ПЕТКО ДИМОВ
ИВАЙЛО ИГНАТОВ
ХРИСТИНА ДОБРЕВА



ПРОТИВОДЕЙСТВИЕ НА ДЕЗИНФОРМАЦИЯТА

Военна академия „Георги Стойков Раковски“

ПЕТКО ДИМОВ
ИВАЙЛО ИГНАТОВ
ХРИСТИНА ДОБРЕВА

ПРОТИВОДЕЙСТВИЕ НА ДЕЗИНФОРМАЦИЯТА

учебник

Военна академия „Георги Стойков Раковски“

София ● 2025

СЪДЪРЖАНИЕ

УВОД 6

Глава първа
ВЪВЕДЕНИЕ И ОСНОВНИ ПОНЯТИЯ 7
Какво представлява дезинформацията 8
Как се разпространява дезинформацията 12
Защо сме уязвими на дезинформация 15
Как да разпознаем дезинформацията 17
Какви са последствията за националната сигурност 21
Как се противодейства на дезинформацията 22

Глава втора
ЗАКОНОДАТЕЛЕН ПОДХОД ЗА БОРБА С ДЕЗИНФОРМАЦИЯТА 25
Нормативни документи в Европейския съюз и НАТО 25
Международни споразумения и конвенции в областта на интернет правото 31
Право на Европейския съюз в областта на авторското право в интернет 32
Закон за авторското право в цифровата епоха – САЩ 32
Българско законодателство, свързано с борбата срещу дезинформацията 33
Етичен кодекс на българските медии 34
Инструментите срещу плагиатство като средство за повишаване на информационната грамотност и противодействие срещу дезинформацията 35
Етични последици от въвеждането на изкуствен интелект в контекста на борбата с дезинформацията 36

Глава трета
КРИТИЧНО МИСЛЕНЕ И РАЗВИТИЕ НА АНАЛИТИЧНИТЕ УМЕНИЯ 39
Основи на критичното мислене 39
Развиване на критичното мислене и аналитичните умения 40
Методи за въздействие върху вземането на решения 43

Глава четвърта
МЕДИЙНА ГРАМОТНОСТ И АНАЛИЗ НА ИНФОРМАЦИЯТА ОТ СОЦИАЛНИТЕ МЕДИИ 46
Какво представлява медийната грамотност 46
Медийната грамотност, като основно средство за борба с дезинформацията 49
Методи за анализ на медийно съдържание 51
Разпространение на дезинформацията в социалните медии 51
Десет начина за манипулиране с помощта на медиите 60

Глава пета
БОРБА С ДЕЗИНФОРМАЦИЯТА В НАЦИОНАЛНОТО ИНФОРМАЦИОННО ПРОСТРАНСТВО 65
Концепция за национално когнитивно пространство и когнитивна война 65
Международни подходи за противодействие на дезинформацията 68
Как се противодейства на дезинформацията – основни подходи и български решения 72
Изграждане на устойчивост срещу дезинформацията 73
Стратегическите комуникации и насоки за борба с дезинформацията 76

Глава шеста
ПРАКТИКА. ИЗГРАЖДАНЕ НА УСТОЙЧИВОСТ СРЕЩУ ДЕЗИНФОРМАЦИЯ 86
Рамка за анализ на чуждестранна когнитивна намеса 86
Примери и казуси от реални ситуации 93

Глава седма
РАБОТА С ДИГИТАЛНИ ИНСТРУМЕНТИ ЗА ПРОВЕРКА НА ФАКТИ И БОРБА С ДЕЗИНФОРМАЦИЯТА 100
Технологични инструменти за борба с дезинформацията 102
Образователен инструмент за борба с дезинформацията 103
Алгоритъм за разпознаване на фалшивите новини 104
Характеристики на сайтовете по отношение на тяхната надеждност като източници на информация 108

Глава осма
ПРАКТИКА.
РАЗПОЗНАВАНЕ НА ТРОЛОВЕ, БОТОВЕ
И ФАЛШИВИ ПРОФИЛИ.....111
Стратегии за тролене по света и у нас 112
Практическо упражнение за разпознаване на трол или бот 115
Упражнение за разпознаване на методи за манипулиране
на аудиторията.....122
Упражнения за разпознаване на фалшиви новини 123
Примерен изпитен тест.....126

ЗАКЛЮЧЕНИЕ 133
ЛИТЕРАТУРА.....134
REFERENCES.....138
ДОПЪЛНИТЕЛНИ ИЗТОЧНИЦИ 142

УВОД

Истината е първата жертва във войната – този израз за първи път е споменат по време на конференция за защита правата на жените през август 1915 г. от Етел Анакин, съпруга на британския политик Филип Сноудън (Snowden 1915). Фразата е още по-актуална днес, когато дезинформацията се утвърди като една от най-значимите асиметрични заплахи за националната сигурност в съвременната информационна среда. В контекста на нарастващите хибридни предизвикателства изграждането на устойчивост срещу дезинформационни въздействия придобива критично значение в сектора на националната сигурност и отбрана.

Именно за изграждане на такава устойчивост сред студентите в област на висшето образование „Сигурност и отбрана“ е предназначен настоящият учебник. Целта е обучаемите да придобият базови знания, умения и компетентности за разпознаване на дезинформацията и изграждане на когнитивна устойчивост и медийна грамотност при анализ на информацията в области на държавното управление. За постигане на тази цел в програмата са включени обзорни теми в областта на критичното мислене и дезинформацията в интернет, както и специфични теми и примери ориентирани към сигурността и отбраната. Методиката за съставяне на учебното съдържание се базира на всеобхватния подход, формиращ основния инструментариум за запознаване с теорията на информационната сигурност, помагаща при решаването на практическите въпроси в професионалната дейност за защитата на информацията.

Глава първа
ВЪВЕДЕНИЕ И ОСНОВНИ ПОНЯТИЯ

Лекцията въвежда обучаемите в темата и дефинира основните понятия: информация; дезинформация; манипулация и пропаганда. Описва се жизненият цикъл, моделът на разпространение в информационните полета и въздействие на дезинформацията. Разглеждат се видовете източници на информация.

Истината е първата жертва във войната,
но тя е и най-силното оръжие
в борбата срещу дезинформацията.

Адаптирано от Етел и Джордж Оруел

В съвременното информационно общество медиите са изключително достъпни и играят ключова роля в оформянето на социалните нагласи. Тази достъпност обаче създава предпоставки за тяхното използване с различни цели, включително за постигане на политическо или икономическо надмощие. Това явление води до т.нар. „информационно разстройство“ – термин, който обхваща разпространението на фалшива, подвеждаща или манипулативна информация.

Разпространението на невярна информация не е нов феномен. Още през VI век пр.н.е. китайският стратег Сун Дзъ в своя трактат „Изкуството на войната“ акцентира върху значението на измамата като инструмент за постигане на надмощие в конфликтите (Sun Tzu 2022). С развитието на периодичните печатни издания и масовите комуникации дезинформацията започва да се използва в по-голям мащаб, особено в периоди на политически и военни кризи. Втората световна война (1939 – 1945) е пример за период, в който този похват достига своя връх. Йозеф Гьобелс, една от водещите фигури в нацистката пропаганда, известен с изказването си, че „една лъжа, повторена 100 пъти, става истина“, е илюстрация на организирания подход към манипулирането на информация (Taylor 1995).

В наши дни с развитието на интернет и социалните медии дезинформацията придобива ново измерение. Глобалната свързаност и скоростта на разпространение позволяват фалшивите новини да достигат до многомилионна аудитория за кратко време. Проучвания показват, че фалшивите новини се разпространяват по-бързо и в по-широк мащаб от истинските. Изследване на 126 000 публикации в Twitter, разпространени от 3 милиона потребители в периода 2006 – 2017 г., разкрива, че най-споделяният 1% от фалшивите новини достигат между 1000 и 100 000 души, докато истинските новини рядко надхвърлят 1000 души аудитория (Vosoughi, Roy & Aral 2018).

Тези тенденции подчертават необходимостта от задълбочено разбиране на основните понятия свързани с дезинформацията, нейните исторически корени и съвременните предизвикателства. Затова изучаването на механизми за противодействие на дезинформацията е от съществено значение за специалистите в областта на сигурността и отбраната.

Какво представлява дезинформацията

Думата „информация“ произлиза от латинската informare, която означава „придаване на форма“. В този контекст „дезинформация“ може да бъде разглеждана като процес на нарушаване или изкривяване на тази форма по време на създаването, съхраняването, предаването и приемането на информация.

През 80-те години на XX век изследвания в областта на организационното управление подчертават ролята на информацията като ключов фактор за иновации и развитие. Установено е, че този фактор позволява на организациите и обществото да разгърнат своите способности и да постигнат високи резултати. На тази основа е формулиран принципът на стратегическото ръководство, че колкото по-ефикасно една организация обработва информацията, толкова по-висока е нейната ефективност, а дезинформацията постига обратното.

Според съобщение на Европейската комисия от 26 април 2018 г., *дезинформацията* се дефинира като *умишлено разпространение на невярна, неточна или подвеждаща информация с цел манипулация на общественото мнение или постигане на конкретни политически, икономически или социални ползи.*[1] Тази дефиниция подчертава основните аспекти на дезинформацията:

[1] European Commission, 2018. *Tackling online disinformation: A European approach*. Съобщение на Европейската комисия от 26 април 2018 г.

– намерение: умишлен характер на разпространението;

– съдържание: невярно, подвеждащо или изопачено;

– цел: манипулиране на общественото мнение или постигане на конкретни стратегически цели.

Дезинформацията следователно представлява не просто изопачаване на информацията, но и инструмент за когнитивно въздействие, който е особено актуален в ерата на цифровите технологии и глобалната свързаност. В медийното пространство дезинформацията често се свързва с разпространението на фалшиви новини, манипулация на съдържание и използването на пропаганда за влияние върху общественото съзнание. Според изследвания на NATO StratCom COE България е една от най-уязвимите държави в NATO, особено в периоди на избори или международни кризи[2].

В държавите, членки на НАТО, дезинформацията се класифицира в три основни категории, които отразяват нейната сложност и многопластовост:

● Misinformation – грешна информация – която се разпространява без зъл умисъл. Това включва неточности породени от незнание или непреднамерени грешки. Например неправилно цитиране на източник или грешка в предаването на новина.

● Disinformation – умишлено разпространение на невярна информация – с цел манипулация или въвеждане в заблуждение. Този вид дезинформация е характерен за пропагандни кампании и политически влияния. Тя може да бъде бяла, сива и черна. Първата е истинска, но подадена със закъснение, което води до неадекватно поведение. Сивата е съвкупност от реални факти и измислици и води до неправилно поведение, а черната е изцяло лъжлива и води до грешни решения.

● Malinformation – истинска информация – използвана злонамерено, за да причини вреда. Това включва изтичане на лични данни, използване на конфиденциална информация извън контекста или манипулация с факти за дискредитиране на определени лица или организации (Wardle & Derakhshan, 2017).

● **Пропагандата**, от друга страна, е *преднамерен опит да се оформи възприятието, да се манипулират познанията и оттам директното поведение на аудиторията*. Според Карл фон Клаузевиц пропагандата е неразделна част от стратегията на войната, тъй като публичната подкрепа е ключов елемент за успеха на всяка военна или политическа

[2] NATO Strategic Communications Centre of Excellence, 2020. *Disinformation in the Digital Age*. Riga: NATO StratCom COE.

кампания. В съвременния контекст пропагандата често се използва в комбинация с дезинформация и фалшиви новини за постигане на стратегически цели.



Фигура 1. Разлика между Misinformation, Disinformation и Malinformation (Wardle & Derakhshan 2017)

Фалшивите новини са специфичен подвид на дезинформацията. Изразът произлиза от *fake news*, често превеждан от английски като „фалшиви новини“, и независимо от разликата между фалшив (fake) и неверен (false) се е наложил първият. Основната разлика произтича от това, че статиите с фалшиви новини имат доза истина, докато другият случай представлява обикновена лъжа. Те представляват информационни съобщения стилизирани като реални новини, но съдържащи *информация, която е напълно невярна или неправомерно присвоена, преувеличена или погрешно представена до степен, че тя вече не е вярна, представена като истинска новина или целенасочено разпространявана дезинформация с цел въвеждане в заблуждение срещу политическа или икономическа изгода*.

В някои формулировки новината се определя като **достоверна, частично достоверна** или **недостоверна**. „Фалшиви новини“ е неологизъм често използван за нежелани псевдоновини или пропаганда, насо-

чена към умишлена дезинформация или генериране на приходи от онлайн реклами. Разпространяването на фалшиви новини е „информационно замърсяване“, което значително се засилва по време на избори.

За улеснение и лесно идентифициране на различните видове дезинформация медийният изследовател от Харвард Клер Уордъл класифицира седем вида според нивото на манипулация (Wardle 2017). В началото са представени по-невинните форми на сатира, докато се стигне до напълно и целенасочено измислено съдържание:

1. Ирония (лека форма, разпространявана от потребителите).
2. Заблуждаващо заглавие (когато заглавието или началото на новината се разминава със съдържанието ѝ).
3. Пристрастие (неточно представяне на информацията за лице или събитие).
4. Фалшив контекст (когато истинска новина е представена на фона на неверен контекст).
5. Измамно или изкривено съдържание (когато истински източници са представени за фалшиви или измислени, като се подбират определени елементи от разказа, без да се представят всички гледни точки по темата).
6. Манипулирано съдържание (когато истинската информация се манипулира, например с подправени снимки).
7. Изфабрикувано съдържание (100% умишлена измама с цел да се заблуди читателят или да навреди).



Фигура 2. Градация на лъжливата информация
Източник: ДИМОВ, П.; ИВАНОВ, Е., 2020. *Фалшивите новини*, стр. 49

За постигане на целите си дезинформацията обикновено се съсредоточава около определени наративи, разкази, истории, които направляват посланията и съответно действията на аудиторията[3]. Според наръчника на командира за стратегически комуникации, „битката на наративите е широкомащабно противоборство в когнитивния и информационния домейн, така както традиционните бойни действия се водят във физическия домейн“ (Techau 2011) и направлява посланията и нейните действия[4].

Как се разпространява дезинформацията

Дезинформацията се разпространява в множество информационни полета, които обхващат когнитивните, информационните и физическите измерения на възприятията и действията в обществото. Именно затова в НАТО са дефинирани пет домейна или зони на операции (суша, море, въздух, космос и киберпространство) и три измерения (когнитивно, информационно и физическо). Разбирането на тези измерения и механизмите, чрез които се осъществява разпространението на дезинформация, е ключово за ефективното противодействие.

Физическото измерение обхваща традиционните канали за разпространение на информация – телевизия, радио, печатни издания и физически инфраструктури като сателити, оптични мрежи и комуникационни съоръжения. Дезинформацията тук се осъществява чрез манипулирани предавания, фалшиви новини или изопачаване на факти, представяни като обективни.

Информационното (виртуално) измерение обхваща дигиталното пространство, включително интернет, социалните медии и телекомуникационните мрежи. То е критична част от информационните операции, особено в контекста на модерните хибридни конфликти. Според „Политиката на НАТО за информационните операции“ информационното пространство представлява „виртуално и физическо пространство, в което се получава, обработва и предава информация“[5]. То включва както самата информация, така и „съвкупността от индивиди, организации и системи, които събират, обработват, разпространяват или действат

[3] MC 422/4. Military formation Operations (MD, 2012).
[4] Пак там.
[5] Пак там.

според дадена информация“, докато киберпространството е интерактивна среда, състояща се от електронни мрежи, интернет и дигитални технологии[6].



Фигура 3. Информация и дезинформация (схема – вариант)

С други думи, виртуалното измерение обхваща всички налични канали за разпространение – телевизия, радио, печат, академични дебати и интернет – и е обект на информационна война[7]. Това е основната среда за дезинформация поради:

– скоростта на разпространение – информацията достига глобална аудитория за секунди;

– масовост – алгоритмите на социалните мрежи подсилват сензационното съдържание;

– анонимност – дезинформацията често произлиза от анонимни или фалшиви профили.

Когнитивното измерение засяга съзнанието, емоциите и поведението на хората. Тук механизмите за дезинформация използват:

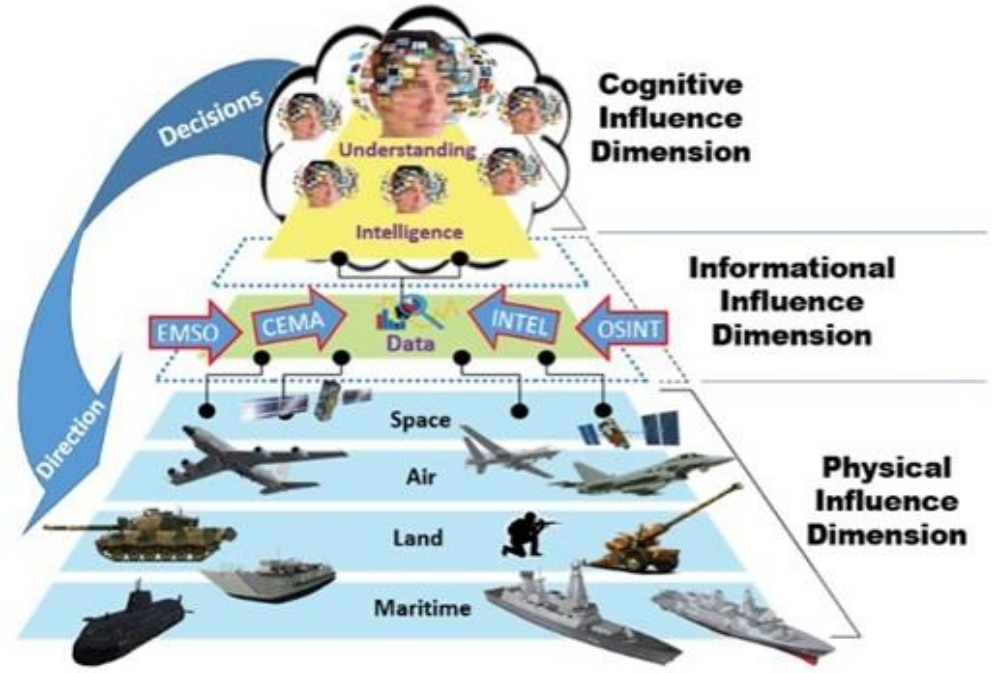
[6] Министерски съвет, 2016. *Национална стратегия за киберсигурност „Киберустойчива България 2020“*.

