да докажат одговорност, но, за властите импликацијата на кинески хакери била повеќе од јасна. Во својот обид да воспостави азиска хегемонија, Кина ја смета Индија за голема пречка. Оваа можна саботажа дојде во време на зголемени воени тензии, со конфронтации кои пламнаа на бројни точки долж спорна граница помеѓу двете држави. Способноста на Пекинг да го притисне својот сосед се протега надвор од конвенционалното бојно поле и сè повеќе вклучува неконвенционални форми на војување.

5.6. Одмрзнување на замрзнатите

Ескалацијата на израелско-палестинскиот конфликт, како и конфликтот во Нагорно- Карабах, како што се развиваше ситуацијата во Украина, не беа апсолутна случајност, туку обид да се разводни концентрацијата на меѓународна помош и фокусот на јавното мислење од Украина, на различни точки во светот. Хибридните закани може да добијат различни форми во различни региони, но тие имаат ист извор и слична цел, која не оди подалеку од она што се смета за сфера од национален интерес од многу малку центри на моќ. Досега видовме прокси активности преку медиуми и дезинформации, сајбер простор, хуманитарни работи, религиозни прашања, билатерални спорови, енергетска безбедност, критично нарушување на инфраструктурата и општа поделба која создава пристрасна атмосфера. Општествената и политичката поларизација, нема да го намалат притисокот во времето кое доаѓа.

[23] https://nsf-journal.hr/online-issues/focus/id/1296
[24] https://www.in4s.net/
[25] https://www.foreignaffairs.com/articles/china/2021-04-02/chinas-unrestricted-war-india

VI. ОТПОРНОСТА КАКО ЗАЕДНИЧКИ ОДГОВОР

За да помогнат во спротивставувањето на хибридните закани и поддршката на креаторите на политиките во одбраната на демократските општества, Хибрид СЕ и Заедничкиот истражувачки центар на Европската комисија[26] изградија модел кој препорачува рамка за сеопфатно преиспитување на отпорноста. **Сеопфатен екосистем за отпорност**, или *Comprehensive Resilience Ecosystem* (**CORE**), истакнува два фактори кога размислуваме за одговор. *Прво*, отворените општества се секогаш повеќе поврзани внатрешно и меѓусебно. *Второ*, секој одговор треба да го вклучи целото општество за ефикасно спротивставување на заканите. За таа цел, претставениот модел се однесува на различни општествени или секторски „простори» (институции, граѓанско општество, услуги), како и различни „нивоа» (меѓународно, национално и локално).

Концептот на резилиентност[27] (отпорност или еластичност) е најновиот безбедносен концепт во делот на кризен менаџмент и цивилна заштита во ЕУ и НАТО. Притоа, степенот на отпорност (еластичност, односно способност да се вратат многу брзо виталните функции на општеството во нормала по соочување со криза) определува колку едно општество е способно брзо да одговори на кризата и да ги врати виталните општествени функции во функција по настанувањето на кризна ситуација.

Преку градењето на отпорност, може да се даде единствен одговор на заканите од различен карактер, без оглед на појавниот облик. Тоа подразбира холистички пристап, стратешко комуницирање, централизирано управување и децентрализирано извршување, базирано на пристапот на човекови права. Треба да се воспостават јасни законски и оперативни рамки кои се компатибилни со заштита на човековите права, како и да се нагласи дека управувањето со кризи е важно не само во случај на терористички напади, туку и при мали инциденти за да се избегне или да се намали влијанието и ескалацијата на кризата. Идентификацијата на соодветна рамка за управување со кризи бара разгледување на две основни прашања. *Првото* е дали управувањето со вонредни состојби ќе го следи пристапот за специфичен ризик или опасност, или ќе има пристап насочен кон сите опасности (*all hazards approach*). Двата пристапи имаат предности и недостатоци. Кога се поставени структури за управување со кризи за одредени видови на закани, може да се воспостават наменски процеси. Сепак, изборот на приод специфичен за опасностите може да биде проблематичен кога природата на инцидентот не е јасна, бидејќи може да предизвика несигурност во однос на применливата рамка за интервенција. *Второто* прашање треба да се осврне на тоа дали обемот на структурите и процедурите за управување со криза треба да бидат специфични за секторите или меѓу секторски. Ако се избере првиот пристап, правната рамка често се усвојува од министерството одговорно за конкретниот сектор или од регулаторот на секторот. Наместо тоа, меѓу секторскиот пристап честопати го прифаќа општото законодавство.

