НАУЧНИ ТРУДОВЕ НА УНСС (5) 2023, ИК – УНСС
ISSN (online): 2534-8957; ISSN (print): 0861-9344; http://unwe-research-papers.org/
DOI: https://doi.org/10.37075/RP.2023.5.03

ИЗГРАЖДАНЕ НА УСТОЙЧИВОСТ В ЕВРОПЕЙСКИЯ СЪЮЗ ВЪВ ВРЕМЕНА НА ПОЛИКРИЗИСНОСТ И ПРЕДИЗВИКАТЕЛСТВА В КОГНИТИВНАТА СФЕРА

Моника Панайотова[1]
e-mail: monika.panayotova@unwe.bg

Резюме

Целта на настоящата публикация е да насочи вниманието върху необходимостта от изграждане на устойчивост в обществата и държавите членки на Европейския съюз във времена на „поликризисност“ и предизвикателства в когнитивната сфера. След анализ на глобалните рискове и хибридните заплахи, както и на появата на изкуствения интелект в съвременната комуникационна и среда за сигурност, се правят определени препоръки и изводи, които да позволят на ЕС да използва потенциала си да бъде многоизмерна сила, преодоляваща некинетичните предизвикателства пред уязвимостите в демократичните общества, умовете и емоциите на гражданите. За целите на изследването са използвани различни методи на политологичен анализ, включително методът на „мисловните карти“, разработен от британския психолог Тони Бюзан, позволяващ синтез на идеи чрез изображения. В навечерието на Европейските избори през 2024 г., публикацията извежда ключови изводи за преодоляване на предизвикателствата, свързани с дезинформацията, управлението на възприятията и психологическата манипулация, водещи до подкопаване на доверието в демократичните институции и до възпрепятстване на вземащите решение да противодействат. Сред тях са: изграждане на устойчивост чрез образование, медийна грамотност, критично мислене, цифрови компетентности, ментална издръжливост; способност не само за бързо, но и бавно мислене; прилагането на експоненциален дизайн на стратегическо мислене; многостранен подход и тясно сътрудничество с НАТО.

Ключови думи: ЕС, поликризи, изкуствен интелект, европейски избори, когнитивна сфера, устойчивост, НАТО, сила

JEL: F50, F53, D81, Z18

Увод

Настоящата публикация има за цел да насочи вниманието върху необходимостта от изграждане на устойчивост в държавите членки, гражданите и лидерите на Европейския съюз (ЕС) във времена на „поликризисност“ и предизвикателства в когнитивната сфера.

[1] Асистент, доктор, катедра „Международни отношения“, факултет „Международна икономика и политика“, УНСС, ORCID: 0000-0003-3370-965X

Темата и анализът по нея са навременни в навечерието на 2024 г., очертаваща се като година на важен избор за нов състав на Европейския парламент и нов политически мандат на европейските институции, през който се очаква реформиране на ЕС и определяне на неговото по-нататъшно бъдеще. Специфичното на тези избори ще бъде, че ще се провеждат в момент на завръщане на войната в Европа, поради руската инвазия в Украйна от 24 февруари 2022 г., нестабилността в Близкия Изток, Южното и Източното съседство на Съюза, както и на активното навлизане на генеративния изкуствен интелект в обществото и икономиката, очертаващи когнитивната област като ново пространство на конкуренция за умовете и сърцата на гражданите.

В тази връзка настоящата студия застъпва тезата, че във времена на „поликризисност“ и хибридни заплахи, в частност предизвикателства в когнитивната сфера, Европейският съюз следва да изгражда устойчивост, бъдейки многоизмерна сила и прилагайки експоненциален дизайн на стратегическо мислене.

За целите на публикацията са прилагани методи на анализ и синтез на първични и вторични източници на информация, обобщение, дедукция и индукция и вторичен анализ на данни. В допълнение е използван методът на „мисловните карти“, разработен от британския психолог Тони Бюзан, позволяващ синтез на идеи чрез изображения, различни цветове, ключови думи и текстови абзаци (Buzan 2011). Методът е приложен с цел по-доброто онагледяване на съдържанието, както и представяне на разработените документи и предприети инициативи от ЕС в когнитивната област, разглеждана в по-широкия контекст на хибридните заплахи.

Разработката е предназначена за специалисти и студенти по европейските въпроси, политическите науки и международните отношения, за практици в публичната сфера и отговорни за политиките, изследователи в неправителствения сектор и академичните среди, както и за всички европейски граждани, които имат интерес по темата.

Хибридни заплахи, в частност предизвикателства в когнитивната сфера

В изкуството на войната, Сун Дзъ казва, че превъзходството не се състои в това да побеждаваш във всяка битка. Да покориш врага, без да воюваш – това е най-голямото превъзходство (Дзъ, 2005). Доброто стратегическо планиране, познаването на противника и неговите уязвимости, познаването на самия себе си и правилното калибриране на силата, позволяват постигане на превъзходство и победа без да бъде водена битка. В

съвременните условия на мащабна цифрова трансформация, на активното навлизане на изкуствения интелект (ИИ) и нови технологии в обществата и икономиките ни, един от най-древните военни трактати запазва своята актуалност, бъдейки прилаган в изцяло нова среда за сигурност.

Конвенционалната война, която мнозина считаха, че е невъзможно да се върне в Европа, заради руската агресия от 24 февруари 2022 г. вече 20 месеца е налице на територията на Украйна. Успоредно с нея, обаче се отваря още едно „бойно поле“ на Стария континент, в което обаче предприеманите действия се движат под военния радар, причинявайки големи поражения върху когнитивните процеси в гражданите и кохезията в европейските общества

Така наречената „когнитивна война“ обединява в едно употребата на кибер, информационни, психологически и способности за социален инженеринг. Тези дейности, провеждани в синхрон с други инструменти на силата, могат да повлияят на нагласите и поведението чрез въздействие, защита или нарушаване на индивидуални и групови когнитивни функции и процеси, за да се получи предимство пред противника (NATO, 2023a). Предназначени са да променят възприятията за реалността, да увеличават противниковите въздействия върху емоционалните и подсъзнателните области, да превръщат манипулацията на цялото общество в нова норма (NATO, 2023b). В тази връзка Организацията на Северноатлантическия договор (НАТО), концептуално очертава когнитивната сфера като шестата оперативна област, наравно със земя, въздух, море, кибер и космос. Европейският съюз на свой ред разглежда предизвикателствата, свързани с нея в по-широката рамка на хибридните заплахи, движещи се в „сивата зона“ между мира и войната.

Когнитивната война може да бъде разглеждана както като самостоятелно явление, така и като част от хибридната война, която е свързана със съчетаването на кинетични с некинетични инструменти и тактики. Кинетичните методи са свързани с употребата на различни видове оръжия и боеприпаси с физическо действие и водят респективно до нанасянето на физически и материални щети, докато некинетичните са често свързани с „нередовната война“ (irregular warfare) и макар да не водят до материални разрушения, често са с много по-трайни негативни последствия.

Некинетичните действия са логически, електромагнитни или поведенчески, като например атака на компютърна мрежа срещу врага или психологическа операция, насочена към него. Макар некинетичните действия да имат физически компонент, последиците, които налагат, са предимно непреки – функционални, системни, психологически или поведенчески (US Air Force, 2007).

Използването на комбинация от икономическа, кибернетична и компютърна война има за цел да насърчи психологическата подривна дейност и да увеличи несигурността или умората в целевата страна или регион (Nate, Ratiu, 2018).

Използвайки дедуктивния метод на разсъждение следва да се отбележи, че докато хибридната война представлява съвкупност от употребата на военни и невоенни средства, конвенционални и неконвенционални тактики, то когнитивната област, използваща изцяло некинетични инструменти, е специфична част от нея, като може да бъде както интегрална, така и самостоятелна. За разлика от хибридната, при която се използват кибератаки срещу критична инфраструктура, икономически санкции, дезинформация, пропаганда, традиционни военни операции, дипломация за постигането на определени стратегически цели, когнитивната сфера е специално насочена към оказване на влияние и манипулиране на психологическите аспекти, вярванията, убежденията и начина на вземането на решения от страна на противника.

Комплексната среда за сигурност, навлизането на изкуствения интелект и експоненциалното развитие на информационните технологии позволява все по-мащабно въздействие и по-висока ефективност на хибридните заплахи. Двете организации ЕС и НАТО в своите стратегически документи от 2022 г. „Стратегически компас“ и Нова стратегическа концепция на Алианса също идентифицират хибридните конфликти и кибератаките като предизвикателства пред своята сигурност.

Отчитайки, че хибридните заплахи са непосредствен риск за двете организации и техните държави, Съвместният изследователски център към Европейската комисия (JRC) и Европейският център за високи постижения в борбата с хибридните заплахи в Хелзинки разработват концептуален модел, който може да бъде адаптиран за нуждите на всяка от организациите и съставляващите ги държави, като идентифицират хибридните предизвикателства на фона на настоящата динамика на средата за сигурност, отчитайки техния еволюиращ и променящ се характер. Концепцията е базирана на следните **четири стълба**, включващи актьори и техните стратегически цели, области, инструменти и фази (Joint Research Centre, 2021).