[7] Пак там.

– манипулация на наративи – конструиране на истории, които целят да оформят общественото мнение или да засилят разделението в обществото;

– пропаганда – насочено въздействие върху възприятията, често комбинирано с емоционални или националистически послания;

– изкривяване на реалността – умишлено смесване на истина и лъжа, за да се затрудни разграничаването между тях.



Фигура 4. Измерения на дезинформацията и механизми на влияние
Източник: RADOSLAVOV, D.; STRAWMAN, 2022. *Strategy For Countering Russian Information Operations And Cognitive Warfare In Bulgaria*. [Дисертация].

Съвременните хибридни конфликти често включват информационни операции и дезинформация като инструмент за подкопаване на стабилността на държави, отслабване на съюзнически структури и предизвикване на вътрешни конфликти. Целта на дезинформацията е да подкопае общественото доверие в институциите чрез разпространение на фалшиви новини, които ги представят като корумпирани и некомпетентни, или да деморализира и разделя обществото.

Социални медии като Facebook и TikTok играят централна роля за дезинформацията, поради това че са мощни инструменти за разпростра-

нението ѝ с широкия си обхват и висока скорост. Техните алгоритми дават приоритет на сензационното съдържание, допускат ботове и фалшиви акаунти, като в същото време липсва критична проверка от потребителите поради някои психологически и социални особености на хората.

Защо сме уязвими на дезинформация

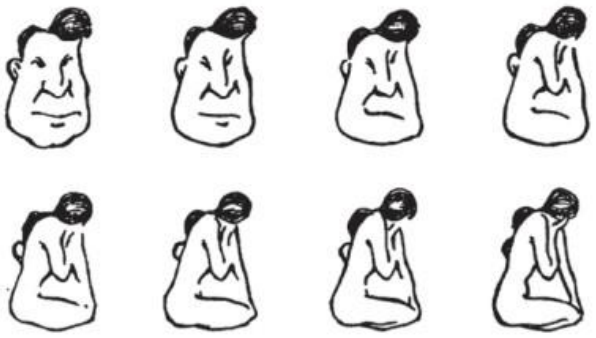
Алгоритмите на социалните медии използват факта, че стопроцентова достоверност на информацията не може да бъде постигната, тъй като тя се формира чрез субективно отражение на реалността. Човешкият мозък има редица когнитивни ограничения:

– бързо формираме мнение и трудно го променяме;

– емоционалното съдържание се запомня по-лесно;

– склонни сме да вярваме на информация, която потвърждава убежденията ни.

Например фигурата по-долу показва как хората формират бързо мнение, което е устойчиво на промяна. Ако погледнете поредицата от рисунки от ляво на дясно ще видите лице на мъж, но ако почнете отзад напред ще видите фигура на жена.



Фигура 5. Пример за формиране на мнение, устойчиво на промяна
Източник: HEUER, R. 1999. *Psychology of Intelligence Analysis.* Pherson Associates, LLC.

С други думи, информацията се изкривява субективно спрямо ограниченията на ума и когнитивните пристрастия. Освен това груповата динамика на социума може да доведе до некритично приемане на манипулирана информация на индивидуално и групово ниво.

Психологическите механизми, с които се съобразяваме на индивидуално ниво, са:

– когнитивни пристрастия – чрез тяхното използване за дезинформация се нарушава познавателният процес и способността за критично мислене;

– визуални манипулации – информацията най-лесно се асимилира чрез изображения, което ги прави мощен инструмент за дезинформация;

– ефект на потвърждението – хората са склонни да търсят и приемат информация, която подкрепя вече съществуващите им вярвания независимо от нейната достоверност. Това улеснява дезинформационните кампании, насочвани към конкретни нагласи или страхове;

– пристрастие към достъпната информация – нашите решения често се базират на информация, която е леснодостъпна, без да се проверява нейният източник или достоверност. В контекста на работещите в сектор „Сигурност и отбрана“ това може да доведе до разпространение на слухове и фалшиви заповеди;

– ефект на внушаемост – в условия на напрежение или несигурност хората са по-податливи на внушения и емоционално натоварена информация;

– друго значимо когнитивно отклонение е ефектът на Дънинг-Крюгер, при който хората с ниски способности при дадена задача са склонни да се надценяват (Kruger & Dunning 1999). Това води до свръхувереност в собствените знания и отхвърляне на фактическа информация или експертни мнения, които противоречат на погрешните вярвания. В сферата на дезинформацията ефектът може да накара хората да разпространяват уверено невярна информация, оказвайки влияние върху други, които бъркат доверието им с достоверност.

Социалните механизми на влияние се образуват от груповото мислене, предразполагащо към конформизъм и създаване на т.нар. „информационни балони“:

– конформизъм – в групова среда индивидите предпочитат да следват общоприетото мнение, дори когато то е погрешно и това води до некритично приемане на фалшива информация;

– социален натиск – желанието за съгласуваност и избягване на конфликти може да ограничи изразяването на съмнения относно достоверността на информацията;

– информационни балони – групи с еднакви нагласи са склонни да подсилват собствените си убеждения, като игнорират алтернативни гледни точки. Това ги прави особено уязвими към целенасочена дезинформация.

Психологическите и социалните механизми, засегнати от дезинформацията, могат сериозно да подкопаят координацията и ефектив-

ността на системата за отбрана на страната. По тази причина е необходимо разработването на стратегии за повишаване на медийната грамотност, критичното мислене и устойчивостта към манипулация в рамките на военните структури.

Как да разпознаем дезинформацията

Дезинформацията и чуждестранното манипулиране на информация и вмешателството са сериозна заплаха за обществото. Те могат да подкопаят демократичните институции и процеси, например изборните, като попречат на хората да вземат информирани решения или ги разубеждават да гласуват. Те могат да поляризират обществото, като настройват различни групи една срещу друга.

Новите технологии дават възможност на враждебните участници да разпространяват дезинформация и да манипулират информацията с невиждани досега мащаб и бързина. По тази причина борбата с дезинформацията и манипулирането на информация е един от най-неотложните въпроси за Европейския съюз и неговите държави членки. Дезинформаторите използват различни техники, за да заблуждават и манипулират хората онлайн, които могат да варират от клониране на законни уебсайтове до умело манипулирани аудио- или видеоматериали (известни като „дълбоки фалшификати“, често създавани с помощта на изкуствен интелект), предназначени да ни въздействат емоционално и да замъглят преценката ни.



Фигура 6. Примерна схема за противодействие на дезинформацията

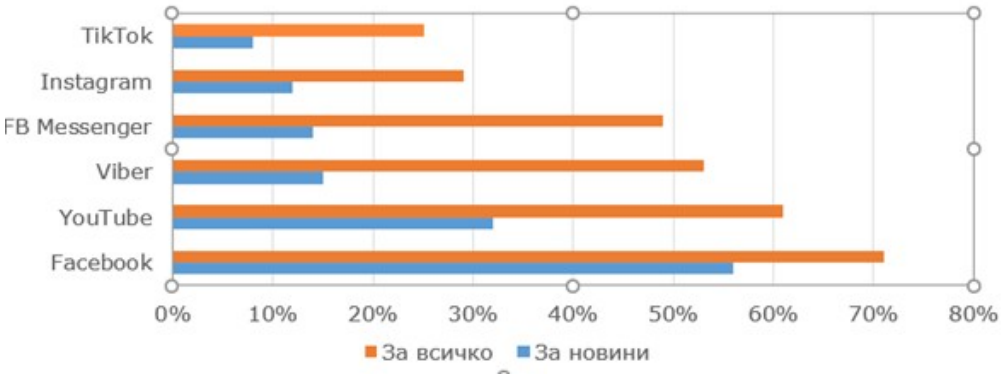
Най-важният показател за надеждността и достоверността на дадена информация е нейният **източник, т.е. откъде произхожда тя**. Най-общо могат да се разграничат два вида източници: директни (първични) и индиректни (вторични).

● Директните източници са основен елемент от първа ръка – пряк участник в събитие или очевидец, първичен писмен документ, видеозапис или снимка, осигуряващи пряко доказателство по даден въпрос.

● Индиректните източници използват един или повече посредници. Това може да е разказана история от дадена медия или от някой друг, който не е присъствал на събитието. Вторичният източник представлява експертна интерпретация или обработка на информацията от първични източници, синтезираща в себе си определено заключение.

Разузнавателните служби класифицират източниците като закрити и открити, а в медиите често употребяват понятието „анонимен източник“, на когото не може да се вярва. За да се провери надеждността на който и да е източник, информацията трябва да се верифицира поне от няколко възможно най-директни източници.

Всяка година институтът за изследване на журналистиката „Ройтерс“ към университета в Оксфорд прави изследване на доверието на европейските граждани към различните медии и източници. В изследването им от 2024 г. онлайн медиите у нас изпреварват телевизията със 73 на 61%. С други думи, вярваме малко повече в интернет, отколкото на новините по телевизията и почти не четем вестници. Като цяло почти към всички новинарски медии у нас има спад на доверието поради високата степен на политическа поляризация в обществото, породена от войната между Русия и Украйна, и усещането, че независимостта им е компрометирана по икономически или политически причини.



Фигура 7. Доверие в българските онлайн медии по данни от https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024/bulgaria

Собствениците на такива медии често споделят вярна или невярна информация, за да повлияят на обществения дебат със стратегическа цел. Фейсбук нарича това *операции за влияние* и разглежда подобни координирани споделяния като бизнес инструмент. В статията си „Операции за влияние: механизъм на действие и противодействие“ Димитър Димитров анализира същността и механизмите на операциите за влияние, както и стратегиите за тяхното противодействие. Той подчертава, че операциите за влияние представляват координирани действия, насочени към манипулиране на общественото мнение и поведение чрез използване на различни информационни канали. Димитров акцентира върху необходимостта от разработване на ефективни контрамерки, включително повишаване на медийната грамотност, изграждане на устойчивост срещу манипулации и създаване на нормативна рамка за защита на информационната среда. Той също така разглежда ролята на междуведомственото сътрудничество и международните партньорства в борбата срещу информационните заплахи (Dimitrov 2018)

Често в практиката се използват различни видове похвати за разпространение на едно и също съдържание чрез множество привидно различни страници, което повишава видимостта на новината или води до сдобиване с повече трафик чрез т.нар. кликбейт (clickbait).

В общоевропейските проучвания за медийна грамотност, издадени от Европейската комисия, се разграничават следните видове лоши практики за разпространение на дезинформация[8]:

1. Дезинформация, свързана с политическата пропаганда. Използва се за манипулиране на нагласите, ценностите и познанието на електората. Въздейства върху емоциите. Например лъжлива новина, публикувана от уебсайта на *ETF News*, според която „папа Франциск подкрепя кандидатурата Доналд Тръмп“.

2. Сензационни заглавия – ШОК! УЖАС! НЕВЕРОЯТНО! Използват се за генериране на трафик към сайтове от типа Bradva, Sekira, Petel, PIK, Blitz и други. Често след кликване на подобни заглавия се отварят изскачащи прозорци с реклами и дори шпионски софтуер. Тяхна разновидност са *фалшивите новини, използващи известни личности*, които привличат вниманието.

3. Спонсорирано съдържание, имащо за цел да продаде нещо. Тук влизат рекламите, умишлено изглеждащи като редакционно съдържание.

[8] EAVI. *Media Literacy for Citizenship*. [Прегледан: 4.02.2020]. [Online]. https://eavi.eu/.

4. Сатира и шега или пародийни публикации, които разсмиват читателя и често носят политическо послание. Те нямат потенциала да нанесат щети, но са подвеждащи. Проблемът възниква, когато потребителите не разберат шегата, извадят историята от контекста и започнат да я споделят в социалните мрежи. Типичен пример е случилото се с френското сатирично списание „Шарли Ебдо“.

5. Използва се страх, който се базира на митове, компромати, мнения и показания, представени като факти, често популяризиращи *расистки* или *сексистки идеи.*

6. Грешка, заблуда или пристрастие в материалите се допускат дори от големите медии, а в интернет пространството е пълно с *измамни уебсайтове* или *профили* в социалните мрежи, които се представят за известна марка или личност.

7. Теория на конспирацията, митове и легенди се използват от авторите на фалшивите новини, защото дават прост и достатъчно интересен отговор на всички проблеми. Използват темите за извънземни, евреи, илюминати, рептили и др., които са направили нещо тайно, без да предложат доказателства за това. Детайлите са представени като абсолютно доказателство, а аргументи изградени върху факти, се поставят под въпрос.

8. Псевдонаука. Доставчици на екологични продукти, чудодейни лекове, както и лечители, отричащи климатичните промени, представят сериозни научни изследвания с преувеличени или неверни твърдения, често противоречащи на експертите, без да се дава сметка каква ще е ползата или какви ще са последиците от тези действия.

9. Подвеждаща информация, слух или мнение, представени като факт. Включва комбинация от достоверно, невярно и частично невярно съдържание. Понякога авторът може и да не знае, че съдържанието е невярно, когато дословно преписва и се позовава на неверни факти или пък при подправено съдържание. *Мнение, с което не сме съгласни, не е невярна новина*, но ако мнението или свидетелството се представят като истина или факт, това може да се окаже твърде объркващо за читателите. *Слуховете* също могат да се разпространяват в социалните мрежи.

10. Фалшификация и модификация на съдържание. *Фалшификацията* представлява изцяло изфабрикувано съдържание, разпространявано умишлено с цел дезинформация. *Модификацията* е умишлено видоизменено съдържание на статистики, инфографики, снимки или видео. Манипулираните *видеоклипове в YouTube* с известни личности са сред най-често срещаните примери. Терминът „дълбоки фалшификации“

(англ. deepfake) произлиза от *deep learning*, и означава техника, използваща изкуствен интелект за коригиране на видеоклипове с помощта на изкуствени невронни мрежи.

Какви са последствията за националната сигурност

Дезинформацията е мощен инструмент в съвременните хибридни конфликти, използван за подкопаване на стабилността на държави, отслабване на съюзнически структури и предизвикване на вътрешни конфликти. Тя може да има сериозни последствия за националната сигурност, като засяга ключови институции, социални връзки и стратегически решения. Последствията за националната сигурност и отбраната на страната могат да включват:

– подкопаване доверието в армията – чрез разпространение на фалшиви новини за корупция, некомпетентност или провалени мисии;

– създаване на напрежение между военнослужещите – чрез манипулация на информация относно командване, заповеди или условия на служба;

– застрашаване провеждането на операции – чрез разпространение на фалшива информация за разположение на войски или оперативни планове, което може да доведе до объркване и провал[9];

– влияние върху морала и единството – чрез насаждане на съмнения относно значимостта на мисията или ефективността на ръководството.

Освен системата за отбрана, трябва да се има предвид, че дезинформацията е „информационно разстройство“, което засяга тъканта на демократичното общество, като:

– подкопава информираното гражданство – гражданите вземат решения на базата на невярна или манипулирана информация;

– влияе на изборите – манипулация на общественото мнение чрез фалшиви новини, насочени кампании и пропаганда;

– засилва социалното разделение – създава „ехокамери“ и „филтърни балони“, които укрепват съществуващите вярвания и предразсъдъци (Sunstein 2019);

– подтиква към насилие чрез разпалване на етнически, религиозни или политически конфликти;

[9] Политика на НАТО за информационните операции (NATO military policy for information operations).

– уврежда международните отношения чрез насаждане на недоверие между съюзници или създаване на погрешни представи за дадена държава.

Дезинформацията може да засегне не само националните граници, но и международните отношения, като влияе на дипломатическите връзки и икономическите процеси. Примери за това са използването ѝ за манипулиране на пазари, налагане на санкции или провокиране на геополитически конфликти.

Дезинформацията представлява сериозна заплаха за националната сигурност, като влияе върху стабилността на държавата, доверието в институциите и социалната сплотеност. Борбата с това явление изисква координирани усилия на държавно, военно и обществено ниво, както и засилване на информираността и медийната грамотност сред гражданите.

Как се противодейства на дезинформацията?

Противодействието на дезинформацията изисква многоаспектен и адаптивен подход, съчетаващ действия на макониво – чрез стратегически политики и институционален капацитет, и на микониво – чрез изграждане на устойчивост у отделния индивид. Разграничаването между индивидуалното и институционалното равнище на реакция не е само аналитичен подход, а отразява реалната необходимост от синергия между гражданското общество, образователната система и държавните органи. В този контекст следващите теми в настоящия учебник разглеждат основните механизми за противодействие на дезинформацията – съответно на индивидуално и институционално (държавно) ниво. Впоследствие първото упражнение за изграждане на устойчивост срещу дезинформацията изисква от обучаемите да помислят за противодействие на дезинформацията чрез институциите на държавно ниво, а следващите – да работят с индивидуални инструменти.

Противодействие на индивидуално ниво

Противодействието на дезинформацията на индивидуално ниво изисква формиране и поддържане на критична информационна култура и когнитивна устойчивост. Това означава способността на отделния индивид да идентифицира и отхвърля подвеждаща или манипулативна информация чрез развитие на аналитично мислене, медийна грамотност и познания за информационната среда (Bergström & Jervelycke Belfrage 2021).