Препорака за надминување на состојбите е примена на *all hazards approach*, односно пристап на адресирање на сите опасности. Посебно е важно да се увиди големата слика, односно критичната инфраструктура да се постави во поширок наместо изолиран контекст- на пример, иако меѓународното еколошко право не ја третира директно критичната инфраструктура, сепак, може да влијае врз определени сегменти. Овие аспекти се важни бидејќи превенцијата е клучна алка во градењето отпорност.

Ефективната стратегија за заштита на критичната инфраструктура главно почива врз два столбови: ефективен **систем за рано предупредување** и ефективно **менаџирање со кризи**. Успешното функционирање на овие два системи придонесува кон мерките за намалување на ризикот, со што, пак, се зголемува безбедноста на критичната инфраструктура. Ефективната стратегија за заштита на критичната инфраструктура во тој контекст треба да обезбеди ефективна проценка на ризикот и соодветна рамка за дејствување. Опасноста од други субјекти кои имаат мрежна и глобална поставеност, но и од потенцијални природни катастрофи, во услови на голем број субјекти (од јавен и приватен сектор, со различни интереси, а истовремено меѓусебно зависни во доменот на давањето услуги), ја наметнува потребата од централизиран начин на одлучување. Централизираниот начин на донесување одлуки, колку и да изгледа, на прв поглед, старомодно и либерално е неопходен заради две причини: *Прво*, преку него се обезбедува ефективна координација во доменот на раното предупредување. Сите инволвирани актери добиваат неопходни информации за состојбата со потенцијалната опасност од природни катастрофи. *Второ*, со централизираниот начин на донесување одлуки сите актери применуваат ист пакет на мерки и стандарди.

Заканите и натаму ќе растат и ќе мутираат. Меѓутоа, ефективната заштита лежи во превенцијата и зајакнувањето на општеството - и во зајакнувањето на правната рамка токму во тој сегмент. Тоа подразбира законски измени и примена на најдобри практики, со воспоставување на целата институционална рамка која од тоа произлегува, како и ефектуирање на фискалните импликации. Сепак, ниту најдоброто законско решение нема да биде ефективно без механизам за имплементација и без за него да се предвидат соодветни фискални импликации. На крајот, градењето партнерства е неопходно, но, тие треба да се засновани на стратешки и институционален пристап, опфаќајќи ги академската и деловната заедница, владините институции и граѓанското општество, со визија за изградба на отпорно општество засновано на едукација и кибернетска култура.

[26] https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/

[27] https://www.nato.int/cps/en/natohq/topics_132722.htm#:~:text=Each%20NATO%20member%20country%20needs,civil%20preparedness%20and%20military%20capacity.

VII. СЕВЕРНА МАКЕДОНИЈА- ПРЕДИЗВИЦИ И ПРЕПОРАКИ

Членството на Северна Македонија во НАТО придонесе националниот систем релативно брзо да преземе определени процеси и концепти. Така, во делот на креирањето политики беа усвоени цела низа на стратешки документи од исклучително значење, како што се **Стратегијата за сајбер одбрана**[28] и **Стратегијата за градење на отпорност и справување со хибридни закани**[29]. Притоа, Стратегијата за градење на отпорност е прилично широко поставена, иако недостигаат извештаи за годишниот напредок, особено што дел од овие прашања се провлекуваат и низ Извештајот за напредокот на Северна Македонија подготвен од Европската Комисија[30].

Согласно Кривичниот законик, ширењето дезинформации не претставува кривично дело, а интернетските медиуми не се регулирани со посебен закон туку се оставени на саморегулација. Ваквиот принцип го охрабруваат меѓународните стандради за медиумско известување, иако во новиот контекст тој е недоволен. Од друга страна, ако се обидете да ги спречите дезинформациите претворајќи ги во кривично дело, тогаш влегувате во една друга сензитивна област, каде што е извонредно тешко да се воспостави баланс помеѓу потребата за безбедност и заштита од дезинформации и она што претставува стандард кај слободата на говор, а во согласност со членот 10 од Европската Конвенција за човековите права. Либералниот периметар се повеќе се стеснува токму поради новиот тип на закани во ново безбедносно опкружување, а личните слободи се ставени на тапет во име на стравот од пандемијата, хибридната војна, инфлацијата, реалната војна во Украина, милионите бегалци од Блискиот исток.