- **Първи стълб: актьорите**, които са държавни и недържавни и имат за основна цел подкопаване способността за вземане на решения на ответната страна.
- **Втори стълб: областите**, които са: 1) инфраструктура; 2) кибер; 3) космос; 4) икономика; 5) военни/отбрана; 6) култура; 7) социална/обществена; 8) публична администрация; 9) правна; 10) разузнаване; 11) дипломация; 12) политическа; 13) информационна (медии).
- **Трети стълб: инструменти, без претенция за изчерпателност**, които са: 1) физически операции срещу критична инфраструктура (засягащи областите: инфраструктура; икономика; кибер, космос; военна/отбрана; информационна; социална/обществена; публична администрация); 2) създаване и използване на зависимост от определена инфраструкту-

ра, включително гражданско-военна зависимост (засягащи областите: инфраструктура; икономика; кибер; космос; военна/отбрана; публична администрация); 3) създаване или използване на икономически зависимости (засягащи областите: икономика; дипломация; политически; публична администрация); 4) преки чуждестранни инвестиции (засягащи областите: икономика; инфраструктура; кибер; космос; военни/отбрана; публична администрация; разузнаване; информационна; политическа; правна); 5) промишлен шпионаж (засягащи областите: икономика; инфраструктура; кибер; космос; разузнаване; информационна); 6) подкопаване на националната икономика на противника (засягащи областите: икономика; публична администрация; политическа; дипломация); 7) използване на икономически трудности (засягащи областите: икономика; публична администрация; политическа; дипломация); 8) кибер-шпионаж (засягащи областите: инфраструктура; космос; кибер; военна/отбрана; публична администрация); 9) кибер-операции (засягащи областите: инфраструктура; космос; кибер; социална/обществена; публична администрация; военна/отбрана); 10) нарушаване на въздушното пространство (засягащи областите: военна/отбрана; социална/обществена; политическа; дипломация); 11) нарушаване на преминаването в териториалните води (засягащи областите: военна/отбрана; социална/обществена; политическа; дипломация); 12) разпространение на оръжия (засягащи областите: военна/отбрана); 13) конвенционални/субконвенционални операции на въоръжените сили[2](засягащи областите: военна/отбрана); 14) опосредствания (прокси) войни[3], паравоенни организации, подставени лица (засягащи областите: военна/отбрана); 15) военни учения (засягащи областите: военна/отбрана; дипломация; политическа обществена); 16) ангажиране на определени диаспори за оказване на влияние (засягащи областите: политическа; дипломация; социална/обществена; култура; разузнаване; информационна); 17) финансиране на културни групи и мозъчни тръстове (засягащи областите: обществена; култура; политика; дипломация); 18) използване на социо-културни различия – етнически, религиозни и културни (засягащи областите: социална/обществена; култура); 19) насърчаване на социални размирици (засягащи областите: инфраструктура; социална/обществена; икономика; политическа); 20) манипулиране на дискуси-

[2] Субконвенционални е общ термин, обхващащ всички военни и паравоенни операции, които са над нивото на мирно съвместно съществуване между държавите и под прага на война, като тероризъм, въстания и др.

[3] Дефиницията, която речникът на Кеймбридж дава за „прокси“ война, е такава, която се води между групи или по-малки държави, всяка от които представлява интересите на други по-големи сили и може да получи помощ и подкрепа от тях.

ите за миграцията с цел поляризиране на обществата и подкопаване на либералните демокрации (засягащи областите: социална/обществена; култура; политическа; правна); 21) използване на уязвимите места в публичната администрация и обществената сфера, включително управление на кризи и извънредни ситуации (засягащи областите: публична администрация; политическа; социална/обществена); 22) насърчаване и използване на корупцията (засягащи областите: публична администрация; икономика; правна; социална/обществена); 23) използване на правни норми, процеси, институции, аргументи (засягащи областите: инфраструктура; кибер; космос; икономика; военни/отбрана; култура; социална/обществена; публична администрация; правна; разузнаване; дипломация; политическа; информационна (медии)); 24) използване на съществуващи пропуски и несигурност в законодателството (засягащи областите: инфраструктура; кибер; космос; икономика; военни/отбрана; култура; социална/обществена; публична администрация; правна; разузнаване; дипломация; политическа; информационна (медии)); 25) подготовка на разузнаването (засягащи областите: разузнаване; военни/отбрана); 26) провеждане на тайни операции (засягащи областите: разузнаване; военни/отбрана); 27) проникване/ инфилтриране (засягащи областите: разузнаване; военни/отбрана); 28) дипломатически санкции (засягащи областите: дипломация; политическа; икономика); 29) провеждане на бойкот (засягащи областите: дипломация; политическа; икономика); 30) използване на посолства (засягащи областите: дипломация; политическа; разузнаване; социална/обществена); 31) създаване на объркване или използване на противоречив наратив (засягащи областите: социална/обществена; информационна (медии); дипломация); 32) използване на миграцията като разменна монета в международните отношения (засягащи областите: социална/обществена; дипломация; политическа); 33) дискредитиране на лидери и/или кандидати (засягащи областите: политическа; публична администрация; социална/обществена); 34) оказване на подкрепа на политически актьори (засягащи областите: политическа; публична администрация; социална/обществена); 35) упражняване на принуда върху политици и/или правителство (засягащи областите: политическа; публична администрация; правна); 36) използване на имиграцията за оказване на политическо влияние (засягащи областите: политическа; социална/обществена); 37) упражняване на медиен контрол и вмешателство в работата на медиите (засягащи областите: информационна (медии); инфраструктура; социална/обществена; култура); 38) провеждане на кампании за дезинформация и пропаганда (засягащи областите: социална/обществена; информа-

ционна; политическа; кибер; култура; публична администрация); 39) оказване на влияние върху учебното съдържание и академичните среди (засягащи областите: социална/обществена; култура); 40) космически (електронни) операции, свързани със заглушаване и подправяне на Глобалната Навигационна Сателитна Система (засягащи областите: космос; кибер; инфраструктура; икономика; военни/отбрана).

- **Четвърти стълб: фазите, които са три**, свързани с инициране, дестабилизация и принуда. Всяка от тези фази има силен психологически компонент и дейностите, свързани с тях като намеса/вмешателство, влияние, операции/кампании, война – в някои случаи се припокриват в различните фази. Може да има или да няма ескалация. Може да има и де-ескалация, която да заблуди „ситуационната осведоменост", прикривайки истинските цели на действието. Това е характерно за пейзажа на хибридните заплахи. Ескалацията и де-ескалацията могат да бъдат хоризонтални и вертикални, което означава, че комбинацията от горепосочените инструменти и начина, по който те биват използвани, става според необходимостта и с цел адаптиране към дадена ситуация.

Предизвикателствата в когнитивната сфера, свързани с използването на некинетични средства като дезинформация, управление на възприятията и психологическа манипулация, водят до подкопаване на доверието в демократичните институции, засилване на поляризацията сред политическите субекти и до разделение в обществото както в национален, така и в международен план. В допълнение появата на все по-крайни по убеждения формации, оспорващи основните демократични ценности, използващи обществените уязвимости с цел ерозия на социалната кохезия и спомагащи за геополитическото позициониране на трети страни в държавите членки на ЕС, води до намаляване на способността на политическите лидери да вземат далновидни решения.

В допълнение в контекста на новите технологии, съвременният историк и философ Ювал Харари в своя статия дава нов ракурс в разделителната линия между автокрации и демокрации. Неговата концепция за „Датаизма" разглежда различните системи на управление като системи за обработка на данни. Разликата между тях се определя от начина, по който обработват данните, а не на база идеологически, етични или политически признаци (Харари, 2018).

Той подчертава, че в исторически план автокрациите са се сблъсквали с огромни затруднения по отношение на иновациите и икономическия растеж, тъй като в края на XX век отвореността и обмена на информация в и между демократичните режими позволява натрупване на повече данни и знание и респективно по-добра обработка на наличната информация. Демокрацията разпределя правомощията за обработка на информация и вземане на решения между много хора и институции, докато диктатурата концентрира информа-

цията и властта на едно място. Докато в края на миналия век демокрациите имат предимство, то появата на изкуствения интелект е силно възможно да промени ситуацията в полза на автокрациите, тъй като ИИ позволява извличане на информация и знание от огромни масиви от данни. Предвид, че машинното обучение функционира по-добре с концентриране на информацията за анализ на едно място, това би дало предимство на по-централизираните системи за обработка на данни спрямо дифузните такива (Harari, 2018).

За разлика от НАТО, която поради експоненциалното развитие на технологиите, осезаемият напредък в науката и знанието за възможностите за въздействие върху човешкия мозък и по-конкретно в неврологията, биохимията, психологията, концептуално очертава когнитивната сфера като самостоятелна, то Европейският съюз все още не я извежда експлицитно и я разглежда в по-широкия контекст на хибридните заплахи. Въпреки това, обаче предвид, че 21 от 31 държави членки на Алианса са членки на ЕС, следва да се вземе под внимание какво влиза в „зрителното поле“ на анализ на Организацията на Северноатлантическия договор. В когнитивната сфера НАТО се стреми към образование, сътрудничество, защита и формиране на определен начин на мислене, умения, способности сред съставляващите я нации, за да могат да защитят основните си демократични ценности. Предоставянето на насоки относно необходимостта от осъзнаване на проблема, от гражданско-военно сътрудничество, от изграждане на обществена устойчивост и от обмен на данни за настоящите и бъдещите рискове, позволява по-доброто вземане на политически решения, развитие на военните способности и укрепване на цялостната сигурност на Алианса (NATO, 2023b).

Поликризисност

Световният икономически форум идентифицира редица рискове и заплахи за сигурността, пред които е изправен светът днес, които са както нови, така и такива, напомнящи за минали предизвикателства. Тези рискове са с многоизмерен характер, обхващат икономически, екологични, геополитически, обществени и технологични аспекти и могат да доведат до катастрофални последици, като например въоръжени конфликти. В Доклада си за глобалните рискове за 2023 г. се използва терминът „поликризисност“, за да се обясни как настоящите и бъдещите рискове могат да си взаимодействат помежду си, за да образуват „поликриза“, представляваща съвкупност от свързани глобални рискове, чието общо въздействие е по-голямо от сумата на съставните му части. В него се призовава за спешни действия и проактивна подготовка на държавите за бъдещи сътресения и конфликти, като се подчертава значението от смекчаването на краткосрочните и дългосрочните рискове, представляващи заплаха от „поликриза“. Кризата, свързана с разходите за живот е определена като най-неотлож-

ния глобален проблем, който води до социални вълнения, докато най-голямата дългосрочна заплаха, която се очертава с времеви хоризонт от десет години се отнася до несправянето с рисковете, свързани с климата.

След две години светът може да бъде изправен пред кризи, свързани освен с разходите за живот, с природни бедствия и екстремни метеорологични явления, с геоикономическа конфронтация, с неуспех в смекчаването на негативните последствия от изменението на климата, ерозия на социалното сближаване и поляризация на обществото, както и с мащабни екологични щети. След десет години, рисковете, свързани с климата и околната среда, включително значителната принудителна миграция, се очаква да са доминиращи в шест от десетте най-големи заплахи в глобален план (Torkington, 2023).