Изследванията показват, че личната мотивация и когнитивните способности играят ключова роля при разпознаване на дезинформация, но те трябва да бъдат подкрепени с образователни политики, насочени към медийна и дигитална грамотност още от ранна възраст (Lewandowsky et al. 2017). Освен това индивидуалното противодействие включва и прилагането на поведенчески техники, като т.нар. „предварителна инокулация“ (inoculation theory), която цели „ваксиниране“ срещу манипулации чрез предварително излагане на примери за дезинформация (Linden et al. 2017). Не на последно място, етичното поведение в дигиталното пространство също е част от индивидуалната отбрана – критично споделяне на информация, проверка на източниците и активна реакция срещу фалшиви твърдения (Wardle & Derakhshan 2017).

Противодействие на институционално (държавно) ниво

На институционално ниво противодействието на дезинформацията изисква интегрирана и стратегическа реакция, съчетаваща законодателни мерки, междуведомствено сътрудничество, комуникационни стратегии и развитие на капацитети за стратегическа комуникация (Serafimova 2025). Според Европейската служба за външна дейност (ЕСВД), държавите следва да изградят национални механизми за ранно предупреждение, анализ и реакция, които включват както граждански, така и военни институции (EEAS, 2022).

Една от основните държавни функции в тази насока е създаването на капацитет за стратегическа комуникация (StratCom), който не само открива и анализира информационни заплахи, но и формира контраразкази, които защитават демократичните ценности и националната сигурност (Pamment, 2020). Важен елемент е и сътрудничеството с гражданското общество, медии и академични институции с цел създаване на общ фронт срещу враждебни информационни операции (NATO StratCom COE, 2021).

Законодателните инициативи, като засилване на прозрачността на онлайн платформите, борба с фалшиви акаунти и мрежи от ботове, също са част от държавната отбрана срещу дезинформацията. Европейският кодекс за поведение срещу дезинформация от 2022 г. (European Commission 2022) е пример за наднационална регулаторна рамка, която следва да бъде адаптирана и прилагана на национално равнище.

Не на последно място, създаването на национални центрове за борба с хибридни заплахи, включително такива с функции по анализ на когнитивната сигурност и обучение на служители в сферата на сигурността и отбраната, е препоръчителна стъпка в системното изграждане на устойчивост срещу дезинформация.

Отворени въпроси за самоподготовка

● Посочете какви са основните характеристики на дезинформацията и как тя се различава от други форми на информационно разстройство.

● В кои измерения и по кои канали се разпространява дезинформацията?

● Кои са основните фактори, правещи хората и обществата уязвими към дезинформация?

● Кои методи и подходи могат да се използват за разпознаване на дезинформация?

● Посочете основните направления, по които дезинформацията влияе върху националната сигурност.

Глава втора

ЗАКОНОДАТЕЛЕН ПОДХОД ЗА БОРБА С ДЕЗИНФОРМАЦИЯТА

Лекция, която цели обучаемите да се научат да разпознават:

- Медийни норми в Европейския съюз и НАТО, което включва новият регламент НИС-2 и Актът за цифрови услуги DSA.
- Нормативната база, разглеждаща престъпления чрез медиите. Авторско право и защита на авторските права.

През януари 2013 г. бе публикуван доклад от Световния икономически форум посветен на „масова цифрова дезинформация[10]“. Той започва с една интересна история как десетки хиляди американци през 1938 г. са объркали излъчването на радио драмата на Хърбърт Уелс *Войната на световете* с истинско нашествие от Марс. Тогава радиото е било нова информационна среда, чиято сила все още не е напълно разбрана – подобно на днешния интернет (Cantril, Hazel, Herta 1940).

Докладът твърди, че днес цифровата дезинформация не се ограничава само до инциденти, а умишлената измама в интернет е напълно реална заплаха за националната сигурност на държавите. Стигна се до това, че някои държави взаимно се упрекват, че използват информационните технологии за влияние, пропаганда и манипулиране на общественото мнение (Stoykov 2018).

Нормативни документи в Европейския съюз и НАТО

В противодействие на „фалшивите новини“ в Европейския съюз бяха създадени редица инициативи и документи, като *Комюнике за онлайн платформите* (май, 2016)[11], *Кодекс за борба срещу незаконната реч*

[10] *Global Risks 2013*. Достъпно на: https://www.scribd.com/doc/119439721/Global-Risks-2013.

[11] European commission, 2016. *Commission staff working document on Online Platforms*. Достъпно на: https://digital-strategy.ec.europa.eu/en/library/commission-staff-working-document-online-platforms [Последно посетен: 31.05.2025].

на омразата (май, 2016)[12] и *Комюнике за борба с незаконното съдържание онлайн* (септември, 2017)[13] и *Резолюция на Европейския парламент за онлайн платформите и единния дигитален пазар от 15 юни, 2017 г.* (2016/2276(INI))[14]. През 2018 г. излезе комюникето *Онлайн платформи и фалшиви новини*, което представлява продължение на създадената през 2015 г. *East Stratcom Task Force*[15] То предлага проучване на възможностите за обществена намеса, като се спазва принципът на субсидиарност и ангажира заинтересованите страни, а именно платформи, новинарски медии, академични и граждански организации, за да се намерят решения съвместими с принципите за свобода на изразяването и медиен плурализъм, залегнал в *Харта на основните права на ЕС*[16].

Хартата на основните права на ЕС/CELEX_12016P[17] защитава специфичните национални идентичности и конституционни традиции на всички държави, членки на ЕС, както и правата и задълженията, произтичащи от тях. Текстове свързани с борбата с дезинформацията насочват към многообразието на култури и традиции на държавите членки, на тяхната национална идентичност, както и към зачитане на принципа на субсидиарност (децентрализация), отговорност към личните данни (добросъвестна обработка, право на достъп от заинтересованото лице, изискване на поправката на тези данни от него), свобода на мисълта, съвестта и религията, свобода на изразяване на мнение и свобода на информация, плурализъм на медиите, академична свобода, защита на интелектуалната собственост, културно, религиозно, езиково многообразие, право на достъп до документи, принцип на пропорционалност, забрана на злоупотребата с право.

---

[12] European commission, 2016. *European Commission and IT Companies announce Code of Conduct on illegal online hate speech*. [Онлайн]. Достъпно на: https://ec.europa.eu/newsroom/just/items/31811/en. [Последно посетен: 31.05.2025].

[13] European commission, 2017. *Communication on Tackling Illegal Content Online - Towards an enhanced responsibility of online platforms*. [Онлайн]. Достъпно на: https://digital-strategy.ec.europa.eu/en/library/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms. [Последно посетен: 31.05.2025].

[14] European Parliament, 2017. *Resolution of 15 June 2017 on online platforms and the digital single market (2016/2276(INI)*. [Онлайн]. Достъпно на: https://op.europa.eu/en/publication-detail/-/publication/60dea0d9-bb0a-11e8-99ee-01aa75ed71a1/language-en. [Последно посетен: 31.05.2025].

[15] European commission, 2018. Countering Disinformation. Questions and Answers about the East StratCom Task Force. [Онлайн]. Достъпно на: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en. [Последно посетен: 31.05.2025].

[16] ОФИЦИАЛЕН ВЕСТНИК НА ЕС, 26.10.2012 г. Харта на основните права на Европейския съюз (2012/C 326/02).

[17] Пак там.



Фигура 8. Мероприятия, предприети от ЕС за борба с дезинформацията[18]

Европейският съюз и НАТО са разработили комплексна правна рамка за противодействие на дезинформацията, която непрекъснато се актуализира според съвременните предизвикателства. През последните години са въведени няколко ключови регулаторни инструмента, които значително разширяват възможностите за контрол върху разпространението на дезинформация.

Директива[19] относно мрежовата и информационната сигурност (NIS2)

Тя влиза в сила през януари 2023 г. и държавите членки следва да я въведат в националното си законодателство до октомври 2024 г. Основно тя въвежда:

- Разширен обхват на задължените субекти, включващ доставчици на публични електронни съобщителни мрежи или услуги.
- Засилени изисквания за управление на риска в областта на киберсигурността.
- По-строги правила за докладване на инциденти.
- По-ефективен надзор и правоприлагане.

---

[18] European commission, N/A. *Tackling online disinformation*. [Online] https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation.

[19] Директивата, за разлика от Регламента, не налага цялостно и директно прилагане в националното законодателство, а определя набор от цели, които да се постигат от страните членки в определен срок. С други думи, директивата дава повече свобода на страната реципиент относно пътя, по който ще достигне до крайната цел.

Основната цел на тази Европейска директива е да повиши нивото на сигурност на държавите членки след започване на войната между Русия и Украйна. Тя трябва да се прилага директно от държавите членки, без да се налага непременно транспониране в националното законодателство. Държавите членки ще трябва да актуализират законодателството си за прилагане на регламента за борба с дезинформацията и манипулирането на алгоритмите. Това включва използване на независими организации за проверка на факти, както и контрол чрез прозрачност на използваните алгоритми за препоръчване на съдържание.

Директивата е първата законодателна инициатива в областта на киберсигурността сред страните членки, но приложението ѝ се оказва трудно, което води до фрагментиране на различни нива във вътрешния пазар на всяка от държавите. В дългосрочен план Директивата би помогнала за повишаване на нивото на киберсигурност в Европа. Дигиталната трансформация се ускорява след COVID-19, а събитията свързани с киберсигурност стават ежедневна грижа за Европейския съюз.

Акт за цифровите услуги (Digital Services Act – DSA)

Оригиналният текст на Акта за цифровите услуги (Digital Services Act – DSA) е публикуван в Официалния вестник на Европейския съюз като Регламент (ЕС) 2022/2065 от 19 октомври 2022 г.[20] Той представлява фундаментална промяна в регулирането на онлайн платформите в ЕС и въвежда:

– задължения за прозрачност относно модерирането на съдържание;

– механизми за докладване на незаконно съдържание;

– засилена защита на правата на потребителите;

– специфични задължения за много големите онлайн платформи;

– система за одит и оценка на риска.

Актът за цифрови услуги (DSA) предоставя защита на правата на потребителите и бизнеса чрез по-високи изисквания за прозрачност към много големите доставчици на цифрови услуги (социални мрежи и търсачки) и предоставяне на по-достъпни и ефективни канали за разрешаване на извънсъдебни спорове с тях. Прилагането на DSA е поетапно, като всички правни норми на регламента влизат в сила на 17.02.2024 г. До 17.02.2023 г. платформите публикуват статистики за Monthly Active

[20] Регламент (ЕС) 2022/2065 от 19 октомври 2022 година относно единния пазар за цифрови услуги и за изменение на Директива 2000/31/ЕО (Акт за цифровите услуги). [Онлайн]. *Официален вестник на ЕС, L 277*, 27.10.2022, стр. 1 – 102. Достъпно на: https://eur-lex.europa.eu/eli/reg/2022/2065/oj. [Последно посетен: 31.05.2025].

Users (MAUs) – месечни активни потребители. До 17.06.2023 г. Европейската комисия определя задължените субекти на база прозрачни критерии за техния мащаб и влияние на пазара в ЕС.

Посоченият акт засяга големите онлайн платформи, търсачки и социални медии като Google Search, Google Maps, Google Shopping, Google Play, YouTube, Facebook, Instagram, Bing, Amazon Marketplace, Apple App, AliExpress, Pinterest, Snapchat, TikTok, Twitter (x.com), Wikipedia, Zalando и др. онлайн търсачки на съдържание, които се ползват от повече от 10% от населението на ЕС (45 млн. потребителя)[21]. Базовите изисквания в този акт налагат всяка организация да има единна точка за контакт с регулаторите, да се докладва за нарушения и инциденти, като се предоставят разбираеми условия за ползване и прозрачност относно рекламни кампании и решения за модерация.

В допълнителните изисквания се посочва, че следва да се създадат вътрешни звена за съответствие, да се изготвят независими годишни одити и да се изпълнят техните препоръки. Това се осигурява със споделяне на информация с регулаторните органи по DSA, достъп на проверени изследователи до данни и инструменти за идентифициране на системни рискове и възможност за препоръчване на съдържание, което не е базирано на „потребителско профилиране“. Освен това новата нормативна уредба препоръчва да се създаде държавно звено за контрол и електронен регистър за сертифицирани органи за извънсъдебно уреждане на спорове (Информационна система за централизирано изграждане и поддържане на регистри (ИСЦИПР)[22].

Кодекс за поведение във връзка с дезинформацията

Кодексът за поведение във връзка с дезинформацията представлява иновативна рамка за справяне с разпространението на невярна информация, договорена от редица заинтересовани страни. Въведен през 2018 г., и доразвит през 2022 г., кодексът цели признаване съгласно Законодателния акт за цифровите услуги.

---

[21] European commission. DSA: Very large online platforms and search engines. Достъпно на: https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops

[22] Министерство на електронното управление. Разработване и прилагане на Референтна архитектура за оперативна съвместимост (РАОС) и на Информационна система за централизирано изграждане и поддържане на регистри (ИСЦИПР). Достъпно на: https://egov.government.bg/wps/portal/ministry-meu/home/programs.projects/projects-progress/projects-opdu1.

На 13 февруари 2025 г. Комисията и Европейският съвет за цифрови услуги официално одобриха включването на Кодекса за поведение във връзка с дезинформацията в законодателния акт за цифровите услуги. Той е първият инструмент от този вид, чрез който заинтересованите участници в сектора се споразумяха и приеха стандарти за саморегулиране с цел борба срещу дезинформацията. Кодексът е ключова част от стратегията на ЕС за борба с дезинформацията и вече се е доказал като ефективен инструмент за ограничаване на разпространението на невярна информация онлайн, включително по време на избори и кризи. Кодексът за поведение съдържа 44 ангажимента и 128 специфични мерки свързани с демонетизацията и намаляване на финансовите стимули за разпространителите на дезинформация[23].

В практиката са известни редица случаи на кражба на персонална идентичност с цел дезинформация в социалните мрежи, най-вече свързани с отговорни държавни институции и политически фигури и разпространение на мнения или новини с потенциален или реален катастрофален ефект. Например през 2017 г. във Facebook съществуваха цели 30 000 акаунта, разпространяващи дезинформация по отношение на френските президентски избори. Освен това според изследванията почти 30% от видимото съдържание в интернет се създава от автоматизирани ботове и тролове.

По тези причини европейската правна рамка определя няколко норми за противодействие на престъпления, свързани с медийното съдържание:

– разпространение на дезинформация, застрашаваща националната сигурност;

– нарушаване на личните данни и неприкосновеността на личния живот;

– клевета и разпространение на неверни твърдения;

– подбуждане към омраза и дискриминация.

Допълнителни международни инструменти са: Кодексът за поведение – доброволен документ на ЕС относно дезинформацията, подписан от големите технологични компании и предвиждащ затваряне на фалшиви акаунти, маркиране на политическа реклама, намаляване на видимостта на дезинформацията, подкрепа за независима проверка на факти,

[23] European commission, 2022. *2022 Strengthened Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

и Планът на ЕС за действие срещу дезинформацията, който се опира на четири стълба[24]:

– подобряване способността на институциите да открият и анализират дезинформация;

– укрепване на координираните и съвместни действия;

– мобилизиране на частния сектор;

– повишаване на осведомеността и устойчивостта на обществото.

Нормативната уредба за борба с дезинформацията представлява динамична система от правила и механизми, която непрекъснато се развива. Успешното противодействие на дезинформацията изисква координирани усилия на национално и международно ниво, както и активно участие на всички заинтересовани страни - от държавните институции до медиите и гражданското общество.

Международни споразумения и конвенции в областта на интернет правото

Бернска конвенция за защита на литературни и художествени произведения от 1886 г. Конвенцията е първият значим международен акт в областта на авторското право. Администрира се от Световната организация по интелектуална собственост (СОИС). Документът установява минимално ниво на защита на авторското право, което държавите, членки по Конвенцията, са длъжни да предоставят на автора през целия му живот от момента на създаване на произведението и 50 години след неговата смърт. Обектите, специфични за информационната революция в края на XX век и интернет, също попадат под неговото действие (Tsakova 2014).

Международна конвенция за авторското право – Женевска конвенция. Подписана е през 1952 г., а действащата редакция на Конвенцията е от 1971г. в Париж. Тя представлява алтернативна възможност на Бернската конвенция с не толкова строги изисквания и е под ръководството на ЮНЕСКО. Минималният срок на защита на авторските права е 25 г. след смъртта на автора.

Договор на Световната организация за интелектуална собственост – СОИС, в областта на авторското право (ДАП). Договорът е приет през 1996 г. в Женева и допълва международните споразумения в областта на авторското право и основно Бернската конвенция. Договорът

[24] *План за действие за борба с дезинформацията, 2018.* https://www.eeas.europa.eu/sites/default/files/disinformation_factsheet_bg.pdf

се появява поради бързото развитие на дигиталните технологии и интернет. За първи път се предвижда защита на компютърните програми и на базите данни.

Споразумението за търговските аспекти на правото на интелектуална собственост – TRIPS (ТРИПС) е прието през 1994 г. и се отнася не само за авторските права, а и за търговските марки, патентните и други права, свързани с интелектуалната собственост. ТРИПС признава, че компютърните програми са литературни произведения, които трябва да бъдат защитени от Бернската конвенция. Споразумението също установява минимални стандарти в областта на защитата на интелектуалната собственост със съответните мерки за защита (Tsakova 2014).

Право на ЕС в областта на закрилата на авторското право в интернет

Директива на Съвета 91/250/ЕИО относно правната защита на компютърните програми. Защитата се прилага към всяка форма на компютърна програма, но не и към идеите, заложени в нея. Компютърните програми се защитават 50 години след смъртта на техния автор, когато той е физическо лице, и 50 години след като програмата е станала достояние на публиката, ако автор е юридическо лице.

Директива на Съвета 96/9/ЕО на Европейския парламент и Съвета за правна закрила на базите данни. Директивата дефинира „бази данни“ като съвкупност от литературни, художествени, музикални и други сбирки от произведения или сбирки от други материали, като текстове, звуци, изображения, цифри, факти и данни. Създават се и правила за защита на базите данни, които не са под опеката на авторското право. Директивата защитава базите данни от нелоялно използване за период от 15 години.