Пример за ваква политика може да биде Канада[31], која предводена од конзервативна влада, во 2015 година усвои ново антитерористичко законодавство, а во 2017 година, предводена од либерална влада, етаблираше нови надлежности за националната агенција за електронски надзор, давајќи и можност тесно да соработува со армијата и да спроведува офанзивни акции кон странски субјекти и да исклучува потенцијални сајбер напади со цел да ја заштити Канада и нејзината критична инфраструктура. Ваквата состојба значеше легализација не само на антиципаторната, туку и на преемптивната самоодбрана во сајбер контекст, што може да биде исклучително опасна практика - односно да се употреби воена сила против напад кој сè уште не се случил.

Токму затоа, поради комплексноста на проблематиката, неопходно е да се гради лична, институционална и општествена, односно национална отпорност, како и свест за опасностите. Иако отпорноста е исклучително широк концепт, неспорно треба да се започне од основните постулати на најизразените проблеми кои потенцијално би ги предизвикала новата безбедносна средина. Неопходна е нова национална безбедносна проценка, но и нова методологија за проценка на ризици. Неопходна е дополнителна регулација во медиумскиот сектор, бидејќи саморегулацијата, очигледно, не е доволна. Таа регулација секако не треба да оди во насока на стеснување на слободата на медиумите, туку во нивна заштита и унапредување, односно, наметнување на еднакви услови и одговорност за електронските портали, но и за останатите регистрирани медиуми. Оваа дополнителна регулација не треба да го зафаќа основањето на медиумите, но треба да создаде регистар на вистински сопственици и да гарантира посочување импресум со уредничка одговорност. Со тоа, традиционалните медиуми, новинарите и уредниците кои професионално ја вршат својата задача, нема да бидат ставени во неповолна положба. Исто така, изворите на финансирање за медиумите како и промената во моделот на финансирање се прашања кои дополнително треба да се размислат. Истото се однесува и на финансирањето на политичките партии и кампањите. Прашање од посебна загриженост е подемот на радикалната десница и отворената поддршка која ја дава на недемократските системи. Оттаму, медиумската писменост и сервисите за проверка на факти се од особено значење, како и активната институционалната транспарентност. Додека, информативниот пејзаж[32] игра улога во проценките на нивоата на ранливост во Западен Балкан. Достапноста на легитимни информации е во центарот на градењето на отпорноста против непријателското влијание.

Сајберсвесноста и сајберкултурата се, исто така, претпоставка за градење на здрави општества. Тоа подразбира не само усогласеност со меѓународните стандарди, туку и диверзификација на изворите на моќ и нејзината концентрација, како и намалување на зависностите помеѓу различни субјекти на критичната инфраструктура, особено во онлајн светот. Системскиот пристап во овој сегмент би значел измена на низа регулативи кои на прв поглед немаат директна врска со градењето на сајберкапацитети, како што се на пример, јавните набавки. Зајакнување на капацитетите на институциите во насока на дигитализација на услугите и справување со заканите од сајбер просторот е неопходност. Ова особено се однесува на институциите кои имаат надлежност во делот на заштита на личните податоци и безбедноста на интернет, како и развој на националната *ЦЕРТ единица* (*Computer Emergency Response Team* - **CERT**) по примерот

28 https://mod.gov.mk/inc/uploads/2021/06/Strategija-za-sajber-odbrana-mk-1-1.pdf
29 https://mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf
30 https://neighbourhood-enlargement.ec.europa.eu/north-macedonia-report-2023_en
31 https://www.cbc.ca/news/politics/trudeau-tracker-anti-terrorism-bill-1.3586337
32 https://www.researchgate.net/publication/361700596_Hybrid_Warfare_in_the_Western_Balkans_How_Structural_Vulnerability_Attracts_Maligned_Powers_and_Hostile_Influence

на Словенија. Зајакнување на медиумскиот сектор и реформа на јавниот радиодифузен сервис се неопходност, како и заштита на достоинството и атрактивноста на новинарската професија. Од друга страна, потребно е регулирање на однесувањето на инфлуенсерите и на вештачката интелигенција, веројатно на глобално ниво, но потребен е локален одговор.