	В доклада се подчертава продължаващото въздействие на настоящите кризи и най-сериозните глобални рискове, които се очаква да се проявят през следващите две години. Те включват:	В дългосрочен план в доклада се набляга на няколко риска, които могат да се превърнат в бъдещи кризи, чийто пик се очаква да бъде през следващите десет години. Те включват:
1.	Криза на жизнения стандарт	Неуспех в смекчаването на негативните последствия о т изменението на климата
2.	Природни бедствия и екстремни метеорологични явления	Неуспешна адаптация към изменението на климата
3.	Геоикономическа конфронтация	Природни бедствия и екстремни метеорологични явления
4.	Неуспех в смекчаването на негативните последствия от изменението на климата	Загуба на биоразнообразие и разрушаване на екосистемите
5.	Ерозия на социалното сближаване и поляризация в обществото	Широкомащабна принудителна миграция
6.	Широкообхватни инциденти, свързани с разрушаване на околната среда	Кризи с недостиг на природни ресурси
7.	Неуспешна адаптация към изменението на климата	Ерозия на социалното сближаване и поляризация на обществото
8.	Мащабни киберпрестъпления и високи нива на кибер-несигурност	Мащабни киберпрестъпления високи нива на кибер-несигурност
9.	Кризи, свързани с природните ресурси	Геоикономическа конфронтация
10.	Широкомащабна принудителна миграция	Широкомащабни инциденти с екологични щети

Източник: Доклад на Световния икономически форум за глобалните рискове за 2023 г.

Фигура 1: „Глобални рискове в двугодишна и десетгодишна перспектива“

Идентифицираните рискове и заплахи както в краткосрочен, така и в дългосрочен план показва необходимостта от изграждане на устойчивост на хибридни заплахи. Всяко от предизвикателствата показва, че няма класически военен характер, както и че респективно не може да бъде преодоляно с използване изцяло на военни средства. Всяка една криза, независимо от източника си на възникване – действия на държавни, недържавни актьори, глобално затопляне, цифрова трансформация, ще бъде умело използвана в полето на когнитивната сфера, създавайки предпоставки за дестабилизация, страх и нестабилност. Ерозията на социалното сближаване и поляризацията в обществото ще бъдат много по-лесно постигани при липсата на целенасочена политика за изграждане на устойчивост както в самите държави, така и в самите граждани. Затова е важно прилагането на по-холистичен подход, който да включва в себе си не само работа с така наречените силови ведомства в държавите членки като министерство на отбраната, министерство на вътрешните работи, но и институциите, отговарящи за образованието, културата, вероизповеданията, които в най-висока степен се занимават с формирането на ума и душата на гражданите през различните поколения.

Учебното съдържание, учебните програми, методите на преподаване, уменията, които се развиват в гражданите и в частност в младите хора, са от ключово значение за изграждането на устойчивост, чрез развитието на критично и експоненциално мислене, медийна грамотност, себеопознаване и ментална издръжливост.

Изграждане на устойчивост

Развитие на критично мислене, медийна грамотност, цифрови умения

Изграждането на устойчивост сред обществото, в отговор на предизвикателствата в когнитивната сфера, е свързано с образованието, културата, развитието на цифрови компетентности, умения за критично мислене и медийна грамотност.

В тази връзка в изпълнение на насоките на Европейската комисия съгласно член 33а, параграф 3 от Директивата за аудио-визуалните медийни услуги за обхвата на докладите на държавите членки относно мерките за насърчаване и развитие на умения за медийна грамотност, е подчертано решаващото значение на медийната грамотност и необходимостта от нейното укрепване, също признати в Плана за действие за европейската демокрация и в Плана за действие за медийния и аудио-визуалния сектор. Тя е ценен инструмент за борба с разпространението на дезинформация, тъй като дава

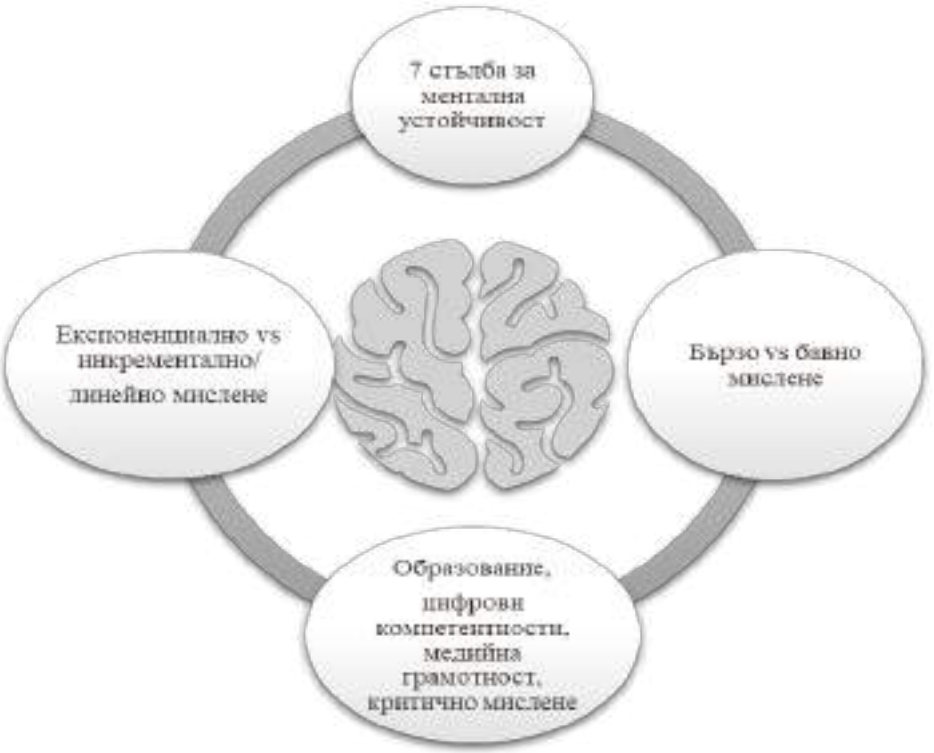
възможност на потребителите да оценяват критично източника на информация и по този начин да откриват невярно или подвеждащо съдържание, както е посочено в Насоките на Комисията за укрепване на Кодекса за поведение във връзка с дезинформацията. В допълнение следва медийната грамотност да не се ограничава до изучаване на инструменти и технологии, а да има за цел хората да придобият уменията за критично мислене, необходими, за да се направи преценка, да се анализират сложни ситуации и да се разпознава разликата между мнение и факт (Европейска комисия, 2023а).

Това показва ключовата роля на образованието за изграждане на грамотност в цифровата ера, умения и компетентности, необходими за дигиталния преход и за развитието на устойчивост в една сложна комуникационна среда, характеризираща се с наличие на изкуствен интелект, възход на нововъзникващи технологии като интернет на нещата, високи нива на дезинформация и фалшиви новини в социалните медии и новинарските сайтове, използване на лични данни от доставчиците на интернет услуги и приложенията.

В тази връзка в наложилата се през годините като общоевропейска – Рамка за цифрова компетентност на гражданите (DigComp), сигурността и безопасността, както и грамотността за работа с данни и информация са идентифицирани като две от петте ключови сфери (Vuorikari, Kluzer, 2022). Чрез тази рамка се развиват и измерват цифровите компететности в сферата на образованието и на пазара на труда, като извън вече посочените две области, останалите три са: ефективни комуникация и сътрудничество чрез цифрови технологии, създаване на цифрово съдържание, разрешаване на проблеми в дигитална среда.

Съгласно Препоръката на Съвета относно ключовите компетентности за учене през целия живот, 2018 г., цифровата компетентност включва „уверено, критично и отговорно използване и ангажиране с цифровите технологии с цел учене, работа и участие в обществото. Тя се определя като комбинация от знания, умения и нагласи“ (Council of the European Union, 2018).

Грамотността за работа с информация и данни дава възможност за изразяване на информационни нужди, намиране и достъп до цифрови данни и информация, оценяване на релевантността на съдържанието и истинността на източниците, ефективно организиране и управление на цифрови данни, информация и съдържание. Сигурността и безопасността от своя страна са свързани със защита на устройствата, личните данни, неприкосновеността на личния живот и цифровото съдържание, осигуряване на физическо и психологическо здраве, насърчаване на социалното благополучие и приобщаване чрез цифровите технологии и отчитане на тяхното въздействието върху околната среда.



Източник: Разработено от автора за целите на студията

Фигура 2: Изграждане на устойчивост

Развитие на психическа издръжливост

Освен развитието на цифрови умения, критично мислене и медийна грамотност, развитието на психическа издръжливост е важен компонент в уравнението за устойчивост на гражданите, лидерите и обществата ни в условията на поликризисност.

Ценни насоки в тази посока могат да бъдат открити в книгата на Лорънс Коулбрук „Психическа издръжливост при специални операции“, в която той изследва непобедимия начин на мислене на „Делта Форс“, военноморските тюлени, армейските рейнджъри и други елитни воини в американската армия, подчертавайки, че основната причина за техния успех са психическата им издръжливост, решителност, устойчивост и способност да контролират естествените си физически и психологически реакции на страх и стрес по време на някои от най-опасните операции. Седемте стълба на менталната издръжливост са своеобразен наръчник за всеки гражданин или лидер, кой-

то би искал да изгради и укрепи своята устойчивост и те съдържат следните основни насоки (Lawrence, 2015).

Първият стълб се отнася до: целеполагане и сегментиране, посредством използване на техниката на разделяне на по-големите цели на по-малки и по-лесно управляеми части или отделни фази. Военноморските тюлени, които успяват да завършат нелекия си продължителен курс на обучение са тези, които разделят голямата цел в краткосрочна, средносрочна и дългосрочна рамка и които фокусират енергията и вниманието си върху конкретен тренировъчен ден, върху последователното, а не едновременно изпълнение на задачите. Това ги предпазва от риска да се откажат, бъдейки обзети от нервност и тревожност за непостижимост на голямата цел.

Вторият стълб се отнася до: контрол на емоциите, посредством дихателната техника 4х4 за премахване на негативните емоции като гняв, страх и тревожност развивайки контрол, което има положително въздействие върху критичното мислене, вземането на решения и фината моторика.