Директива 2001/29/ЕС на Европейския парламент и Съвета за хармонизиране на някои аспекти на авторското право и сродните права в информационното общество. Чрез нея на практика ЕС се присъединява към Договора на Световната организация за интелектуална собственост в областта на авторското право (ДАП) (Tsakova 2014).

Закон за авторското право в цифровата епоха – САЩ

Този нормативен акт е познат като Закон за авторските права в дигиталното хилядолетие (Digital Millenium Copyright Act – DCMA). Той

отива значително напред и повишава отговорността за нарушаване на авторски права в интернет и в същото време защитава информационните посредници от отговорност за действията на потребителите. Законът разглежда две форми на технологична защита – неоторизиран достъп и взлом на защитата от копиране. Предвижда и предварителна регистрация с депониране на екземпляр в US Copyright Office към библиотеката на Конгреса на САЩ. Регистрацията дава редица преимущества и преди всичко обезпечава доказателствата при евентуален бъдещ иск. DCMA изключва регистрацията на чуждестранни обекти на авторското право (Tsakova 2014).

Българско законодателство, свързано с борбата срещу дезинформацията

В България няма специализиран закон, насочен изцяло към борбата с дезинформацията. Съществуват обаче нормативни актове и инициативи, които частично адресират този проблем чрез регулиране на медийната среда, защита на личните данни и електронните съобщения.

Закон за радиото и телевизията (ЗРТ) – регулира дейността на радио- и телевизионните оператори в България. Въпреки че в Закона не се използва терминът „дезинформация“, той съдържа разпоредби насочени към гарантиране на достоверността и обективността на медийното съдържание. Например чл. 10, ал. 1, т. 6 постановява, че доставчиците на медийни услуги са длъжни да „предоставят обективна информация и да не допускат предавания, които подбуждат към насилие или омраза“.

Закон за електронните съобщения (ЗЕС) – през 2023 г. беше предложен законопроект за изменение и допълнение на ЗЕС, който включва мерки за предотвратяване на дезинформация в интернет средата. Чрез тях се предвижда надзор за предотвратяване на дезинформация в интернет пространството.

Закон за защита на личните данни (ЗЗЛД) – регулира обработването на лични данни и е съобразен с Общия регламент за защита на данните (GDPR) на ЕС. В контекста на дезинформацията законът предоставя механизми за защита на физическите лица от неправомерно разпространение на лична информация, което може да бъде използвано за манипулация или разпространение на невярна информация.

Инициативи и предложения за законодателни промени – през 2023 г. коалицията „Продължаваме Промяната – Демократична България“ предложи законопроект, насочен към борбата с дезинформацията и неавтентичното поведение в социалните мрежи. Предложението включва

мерки за превенция на дезинформацията чрез изменения в Закона за електронните съобщения.

Етичен кодекс на българските медии

В борбата срещу дезинформацията основополагащо значение има етичният ангажимент на медиите да предоставят на обществото точна и проверена информация. В този контекст Етичният кодекс на българските медии съдържа конкретни принципи и добри практики, насочени към гарантиране на достоверност и обективност. В него се казва, че медиите трябва да предоставят винаги достоверна информация на обществото.

Точността е основен стандарт в журналистическата дейност и важен инструмент в противодействието на дезинформацията. Медийните организации и журналистите са задължени да предоставят на обществото проверена информация без преднамерено изопачаване или укриване на факти. Те не трябва да разпространяват данни, за които е известно, че са неверни и следва да избягват подвеждащи материали, като ясно обозначават манипулирани текстове, документи, образи или звукови записи. Фактите трябва да бъдат ясно разграничени от коментарите и предположенията. Анализите и коментарите трябва да представят различни гледни точки с цел обективност. При отразяване на спорове е необходимо да се предостави възможност на засегнатите страни да изразят своята позиция.

Поправката на неточности е друг важен аспект на професионалната журналистика и отговорно отношение към публикуваната информация. В случай на неточност медиите трябва да публикуват своевременна и видима корекция, когато се докаже, че дадена информация е била неточна или подвеждаща. При необходимост следва да поднесат извинение за разпространяване на грешна информация. Също така трябва да се предоставя право на отговор на лица и организации, засегнати от неточни или подвеждащи публикации.

Източниците на информация също са разгледани в кодекса. Правилното посочване и проверка на източниците е критично за предотвратяване на дезинформацията. Медиите трябва да проверяват достоверността на информацията чрез различни източници преди публикуването ѝ. Където е възможно, те следва да посочват произхода на информацията, за да осигурят прозрачност. Добре е да бъдат предпочетени идентифицирани източници пред анонимни, тъй като последните затрудняват обществото да прецени тяхната надеждност. Поверителните източници трябва да бъдат защитени, когато това е необходимо. Всяка непотвърдена ин-

формация следва да бъде ясно обозначена, за да се избегне разпространението на потенциално подвеждащи данни. Спазването на тези принципи е от съществено значение за укрепване на медийната среда и ефективно противодействие на дезинформацията в обществото.

Българското законодателство също определя редица норми, сред които най-съществен е Законът за защита на авторските права, който може да се използва в борбата с фалшивите новини и дезинформацията.

Директива 2019/790 относно авторското право в цифровия единен пазар въвежда:

– нови правила за използване на защитено съдържание от онлайн платформи;

– механизми за справедливо възнаграждение на създателите на съдържание;

– изключения за текст и извличане на данни за научни изследвания;

Законът за рекламата също въвежда редица забрани, които позволяват сваляне на сайтове от Държавната комисия по хазарта.

За да бъде една творба под закрилата на авторското право, тя трябва да е оригинално творение. Оригиналността се отнася както до съдържанието, така и до формата. За създателя на интелектуална творба авторското право в основата си е правото да се уважава неговата творба и правото на печалба от нея, като се събират доходите, получени от използването на творческото усилие на автора. Идеята за закрила на авторското право възниква едва с появата на печатарската техника, която дава възможност за копиране на литературни творби чрез механични процеси вместо преписването им на ръка.

Инструментите срещу плагиатство като средство за повишаване на информационната грамотност и противодействие на дезинформацията

Разбирането и прилагането на инструменти за откриване на плагиатство все повече се утвърждава като ключово умение в борбата срещу дезинформацията. Тези софтуерни решения не само откриват съвпадения с други източници, но и насърчават култура на академична и информационна етика. Чрез сравнение с обширни бази данни от академични трудове, уеб страници и публикации системите генерират доклади, които подчертават сходства и евентуални неправомерни заимствания (Bretag & Mahmud 2009). От гледна точка на противодействието на дезинформаци-

ята тези технологии имат важно образователно измерение. Когато студентите използват подобни инструменти, те развиват умения за критично мислене, усвояват принципите на етичното използване на източници и научават как да избягват неволно възпроизвеждане на фалшива или манипулирана информация (Sutherland-Smith 2010).

Способността да се интерпретират правилно докладите на софтуера против плагиатство е ключова за успешното им прилагане. Не всеки маркиран текст е доказателство за плагиатство – необходима е преценка основана на контекст, разбиране на цитирането и коректната употреба на източници (Howard 2007). Това изисква обучение както на преподаватели, така и на обучаеми, тъй като грамотността в работата с информация е важна предпоставка за устойчивост срещу дезинформация.

Софтуерите срещу плагиатство стимулират и усвояването на умения за ефективно търсене, оценка и проверка на информация – ключови елементи от информационната грамотност (Purdy 2009). Вместо да се използват предимно като инструмент за санкции, тези системи трябва да се разглеждат като част от по-широк подход към етичното използване на информация, спазването на авторското право и изграждането на академична почтеност.

Технологичното развитие доведе до усъвършенствани системи, които вече се интегрират с платформи за дистанционно обучение и поддържат множество езици – критичен фактор в глобалния обмен на информация. Това подчертава необходимостта преподавателите да поддържат дигитална компетентност и да бъдат подготвени да обучават в условия на информационен натиск и дезинформация (Scanlon & Neumann 2002). Следователно използването на инструменти за проверка на оригиналността следва да бъде интегрирано в стратегиите за противодействие на дезинформацията, тъй като допринася за изграждането на етично, информирано и критично мислещо общество.

Етични последици от въвеждането на изкуствения интелект в контекста на борбата с дезинформацията

Развитието на изкуствения интелект (ИИ) променя из основи дигиталната среда, включително образованието, комуникацията и медийното потребление. Докато AI инструментите като ChatGPT, алгоритми за анализ на съдържание и автоматични системи за откриване на фалшиви новини предлагат значителен потенциал в борбата с дезинформацията, те също така поставят редица етични въпроси, свързани с поверителност, пристрастия и отговорност (Georgiev 2022).

Пристрастия и увековечаване на неравенствата. Алгоритмите на изкуствения интелект се обучават върху големи масиви от данни, които често отразяват съществуващи социални предразсъдъци. В контекста на дезинформацията това означава, че AI системите могат неволно да поддържат или дори да засилят определени наративи, които обслужват пропагандни или манипулативни интереси (O'Neil 2016). Необходими са прозрачност и механизми за проверка, за да се гарантира, че използваните AI системи идентифицират манипулации, а не ги възпроизвеждат.

Поверителност и събиране на чувствителна информация. Системите, предназначени за откриване на дезинформация, често обработват огромни количества данни от социални медии, форуми и комуникационни платформи. Тази дейност повдига въпроси относно правото на лична неприкосновеност и възможността за злоупотреба с чувствителна информация (Zuboff 2019). Спазването на етични стандарти при събирането и анализирането на данни е от ключово значение за поддържане на общественото доверие.

Надеждност на решенията, взети от AI. Използването на автоматизирани инструменти за категоризация на съдържание като „фалшива новина“ трябва да бъде внимателно обмислено. Прекаленото разчитане на ИИ в тази сфера може да доведе до „фалшиви положителни“ или „фалшиви отрицателни“ резултати, с потенциално сериозни последици – включително цензура или неправомерно блокиране на легитимна информация (Biesta 2013).

Рискове за академичната и информационната почтеност. Технологиите с ИИ се използват все по-често в образователната сфера, включително и за създаване на съдържание. Това поражда нови етични предизвикателства – като възможността за злоупотреба чрез плагиатство или манипулация. Преподавателите са изправени пред необходимостта да обучават учащите не просто в ползването на тези технологии, но и в критичната им оценка и отговорно използване (Scanlon & Neumann 2002).

Баланс между автоматизация и човешка преценка. AI системите не притежават емпатия, културен контекст или морална отговорност. Затова е важно да не се подценява ролята на човешкия фактор при анализ и верификация на информация, особено в ситуации, където решенията могат да повлияят върху репутации или обществени нагласи.

Изкуственият интелект може да бъде мощен съюзник в борбата срещу дезинформацията, но неговото използване трябва да бъде придружено от ясни етични насоки, правна рамка и обществен контрол. Внедряването на AI в този контекст изисква балансиран подход, който съчетава технологична ефективност с уважение към правата, свободите и достойнството на индивида.

Отворени въпроси за самоподготовка

● Кога влиза в сила Директивата NIS-2 и какъв е крайният срок за въвеждането ѝ в националното законодателство на държавите членки?

● Кои са основните елементи на Акта за цифровите услуги?

● Кои са четирите стълба на Плана за действие на ЕС срещу дезинформацията?

● Какво въвежда Директива 2019/790 относно авторското право в цифровия единен пазар?

● Избройте международни споразумения и конвенции в областта на интернет правото.

● Какви са етичните последици от ползване на изкуствен интелект в образованието?

Глава трета

КРИТИЧНО МИСЛЕНЕ И РАЗВИТИЕ НА АНАЛИТИЧНИТЕ УМЕНИЯ

- Развитие на уменията за критично мислене на обучаемите.
- Дава основни понятия за дигитална грамотност и анализ в сферата на дезинформацията.

Информационната среда в съвременния свят изисква задълбочен критичен анализ и систематична оценка, особено в контекста на нарастващите предизвикателства, свързани с дезинформацията. Способността за критично мислене и анализ се превръща в ключова компетентност за навигация в сложния информационен пейзаж.

Основи на критичното мислене

Критичното мислене е *интелектуално дисциплиниран процес на активно и умело концептуализиране, анализиране, синтезиране и оценяване на информация, която е събрана чрез наблюдение, опит, размисъл, разсъждение или комуникация* (Paul, Elder 2006). То е ключово умение в борбата с дезинформацията, което дава възможност на хората да оценяват истинността на информацията и да разбират мотивите зад нейното разпространение.

Според Пол и Елдър критичното мислене е процес на систематична и обективна оценка на информацията. Основните му елементи включват:

– анализ на източници – обучение за оценка на надеждността на източниците чрез анализ на техния авторитет, мотивация и контекст;

– проверка на факти – насърчаване на култура на проверка на фактологичната точност преди споделяне на информация;

– разпознаване на когнитивни предразсъдъци – идентифициране на често срещани когнитивни грешки, като потвърждаващо пристрастие и ефект на авторитета.

Левандовски и съавторите му (Lewandowsky et al. 2012) подчертават значението на специфични когнитивни умения за критичното мислене:

– метакогнитивна осведоменост – способността да се наблюдават и оценяват собствените мисловни процеси;

– разпознаване на манипулативни техники – идентифициране на техники като подвеждащи генерализации и емоционални апели;

– анализ на аргументативни структури – изследване на логиката и последователността на даден аргумент.

Развиване на критичното мислене и аналитичните умения

Развитието на критично мислене изисква теоретични знания и практически упражнения, които могат да се опишат с три основни стъпки:

а) Систематичен анализ на източниците.

- Оценка на авторитет и експертиза.
- Проверка на актуалност и релевантност.
- Анализ на методология и данни.
- Проследяване на цитирания и референции.

б) Оценка на достоверността.

- Триангулация на информацията чрез сравнение на множество независими източници.
- Проверка на фактологична точност.
- Идентифициране на противоречия и анализ на контекста.

в) Разпознаване на логически грешки.

- Разкриване на Ad hominem аргументи.
- Идентифициране на фалшиви дихотомии и причинно-следствени заблуди.

Критичното мислене е основен компонент в изграждането на когнитивна устойчивост срещу дезинформация, като същевременно подпомага развитието на креативността и аналитичните умения. Това изисква интегриране на структурирани теоретични знания и практически упражнения в ежедневната подготовка както на военнослужещи, така и на гражданското население.

Уайнбърг и МакГрю (Wineburg & McGrew 2019) предлагат *рамка за развиване на аналитични умения:*

- Латерално четене.
- Проследяване на произход на информация.
- Сравнителен анализ на източници.

● Контекстуализация на съдържание

Критичното мислене е способността да се анализира информацията обективно, да се оценяват доказателствата и да се вземат информирани решения. То включва умения за логически анализ, разпознаване на когнитивни предразсъдъци и изграждане на аргументирани заключения. Основни елементи на критичното мислене са:

– анализ на източници – обучение за оценка на надеждността на източниците, като се вземат предвид техният авторитет, мотивация и контекст;

– разпознаване на когнитивни предразсъдъци – насочване на вниманието към често срещани когнитивни грешки, като потвърждаващо пристрастие (confirmation bias) или ефект на авторитета;

– проверка на факти – насърчаване на култура на проверка на факти преди споделяне на информация.

Критичното мислене може да се въвежда в обучението чрез провеждане на дискусии по актуални теми, при които участниците трябва да представят аргументи и да анализират противоположни гледни точки. Главните бариери за критичното мислене са инстинктивното егоцентрично и социоцентрично мислене на хората в т.ч. и военнослужещите. Егоцентричното мислене е емоционално наситено. Когато се усеща неуспех възникват защитните механизми – арогантност, апатия, отчуждение, индивидуализъм, негодувание, депресия, гняв, раздразнителност. Социоцентричното мислене възприема предразсъдъците на нацията, общността, племето, религията или групата с техните вярвания, обичаи и принципи и се поставя над всички и всичко. Критичното мислене не допуска наличието на групов егоизъм, външен контрол и предпоставено подчинение.

Друга важна способност е развитието на креативността на обучавания. Тя води до принуждаване на ума да поеме по нов път, като открива нови невронни връзки:

$$C = f(K, I, E), \tag{1}$$

където креативността (C) е функция (f) на знанието (K – knowledge), въображението (I – imagination) и оценката (E – evaluation) при разглеждане на определена идея или ситуация.

За да бъдат ефективни, образователните инициативи трябва да интегрират медийната грамотност и критичното мислене в ежедневната подготовка на военнослужещите и гражданското население. За тази цел следва да се разработят учебни материали и курсове, които включват теоретични знания и практически упражнения за медийна грамотност и

критично мислене. Най-важните стъпки, които следва да предприемем за подобряване на критичното мислене, са следните:

– стъпка 1 – да разберем, че умовете ни са податливи;

– стъпка 2 – да разберем, че това включва и нашия собствен ум;

– стъпка 3 – да разберем последствията от стъпка 2;

– стъпка 4 да помогнем на другите да стигнат до стъпки 1 и 2.

Критичното мислене не е нещо, с което се раждаме, а е умение, което можем да развиваме през целия си живот. Ето няколко действия, които можем да предприемем за тази цел:

● Задаване на въпроси – винаги задавайте въпроси, когато се сблъскате с нова информация или проблем. Питайте се какво знаете за ситуацията, какво искате да научите още и какви са възможните решения.

● Проучване на различни гледни точки – търсете различни източници на информация и анализирайте различните гледни точки по даден въпрос. Не се задоволявайте с първоначалната информация, която сте получили.

● Оценка на доказателствата – проверявайте доказателствата и аргументите, които поддържат определено твърдение. Внимателно изследвайте техните източници и съответствие с научните факти.

● Упражняване на логика – практикувайте логическите стъпки при анализирането на проблеми и намирането на решения. Обучавайте се да правите заключения на базата на факти и логика, а не на емоции.

● Учене от грешки – не се страхувайте да признавате своите грешки и да се коригирате. Осъзнаването на грешки и поучаването от тях е важна част от процеса на развиване на критичното мислене.