Усвојувањето на предлог Законот за критична инфраструктура кој е во завршна фаза во Министерството за одбрана значително ќе допринесе за зајакнувањето на отпорноста. Од системски решенија, неопходна е брза имплементација на идејата за реформа на системот за кризен менаџмент и цивилна заштита, затоа што отпорноста подразбира брз повратво нормално функционирање по евентуален шок или кризно сценарио, а не отсуство на кризи. Дополнително, неопходно е да се обрне повеќе внимание на верските организации и нивно системско интегрирање во поширокатаопштествена констелација. За жал, антиродовите движења се повеќе земаат на замав, како и пророски наратив, токму од поединци кои доаѓаат од определени идеолошки проминенции. Отпорност во справувањето со притисокот и малигните влијанија мора да покажат и културните институции. Особено за оние кои доаѓаат од подготвени субјекти, вешти во искористувањето и манипулирањето со верските и социјалните прашања за политичка придобивка со дезинформации распространети преку социјалните медиумски платформи, религиозни и културни институции, прокси и сајбер упади против мрежите. Покрај тоа, градењето доверба во институциите се уште е суштинско за стабилност на системот и владата.

За намалување на ризиците[33] поврзани со малигно влијание државата мора да биде функционална и силна. Оттаму, борбата со корупцијата, подобрувањето на јавните услуги, зголемувањето на животниот стандард, не се само фрази од политичките говори во процесот на пристапувањето во Европската Унија, туку и потреба за активно градење на отпорност.

Граѓанското општество игра особена улога во процесот на создавање на отпорност. Граѓанските организации треба да продолжат како активен коректор и набљудувач на состојбите, додека помалите локални организации, кои најдобро ја познаваат состојбата во внатрешноста треба да ја задржат улогата на креатори на општествен ангажман за младите надвор од метрополата. Зајакнатото младинско учество во процесите на одлучување и креирање на политики, е исто така одбрана од негативните влијанија и хибридните закани, а инклузијата е прв чекор кон неутрализирање на радикалите и како таква, е неопходна за градење на силни општествени заедници.

Во современи услови на климатските промени, но и на воената агресија на Русија во Украина градењето на енергетска независност е важна алатка за создавањето отпорност и справувањето со последиците од климатските промени. Не помалку важно е обезбедувањето ресурси на примарната здравствена заштита во регионалните и локалните здравствени центри, со цел намалување на оптовареноста на централните капацитети и правилно распределување и искористување на ресурсите. Конечно, адаптирањето на институциите кон промените придонесува за прифаќањето на општествената динамика кон хибридните закани, кои иако не ја менуваат својата суштина, ги менуваат формата и обликот на дневна основа.

Хибридните закани имаат заеднички именител, но се исклучително диверзифицирани. Токму затоа, во сите критични области, неопходно е да се работи на подигање на свесноста и знаењата за критичната инфраструктура, активно градење на партнерстава и сојузи, зајакнување на правната и институционалната рамка, како и градењето на капацитети. Неопходен е телеолошки пристап и заеднички одговор на сите вклучени актери, како и промовирање на науката и образвоанието во насока на надминување на предизвиците./

[33] https://intapi.sciendo.com/pdf/10.2478/seeur-2022-0018

БИБЛИОГРАФИЈА И КОРИСТЕНИ ИЗВОРИ

1. Bertolini, Minicozzi and Sweijs (2023) Ten Guidelines for Dealing with Hybrid Threats- A Policy Response Framework, https://hcss.nl/wp-content/uploads/2023/04/Guidelines-for-the-Deterrence-of-Hybrid-Threats-HCSS-2023.pdf

2. CBC (2016) Trudeau tracker: Promised changes to anti-terrorism law C-51 still months away, https://www.cbc.ca/news/politics/trudeau-tracker-anti-terrorism-bill-1.3586337

3. CCDCOE, the Talin manual https://ccdcoe.org/research/tallinn-manual/

4. Disinfo.eu (2023) Foreign elections interference- an overview https://www.disinfo.eu/publications/foreign-election-interferences-an-overview-of-trends-and-challenges/