Третият стълб се отнася до: визуализирането на потенциален сценарий на предстоящото, посредством техниката на визуализация, позволяваща ефективното оценяване на високорискови и стресови ситуации, които могат да възникнат по време на бойна операция, водеща до изостряне на вниманието, избягване на разсейващи фактори и постигане на конкретните цели.

Четвъртият стълб се отнася до: позитивното говорене на себе си, тъй като посредством тази техника се изграждат и развиват самоувереност, устойчивост и сила, необходими за постигане на желаните цели или преодоляване на съществуващи препятствия.

Петият стълб се отнася до: дистанциране от емоциите, посредством техниката на разделяне на дадена ситуация, проблем на части или категории без да се допуска тяхното смесване. По време на бойна операция се налага потискане на естествените човешки реакции на страх, смърт, разрушение, случващи се наоколо, тъй като това би възпрепятствало запазването на концентрацията върху постигане на конкретната цел.

Тази техника се използва и при наличие на риск от когнитивен дисонанс между чувства или мисли, които си противоречат.

Шестият стълб се отнася до: планиране на неочаквани, извънредни ситуации, посредством техниката за разглеждане на цялата предстояща операция от началото до края и обсъждане на всички възможни алтернативни действия, които биха били предприети. Това позволява на отделните лица и екипи да се подготвят за това, което може да се случи на различни етапи от операцията, и да разработят жизнеспособен план за действие. Тази техника е свързана също с визуализирането, като тя е средство за изграж-

дане на увереност и способност за бърза реакция при препятствие или неуспех.

Седмият стълб се отнася до: фокус и концентрация, тъй като посредством тази техника се развива умението за концентриране и повишено внимание във високорискови и високостресови ситуации

В случаите на така наречената „мъгла на войната“, това са непредвидени обстоятелства и хаос, които могат да настъпят при бойните действия и независимо колко добър да е бил първоначалният план за действие, да доведат до неговото отклонение или провал. В такива ситуации се прилага модифицирана версия на седемте стълба техника за бърз отговор, която включва: контрол на емоциите; говорене на себе си; оценка на ситуацията и на всяка заплаха за изпълнение на мисията, за собствената сигурност и оцеляване, както и за тази на екипа; определяне на подходящ курс на действие и отговор на възникналата ситуация; предприемане на действия и повтаряне на този цикъл от техники, докато целта не бъде постигната или ситуацията не се възстанови.

Развитие на способност не само за бързо, но и бавно мислене

За да се изградят устойчиви общества, способни да устоят на различни видове кризи, от съществено значение е да се развива както психическа издръжливост на индивидуално, професионално и лидерско ниво, така и способност да мислят не само бързо, но и бавно.

Спечелилият нобелова награда бихейвиорист Даниел Канеман очертава начина, по който хората вземат решения, уязвимостите свързани с това, и двете системи на мислене, с които разполага човек, а именно да мисли бързо и бавно (Kahneman, 2011). Той счита, че когнитивните способности могат да бъдат отслабени от социалните медии и различните „смарт“ устройства, тъй като бързината, с която се разпространява информацията чрез съобщения или новинарския поток налага да „мислим бързо“, което е свързано повече с импулсивност и емоционалност, отколкото с рационалност и разум, характерни за „мисленето бавно“.

Новинарските емисии и търсачките, които предлагат резултати, съответстващи на предпочитанията на хората, увеличават предубеждението за потвърждаване, при което те интерпретират новата информация така, че да потвърди техните предварителни убеждения. Приложенията за социални съобщения бързо обновяват потребителите с нова информация и изместват възприятието за важност основно към скорошните събития спрямо тези от миналото. Сайтовете за социални контакти предизвикват социално доказване, при което хората като потребители на съдържание имитират и утвърждават действията и убежденията на другите, за да се впишат в определени

социални групи, които от своя страна се превръщат в „ехо-пространства“ на конформизма и груповото мислене. Дори утвърдени и авторитетни новинарски агенции вече публикуват емоционални заглавия, за да насърчат „вирусното“ разпространение на своите новинарски статии (NATO, 2023c).

Битката между бързо и емоционално докосващо съдържание и достоверно и стигащо до разума такова, не е никак лека за традиционните обществени медии. За да продължат да следват високи стандарти за достоверност на информацията и плурализъм на мненията, устоявайки на конкуренцията на така наречените „нови дилъри на информация“, разполагащи с бързина, сензационност и сила за емоционално манипулиране, е важно да продължат да бъдат подкрепяни от институциите, отговорните за политиките и гражданите.

Фейсбук и други социални мрежи правят целенасочено проучване на понятието „емоционално заразяване“ за повече от 689 000 потребители, показващо, че ако на един член на социална мрежа се предоставят повече отрицателни новини, публикациите му в мрежата са значително по-негативни. Обратното е валидно и за положителните новини. Този широкомащабен експеримент за емоционално манипулиране кара медийните потребители да осъзнаят колко са уязвими спрямо своите „дилъри на информация“ и как свободният избор липсва, тъй като избираме нещо, което сме обусловени да изберем и мислим, това за което ни е повлияно да мислим (Аберкан, 2020).

В допълнение следва да се отбележи, че за да повлияят медиите на един международен конфликт, следните фактори са от голямо значение: 1) липсата на консенсус сред политическия елит по стратегически въпроси и политики; 2) непоследователна и колебаеща се политика на правителството или на международна организация; 3) слаб политически контрол върху ситуацията; 4) ситуация, при която резултатите от външната политика са видими и те са негативни; 5) лоша комуникация към публиката; 6) високо ниво на свободен достъп до информация (Цеков, 2017). Затова стратегическата комуникация, използвана от институциите, политиците и евроатлантическите организации, играе важна роля в предотвратяването на тези фактори. Тя може да помогне за подобряване на информационната среда, за укрепване на доверието на гражданите, като създава по-добро разбиране на фактите и ситуацията, и демонстрира съгласуваност между институциите по стратегически важните въпроси.

Освен стратегическата комуникация следва и гражданите като ползватели на информация да работят за собствената способност на ума им да преодоляват четирите потенциални когнитивни изкривявания на информация, идентифицирани от Идрис Аберкан, изследващ пътя към „невромъдростта“.

Когнитивно изкривяване 1, което се получава поради придаване на по-голямо значение на това, което потвърждава вярванията на човек, отколкото

онова, което ги накърнява. Нарича се „изкривяване на потвърждението“ и се дължи на допускането, че на мозъка му харесва, когато убежденията му се потвърждават.

Когнитивно изкривяване 2, което се получава поради „изкривяване на запомненото“. Спомените се оказват пристрастни и ненадеждни, поради склонността на мозъка да запомня всичко, което го успокоява и да забравя или отхвърля онова, което нарушава вътрешното равновесие на човек.

Когнитивно изкривяване 3, което е свързано с „изкривяване на непредставителността“ и се дължи на допускането, че всичко, с което човек храни своя ментален живот вече е било подбрано пристрастно и частично от медиите, които говорят повече за лошото, отколкото за доброто, защото злото омагьосва и впечатлява.

Когнитивно изкривяване 4, което е свързано с „изкривяване на шоковия ефект“ поради допускането, че лошата новина впечатлява повече мозъка на човек от добрата и лошите новини се запомнят повече от добрите (Аберкан, 2020).

Очертаването на когнитивната област като бойно поле е възможно както поради развитието на технологиите, наличието на невралгии в държавите и организациите, външната намеса и хибридните заплахи, поради вече представените уязвимости в самите хора, съставляващи обществото, така и поради липсата на експоненциално мислене в отговорните за политиките.

Развитие на експоненциален дизайн на мислене

Изключителната комплексност на заплахите, които се случват паралелно в „офлайн“ и „онлайн“ среда, бъдейки с различен профил „кинетичен“ или „некинетичен“, налага промяна не само в процеса, но и в подхода на вземане на решение.

Динамиката на поява на предизвикателствата в средата за сигурност предполага не само реципрочна скорост на отговор, но и така наречения „експоненциален“ дизайн на мислене.

Предприемачът Марк Бончек пръв развива идеята за експоненциален начин на мислене, свързвайки го с експоненциалния растеж на технологиите и експоненциално развиващия се свят. Той отбелязва, че инкрементalният начин на мислене води до стремеж към правене на нещата по по-добър начин и задоволяване с 10% подобрение на резултата, докато експоненциалният се стреми към правене на нещата по различен, иновативен начин и постигане на в 10 пъти по-добър резултат (Bonchek, 2016).

Линейното мислене допуска, че промените или прогресът че случват в постоянен ритъм. Инкременталното мислене, което е специфична форма на линейното се фокусира върху поетапното, на малки крачки подобрение.

Експоненциалното мислене от своя страна предполага, че промените или напредъкът могат да настъпят с ускорена или умножена скорост. Такъв дизайн на мислене насърчава към иновативност и креативност и позволява както по-доброто разбиране на ситуации с нелинеен растеж, например като навлизането на изкуствения интелект в обществото и икономиката ни и появата на некинетични заплахи, така и подпомага процеса на предвиждане на бързи промени и тенденции. Този начин на мислене позволява промяна на перспективата и поглед върху първопричините за даден проблем или група проблеми, а не върху непосредственото му/им разрешаване. Изкореняването на първопричините би имало много по-голямо въздействие, отколкото отстраняването на текущия проблем или група от проблеми.

Към настоящия момент вземащите решение и евро-атлантическите институции прилагат линеен и постепенен начин на мислене, свързан със стремеж към подобряване на съществуващото, към решаване на проблемите. През годините това се е утвърдил като логичен подход, носещ своята добавена стойност. Съвременните тенденции в средата за сигурност, обаче, ни показват, че в бъдеще този начин на мислене и действие ще бъде във все по-ниска степен ефективен. Докато стратегиите продължават да бъдат огледало на настояща действителност, а не да чертаят бъдещето, те все по-бързо ще остаряват преждевременно, бъдейки неспособни да поддържат и изграждат основан на реда, а не на силата ред в международните отношения.