● Практикуване на дебат – участието в дебати или обсъждания с други хора развива нашата способност да изслушваме и анализираме различни мнения. Това насърчава критичното мислене, като се изисква да намираме аргументи и факти, които да подкрепят нашите позиции.

● Разрешаване на проблеми чрез реални ситуации – поставяйте себе си в реални ситуации и предизвикателства, които изискват решения. Например как бихте реагирали на конфликтна ситуация на работното място или как бихте се справили със сложна етична дилема.

● Четене и изследване на различни теми – чрез четене на разнообразни книги, статии и научни изследвания разширяваме нашия обзор и се научаваме да разглеждаме проблемите от различни гледни точки.

● Използване на мисловни карти (mind maps) – създаването на мисловни карти е отличен начин да визуализираме и организираме информацията. Това ни помага да обединим фактите и идеите и да създадем по-ясна картина на проблемите.

Методи за въздействие върху вземането на решения

В природата на човека е заложено вярването, че винаги взима най-логичните решения във всяка нормална ситуация. Дори когато след това се окаже, че решението не е правилно, обикновено вместо да признаем грешката си, започваме да търсим причини във външни фактори, промяна на обстановката, лошо стечение на обстоятелствата и други оправдания извън нас.

През 1972 г. учените Даниел Канеман (Daniel Kahneman) и Амос Тверски (Amos Tversky) въвеждат понятието когнитивни пристрастия (cognitive biases). Това е свойство на човешкия мозък да се влияе при вземането на решения от малки и незначителни на пръв поглед обстоятелства, като това обикновено се случва на подсъзнателно ниво. Когнитивните пристрастия (склонности) са систематични грешки в мисленето, възникващи когато хората обработват и интерпретират информация за света около тях. Те засягат решенията и преценките им. Тази способност (или недостатък) на човешкия мозък се изучава и използва от специалистите по маркетинг, за да насочат потенциалния клиент да вземе „правилното решение“ и да закупи съответния продукт, т.е. да повлияят на неговото мислене и поведение. Подобни цели се преследват и с разпространяването на дезинформация и фалшиви новини, което означава, че може да се използват същите подходи. Затова е важно да ги познаваме и да не им се поддаваме.

Страх от загуба (Loss Aversion)

Хората предпочитат да не загубят нещо, което вече имат, спрямо това да опитат да спечелят нещо с еквивалентна стойност. С други думи, за повечето хора би било по-неприятно да загубят 100 лева, отколкото да пропуснат възможността да спечелят същата стойност. Това явление се нарича loss aversion и е част от човешката ни природа. В маркетинга то се прилага, като се предлага безплатно дадена стока или услуга, безплатна мостра, сериозна отстъпка от цената, безплатен период за ползване или различни варианти на посочените. В този случай получателят няма финансови ангажименти, но вероятността да се привърже към продукта и след това да не желаете да се разделите с него е голяма. Това съответно означава, че ще трябва да го закупи, което е и целта на другата страна. Бъдете внимателни когато ви предлагат стоки, услуги и информация безплатно!

Бонус за ограничен период (Limited Time Bonus)

Това е продължение на предишния метод за влияние върху решенията на човека. Към основния продукт се предлагат безплатно още един или няколко допълнителни продукта, но само ако го бъде закупен в момента. Ако не го направите, ще останете с неприятното чувство, че сте изпуснали невероятно предложение. Обикновено бонусите са примамливи, но ненужни, непотребни и стойността им е незначителна в сравнение с основния продукт.

Таймер с обратно броене (Countdown Timer)

Таймерът с обратно броене засилва чувството за спешност и задейства принципа за недостиг. След изтичане на времето потребителят никога повече няма да може да се сдобиете с този продукт или поне не на толкова изгодна цена. Като пример за прилагането на метода може да бъде отброяване на време за безплатна регистрация на потребители в сайт, след което регистрацията ще става само срещу заплащане. Обикновено целта е събиране на информация (имейли) за последващо изпращане на различни оферти, послания и друга информация.

Пристрастието към недостига (The Scarcity Bias)

В този случай вместо от време потребителят е притиснат от ограниченото количество на продукта. Останали са само няколко последни бройки от него и сте на път да изпуснете тази изгодна оферта, затова внушението е да побързате.

Голямо търсене (Big Demand)

В сладкарница ви предлагат да опитате два вида бисквити. Едната тава е препълнена, а в другата са останали само няколко бройки, като според служителите причината за това е голямото търсене на втория вид. Вие опитвате от двата вида и установявате, че втория вид наистина са похубави, въпреки че в действителност са едни и същи. Добре е да се вслушвате в мнението и съветите на другите, но да вземате обективно и безпристрастно решение.

Социално доказателство (Social Proof)

Още Аристотел е казал, че „Човекът е социално животно“. Хората открито или скрито се сравняват един с друг, искат да бъдат харесвани и приемани от обществото и се влияят от мнението на болшинството. Терминът „социално доказателство“ е въведен през 1984 г. от Робърт Чалдини (Cialdini 2008) и е психологически и социален феномен, при който хората копират действията на другите, когато реагират в дадена ситуация. След като всички в обществото правят нещо (купуват даден продукт, ползват определена услуга, имат акаунт в популярен сайт), значи аз трябва да правя същото, за да не изглеждам асоциален, старомоден или отритнат от обществото. Критичното мислене изисква да се съобразяваме се с общественото мнение, но да взимаме решения на базата на нашите собствени интереси.

Отворени въпроси за самоподготовка

- Избройте техники за критичен анализ на публикувана новина в социалните медии.
- Как алгоритмите на социалните медии влияят върху разпространението на дезинформацията?
- Анализирайте как съвременните технологии могат едновременно да улеснят разпространението на дезинформация и да помогнат за противодействие срещу нея.

Глава четвърта

МЕДИЙНА ГРАМОТНОСТ И АНАЛИЗ НА ИНФОРМАЦИЯТА ОТ СОЦИАЛНИТЕ МЕДИИ

❖ Лекцията навлиза в полето на медийната грамотност, необходима за борба с дезинформацията.

❖ Разглежда се влиянието на социалните мрежи и начините за техния анализ.

България е най-уязвима по отношение на дезинформацията сред държавите от ЕС, заключават авторите на проучването Индекс за медийната грамотност (2022)[25]. Причините за ниската медийна грамотност са лошото качество на образованието, състоянието на медиите (конкретно медийната свобода) и ниското междуличностно доверие.

Какво представлява медийната грамотност

През 2011 година UNESCO издава ръководство за медийна грамотност за учители Media and Information Literacy Curriculum for Teachers[26], в което понятията медийна и информационна грамотност (MIL) са определени като общ комплекс от взаимносвързани дисциплини. Според Ръководството притежаването на тези знания и умения позволява на хората да оценяват медиите като източници на информация и по този начин да опознават света, да вземат информирани решения, да се чувстват членове на обществото и да имат възможност да учат през целия си живот. Медийната грамотност е дефинирана като самостоятелно понятие, включващо следните елементи:

[25] Lessenski, M. 2022. *How It Started, How It is Going: Media Literacy Index 2022*. София: Институт „Отворено общество“. [Онлайн]. Достъпно на: https://osis.bg/wp-content/uploads/2022/10/HowItStarted_MediaLiteracyIndex2022_ENG_.pdf [Последно посетен: 31.05.2025].

[26] Media and information literacy curriculum for teachers. [online] Available from: https://unesdoc.unesco.org/ark:/48223/pf0000192971.

– място, роля и функции на медиите като източници на информация;

– необходими условия, при които медиите могат пълноценно да изпълняват тези функции;

– критично отношение към предоставяната от медиите информация;

– двупосочно взаимодействие между гражданите и медиите;

– развиване на умения за създаване на потребителско съдържание.

Документът разширява и допълва рамката с компетентности, като включва в нея още понятия като библиотечна, новинарска, филмова, телевизионна, игрова и рекламна грамотност. Всички те изграждат единна структура на медийната и информационната грамотност.

В контекста на дигиталните компетентности информационната грамотност (Information literacy) е по-общо понятие и означава притежаването на знания и умения за търсене, намиране и обработка на информация чрез електронни устройства. Медийната грамотност (Media literacy) са знанията и уменията за достъп и анализ на медийни съобщения, както и за създаването им.

Съществуват множество определения за медийна грамотност, но няма официално дефинирано понятие (Игнатов, 2024). В повечето от изследваните източници в тази връзка се откриват няколко основни теми, които в един или друг вид присъстват в тях, а именно:

– възможността медиите да имат негативно влияние върху отделната личност, групи или обществото като цяло;

– хората с висока медийна грамотност са по-защитени от потенциалното негативното влияние на медиите;

– медийната грамотност се придобива и развива чрез обучение, като този процес е непрекъснат;

– съществува минимален набор от знания, но няма горна граница;

– високата медийната грамотност изисква притежаването на широк спектър от когнитивни, аналитични, емоционални, естетически, морални и множество други умения;

– в основата на медийната грамотност стоят уменията за изследване, анализ и оценка на информацията и нейните източници по системен начин.

Медийната грамотност позволява увереното извършване на дейности, без които е невъзможно да се живее пълноценно в съвременното информационно общество. Тези дейности включват:

– търсене и намиране на информация от множество източници;

– анализ и оценка на получената информация и медийните послания;

– критичен поглед върху достоверността на информацията и нейните източници;

– правилно разбиране на явните и скритите послания в медийните съобщения;

– познаване и установяване наличието на опити за заблуждаване, манипулиране и измами чрез медийните съобщения.

Медийната грамотност е многокомпонентно понятие, но три елемента имат най-голяма тежест при работа с медии и медийна информация. Първият от тези компоненти е личният фокус, което се явява нашата връзка с медийното съобщение. Личния фокус е причината да търсим тази информация и включва нашите интереси, предпочитания и ценностна система. Търсенето на информация е свързано със задоволяване на нашите потребности в дадена област, където имаме професионални, лични или други интереси. Познанията в определена област ни дават възможност да открием и разберем медийното съобщение, докато в друга сфера е възможно това да не се случи.

Вторият основен компонент са моделите на възприемане на информацията. Това е начинът на интерпретиране на получената информация на базата на знанията и опита, които притежаваме. Вероятността за неправилна интерпретация на информация в позната за нас област е помалка, отколкото в такава, в която нямаме необходимите знания.

Третият компонент са нашите практически умения за работа и създаване на медийно съдържание. В тях влизат основни умения като четене, писане, критично мислене, анализ, синтез, оценка и др. Познаването на информационните системи, приложенията, които ползваме, техните характеристики, функции и възможности допълват набора от практически умения.

Високата информационна и медийна грамотност ни позволява да се ориентираме правилно в огромния поток от информация около нас. Медийната грамотност е предпоставка за намиране на вярната информация, на базата на която да вземем правилните решения. Тя ни помага да се справяме ежедневно с информационни проблеми от различни естество, като например:

– разпознаване на фалшиви новини;

– опити за манипулация чрез медийни съобщения;

– винаги да се търсят други алтернативни източници, чрез които да потвърдим или опровергаем дадената информация;

– отговорност при създаване, разпространение и споделяне на информация;

– умения за анализ на статистически данни;

– умения за медийна хигиена и дигитална безопасност;

– участие в обществения живот;
– обучение и образование.

Медийната грамотност като основно средство за борба с дезинформацията

Според ЮНЕСКО медийната грамотност представлява *набор от умения, които позволяват на хората да получават достъп, анализират критично, оценяват и създават медийно съдържание във всички формати.*[27]

Основни нейни компоненти са:

– способност за анализ на медийни съобщения

– разбиране на методите за създаване и разпространение на информация;

– оценка на достоверността на източниците;

– разпознаване на манипулативни техники.

Видно е, че медийната грамотност се простира отвъд традиционното разбиране за способност за четене и писане. Тя включва цялостен набор от умения, които позволяват на хората да анализират, оценяват и създават медии във всички форми. Поради тази причина се превръща в основно оръжие срещу дезинформацията и помага в разбирането как са изградени медийните съобщения, на какви цели служат и как влияят на аудиторията. По тези причини първо ще разгледаме жизнения цикъл на дезинформацията, за да се запознаем със съвременните предизвикателства и инструментите, с които тя се разпространява в медиите.

Жизненият цикъл на дезинформацията се разбира като последователност от етапи, които водят до умишлено разпространение на невярна или подвеждаща информация. Този процес обикновено започва със създаването или фабрикуването на дезинформация, последвано от нейното разпространение, разширяване и в крайна сметка приемането или вярата в нея от обществеността, което може да има значително социално и политическо въздействие.

● Първият етап, на създаване, често произтича от различни мотиви, като политическа печалба, финансова печалба или социално влияние. По време на този етап актьорите, независимо дали са спонсорирани от държавата, групи или отделни лица, създават послания, които имат за цел да заблудят или манипулират публиката. Например проучването на

[27] ЮНЕСКО, 2021. [Online]. *Media and Information Literacy Curriculum for Educators and Learners.* Available from: https://www.unesco.org/mil4teachers/en/curriculum.

Бенет и Ливингстън (Bennett, Livingston 2018) относно реда за дезинформация изследва как държавните актьори използват стратегическата комуникация, за да създават разкази, служещи на техните интереси, като създават ехо камери, които могат да повлияят както на вътрешните, така и на международните възприятия.

● На второ място, разпространението на дезинформация става по множество канали, избрани според типа на целевата аудитория.

● Следващият етап на усилване настъпва, когато дезинформацията придобие сила и видимост. Тук известни личности, ботове или ехо камери могат допълнително да разпространяват лъжите, като им придават вид на легитимност или достоверност. Това е мястото, където концепцията за „фалшиви новини“ може да заживее свой собствен живот.

● Последният етап на приемане включва публиката, която я приема в своите системи от вярвания. Както показват изследванията на Найън и Райфлър (Nyhan, Reifler 2010), след като се повярва на дезинформация, тя може да бъде невероятно устойчива на корекция, дори когато е представена с фактическа информация.

По време на всеки етап от този жизнен цикъл има възможности за намеса за предотвратяване на разпространението или смекчаване на въздействието на дезинформацията. Тези интервенции могат да включват обучение за дигитална грамотност, механизми за проверка на фактите и промени в политиките на платформите на социалните медии, за да се намали разпространението и влиянието на дезинформацията.

Дезинформацията процъфтява от деликатното взаимодействие между различни елементи на комуникационния модел, което, когато бъде експлоатирано, може да доведе до широко разпространена вяра във фалшиви разкази. Основните аспекти в разпространението на дезинформация включват източник, съобщение, среда, получател, механизъм за обратна връзка и по-широкия социокултурен контекст, в който тя действа.

Самото съобщение е критичен елемент, пригоден да предизвиква емоционални реакции или да потвърждава съществуващи предразсъдъци. Дезинформацията често включва зърна на истината, тактика, която повишава достоверността и улеснява разпространението на подвеждащо съдържание (Lewandowsky, Ecker & Cook 2017). Начинът, по който едно послание е оформено, времето му и съгласуването му с културни разкази или текущи събития могат значително да увеличат въздействието му.

Фалшивото съдържание, генерирано от потребителите, води до замърсяване на информационното пространство. В социалните медии често се случва публикуващия да се представя за някои друг, като форма на

погрешно възприемана анонимност. Много престъпници си създават изкуствен профил и така се представят пред потенциалните си жертви, преди да се срещнат с тях.

Тъй като гражданите все повече получават своята информация от социалните медии, те се нуждаят от умения не само за оценка на съдържанието, но и за разбиране на алгоритмите, които може да оформят техния информационен пейзаж, като:

– информационни филтърни балони;

– ехо камери;

– персонализирани информационни потоци, които могат да засилят дезинформацията.

Методи за анализ на медийно съдържание

Има два основни метода за анализ –т.нар. CRAMPP анализ и методът на триангулации на източниците. CRAMPP анализът е адаптиран акроним на стъпки за анализ на информацията, предложени от Center for Media Literacy, както следва: Content (съдържание); Reason (причина); Audience (аудитория); Method (метод); Purpose (цел) и Producer (създател)[28].

Триангулацията на източници включва: проверка на множество независими източници; сравнителен анализ на гледни точки и оценка на първични и вторични източници.

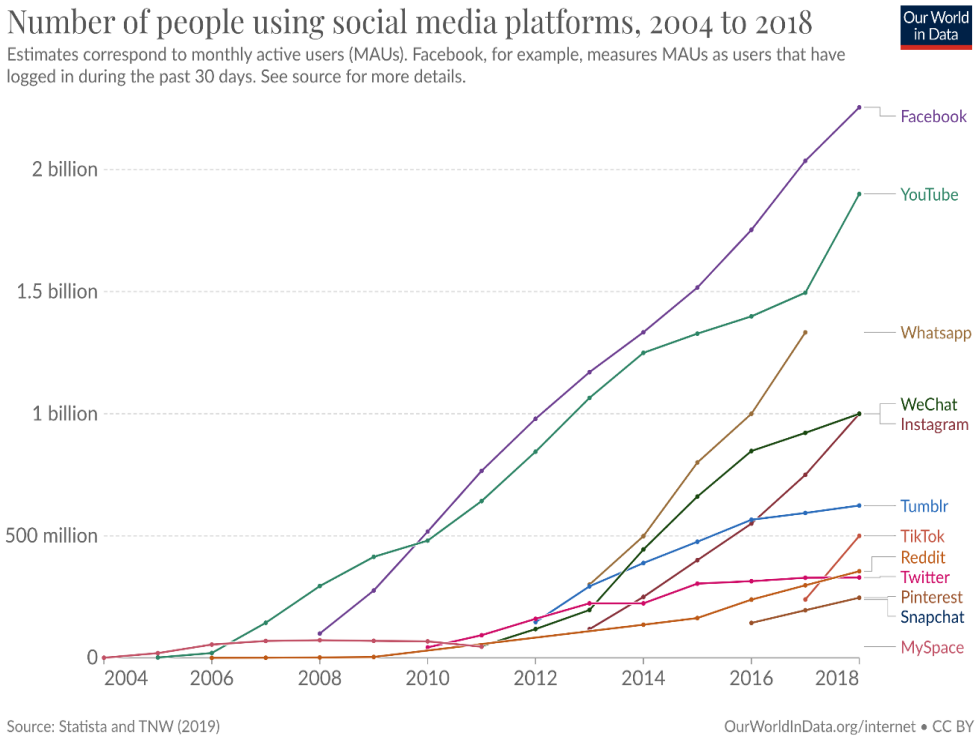
Разпространение на дезинформацията в социалните медии

Годишният доклад за цифровите новини за 2023 г. на Института за изследване на журналистиката „Ройтерс“ (Reuters)[29] посочва, че 73% от българските потребители използват социалните медии като източник на новини. Средната стойност на този показател за всички държави обхванати от изследването е 30%, а за Европа – 40%. Българите се доверяват най-много в Европа на социалните медии като Facebook и YouTube. Ня-

[28] SHARE, J.; JOLLS, T.; THOMAN, E., 2005. *5 five key questions that can change the world. Lesson Plans for Media Literacy*. Center for Media Literacy. Достъпно на: https://mlw.namle.org/wp-content/uploads/2015/07/cml25lessons.pdf.