5. Dolan (2022) Hybrid Warfare in the Western Balkans: How Structural Vulnerability Attracts Maligned Powers and Hostile Influence, https://intapi.sciendo.com/pdf/10.2478/seeur-2022-0018

6. DW (2020) Fake 'NATO' email informs Lithuania of troop pullout https://www.dw.com/en/malign-actor-poses-as-nato-chief-emails-lithuania-saying-troops-are-pulling-out/a-53209653

7. EU (2008) Council Directive 2008/114/EC https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:en:PDF

8. EU (2017) Communication from the Commission to the European Parliament and the Council on a more Effective Return Policy in the European Union - A Renewed Action Plan, Com/2017/0200 Final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0200

9. EU (2022) Directive 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance) https://eur-lex.europa.eu/eli/dir/2022/2557/oj#:~:text=Council%20Directive%202008%2F114%2FEC%20%284%29%20provides%20for%20a%20procedure,cross-border%20impact%20on%20at%20least%20two%20Member%20States.

10. Euronews (2022) Cyberattacks likely to rise in wake of Ukraine War. This is what Estonia learnt from Web War One https://www.euronews.com/next/2022/05/26/cyberattacks-likely-to-rise-in-wake-of-ukraine-war-this-is-what-estonia-learnt-from-web-wa

11. European Commission (2016) Communication https://eur-lex.europa.eu/resource.html?uri=cellar:9aeae420-0797-11e6-b713-01aa75ed71a1.0022.02/DOC_1&format=PDF

12. European Commission (2023) Nєrth Macedonia progress report https://neighbourhood-enlargement.ec.europa.eu/north-macedonia-report-2023_en

13. Fiott & Parkes (2019) PROTECTING EUROPE-the EU's response to hybrid threats https://www.iss.europa.eu/content/protecting-europe-0

14. Foreign Affairs (2021) China's Unrestricted War on India- Beijing Bullies Its Neighbor by Unconventional Means https://www.foreignaffairs.com/articles/china/2021-04-02/chinas-unrestricted-war-india

15. HybridCoE (2023) Hybrid threats: A comprehensive resilience ecosystem https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/

16. Iasiello (2017) Russia's Improved Information Operations: From Georgia to Crimea https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2931&context=parameters

17. Murphy (2016) Understanding Russia's Concept for Total War in Europe, https://www.heritage.org/defense/report/understanding-russias-concept-total-war-europe

18. NATO (2010) Strategic concept https://www.nato.int/cps/en/natohq/topics_82705.htm

19. NATO (2023) Resilience, civil preparedness and Article 3
https://www.nato.int/cps/en/natohq/topics_132722.htm#:~:text=Each%20NATO%20member%20country%20needs,civil%20preparedness%20and%20military%20capacity.

20. Per Corcordiam (2020)
https://www.marshallcenter.org/sites/default/files/files/2020-03/percon_v10n1_eng_0.pdf

21. Rodriguez, Walton, and Chu (2020) Putting the "FIL" into "DIME": Growing Joint Understanding of the Instruments of Power
https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2106566/putting-the-fil-into-dime-growing-joint-understanding-of-the-instruments-of-pow/

22. Rumer (2019) The Primakov (Not Gerasimov) Doctrine in Action
https://carnegieendowment.org/files/Rumer_PrimakovDoctrine_final.pdf

23. Trifunovic & Obradovic (2020) Hybrid and Cyber Warfare – International Problems and Joint Solutions
https://nsf-journal.hr/online-issues/focus/id/1296

24. US Elections assistance Comission (2017)
https://www.eac.gov/sites/default/files/eac_assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf

25. Влада на Република Северна Македонија (2021) Стратегијата за градење на отпорност и справување со хибридни закани.

26. Министерство за одбрана на Република Северна Македонија (2020) Стратегија за сајбер одбрана

27. РСЕ (2022) Естонија одбила масовен сајбер напад по отстранувањето на советски споменик
https://www.slobodnaevropa.mk/a/31994141.html

28. РСЕ (2022) Естонија отстранува советски споменици од Втората светска војна
https://www.slobodnaevropa.mk/a/31990820.html