Както се твърди в една известна мисъл, приписвана на водещия мислител в мениджмънта, предприемачеството и иновациите – Питър Дракър – „най-добрият начин да предвидиш бъдещето е като го създадеш“ (Дракър, 2013). Във времена на поликризисност, стратегиите и плановете в областта на хибридните заплахи, в частност в когнитивната сфера следва едновременно да управляват настоящето, но и да създават бъдеще, да формират нова реалност. Те следва да поддържат динамично равновесие между приемственост и промяна, но за целта следва да се изготвят и прилагат от хора, притежаващи не само инкрементално, но и експоненциално мислене.

Това, което се наблюдава към момента като дебат в европейските институции е основно свързано с реформа на начина на вземане на решения в ЕС чрез преминаване в максимална степен към прилагане на квалифицирано мнозинство, включително и за решения в областта на общата външна политика и политика за сигурност, вместо единодушие. Привържениците на тази реформа считат, че квалифицираното мнозинство ускорява динамиката, стимулирайки страните да формират коалиции на сходно мислещите и да постигат по-бързо консенсус. Следва да се отбележи, че бързото формиране на решение не означава устойчиво и трайно във времето съгласие по даден проблем.

Скоростта и далновидността следва да се постигат не с елиминиране на самостоятелната тежест на отделните държави, а с иновативен подход към новата среда за сигурност. Така както все повече прогресивно мислещи бизнес лидери осъзнават, че да конструират бизнес стратегиите и плановете си в един високо технологичен и експоненциално развиващ се климат по утвърдения линеен начин вече не е работещо, така и политическите лидери и военни стратези следва да отчитат новите реалности, пред които е изправен светът.

Подходът на ЕС и превръщането му в многоизмерна сила

Живеейки във времена на „поликризисност“, в които настоящите и нововъзникващите глобални рискове се комбинират, от съществено значение е Европейският съюз да се развива и да бъде възприеман като „многоизмерна сила“, която използва своите инструменти на мека, икономическа, нормативна, военна, спокойна, интелигентна и трансформираща сила по балансиран и ефективен начин (Panayotova, 2023).

Съюзът е нормативна сила, тъй като има правомощията да приема правно обвързващи решения, които могат да окажат значително въздействие върху държавите членки и тяхната способност да се справят с „поликризисността“. Той също така може да е и „спокойна сила“ по думите на българо-френския философ Цветан Тодоров, което се изразява в способността на ЕС да се противопоставя на агресията, като същевременно провежда политика на сигурност, основана на мира. Интелигентната сила, формулирана от Дж. Най е свързана със способността да се съчетават ресурсите на твърдата и меката сила в ефективни стратегии (Най, 2013), и тя също е от решаващо значение за справянето с многоизмерните глобални рискове. Трансформативната сила, според Марк Ленард, се отнася до широкото и дълбоко влияние на ЕС, което може да доведе до постоянна промяна, след като държавите станат част от неговата сфера на влияние (Ленард, 2005).

За да може да се справи с „поликризисността“ ЕС следва да бъде „многоизмерна сила“, което означава да съумява според комплексните предизвикателства да определя и използва различните инструменти в ефективни комбинации от видове сила. Това ще даде на Съюза конкурентно предимство и ще помогне на държавите членки и техните граждани да бъдат устойчиви на постоянните промени и поликризи, пред които са изправени.

Източник: Разработена от автора

Фигура 3: ЕС като многоизмерна сила

Макар да има видимо осъзнаване от страна на ЕС за необходимостта от изграждане на устойчивост срещу хибридните заплахи и предизвикателства пред европейската демокрация, прекалената активност на отделните европейски институции, свързана със създаване на редица самостоятелни анализи, концепции, решения, комуникации, комисии, води до появата на „лабиринт от прекомерна информация“, създаващ усещането за липсата на единен и холистичен подход.

Въпреки това обаче, включително и с помощта на метода на мисловните карти ще бъде направен опит за структуриране на съществуващата информация с цел онагледяване на европейския подход и инструменти в хибридната, и в частност когнитивната област.

За целта ще бъдат очертани две направления на действие. От една страна – стратегическата рамка за борба с хибридните заплахи. От друга страна – наборът от документи, инициативи, законодателство, свързани със запазване на информационната и медийната среда в ЕС чрез предпазването ѝ от външната намеса, манипулирането на информация, дезинформация, пропаганда и други заплахи, които биха могли да подкопаят демократичните процеси и свободния обмен на информация.

По отношение на първото направление, без претенция за изчерпателност ще бъдат представени: Съвместната рамка за борба с хибридните заплахи от 2016 г.; Съвместното съобщение от 2018 г. относно повишаването на устойчивостта и укрепването на способностите за справяне с хибридните заплахи; Стратегически компас от 2022 г., надграждащ Глобална стратегия на ЕС в областта на външната политика и политика на сигурност; Сътрудничество ЕС-НАТО и мултилатералния подход.

Отчитайки значителните промени в средата за сигурност, особено идващи от източното и южното съседство на Съюза, в **Съвместната рамка за борба с хибридните заплахи от 2016 г**., ЕС насочва вниманието върху необходимостта от адаптиране и укрепване на своите способности за сигурност, от взаимодействие с НАТО по темата и от предприемането на ответни действия, свързани с подобряването на осведомеността, изграждането на устойчивост, предотвратяването, реакцията при кризи и възстановяването. Документът отбелязва тясната връзка между външната и вътрешната сигурност и макар че основната отговорност за противодействие на хибридните заплахи е на държавите членки, много от заплахите са общи и имат трансграничен характер, което предполага постигане на задоволително ниво на ситуационна осведоменост, по-тясно взаимодействие между страните, обмен на разузнавателна информация и данни между отделните сектори, ЕС, неговите държави членки и партньори. Очертани са действия за изграждането на устойчивост в области като киберсигурността, критичната инфраструктура, защитата на финансовата система от незаконна употреба и противодействието на насилническия екстремизъм и радикализацията.

В контекста на темата на настоящата разработка, документът също дава две важни определения – за хибридни заплахи и за устойчивост. Признавайки липсата на единна дефиниция за хибридните заплахи и отбелязвайки, че определенията трябва да се запазят гъвкави, за да отразяват тяхното развитие, документът обобщава, че понятието обхваща комбинацията от насилнически и подривни дейности, конвенционални и неконвенционални методи (т.е. дипломатически, военни, икономически, технологични), които се използват по координиран начин от държавни или недържавни субекти с цел постигане на конкретни цели, в отсъствието на официално обявена война. Обикновено акцентът е върху използването на слабите места на набелязаната цел и създаването на неяснота, с което да се възпрепятстват процесите на вземане на решения. Масовите дезинформационни кампании, използването на социалните медии за контрол на политическия наратив или за радикализиране, набиране и командване на подставени лица могат да бъдат средства за хибридни заплахи. Устойчивостта се отбелязва, че е способността за издържане на стрес и възстановяване, която се увеличава постепенно вследствие на придобития от предизвикателствата опит. За да се противодейства ефективно на хибридните заплахи, се отбелязва в документа, че трябва да се обърне внимание на потенциалните уязвими места на ключовите инфраструктури, веригите за доставки и обществото (Европейска комисия, 2016).

Съвместното съобщение от 2018 г. относно повишаването на устойчивостта и укрепването на способностите за справяне с хибридните за-

плахи е в отговор на наблюдаваните тенденции в опит за дестабилизиране на държавите членки чрез подкопаване на общественото доверие в правителствените институции, ЕС и разклащане на основните ценности на обществата чрез кибератаки, смущаващи икономиката и обществените услуги, целенасочени кампании за дезинформация, враждебни военни действия. В тази връзка и в унисон с усилията на Съвета се подчертава необходимостта от укрепване на капацитета на ЕС и неговите държави членки за откриване, предотвратяване и реагиране на хибридни заплахи в области като киберсигурността, стратегическата комуникация и контраразузнаването. Освен това се обръща специално внимание на необходимостта от подобряване на устойчивостта по отношение на химичните, биологичните, радиологичните и ядрените заплахи (Европейска комисия, 2018).

Прави се заявка за работа в пет основни направления, с които да бъдат ангажирани Звеното за синтез на информацията за хибридните заплахи в рамките на Центъра на ЕС за анализ на информация (класифицирана и общодостъпна) към Европейската служба за външна дейност, създадено през 2016 г., ЕК и Европейският център за високи постижения в борбата с хибридните заплахи в Хелзинки, създаден през април 2017 г. В отговор на променящите се заплахи се предприемат действия за: 1) ситуационна осведоменост – чрез подобряване на способността за откриване на хибридни заплахи и повишаване на експертизата в Звеното, за да бъде обхванат пълният спектър от хибридни заплахи; 2) засилени действия срещу химични, биологични, радиологични и ядрени заплахи; 3) стратегическа комуникация, чрез повишаване на осведомеността, образоване на широката общественост, за да различава информацията от дезинформацията и съгласувано разпространение на информация между съществуващите структури; 4) изграждане на устойчивост и възпиращ ефект в сектора на киберсигурността чрез „инструментариум за кибердипломация“, осъзната необходимост от съвместна сигурна комуникационна мрежа между европейските институции и от ситуационна осведоменост за по-ефективна координация на техническо, оперативно и стратегическо/политическо равнище, укрепване на способностите за кибернетична отбрана, образование и обучение; 5) изграждане на устойчивост срещу вражеска разузнавателна дейност чрез засилено и ефективно сътрудничество между държавите членки, в съответствие с приложимите европейски и национални норми, както и чрез увеличаване на способностите на институциите на ЕС.

Документът подчертава, че изборните периоди са особено уязвими за кибератаки и онлайн манипулации. Тези атаки включват нападения срещу изборната инфраструктура, дезинформационни кампании и кибератаки от трети държави с цел нарушаване на демократични избори. Отделено е внимание

и на Работната група East StratCom на ЕС, създадена след март 2015 г., води усилията за борба с дезинформацията от чуждестранни източници. Нейните анализи повишават осведомеността относно руската дезинформация.