[29] Newman, N.; Fletcher, R.; Eddy, K., Robertson, C.; Nielsen, R. K. *Digital News Report 2023*. Reuters Institute for the Study of Journalism. DOI: 10.60625/risj-p6es-hb13.

кои от тези социални медии съществуват от много години, но други, стартирали доста по-късно, като TikTok, също вече достигат в челната петица по доверие на българите.



Фигура 9. Брой на хората, използващи социални медии

Като пример за влиянието на TikTok можем да вземем президентските избори в Румъния през 2024 г. Крайнодесният кандидат Калин Джорджеску, дотогава слабо познат на обществеността, изненадващо спечели първия тур на изборите, като основно разчиташе на кампания чрез видеа в платформата. Този неочакван резултат предизвика подозрения за манипулация и външна намеса. Румънските власти изразиха опасения, че чрез TikTok е била осъществена мащабна кампания за дезинформация, целяща да повлияе на изборния процес. Съветът за електронни медии в Румъния призова Европейската комисия да разследва ролята на платформата в изборите.

От своя страна TikTok заяви, че не са открити доказателства за „операция на скрито влияние“ или външна намеса във връзка с изборите. Компанията посочи, че е премахнала над 66 000 фалшиви профила и милиони фалшиви лайкове и последователи, свързани с публикации на румънски език, но не уточни дали тези действия са били свързани с ботове за предизборна дейност или конкретен кандидат. Въпреки това румънските власти продължиха да изразяват съмнения относно влиянието на TikTok върху изборите. Заместник-председателят на румънския телекомуникационен регулатор дори призова за временно спиране на платформата в страната до изясняване на обстоятелствата около потенциалната ѝ роля в изборния процес.

TikTok предизвиква противоречия в различни държави поради опасения относно сигурността на данните, поверителността, влиянието върху младежите и възможността за държавно влияние от страна на Китай. Например в САЩ TikTok се превърна в оръжие за изнудване в сложните икономически отношения между Китай и САЩ. Върховният съд единодушно потвърди закон, изискващ TikTok да се откаже или да бъде забранен, поради това че китайският контрол върху приложението създава риск за националната сигурност.

Други страни, които забраняват TikTok, са Индия, която забранява редица китайски приложения, Канада и Франция – в държавната администрация, а Австралия е обявила повишено внимание. В някои европейски държави, като Албания, има разследвания с мотиви, че обработва данни на деца в разрез с GDPR. Пакистан, Нова Зеландия и Япония също изказват опасения относно влиянието върху младите хора и разпространението на дезинформация.

Facebook и YouTube също са ключови играчи в борбата за информационно влияние сред страните в ЕС и НАТО. През 2020 г. Facebook премахна над 50 мрежи от профили, свързани с дезинформационни операции от държави като Русия, Китай и Иран. Сред тях бе разкрита мрежа, свързана с руската Агенция за интернет изследвания (IRA), която разпространяваше пропаганда за разделение в западните общества.

Информационната и медийната грамотност са свързани с динамичния процес на глобализация и дигитализация на информацията. В условията на бързо развиващото се информационно общество стартова точка за търсене на каквато и да е информация става световната мрежа.

За повечето хора в днешния забързан свят е валиден т.нар. „принцип на най-малкото усилие“, според който човек е склонен да се задоволи с информация с по-ниско качество, когато по-лесно я намира. Това обяснява защо хората ползват най-често свободния интернет вместо лицензи-

рани бази данни или онлайн списания. Потребителите трябва да имат необходимите знания, умения и опит, за да могат да оценят получената информация и да разпознаят опитите за манипулация.

Медийната грамотност е важна за изграждането на устойчивостта на обществото срещу дезинформацията. Способността за достъп до медиите, за критично им разбиране и взаимодействието с тях е от решаващо значение. Медийната грамотност дава възможност на гражданите да се ориентират в модерната цифрова новинарска среда и да правят добре информиран избор. Особено важно е да се научим как да разпознаваме дезинформацията от ранна възраст. В това отношението образованието играе решаваща роля за осигуряването на медийна грамотност на обществото.

Индексът за медийна грамотност е инструмент за оценка и класиране на обществата по отношение на техния потенциал за устойчивост в условията на явленията пост-истина, фалшиви новини и дезинформация. Моделът използва няколко показателя – качество на образованието, свобода на медиите, доверие в обществото и използване на нови инструменти за участие. Индексът преобразува данните в стандартизирани оценки от 0 до 100 (от най-ниска до най-висока) и класира държавите в Европа от 1 до 41 (от най-висока до най-ниска позиция).

България е на последно място сред държавите от ЕС в Индекса за медийна грамотност за 2023 година. България заема 35-о място от общо 41 оценени страни в Европа, което я поставя сред държавите, които са най-уязвими към дезинформацията. В сравнение с индекса за 2022 г. България пада с две места – от 33-о място през 2022 г. до 35-о място през 2023 г., като губи и 2 точки – от 33 точки през 2022 г. до 31 точки през 2023 г. България се представя най-зле по индикаторите, свързани с образованието и свободата на медиите, а най-добре по индикаторите, свързани с новите форми на гражданско участие.

Усещали ли сте някога необходимостта да реагирате незабавно на публикация в социалните медии? Когато попадате на видеоматериали или новинарски истории, които провокират вашето недоволство, страхове или желания, може да почувствате необходимост да направите нещо по този въпрос. Дезинформаторите често се възползват от човешката природа, за да ви накарат да споделяте и реагирате бързо. Бъдете предпазливи със съдържание, което ви очарова, натъжава или шокира, тъй като може да бъде инсценирано или създадено да ви манипулира. Защитата от манипулации се осъществява чрез придържане към надеждни новинарски източници. Добре е да се избягва споделянето на информация от анонимни публикации в социалните медии, непознати уебсайтове или

статии с кликбейт заглавия, като например „Няма да повярвате какво следва!“.

След започване на войната между Русия и Украйна стана ясно, че правителството на САЩ със сигурност си сътрудничи с Facebook за идентифициране на кампании за дезинформация, насочени към подкопаване на доверието в изборния процес. Създаването на Център за кибер- и инфраструктурна сигурност (CISA) подпомогна бързото откриване на такива заплахи.

През 2018 г. Европейската комисия стартира Кодекс за борба с дезинформацията, който задължава платформи като Facebook да докладват за усилията си в ограничаване на манипулативни кампании. Австралия също създаде Център за стратегически комуникации, който работи с Facebook за засичане на дезинформация, насочена към обществени кризи, включително COVID-19. Допълнително Facebook разработи CrowdTangle инструмент, който помага на изследователи и правителствени агенции да проследяват разпространението на съдържание и да идентифицират дезинформационни кампании.

През 2022 г. YouTube също премахна хиляди канали, свързани с китайски и руски държавни пропагандни мрежи, които разпространяваха манипулативна информация за войната в Украйна. В контекста на войната, украинските власти предоставят информация за фалшиви профили и видеа на YouTube, които се използват за разпространение на проруската пропаганда. Платформата използва DeepMind, технология на Google за идентифициране на подвеждащо съдържание и алгоритми за препоръки, които дават приоритет на надеждни източници. Франция също стартира програма за сътрудничество с YouTube за ограничаване на пропагандни видеа по време на изборите, включително чрез обвързване на видеата с официални източници.

В България Facebook стартира кампания за медийна грамотност насочена към младите хора, за да ги научи как да разпознават дезинформация. През 2023 г. правителството на Индия блокира YouTube канали, идентифицирани като част от мрежи за дезинформация свързани с Пакистан. Тези канали разпространяваха съдържание насочено към създаване на социално напрежение.

Ролята на социалните медии в разпространение на дезинформацията е значителна, тъй като тези платформи фундаментално промениха пейзажа на споделяне и потребление на информация. Сайтовете на социалните медии с техните обширни мрежи от потребители и сложни алгоритми са плодородна почва за бързото разпространение на невярна информация. Феноменът не е просто случаен, а продукт на присъщи характеристики на тези платформи, даващи приоритет на съдържание, което е

вероятно да ангажира потребителите, често независимо от неговата фактическа точност.

На първо място, социалните медии имат многостранен ефект на усилване на информацията, тъй като потребителите нерядко са пристрастни и склонни да споделят съдържание, което е в съответствие с техните съществуващи вярвания и ценности. Емоционалното съдържание, особено това, което предизвиква силни реакции като страх, гняв или изненада, се споделя по-често и по-бързо от неутралното съдържание. Тази тенденция може да бъде манипулирана от агенти на дезинформация, създаващи съобщения с цел да задействат емоционален отговор, като по този начин гарантират широкото им разпространение.

Тези фактори се използват от алгоритмите, управляващи социалните медийни платформи, проектирани да увеличат максимално ангажираността на потребителите чрез представяне на съдържание, което вероятно ще задържи вниманието им, и бързо взаимодействие. Тъй като сензационните и спорните материали често предизвикват повече ангажираност, дезинформацията може да бъде предпочитана от тези алгоритми, като по този начин достига до по-широка аудитория. Трябва да се отбележи обаче, че тези платформи не са пасивни участници, техният избор на дизайн влияе върху потока от информация и има осезаеми последици върху естеството на публичните дискусии.

Пример за това са въведените от Мета т.нар. фактчекъри след започване на войната между Русия и Украйна за проверка на фалшивите новини. Те проверяват много малка част от новините, но с това учеха алгоритъма как да действат при наличие на подобно съдържание. За съжаление назначените фактчекъри бяха по-скоро проатлантически насочени и след избора на президента Тръмп от Мета решиха да ги премахнат и да взимат предвид мнението на рейтингова система от общността. Сега, когато една група хора докладва определен пост за дезинформация, алгоритъмът ще го избута назад в класирането.

Друг ключов елемент в разпространението на дезинформация чрез социалните медии е концепцията за ехо камери и филтърни балони, където потребителите са изолирани от противоположни гледни точки и са изложени предимно на информация, която засилва съществуващите им перспективи. Този социален феномен се засилва от алгоритмите на платформата, които подготвят съдържание въз основа на потребителски взаимодействия, като ефективно създават все по-труден за прекъсване цикъл. Такива среди благоприятстват неконтролираното разпространение на дезинформация, тъй като потребителите в тези балони е по-малко вероятно да се натъкнат на коригираща информация или предизвикателство към техните вярвания.

Трябва също да се признае ролята на ботовете и организираните групи за разширяване на дезинформацията. Автоматизираните акаунти или ботове се използват за симулиране на активност в социалните медии, като изкуствено завишават обхвата и очевидната подкрепа за определени разкази. Стратегическото пускане на дезинформация от държавни или недържавни участници по подобен начин използва свързаността на социалните медии, като възнамерява да повлияе на общественото мнение или да наруши социалното сближаване. Тези оркестрирани усилия усложняват откриването и смекчаването на дезинформацията, тъй като наслояват сложни методи върху вече благоприятната социална динамика. Днес са налице редица технологии, като Deepfake и Chat GPT, за автоматично създаване на съдържание.

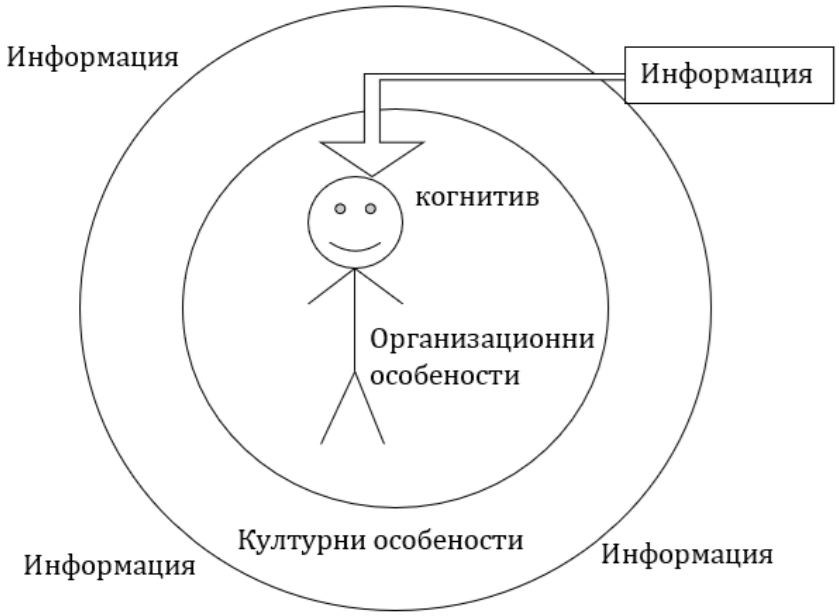
За да се противодейства на отрицателното въздействие на социалните медии върху разпространението на дезинформация, бяха предложени няколко подхода. Повишената прозрачност и отчетност на алгоритмите, използвани от платформите, по-добрите практики за модериране на съдържанието и обучението за цифрова грамотност за потребителите се разглеждат като стъпки към смекчаване на разпространението на невярна информация. Освен това разработването на технологични решения, като автоматизирани инструменти за проверка на факти и изкуствен интелект, които могат да идентифицират и маркират подозрително съдържание, предлага надежда за изграждане на по-устойчиви информационни екосистеми.

Дезинформацията е голям проблем за националната сигурност в съвременната цифрова среда, където бързото разпространение на съдържание често надделява над проверката на неговата точност. Затова от основно значение за държавното управление е да се проучат и приложат ефективни **средства за защита** на системата за отбрана и стратегии за насърчаване на устойчивостта.

Борбата с дезинформацията е многостранна дейност, но най-основният компонент в тази борба е образованието. Чрез интегрирането на медийната и информационната грамотност в образователните програми гражданите могат да придобият жизненоважни умения за критично анализиране и оценка на източниците на информация. Това трябва да включва упражнения, разкриващи тактиките в кампаниите за дезинформация, като емоционална манипулация и използване на полуистини или умишлено погрешно контекстуализирани факти. Освен това образователната система трябва да насърчава култура на скептицизъм и непрекъснато проучване, като дава възможност на учениците да задават въпроси и да разследват, преди да приемат информацията за истина.

Нещо повече, насърчаването на устойчивостта срещу дезинформация в обществото трябва да се простира и извън образователния сектор. Затова периодично следва да се отпуска финансов ресурс за провеждане на информационни кампании. Медийните организации играят важна роля. За да провеждат качествени информационни кампании за осведомяване, те следва да развиват своите отдели за проверка на фактите и да насърчават прозрачността по отношение на изходните материали и журналистическите процеси. Добра практика е изданията да приемат етичен кодекс, който подчертава необходимостта от борба с дезинформацията (Wardle & Derakhshan 2017).

На индивидуално ниво когнитивната устойчивост може да бъде подобрена чрез повишаване на осведомеността за психологическите тенденции, които правят хората податливи на дезинформация, като пристрастия към потвърждението и ефекта на илюзорната истина. Потребителите на социалните медии трябва да бъдат обучени относно значението на проверката на информация чрез надеждни източници и въздействието от споделянето на непроверено съдържание онлайн. Инициативи от типа на кампании за дигитална хигиена, които се застъпват за критично мислене преди споделяне на съдържание, също могат да допринесат за поздравословна информационна екосистема.



Фигура 10. Мисловен модел (визуално онагледяване)

Технологичните компании и платформи играят може би една от най-важните роли в битката срещу информационния безпорядък. Те притежават инструментите и възможностите да идентифицират и намалят разпространението на дезинформация. Чрез използването на усъвършенствани алгоритми и изкуствен интелект тези платформи могат да открият модели, предполагащи кампании за дезинформация, и бързо да действат, за да намалят обхвата им. Независимо от това тези мерки трябва да бъдат щателно балансирани, за да се избегне нарушаването на свободата на изразяване и правото на неприкосновеност на личния живот.

Публичните институции, включително правителствата, имат властта да подкрепят борбата срещу дезинформацията чрез законодателство и публична политика. Налагането на прозрачност в политическата реклама и финансирането ѝ може да помогне да се предотврати манипулирането на електората от операции за чуждестранно влияние и генерирана от вътрешния пазар дезинформация. Въпреки това регулаторните интервенции трябва да бъдат внимателно изработени, за да се предотврати прекомерното използване и непреднамереното потискане на легитимния дискурс.

В крайна сметка устойчивостта срещу дезинформацията е непрекъснат процес, който включва образование, технологии, обществена политика и лична отговорност. Всяка заинтересована страна трябва да допринесе за създаването на обществена норма, която цени истината и се бори с лъжите. Въпреки че няма панацея за пълното изкореняване на дезинформацията, сериозният ангажимент към тези средства ще подобри значително здравето на информационното пространство и устойчивостта на обществата към заплахите, породени от информационния безпорядък.

Служителите в сигурността и отбраната играят ключова роля в противодействието на дезинформацията чрез осъзнато и отговорно поведение онлайн, затова предоставяме някои **съвети за приемливо поведение в социалните медии от тяхна страна**.

● Винаги бъдете критични към информацията, която срещате в социалните мрежи.

● Ориентирайте се към надеждни източници и насърчавайте останалите да правят същото.

● Служителите трябва да се придържат към етични стандарти, като избягват споделянето на непроверена или подвеждаща информация. Вашето поведение онлайн е отражение на организацията, която представлявате, и може да повлияе на общественото мнение.

● Обучавайте семейството и близките си относно рисковете от споделяне на фалшива информация.

● Избягвайте съдържание, което се базира на емоционални послания, сензации или липса на конкретика.

● Споделяйте само данни и новини, които са потвърдени от официални или реномирани източници. Избягвайте съдържание, което поляризира обществото или подбужда конфликти.

● Бъдете внимателни към координирани усилия за разпространение на дезинформация, като използването на ботове или фалшиви профили. Сигнализирайте за такива кампании на платформите или на компетентните органи.

● Ако публикувате съдържание от името на вашата организация, уверете се, че то е в съответствие с установените правила и е проверено за точност.

● Избягвайте публикуването на политически пристрастни изказвания, които могат да подкопаят доверието във вашата служба.

● Помислете какво може да се разчете от снимките и видеоклиповете, които публикувате – контекст, послание, скрити детайли. Избягвайте споделяне на изображения, които могат да бъдат манипулирани или използвани за пропаганда.

● Сигнализиране за проблеми – ако установите разпространение на дезинформация, обърнете се към съответните платформи или вътрешни звена за комуникация.

● Обучение и подготовка – участвайте в обучения, свързани с разпознаване и противодействие на дезинформацията.

Отговорното поведение в социалните мрежи е ключово за борбата с дезинформацията. Като служители в сектор „Сигурност“ вашето влияние върху обществото е значимо, а действията ви могат да допринесат за запазване на доверието и стабилността му.

Десет начина за манипулиране с помощта на медиите

Американският лингвист, философ, когнитивен изследовател и политически активист Аврам Ноам Чомски (Avram Noam Chomsky) в своите изследвания е дефинирал десет основни метода за манипулация на общественото мнение чрез медиите.

1. Стратегията на отвличане на вниманието

Основният елемент на социалния контрол е стратегията за отвличане на вниманието, която има за цел да отклони общественото внимание

от важни въпроси и промени, определени от политическите и икономическите елити, чрез наводняване или непрекъснато разсейване и незначителна информация. Стратегията за отвличане на вниманието е от съществено значение за предотвратяване на интереса към основните проблеми на обществото към настоящия момент.

„Поддържането на общественото внимание отклонено от реалните социални проблеми, завладяно от въпроси без реално значение. Дръж обществеността заета, за да няма време за мислене, или „от полето – в кошарата, както и всички други животни“[30].

2. Създават се проблеми, а след това се предлага начин за решаването им

Този метод е наречен „проблем-реакция-решение“. Създава се проблем, един вид „ситуация“, разчетена така, че да предизвика реакция сред хората, за да поискат те самите приемането на мерки, които са необходими на управляващите кръгове. Например допускане на ескалация на насилие в градските райони или кървави терористични актове с цел гражданите да изискват приемането на закони, насочени към засилване мерките за сигурност и политики, засягащи гражданските свободи. Друг пример е да се предизвика икономическа криза, за да се приеме като необходимо зло нарушението на социалните права и съкращаване на социалните услуги.

3. Методът на постепенното прилагане

За да се постигне приемането на непопулярни мерки, е достатъчно те да се въвеждат постепенно, ден след ден, година след година. Именно по този начин бяха наложени принципно нови социално-икономически условия (неолиберализъм) през 80-те и 90-те години на миналия век. Ако минимизирането на функциите на правителството, приватизацията, несигурността, масовата безработица и заплатите, които вече не осигуряват достоен живот се случат по едно и също време, най-вероятно това би довело до революция.

---

[30] Emissary Publications, 1991. *Silent Weapons for Quiet Wars*. [Онлайн]. Достъпно на: https://ia902909.us.archive.org/28/items/SilentWeaponsForQuietWarsOriginalDocumentCopy/Silent%20Weapons%20for%20Quiet%20Wars%20Original%20Document%20Copy.pdf.

4. Отлагане на изпълнението

Друг начин да се прокара едно непопулярно решение е да се представи като „болезнено и необходимо“ и да се получи в един момент съгласието на гражданите за неговото прилагане в бъдеще. Много по-лесно е хората да се съгласят на жертви в бъдещето, отколкото в момента. Първо, защото това не се случва веднага. Второ, защото повечето хора винаги са склонни да таят наивна надежда, че „утре нещата ще се подобрят“ и че тези жертви, които са поискани от тях, могат да бъдат избегнати. Така се предоставя на гражданите повече време да свикнат с идеята за промени и смирено да ги приемат, когато му дойде времето.

5. Отношение към хората като към малки деца

В по-голямата си част пропагандните изяви, предназначени за широката общественост, използват такива аргументи, символи, думи и интонация, като че ли става дума за деца в училищна възраст със забавено развитие или с психически увреждания. Колкото по-настойчиво някой се опитва да заблуди слушателя, толкова повече той се опитва да използва инфантилни словесни форми. Защо? Ако някой се отнася към човек така, сякаш той е на 12 или по-малко години, по силата на внушението в отговор също ще липсва критична оценка, което е типично за деца на подобна възраст.

6. Да се атакуват емоциите на човека в по-голяма степен, отколкото мисленето му

Въздействието върху емоциите е класически метод, който има за цел да гарантира, че ще се блокира способността на хората да правят рационален анализ, а в крайна сметка дори и на способността им за критично осмисляне на събитията. От друга страна, използването на емоционалния фактор може да отвори вратата към подсъзнанието, за да се вкарат там мисли, желания, страхове, притеснения, принуждения или устойчиви модели на поведение.

7. Да се държат хората в неведение, като се култивира посредственост

С това се гарантира хората да не са в състояние да разберат техниките и методите, използвани за контрол над тях против волята им. Качеството на образованието, предоставяно на по-нисшите класи на обществото, трябва да е толкова оскъдно и посредствено, че да може невежеството, което ги разделя от върхушката, да остане на такова ниво, което нисшите класи да не могат да преодолеят.

8. Насърчаване на гражданите да се възхищават на посредствеността

Културните и интелектуалните стандарти умишлено се понижават, за да се създаде общество, което не се стреми към знания, а се задоволява с леснодостъпни и повърхностни форми на забавление. Ако хората са в състояние на невежество или са заети с несъществени теми, те не разбират реалните проблеми и не могат да изискват промени или да се противопоставят на несправедливости. Това прави обществото по-пасивно и податливо на внушения. Чомски разглежда този метод като инструмент за социален контрол, използван от елитите, за да поддържат властта си, като лишават масите от възможността да мислят критично и независимо.

9. Засилване на чувство за вина

Заставя се отделният човек да вярва в това, че самият той е виновен за собственото си нещастие поради липса на умствени способности, умения или усилия. В резултат, вместо на бунт срещу икономическата система, човек започва да се занимава със самоунижение, самоунищожаване, да обвинява за всичко себе си, което го води неминуемо до тотална и нескончаема депресия, като всичко това води към апатия и бездействие.

10. Да се знае за хората повече, отколкото те самите знаят за себе си

През последните 50 години напредъкът в областта на науката доведе до образуването на все по-разширяваща се пропаст между знанията

на обикновените хора и информацията, която притежава и използва управляващата класа. Благодарение на биологията, неврологията и приложната психология „системата“ има на разположение най-съвременни знания за човека, в областта на физиологията и психологията. Системата е в състояние да научи за обикновения човек повече, отколкото той знае сам за себе си. Това означава, че в повечето случаи системата има по-голяма власт и в много по-голяма степен контролира и управлява хората, отколкото те могат сами да се контролират.

Отворени въпроси за самоподготовка

- Дайте определение за медийна грамотност.
- Кои са основните методи за анализ на медийно съдържание?
- Избройте основните характеристики на социалните медии, които дават приоритет на съдържанието.
- Какви правила трябва да се следват при споделяне в социалните медии?
- Какво разбирате под „замърсяване на информационното пространство“?

Глава пета

БОРБА С ДЕЗИНФОРМАЦИЯТА В НАЦИОНАЛНОТО ИНФОРМАЦИОННО ПРОСТРАНСТВО

- Лекцията разглежда различни аспекти на противоборството в националното когнитивно пространство в областта на сигурността и отбраната.
- Основен акцент е поставен върху концепцията за когнитивна война, изграждане на устойчивост срещу дезинформация в обществото и стратегическите комуникации.

В съвременния свят информационната среда се е превърнала в ключово бойно поле. Националното когнитивно пространство е изложено на системни атаки чрез дезинформация, пропаганда и психологически операции. Дигиталната дезинформация вече не е просто инцидентен проблем, а реална заплаха за националната сигурност и стабилност. Държави и организации активно използват когнитивни операции за манипулиране на общественото мнение и стратегическо влияние върху политически и социални процеси. В тази връзка е необходимо задълбочено познаване на концепцията за националното когнитивно пространство, когнитивната война, стратегическите комуникации и механизмите за изграждане на устойчивост срещу дезинформация.

Концепция за национално когнитивно пространство и когнитивна война

Националното когнитивно пространство представлява съвкупност от идеи, ценности, вярвания и наративи, които формират възприятията и поведението на дадено общество. Концепцията произтича от теорията на Джоузеф Най (1990 г.), която акцентира върху културното и информационното влияние в международните отношения. В нея се твърди, че когнитивното пространство значително влияе върху социалното и политическото поведение, както и върху отговорите на вътрешни и външни пре-

дизвикателства, пред които е изправена една страна. Затова дезинформацията, разпространението на пропаганда и насърчаването на идеологии могат да се разглеждат като усилия за насочване на когнитивното пространство в полза на определени интереси или чужди наративи. Един от първите примери за провеждане на чуждестранна когнитивна военна операция е този с Троянския кон, който троянците сами внесли в крепостта след като Одисей съчинява история, с която ги накарал да вярват, че това е принос за боговете.

Според древния китайски теоретик Сун Дзъ победата във войната зависи изключително много от умелото използване на измама. В неговия труд той пише, че войната се основава на дезинформация и когато сме готови да атакуваме, трябва да изглеждаме уязвими; когато разгръщаме силите си, трябва да изглеждаме пасивни; когато се приближаваме, трябва да накараме противника да повярва, че сме далеч и когато сме далеч, трябва да го накараме да повярва, че сме близо.

По-късно в книгата „Принцът“ Николо Макиавели развива тезата, че един владетел трябва да умее да заблуждава околните, като редува звяра и човека в себе си. В книгата „Моята борба“ на Адолф Хитлер се доразвива идеята, че пропагандата е изкуство и тя се изразява в способността да събуждаш въображението на публиката чрез апел към нейните емоции, в намирането на подходящата психологическа форма, която да привлече вниманието и да се хареса на сърцата на националните маси. В подкрепа на това през 1933 г. той назначава Йозеф Гьобелс за първия министър на пропагандата, който казва, че една лъжа повторена сто пъти става истина.

По време на войната в Ирак 2003 – 2011 г. особено много се подчерта важността на информационните операции и контрола върху потока от информация. В съвремието Народната освободителна армия на Китай предлага теорията за трите войни през 2003 г. Това включва психологическа война, която подкопава потенциала на врага да води бойни операции, медийната война, която формира вътрешното и международното обществено мнение и правната война, която разчита на международното и вътрешното право за отстояване на китайските интереси. Впоследствие тази теория прераства в „Неограничена война“ със силен акцент върху политическите и икономическите активи.

През 2013 г. генерал Валерий Герасимов (Gerasimov 2013), началник на Генералния щаб на въоръжените сили на Руската федерация, издаде доктрина на тоталната война, в която се подчертава необходимостта да се преразгледат традиционните форми и начини на водене на война и да се противостои на ограниченията. Това следва да стане, като се излезе

отвъд границите на конвенционалната война (дестабилизиране и подкопаване на друго общество, поляризиране на общественото мнение, разпространение на противоречиви наративи, радикализиране на определени групи и т.н.)

Понятието за когнитивна война изследва потенциалната манипулация, осъществявана от враждебни актьори чрез използване на постиженията на когнитивната наука, включително пропаганда и дезинформация (Claverie 2025). Тя е допълнение към други инструменти и засяга нагласите и поведението, като влияе, защитава или нарушава когнитивното ниво на индивид, група или население. Тази форма на конфликт обхваща операции, насочени към нарушаване на мисловните процеси на противника и промяна на способността му за вземане на решения чрез използване на научен подход. Тези операции целят да изкривят, предотвратят или унищожат мисловните процеси, осведомеността за ситуацията и способността за вземане на решения на противника, като се използват научни и технологични и по-специално дигитални средства. Това включва създаване на фалшиви разкази, разпространение на дезинформация и фалшиви новини, подвеждане на общественото мнение, объркване на публичния дискурс и подкопаване на общественото доверие и устойчивост.

За противодействие на неконвенционалните оръжия на словото и образа се дефинира нова изследователска област, известна като „когнитивна сигурност“ (Claverie 2025). Тази трансдисциплинарна област има за цел да разбере заплахите, които хибридните войни използват в момента, и да определи подходящите мерки срещу некинетични офанзиви, включително дезинформацията. Когнитивната сигурност разглежда дезинформацията в контекста на подкопаването на доверието и създаването на ехо камери, където хората се изолират в рамките на собствените си културни и идеологически балони. Това изолиране, подхранвано от алгоритми и лични интереси, допълнително улеснява разпространението на дезинформация, тъй като индивидите рядко се сблъскват с противоречиви гледни точки, което възпрепятства критичното мислене и задълбоченото разбиране на информацията.

Когнитивната война е част от хибридната, некинетична форма на конфликт, включва използването на информация за влияние върху възприятията и решенията на противника, като комбинира различни видове психологически, информационни операции и манипулация чрез социалните медии. НАТО определя когнитивната война като дейности, провеждани в синхрон с други инструменти на властта, за да повлияят на нагласи и поведение чрез влияние, защита или нарушаване на познанието на индивидуално, групово или популационно ниво с цел получаване на предимство пред противник (Wanyana 2025).



Фигура 11. Схема за онагледяване на когнитивното пространство

Въздействието на когнитивната война върху социалната сплотеност и стабилност представлява сериозна заплаха за националната сигурност. Чрез създаване на вътрешни разделения и подбуждане на конфликти враждебните актьори могат да отслабят обществото отвътре, като го направят по-уязвимо на външни влияния и заплахи, затова от изключително значение за сигурността е да се изгради национална устойчивост срещу дезинформацията.

Международни подходи за противодействие на дезинформацията

Реакциите на различните държави към заплахата от дезинформация варират в зависимост от националната им култура, институционална зрялост, информационна инфраструктура и социална устойчивост.

1. Финландия приема образованието като средство за устойчивост. Те възприемат дезинформацията не просто като заплаха за сигурността, а като дългосрочно образователно предизвикателство. Още от началните класове в образователната система се интегрират дисциплини по медийна и информационна грамотност, насочени към развитието на критическо

мислене и разпознаване на манипулативни наративи[31]. Учителите се обучават специално как да преподават теми свързани с дезинформация и пропаганда, включително чрез използване на симулации и игрови методи.

2. Швеция залага на комуникационна устойчивост и междуинституционална координация. Шведската философия включва висока степен на прозрачност, институционално доверие и стратегическа комуникация. Създадената Шведска агенция за психологическа защита (Myndigheten för psykologiskt försvar) координира действията на държавни структури, частния сектор и медиите с цел изграждане на обществена устойчивост към информационни атаки[32]. Обществените радио- и телевизионни оператори разполагат с протоколи за отразяване на дезинформационни кампании в реално време.

3. Германия е сред първите държави в ЕС, които прилагат строга правна рамка по отношение на онлайн съдържанието. Законът за прилагане на мрежовото съдържание (Netzwerkdurchsetzungsgesetz – NetzDG) изисква от социалните платформи да премахват незаконно или фалшиво съдържание в срок до 24 часа[33]. Това е съчетано с държавна подкрепа за обучителни програми и фактически инициативи като Correctiv, която функционира като независим център за проверка на факти.

4. В САЩ се прилага интегрирана реакция чрез публично-частно партньорство. Дезинформацията е третирана като стратегическа заплаха за националната сигурност. Министерството на вътрешната сигурност (DHS) създаде специални звена за мониторинг на чуждестранни дезинформационни кампании, като работи в тясно сътрудничество с технологични гиганти и разузнавателни структури[34]. Особено внимание се отделя на образователни кампании като Think Before You Link, насочени към служители на правителствени институции и отбранителни агенции.

5. Естония е цифрова държава с активна информационна отбрана и има дългогодишен опит в кибератаките, възприема дезинформацията като част от информационната война. В отговор страната развива система

[31] OECD. Future of Education and Skills 2030: Conceptual learning framework. Paris: OECD, 2020.

[32] Swedish Government. Sweden's Psychological Defence Agency - Annual Report 2022. Stockholm: Myndigheten för psykologiskt försvar, 2022.

[33] Bundesministerium der Justiz. Netzwerkdurchsetzungsgesetz (NetzDG). Berlin: BMJ, 2017.

[34] DHS (Department of Homeland Security). Combatting Foreign Influence and Disinformation. Washington D.C., 2022.

за комуникационна отбрана, включваща участие на граждански доброволци в симулации и обучения[35]. Освен това държавата подпомага независими журналистически разследвания на враждебни информационни операции.

6. Франция прилага проактивна стратегия за разобличаване на фалшиви новини чрез държавна агенция Viginum, създадена през 2021 г. Агенцията наблюдава чужди опити за намеса в информационната среда и работи съвместно с медиите за оповестяване на фалшиви твърдения[36]. Френските институции провеждат пресконференции и публикуват опровержения в реално време, особено по време на изборни кампании.