В контекста на процеса на стратегическо преосмисляне на средата за сигурност, който кулминира през 2022 г. с появата на **Стратегическия компас**, следва да се отбележи, че в анализа на рисковете и заплахите, ЕС идентифицира хибридните конфликти и кибератаки, отбелязвайки, че Съюзът е изправен пред предизвикателства от страна на държавни и недържавни участници, които използват хибридни стратегии, кибератаки, кампании за дезинформация и намеса в политическите процеси и изборите. В допълнение отбелязва значението на нововъзникващи и разрушителни технологии като изкуствения интелект, които конкурентите използват, за да придобият стратегически предимства, като изострят съществуващите заплахи и въвеждат нови предизвикателства (Council of the European Union, 2022).

Политиката на ЕС за противодействие на хибридните заплахи се основава на четири основни стълба: 1) ситуационна осведоменост, която предоставя на държавите членки информирани за предизвикателствата и насърчава обща стратегическа култура; 2) устойчивост, която обхваща капацитета на ЕС да предотвратява, да се противопоставя и възстановява от многостранни хибридни атаки, като същевременно оказва подкрепа на съседните региони да изграждат устойчивост, вкл. чрез използването на мисии на ОПСО (общата политика за сигурност и отбрана на ЕС); 3) възможности за отговор, от дипломация, през ОПСО и механизми за управление на кризи до екипи за бързо реагиране и ограничителни мерки; и 4) сътрудничество, отразяващо ангажимента за съвместни усилия с международни партньори, организации и гражданското общество, с акцент върху укрепването на устойчивостта в обществата както в рамките на Съюза, така и в границите в близост до него и отвъд (EEAS, 2022).

Документът очертава цялостна стратегия за повишаване на устойчивостта срещу хибридни заплахи, кибератаки, външна намеса и манипулиране на информацията. В него се подчертава необходимостта от координиране на инструментите на ЕС в така наречен „хибриден инструментариум“, включващ превантивни и ответни мерки, изграждане на обществена и икономическа устойчивост и провеждане на кибердипломация.

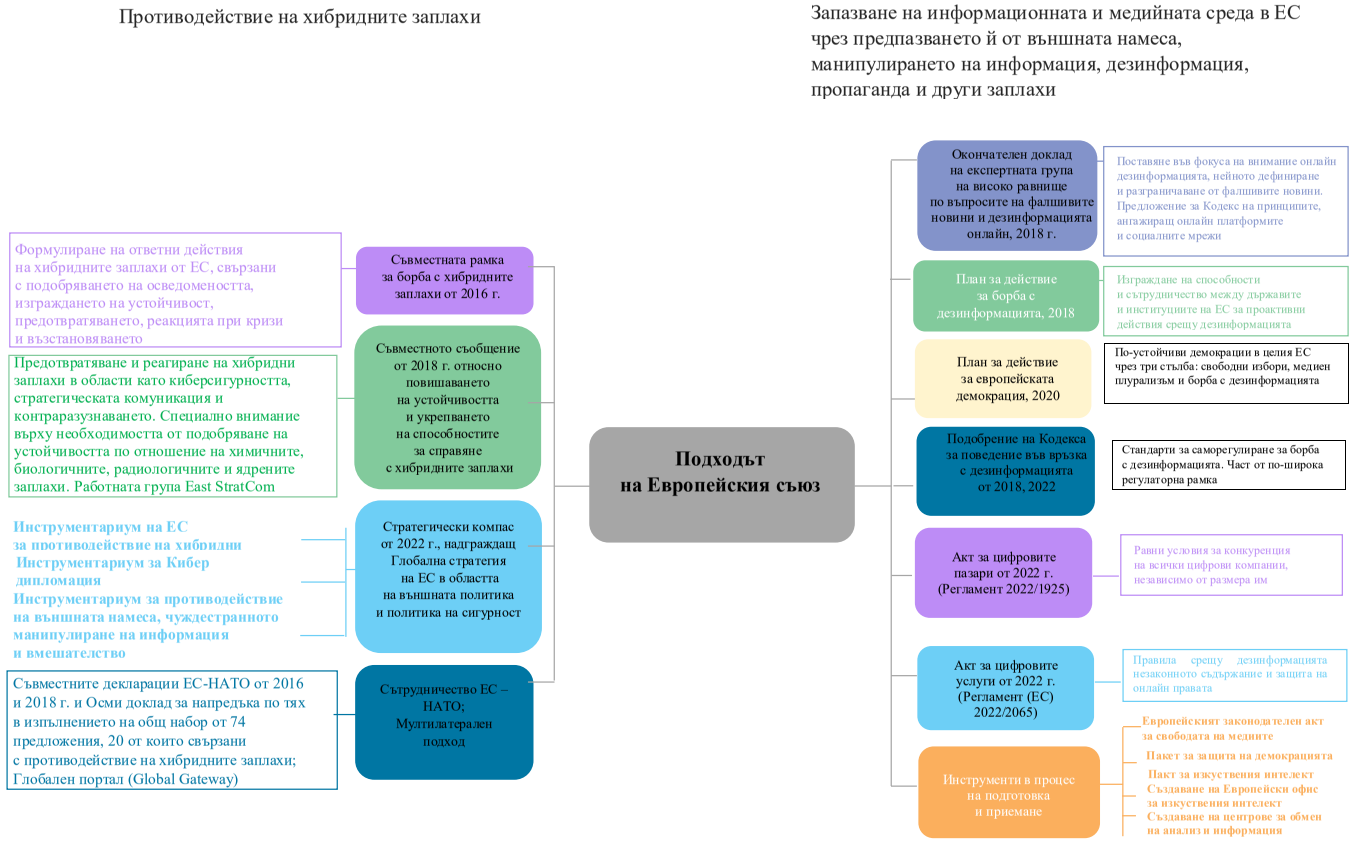
Трите акцента в документа са върху създаването на инструментариум на ЕС за противодействие на хибридни заплахи, инструментариум за кибердипломация и инструментариум за противодействие на външната намеса и манипулирането на информация. В стратегията се подчертава също така значението на обществената устойчивост, надеждния достъп до информация и сътрудничеството с международни партньори и организации като

НАТО, Г-7, гражданското общество и ООН за справяне с тези многоаспектни предизвикателства.

Съгласно съвместните декларации между ЕС и НАТО от 2016 и 2018 г. и Осмия доклад за напредъка по тях се наблюдава изпълнението на общ набор от 74 предложения, 20 от които са свързани с противодействие на хибридните заплахи. В третата съвместна декларация от януари 2023 г. се потвърждава непоколебимият ангажимент на двата съюза да продължат да укрепват, разширяват и задълбочават сътрудничеството, за да се справят по-специално с нарастващата геостратегическа конкуренция, въпросите на устойчивостта, защитата на критичните инфраструктури, нововъзникващите и разрушителни технологии, космическото пространство, последиците за сигурността от изменението на климата и противодействието на чуждестранното манипулиране на информация и вмешателство (Council of the European Union, 2016). Допълнителна възможност за мултилатерален подход в областта е свързан с идеята за укрепване в рамките на Глобалния портал на информационния обмен на световно ниво и засилване на сътрудничеството и координацията със съмишленици в трети държави с цел стимулиране на медийната екосистема (EPRS, 2023).

По отношение на второто направление Запазване на информационната и медийната среда в ЕС чрез предпазването ѝ от външната намеса, манипулирането на информация, дезинформация, пропаганда и други заплахи, са предприети към момента следните ключови инициативи:

- **Окончателен доклад на експертната група на високо равнище по въпросите на фалшивите новини и дезинформацията онлайн, 2018 г**., който поставя във фокуса на внимание проблемите, свързани с онлайн дезинформацията, а не с фалшивите новини, давайки следното определение за дезинформация: невярна, неточна или подвеждаща информация, предназначена, представена и оповестявана с цел печалба или умишлена вреда на обществото. Препоръчва: насърчаването на медийната грамотност, създаване на инструменти срещу дезинформацията за потребители и журналисти, подкрепа за разнообразие и устойчивост в медиите и провеждане на научни изследвания за въздействието на дезинформацията в Европа. Лансира се идеята за създаването на Кодекс на принципите, с който да се ангажират онлайн платформите и социалните мрежи (Европейска комисия, 2018).



Източник: Разработено от автора, чрез използван темплейт за „мисловна карта“ със свободен достъп от „TemplateLab”

Фигура 4: Подход на Европейския съюз в когнитивната област, разглеждана в по-широкия контекст на хибридните заплахи

- **План за действие за борба с дезинформацията, 2018** г., в който се подчертава, че дезинформацията, като динамично предизвикателство, може сериозно да влияе върху демократичните процеси и обществения дебат. В тази връзка за борба с този проблем, е необходим координиран, съвместен и устойчив подход в Европейския съюз. Предложен е набор от действия за изграждане на способности и укрепване на сътрудничеството между държавите членки и институциите на ЕС с цел проактивни действия срещу дезинформацията, включващ: 1) подобряване на откриването, анализа и разобличаването на дезинформацията; 2) засилване на сътрудничеството и съвместна реакция на дезинформацията; 3) мобилизиране на частния сектор за борба с дезинформацията и 4) повишаване на осведомеността и устойчивостта на обществото (ЕСВД, 2018).
- **План за действие за европейската демокрация, 2020** г., целящ оправомощаване на гражданите и изграждане на по-устойчиви демокрации в целия ЕС в отговор на предизвикателствата пред демократичните системи, породени от нарастващия екстремизъм и дистанцията между политиците и електората. Документът включва предприемане на действия в три основни стълба: 1) насърчаване на свободни и честни избори, чрез законодателство за прозрачността на спонсорираното политическо съдържание (т. нар. „политическа реклама“) и преразглеждане на правилата за финансиране на европейските политически партии; 2) подкрепа за медийната свобода и плурализъм чрез насърчаване безопасността на журналистите; финансови проекти за правна помощ на журналисти; обзор на собствеността върху медиите; 3) борба с дезинформацията чрез подобряване на съществуващите и появата на нови инструменти срещу външна намеса, както и чрез подобряване на Кодекса за поведение и по-стабилна рамка за мониторинг на неговото прилагането (Европейска комисия, 2020).
- **Подобрение на Кодекса за поведение във връзка с дезинформацията от 2018, 2022** г. Кодексът за поведение във връзка с дезинформацията от 2018 г. събира участници от сектора, които се ангажират на доброволен принцип да полагат усилия за борба с дезинформацията. Кодексът, част от стратегията на ЕС срещу дезинформацията, се доказва във времето като ефективен инструмент за ограничаване на разпространението на дезинформация онлайн по време на избори, кризи, като тази, свързана с пандемията от COVID-19 и конфликти като войната в Украйна. През 2022 г. се прави подобрение на съдържанието му, като се укрепва с по-подробни ангажименти и мерки за: 1) разширено участие: кодексът да не е насочен само към големите платформи Meta, Google,

Twitter, TikTok, Amazon и Microsoft, но да включва и различни участници, които имат роля за смекчаване на разпространението на дезинформация, и да е отворен за присъединяване от нови участници; 2) намаляване на финансовите стимули за разпространение на дезинформация, като се гарантира, че разпространителите на дезинформация не се възползват от приходите от реклама; 3) обхващане на нови манипулативни поведения, като фалшиви профили, ботове или злонамерени дълбинни фалшификати, разпространяващи дезинформация; 4) предоставяне на потребителите на по-добри инструменти за разпознаване, разбиране и сигнализиране на дезинформацията; 5) разширяване на проверката на факти във всички държави от ЕС и на всички езици на ЕС, като се гарантира справедливо възнаграждение на проверителите на факти за тяхната работа; 6) гарантиране на прозрачна политическа реклама, като се предоставя възможност на потребителите лесно да разпознават политическите реклами благодарение на по-доброто етикетиране и информация за спонсорите, разходваните средства и периода на показване; 7) оказване на по-добра подкрепа на изследователите, като се подобрява достъпът им до данните на платформите; 8) оценяване на собственото въздействие чрез стабилна рамка за мониторинг и редовно докладване от платформите относно начина, по който изпълняват ангажиментите си; 9) създаване на център за прозрачност и работна група за лесен и прозрачен преглед на прилагането на кодекса, като по този начин последният се поддържа пригоден за бъдещето и за използване по предназначение.

Кодексът има за цел да бъде признат като кодекс за поведение съгласно Законодателния акт за цифровите услуги, с цел намаляване на рисковете за големите онлайн платформи, произтичащи от дезинформацията.

- **Акт за цифровите пазари от 2022 г**., имащ за цел да осигури равни условия на конкуренция за всички дигитални компании, независимо от размера им, като по този начин малките и стартиращи предприятие, носители на иновативност ще могат да се възползват от Единния цифров пазар, без да бъдат възпрепятствани или ограничавани от големите платформи, превърнали се през годините в „пазачи на информационния вход“ между малкия бизнес и потребителите на интернет (Европейски парламент, 2021).
- **Акт за цифровите услуги от 2022 г**. (Регламент (ЕС) 2022/2065), имащ за цел създаването на по-безопасно цифрово пространство за потребителите и компаниите, защитавайки основните права онлайн. Актът се стреми да преодолее предизвикателствата, свързани с незаконната търговия и обмен на стоки, услуги и съдържание в онлайн среда, както и

с разпространението на дезинформация посредством алгоритми. Премахването на незаконно съдържание ще се ускори, а правилата относно вредното съдържание (като политическа дезинформация) ще бъдат по-ясни, включително във връзка със защитата на свободата на изразяване (Европейски парламент, 2021).

- Очакванията към двата акта за цифровите пазари (който се прилага от 2 май 2023 г.) и услуги (който ще се прилага от 17 февруари 2024 г.) са да създадат по-безопасна, по-справедлива и по-прозрачна онлайн среда.
- В допълнение, сред водещите инструменти, които са в процес на подготовка и приемане са:
- **Европейският законодателен акт за свободата на медиите**, предложен от Европейската комисия като набор от правила за защита на плурализма и независимостта на медиите в ЕС. Регламентът включва предпазни мерки срещу политическа намеса в редакционните решения и срещу наблюдението. В него се поставя акцент върху независимостта и стабилното финансиране на обществените медии, както и върху прозрачността на собствеността върху медиите и разпределението на държавната реклама (European Commission, 2022).
- **Пакет за защита на демокрацията**, обявен през февруари 2023 г. и имащ за цел да обхване прегледа на изпълнението на Плана за действие за европейската демокрация и да разгледа начините за по-нататъшно укрепване на демократичната устойчивост, като се вземат предвид препоръките на Конференцията за бъдещето на Европа (EPRS, 2023).
- **Пакт за изкуствения интелект** – през април 2021 г. Европейската комисия представя първата регулативна рамка за изкуствения интелект, предвиждаща класификация на системите в групи според риска за потребителите, като системите с по-висок риск, засягащи основни права се посочва, че ще бъдат регулирани по-строго (European commission, 2021). Преди да се приеме окончателно и подготви за прилагане актът за ИИ, на 24 май 2023 г. европейският комисар по въпросите на вътрешния пазар Тиери Бретон обявява намерението си да създаде доброволен пакт за изкуствен интелект, в който да участват европейски и неевропейски компании.
- **Създаване на Европейски офис за изкуствения интелект** – Европейският парламент предлага създаване на независима служба на ЕС за ИИ със собствена правосубектност, финансиране и персонал (EPRS, 2023).
- **Създаване на центрове за обмен на анализ и информация** – предложение от февруари 2023 г. на Европейската служба за Външна дейност, която от 2015 г. е основният двигател на усилията за противодействие

на (руската) дезинформация и чуждестранното манипулиране на информация и вмешателство. Целта е да се стимулира междуправителственото и междуинституционално сътрудничество, както и това със всички заинтересованите страни за обмен на информация и добри практики посредством стандартизиране и обединяване на познанията за инфраструктурата и поведението на актьорите, източниците на заплаха, както и за вече случили се инциденти в областта.

Създаден като проект за мир, ЕС избягва да използва терминологията на войната и не идентифицира експлицитно когнитивната война, а поставя рисковете, свързани с нея в по-широкия контекст на хибридните заплахи. Предвид обаче, че тя е под прага на въоръжения конфликт и атакува в най-висока степен същността на Съюза – неговите демократични устои, ценностите, вярванията на гражданите в европейския проект, когнитивните или психологическите аспекти от поведението на вземащите решение, следва да бъде част от процеса на стратегическо мислене.

Евентуалното преразглеждане на Стратегическия компас през 2025 г. би могло да бъде възможност да се постави специален акцент върху когнитивната сфера, както и върху необходимостта държавите членки да разработят стратегии за противодействие според спецификите във всяка една от страните. За целта европейските лидери и отговорните за политиките следва да възприемат Европейския съюз като многоизмерна сила, да приложат холистичен подход и експоненциален дизайн на стратегическо мислене.

Заключение

В заключение, публикацията извежда пет основни извода, базирани на следните ключови анализирани момента:

- глобалните рискове, имащи икономически, екологичен, геополитически, обществен и технологичен характер, създаващи „поликризисност“ и комплексна заплаха пред сигурността;
- появата на изкуствения интелект, който бива използван като инструмент за дезинформация и потенциално конкурентно предимство на автократичните режими, боравещи централизирано с големи масиви от информация и данни;
- когнитивната сфера, която се превръща в ново бойно поле, в което все по-централно място заема съревнованието за умовете и емоциите на гражданите и използването на уязвимостите в демократичните общества;
- начините за изграждане на устойчивост чрез образование, медийна грамотност, критично мислене, цифрови компетентности, ментална издръжливост;

– потенциала на Европейския съюз да бъде „многоизмерна сила“, разполагайки с инструментите на нормативна, мека, икономическа, военна, спокойна, интелигентна и трансформативна сила;
– инициативите и стратегическите документи към края на 2023 г., които ЕС развива в по-широкия контекст на хибридните заплахи.

В резултат на гореизложеното следва да се отбележат следните пет извода и препоръки, които да позволят на ЕС да преодолява по-ефективно некинетичните предизвикателства, използващи както умовете и емоциите на гражданите, така и уязвимостите в демократичните държави и общества:

1. За да се справи ефективно с рисковете на „поликризисността“, Европейският съюз трябва да се превърне в „многоизмерна сила“. Това означава да развие способността си за идентифициране и използване на разнообразен набор от инструменти в стратегически комбинации, съобразени със сложността на разглежданите предизвикателства. Този подход не само ще осигури на Съюза конкурентно предимство, но и ще повиши устойчивостта на държавите членки и техните граждани в условията на непрекъснати промени и сложни по своя характер едновременно случващи се глобални рискове пред сигурността.
2. Стратегиите и инициативите, насочени към справяне с хибридните заплахи, особено в когнитивната област, трябва да изпълняват двойна роля. Те трябва не само да се справят с непосредствените предизвикателства, но и активно да допринасят за формирането на бъдещата реалност. От съществено значение е постигането на динамичен баланс между запазването на приемствеността и приемането на промените. От решаващо значение, за да се постигне това е: от една страна, тези стратегии и планове да се изготвят и изпълняват от лица, които притежават не само инкрементално мислене, но и способност за експоненциално мислене, и от друга страна, да се прилагат в общества, с изградена устойчивост и способност не само за бързо, но бавно и критично мислене.
3. Прилагането на експоненциален дизайн на стратегическо мислене е от ключово значение в новата среда за сигурност, тъй като той е свързан с иновативност, гъвкавост и намиране на интегрирани и трансформативни решения, в преодоляването на некинетични заплахи с висок потенциал за разрушителна сила, особено в демократичните общества. Той може да насърчи устойчивостта чрез предвиждане и подготовка за неочаквани и бързо ескалиращи заплахи, намаляване на уязвимостта и подобряване на възможностите и скоростта за реагиране в условия на предвидима непредвидимост.

4. За да се създадат устойчиви общества, които могат да устоят на различни форми на кризи, на промени в комуникационната и средата за сигурност, е жизненоважно да се развива ментална устойчивост на индивидуално, професионално и лидерско равнище сред гражданите и отговорните за политиките, както и способност за медийна грамотност, добро калибриране между разум и емоция, критично мислене.
5. Експлицитното извеждане на когнитивната област в процеса на преоценка на Стратегическия компас през 2025 г., както и по-тясното координиране с НАТО чрез своеобразно „разделение на труда“ и създаване на единен понятиен апарат в областта, са от важно значение, за да може ЕС да изгради своята устойчивост и капацитет за противодействие.

Използвана литература

Аберкан, И. (2020). Освободи своя мозък, Издателство: Изток-Запад. (Aberkan, I., 2020, Oslobodi svoya mozuk, Izdatelstvo: Iztok-Zapad).

Дзъ, С. (2005). Изкуството да побеждаваш, Военно издателство. (Dza, S., 2005, Izkustvoto da pobezhdavash, Voenno izdatelstvo).

Дракър, П. (2013). Дракър за всеки ден, Класика и Стил. (Drakar, P., 2013, Drakar za vseki den, Klasika i Stil).

Европейска комисия. (2016). Съвместна рамка за борба с хибридните заплахи – ответни действия на Европейския съюз, (Evropeyska komisia, 2016, Savmestna ramka za borba s hibridnite zaplahi – otvetni deystvia na Evropeyskia sayuz), available at: https://eur-lex.europa.eu/legal-content/BG/ALL/?uri=CELEX%3A52016JC0018 (accessed 1 November 2023)

Европейска комисия. (2018a). Повишаване на устойчивостта и укрепване на способностите за борба с хибридните заплахи, (Evropeyska komisia, 2018a, Povishavane na ustoychivostta i ukrepvane na sposobnostite za borba s hibridnite zaplahi), available at: https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:52018JC0016 (accessed 1 November 2023)

Европейска комисия. (2018b). Борба с онлайн дезинформацията: експертна група се застъпва за повече прозрачност на онлайн платформите, (Evropeyska komisia, 2018b, Borba s onlayn dezinformatsiyata: ekspertna grupa se zastapva za poveche prozrachnost na onlayn platformite), available at: https://ec.europa.eu/commission/presscorner/detail/bg/ip_18_1746 (accessed 1 November 2023)

Европейска комисия. (2020). План за действие за европейската демокрация: за подсилване на демокрациите в ЕС, (Evropeyska komisia, 2020, Plan za deystvie za evropeyskata demokratsia: za podsilvane na demokratsiite

v ES), available at: https://ec.europa.eu/commission/presscorner/detail/bg/ip_20_2250 (accessed 1 November 2023)

Европейска комисия. (2022). Дезинформация: Комисията приветства новия укрепен и по-всеобхватен Кодекс за поведение във връзка с дезинформацията, (Evropeyska komisia, 2022, Dezinformatsia: Komisiyata privetstva novia ukrepen i po-vseobhvaten Kodeks za povedenie vav vrazka s dezinformatsiyata), available at: https://ec.europa.eu/commission/presscorner/detail/bg/ip_22_3664 (accessed 1 November 2023)

Европейска комисия. (2023a). Съобщение на Комисията. Насоки съгласно член 33a, параграф 3 от Директивата за аудио-визуалните медийни услуги за обхвата на докладите на държавите членки относно мерките за насърчаване и развитие на умения за медийна грамотност, (Evropeyska komisia, 2023a, Saobshtenie na Komisiyata. Nasoki saglasno chlen 33a, paragraf 3 ot Direktivata za audio-vizualnite mediyni uslugi za obhvata na dokladite na darzhavite chlenki otnosno merkite za nasarchavane i razvitie na umenia za mediyna gramotnost), available at: https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:52023XC0223(01)&from=EN#ntr4-C_2023066BG.01000301-E0004 (accessed 1 November 2023)

Европейски парламент. (2021). Законодателните актове на ЕС за цифровите пазари и цифровите услуги, (Evropeyski parlament, 2021, Zakonodatelnite aktove na ES za tsifrovite pazari i tsifrovite uslugi), available at: https://www.europarl.europa.eu/news/bg/headlines/society/20211209STO19124 (accessed 1 November 2023)

ЕСВД. (2018). План за действие за борба с дезинформацията, (ESVD, 2018, Plan za deystvie za borba s dezinformatsiyata), available at: https://www.eeas.europa.eu/node/54831_et?page_lang=bg (accessed 1 November 2023)

Ленард, М. (2005). Защо Европа ще управлява XXI век, издателство Обсидиан. (Lenard, M., 2005, Zashto Evropa shte upravlyava XXI vek, izdatelstvo Obsidian).

Най, Д. (2013). Бъдещето на силата, Военно издателство. (Nay, D., 2013, Badeshteto na silata, Voenno izdatelstvo).

Регламент (ЕС) 2022/2065 на Европейския парламент и на Съвета от 19 октомври 2022 година относно единния пазар на цифрови услуги и за изменение на Директива 2000/31/ЕО (Акт за цифровите услуги) (текст от значение за ЕИП), Официален вестник на ЕС, L 277/1, (Reglament (ES) 2022/2065 na Evropeyskia parlament i na Saveta ot 19 oktomvri 2022 godina otnosno edinnia pazar na tsifrovi uslugi i za izmenenie na Direktiva 2000/31/EO (Akt za tsifrovite uslugi) (tekst ot znachenie za EIP), Ofitsialen vestnik na ES, L 277/1), available at: https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32022R2065 (accessed 1 November 2023)

Харари, Ю. (2018). Homo deus. Кратка история на бъдещето, Изток-Запад. (Harari, Yu., 2018, Homo deus. Kratka istoriya na badeshteto, Iztok-Zapad).

Цеков, И. (2017). Променящата се природа на конфликта в началото на 21 век, Международни отношения, бр. 3/2017 г. (Tsekov, I., 2017, Promenyashtata se priroda na konflikta v nachaloto na 21 vek, Mezhdunarodni otnosheniya, br. 3/2017 g.).

Bonchek, M. (2016). How to Create an Exponential Mindset, available at: https://hbr.org/2016/07/how-to-create-an-exponential-mindset (accessed November 1, 2023)

Council of the European Union. (2016). Eighth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017, available at: https://www.consilium.europa.eu/media/65080/230616-progress-report-nr8-eu-nato.pdf (accessed November 1, 2023)

Council of the European Unioon. (2018). Council Recommendation on Key Competences for Life- long Learning, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018H0604(01) (accessed 1 November, 2023)

Council of the European Union. (2022). A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security, available at: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf (accessed November 1, 2023)

EEAS (European External Action Service). (2022). Countering hybrid threats, available at: https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en (accessed November 1, 2023)

EPRS (European Parliamentary Research Service). (2023). Future Shocks 2023: Anticipating and weathering the next storms, available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2023)751428 (accessed November 1, 2023)

European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 (accessed November 1, 2023)

European Commission. (2022). European Media Freedom Act: Commission proposes rules to protect media pluralism and independence in the EU, available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5504 (accessed November 1, 2023)

Harari, Y. (2018). Why Technology Favors Tyranny, available at: https://www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330/ (accessed November 1, 2023)

Joint Research Centre (European Commission). (2021). The landscape of hybrid threats, available at: https://op.europa.eu/en/publication-detail/-/publication/b534e5b3-7268-11eb-9ac9-01aa75ed71a1/language-en (accessed November 1, 2023)

Kahneman, D. (2011). Thinking, Fast and Slow, Penguin Books, London.

Lawrence, C. (2015). Special Operations Mental Toughness: The Invincible Mindset of Delta Force Operators, Navy SEALs, Army Rangers & Other Elite Warriors, pp. 76-87.

Nate, S., Ratiu, A. (2018). Non-Kinetic Warfare Challenges of the Information Ecosystem's Phenomenology – The Pattern to a New Battleground, DOI: 10.1515/kbo-2018-0022

NATO. (2023a). Cognitive Warfare: Strengthening and Defending the Mind, available at: https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/ (accessed on November 1, 2023)

NATO. (2023b). Cognitive Warfare: Beyond Military Information Support Operations, available at: https://www.act.nato.int/article/cognitive-warfare-beyond-military-information-support-operations/ (accessed on November 1, 2023)

NATO. (2021). Countering cognitive warfare: awareness and resilience, available at: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html (accessed November 1, 2023)

Panayotova, M. (2023). Can the European Union be a „Change master" in the climate change – defence nexus?, Philosophical Alternatives journal, issue 3.

Torkington, S. (2023). We're on the brink of a 'polycrisis' – how worried should we be?. World Economic Forum, available at: https://www.weforum.org/agenda/2023/01/polycrisis-global-risks-report-cost-of-living/ (accessed November 1, 2023)

US Air Force. (2007). Operations and Organizations; Air Force Doctrine Document 2, available at: https://irp.fas.org/doddir/usaf/afdd2.pdf (accessed November 1, 2023)

Vuorikari, R., Kluzer, S. & Punie, Y. (2022). DigComp 2.2: The Digital Competence Framework for Citizens – With new examples of knowledge, skills and attitudes, DOI:10.2760/490274, JRC128415, available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC128415 (accessed November 1, 2023)

***

BUILDING RESILIENCE IN THE EUROPEAN UNION IN TIMES OF POLYCRISIS AND CHALLENGES IN THE COGNITIVE DOMAIN

Assist. Prof. Monika Panayotova, PhD
International Relations Department
Faculty of International Economics and Politics
University of National and World Economy
e-mail: monika.panayotova@unwe.bg

Abstract

This aim of this publication is to draw attention to the need to build resilience in the societies and Member States of the European Union in times of "polycrisis" and challenges in the cognitive domain. Following an analysis of global risks and hybrid threats, as well as the emergence of artificial intelligence in today's communication and security environment, certain recommendations and conclusions are drawn to enable the EU to exploit its potential to be a "multidimensional power", overcoming non-kinetic challenges to vulnerabilities in democratic societies, citizens' minds and emotions. In this research, a range of political science analysis methods were employed. In addition, the "mind maps" technique of the British psychologist Tony Buzan was implemented by enabling the synthesis of ideas through visual representations. On the eve of the European elections in 2024, the publication draws key conclusions and recommendations for overcoming the challenges of desinformation, perception management and psychological manipulation, which undermine trust in democratic institutions and prevent decision-makers from countering them. These include: building resilience through education, media literacy, critical thinking, digital competencies, mental toughness; the ability to think not only fast but also slow; the application of exponential design to strategic thinking; multilateralism and close cooperation with NATO.

Keywords: EU, polycrisis, AI, European elections, cognitive domain, resilience, NATO, power

JEL: F50, F53, D81, Z18