7. Украйна е златен пример за информационна мобилизация в условия на война. В контекста на продължаващата агресия от страна на Руската федерация Украйна изгради уникален модел на информационна мобилизация. Сайтове като StopFake.org разобличават руските наративи, докато доброволчески „информационни армии“ създават и разпространяват проверена информация[37]. Социалните мрежи се използват активно от правителството за бърза реакция при разпространение на слухове и фалшиви новини.

Таблица 1. Основна философия за борба с дезинформацията на различните държави

Държава	***Основна философия***	***Ключови решения и практики***	***Институция***
Финландия	Превенция чрез образование	– обучение по медийна и дигитална грамотност от начално училище	Министерство на образованието
		– тренинг на учители за разпознаване на пропаганда	
Швеция	Превенция чрез образование,	– междуинституционална координация и превенция чрез медиите	Агенция за психологическа защита

[35] Estonian Ministry of Defence. National Defence Development Plan 2021–2030. Tallinn: MoD, 2021.

[36] Gouvernement.fr. Présentation de l’agence VIGINUM. Paris: Secrétariat Général de la Défense et de la Sécurité Nationale, 2022.

[37] StopFake. Reports and Analysis on Russian Propaganda, 2023. [Онлайн] Достъпно на: https://stopfake.org/en

	комуникация и доверие	– протоколи за комуникация при кризи	
Германия	Правна отговорност на платформите и централизация	– закон NetzDG и глоби за фалшиво съдържание	Федерално министерство на правосъдието
		– подкрепа за независими фактчекъри	
САЩ	Стратегически комуникации и технологично партньорство	– наблюдение на чужди кампании	DHS/FBI/Think Before You Link
		– партньорство с платформи	
		– образователни кампании	
Естония	Обществено участие и активисти с дигитална грамотност	– информационни доброволци	Министерство на отбраната на Естония
		– симулации	
		– комуникационна отбрана в Министерството на отбраната	
Франция	Стратегически комуникации и централизация	– агенция Viginum	SGDSN/ Viginum
		– официални опровержения	
		– мониторинг в реално време	
Украйна	Информационна мобилизация в условия на война. Обществено участие и активизъм	– StopFake.org	Центрове за стратегическа комуникация
		– доброволчески екипи	
		– активна комуникация в социални мрежи	

Противодействието на дезинформацията в международен план показва, че няма универсален модел, но ясно се открояват няколко философски подхода: образователна превенция, институционална координация, регулация на платформите, проактивна държавна комуникация и гражданско участие. Успешните примери доказват, че устойчивостта срещу дезинформация се постига чрез съвместни усилия между институции, медии и общество.

Как се противодейства на дезинформацията – основни подходи и български решения

Дезинформацията се превърна в стратегически инструмент за влияние върху общественото мнение, политическите процеси и националната сигурност. В контекста на нарастващи хибридни заплахи държавите от Европейския съюз и НАТО, включително България, развиват политики, институции и инструменти за противодействие на дезинформацията в следните направления:

1. Откриване и верификация на информация. Първият етап на противодействие е свързан с уменията за критично четене, анализ на метаданни, източници, контекст, разпознаване на емоционално наситено съдържание и използване на инструменти за проверка на факти (fact-checking) или софтуерни инструменти (напр. InVID, Hoaxy, NewsGuard), които подпомагат идентифицирането на фалшиво съдържание, фалшифицирани изображения и координирани кампании.

2. Повишаване на медийната и цифровата грамотност. Ключов елемент в борбата срещу дезинформацията е образованието. Устойчивите общества са тези, в които гражданите притежават умения да разпознават манипулативни наративи. В България се развиват програми за медийна грамотност в училищата, както и обучителни курсове за преподаватели и държавни служители.

3. Изграждане на когнитивна устойчивост. Под „когнитивна устойчивост“ се разбира способността на индивидите и обществата да устояват на опити за психологическо и информационно въздействие. Това включва обучение по критично мислене, симулации на информационни атаки, стратегическа комуникация и изграждане на доверие в легитимните източници, подготовка на гражданите и институциите за разпознаване на манипулативни наративи.

4. Законодателство и регулации. Законодателството в областта на защитата на личните данни (напр. GDPR), контролът върху социални платформи и сътрудничеството между държавни и неправителствени структури за създаване на институционален регулационен отговор е от ключово значение за ограничаване на дезинформацията.

Налице са някои български инициативи и добри практики, които ще разгледаме:

1. Factcheck.bg (Асоциация на европейските журналисти – България) е първата професионална българска платформа за проверка на факти, създадена през 2021 г. Тя следи за фалшиви новини в медиите, социалните мрежи и публичния дискурс. Платформата използва методология, съответстваща на международните стандарти (IFCN) и партнира с Европейския център за медийна грамотност (EDMO).

2. Центърът за изследване на демокрацията (ЦИД) изследва хибридни заплахи, руско влияние и дезинформационни мрежи в България и региона. Организацията издава редовни доклади и препоръки към институциите и взима участие в европейски проекти като Disinformation Resilience Index.

3. Фондация „Медийна грамотност за всеки“ развива програми и обучения за деца, учители и родители, целящи изграждане на критично мислене. Работи активно с Министерството на образованието и науката по внедряване на теми по медийна грамотност в учебните програми.

4. Държавна агенция „Национална сигурност“ (ДАНС) и МВР извършват наблюдение на дезинформационна дейност, включително за координирани враждебни кампании от чужди държавни актьори.

Министерството на отбраната е в процес на изграждане на звена за стратегически комуникации, чиято роля е да разпознават и неутрализират дезинформационни кампании в отбранителния сектор. Те разработват ръководства, провеждат учения и участват в съвместни проекти с НАТО и ЕС. В момента се работи по актуализация на стратегически документи за противодействие на хибридни заплахи, които ще включват мерки за информационна сигурност, комуникационна устойчивост и сътрудничество между институциите.

Ефективното противодействие изисква комплексен подход, включващ институционални, образователни, технологични и регулаторни мерки. България разполага с активни организации, експерти и стратегии, които служат като добра база за развитие на национална когнитивна устойчивост и интегрирана защита от информационни атаки.

Изграждане на устойчивост срещу дезинформацията

Устойчивостта е способността на система, организация или общество да издържат на сътресения, да се адаптират към промените и да се възстановяват бързо от прекъсвания. Устойчивите системи се характеризират със способността бързо да откриват и гъвкаво да реагират на заплахи.

В системата на националната сигурност това включва идентифициране на уязвимости в организацията и различните елементи на хибридни заплахи, като кибератаки, кампании за дезинформация или икономически и политически принуди, и своевременно преминаване към подходящи контрамерки. Организацията или обществото, което е устойчиво, може бързо да се адаптира и да реагира на променящата се природа на

хибридни заплахи и психологически информационни операции, като по този начин смекчава тяхното въздействие.

Чрез справяне с уязвимости като социални неравенства, слабо състояние на демокрацията и демократичните институции или корупция една устойчива система може да намали своята податливост към хибридни заплахи. Това може да включва инвестиране в демократично образование, разнообразяване на социалните политики, подобряване на комуникацията и координацията между различни заинтересовани страни и подобряване на общата готовност.

Устойчивостта често се гради върху координация и сътрудничество между различни заинтересовани страни, включително държавни органи, частния сектор, групи на гражданското общество и международни партньори. В контекста на хибридните заплахи ефективната координация и сътрудничество са от решаващо значение за споделяне на информация, разузнаване и ресурси и за разработване на съвместни стратегии и отговори. Съвместните усилия на различните заинтересовани страни водят до подобряване на способността за идентифициране, възпиране и смекчаване на хибридните заплахи.

Обществената устойчивост е способността на дадена общност, общество или нация да устои, да се адаптира и да се възстанови от неблагоприятни събития или предизвикателства, като природни бедствия, икономически сътресения, пандемии, социални вълнения, или външни заплахи, като дезинформация и кибератаки.

В стремежа си да осигури устойчивост срещу дезинформацията, Европейският съюз създаде East StratCom през 2015 г., с цел идентифициране и разкриване на чуждестранни дезинформационни кампании. През 2018 г. беше въведен кодекс на добрите практики относно дезинформацията. Същата година е представен първият план за действие срещу дезинформацията, включващ мерки за подобряване на откриването на дезинформация, координиране на ответните мерки срещу дезинформационни кампании, сътрудничество с онлайн платформи и укрепване на медийната грамотност сред гражданите. Впоследствие беше въведен Законът за цифровите услуги (DSA).

Някои държави, като Република Молдова, създадоха свои центрове за стратегически комуникации и противодействие на дезинформацията. В резултат те разработиха национален механизъм за устойчивост на информацията – сложен инструмент за картографиране и оценка на уязвимостите, тяхното идентифициране и изследване, разбиране и защита на медийната среда. Друг пример е разработеният в Националния университет по отбрана във Вашингтон специален инструмент, рамка за създаване на стратегия за неконвенционална война и противодействие на чуждестранни когнитивни информационни операции.



Фигура 12. Рамка за създаване на стратегия за противодействие на чуждестранни когнитивни информационни операции.
Адаптирана от RADOSLAVOV, D., 2022. *Strawman Strategy for Countering Russian Information Operations and Cognitive Warfare in Bulgaria*. [Дисертация].

Един от ключовите примери за съвременна когнитивна война може да се види в стратегическите комуникационни усилия на терористични организации като Ислямска държава. Те са използвали наративни стратегии, за да се представят като еманципатори в регионите, които контролират, като използват исторически недоволства и предлагат алтернативна политическа визия на уязвимата публика. Държавите са изправени пред предизвикателството да се противопоставят на тези разкази, без да им придават истинност или да изглеждат потиснически. В отговор стратегическите комуникатори трябва да изработят контраразкази, които деконструират историята на противника, подчертават неговите заблуди и представят убедителна алтернатива, която е в съответствие с демократичните ценности и правата на човека.

Изграждането на устойчивост в когнитивната област е съществен компонент от стратегията за национална сигурност. Устойчивостта тук се отнася до способността на националното когнитивно пространство да устои, да абсорбира и да се възстанови от психологически, информационни операции и други форми на когнитивна агресия. В тази сложна област правителствата, институциите за сигурност и въоръжените сили трябва да разработят стабилни стратегии за защита на умовете на населението от манипулация и експлоатация.

Първо, важно е да се разбере, че когнитивната устойчивост обхваща широк спектър от инициативи, от обучение на обществеността за дезинформация и пропаганда до усъвършенствани контрамерки срещу психологическите операции (PSYOPS). Според Сънстейн (Sunstein 2019) разпространението на невярна информация подчертава необходимостта медийната грамотност и уменията за критично мислене да бъдат вплетени в тъканта на образователните системи като средство за борба с влиянието на фалшивите новини и повишаване на когнитивната устойчивост.

Друг аспект на устойчивостта е култивирането на социално сближаване и доверие в институциите. Обществената връзка и общественото доверие действат като бастиони срещу враждебните разкази, насочени към сеене на раздори. Както Фукуяма (Fukuyama 1995) твърди, социалният капитал или доверието и нормите, които се развиват в едно общество, играят ключова роля за успеха на държавата. Нация със силен социален капитал е в по-добра позиция да устои на когнитивни заплахи, тъй като нейните граждани са по-склонни да се държат заедно и да подкрепят авторитетни източници на информация.

И накрая, международното сътрудничество допринася за когнитивната устойчивост. Необходимо е дейно участие в инициативи на НАТО за укрепване на взаимната подкрепа в противодействието на кампаниите за дезинформация, обединяването на ресурси и споделяне на добри практики с партньорите. Споделянето на разузнавателна информация за заплахите и координирането на стратегически комуникации може да подобри колективната когнитивна устойчивост на съюзниците, което прави по-трудно за противниците да организират ефективни когнитивни атаки.

Ключовата роля на стратегическите комуникации за защита на националните интереси и предотвратяване на външна намеса е все по-очевидна. Ефективната комуникация позволява на държавата да поддържа контрол върху националния информационен поток, да противодейства на враждебните наративи и да гарантира, че общественото мнение е информирано и устойчиво на манипулации.

Стратегическите комуникации и насоки за борба с дезинформацията

Стратегическите комуникации представляват комуникация чрез думи и дела в преследване на национални стратегически цели, като съгласуваността и последователността са от съществено значение (Cornish, Yorke, Lindley-French 2011). Способността да се проектира и поддържа

образ, който е в съответствие с националните интереси и ценности, като същевременно ефективно се противопоставя на дезинформацията и враждебните разкази, е ключов елемент на съвременното държавно управление и е от съществено значение за поддържане на целостта на когнитивното пространство срещу атаката на съвременните психологически операции.

Точно с тази цел в НАТО през 2009 г. е приета концепция за стратегическите комуникации, според която *те представляват координирано използване на комуникационните дейности и способности, като публична дипломация, военен PR, информационни и психологически операции, в зависимост от случая – в подкрепа на политиките, операциите и дейностите за постигане на целите на организацията*[38]. Описаните елементи на това определение налагат систематични усилия на правителството да разбере, информира, убеди или повлияе на възприятията и поведението на целевите аудитории, културното разпространение и международното излъчване, като гарантира, че националният разказ е в съответствие със стратегическите цели на държавата. С други думи, принципите на стратегическите комуникации в националното когнитивно пространство се въртят около *съгласуваност, координация и последователност*.

Съгласуваността се отнася до съгласуването на посланията с националните ценности и политики, като се гарантира, че всяка комуникация подсилва предвидения наратив. Координираните усилия между правителствени агенции, военни клонове и други национални участници са от решаващо значение за предоставянето на последователно послание. Освен това са необходими постоянство и последователност във времето, за да могат посланията да пуснат корени и да повлияят ефективно на общественото мнение.

Основните методи за стратегически комуникации използват завладяващи разкази и различни медийни платформи за разпространение на стратегически послания. Една такава платформа, която може да бъде използвана за самостоятелни упражнения е Pavilion. Dinfos Online Learning[39]. Тя обхваща предметни области като основи на комуникациите, управление на кризи, операции за следкризисно възстановяване. В нея са посочени начини за представяне на информацията пред различните видове въоръжени сили: въздушни, сухопътни, военноморски и съвмес-

[38] NATO Strategic Communications Policy, Brussels, 2009.

[39] Pavilion. Dinfos Online Learning. Defense Information School (DINFOS) https://pavilion.dinfos.edu/Article/Article/3582943/types-of-information-disorder/.

тни сили и са предоставени различни статии, наръчници за самостоятелно изготвяне на документи, както и шаблони за изграждане на поведение и самооценка след провеждане на операции, политики и доктрини в различните области.

Стратегическите комуникации също включват противодействие на дезинформация и пропаганда от враждебни субекти. Борбата с дезинформацията е в голяма степен битка на наративи. За да бъдат успешни стратегическите комуникации в тази борба, те трябва активно да промотират положителни и основани на факти разкази, които подкрепят основните ценности на обществото. Чрез запълване на информационното пространство с такива повествования държавата може да намали влиянието на дезинформацията и да укрепи обществената устойчивост. Това би могло да включва използването на организации за проверка на фактите, бързи опровержения и разяснения на неверни твърдения и създаване на алтернативно съдържание, което намалява достоверността и въздействието на противопоставящите се разкази.

Ефективността на стратегическите комуникации може да бъде значително повишена чрез използване на завладяващи истории и лични свидетелства, които създават емоционална връзка с аудиторията. Тези методи помагат посланията да бъдат по-запомнящи се и убедителни, което е особено важно при противодействието на дезинформацията, често разчитаща на емоционални апели.

И накрая, измерването и оценката са критични за разбирането на въздействието на стратегическите комуникационни инициативи. Чрез анализиране на данни от различни източници, включително проучвания на общественото мнение и анализи на социалните медии, властите могат да преценят ефективността на своите комуникации и да коригират съответно своите стратегии. За да бъдат ефективни контранаративите, те трябва да бъдат насочени към конкретните нужди, интереси и вярвания на целевата аудитория. Използването на анализ на личността позволява на стратегическите комуникатори да създадат послания, които резонират с аудиторията, и да оспорят дезинформацията по начин, който е най-вероятно да бъде приет. Вместо директно да опровергават дезинформацията, стратегическите комуникатори могат да бъдат по-ефективни, като създават и разпространяват позитивни алтернативни наративи, предлагащи достоверна и привлекателна алтернатива на неверните твърдения. Този подход помага да се избегне неволното подсилване на дезинформацията чрез нейното повторение.

Стратегическите комуникации координирано използват редица информационни инструменти в синхронизация с кинетичните действия за намеса в процеса на вземане на решения от страна на противниците,

като пряко манипулират информационна и аналитична рамка, оказват влияние върху определени лидери или косвено влияят върху групи от хора (т.е. политически партии, профсъюзи и граждански организации), чиито реакции засягат ръководството на дадена страна.

Типологията на информационните дейности в отбраната включва пет типа действия, показани на фигура 13. Опитът показва, че всички тези дейности (независимо дали имат онлайн или офлайн ефект) се използват комбинирано и се синхронизират с кинетичните действия, като обхващат три типа аудитория – противник, собствено население и международна общност.



Фигура 13. Класификация на информационните инструменти.
Източник: ДИМОВ, П., 2018. *Приложение на уеб технологиите за защита на националната сигурност*. София: Диомира.

В рамките на спектъра на сигурността и отбраната могат да се посочат няколко ефективни препоръки за противодействие на институционално ниво срещу дезинформацията:

Първо, на политическото ниво е необходимо да се признае, че когнитивното пространство е толкова оспорвано, колкото и физическото. Това налага интегрирането на стратегическите комуникации и мерки за борба с дезинформацията във всички нива на разработване на политики и планиране на отбраната. Например политиката на Министерството на отбраната относно стратегическите комуникации трябва да включва не

само протоколи за съобщения и разпространение на информация, но и мерки за наблюдение, противодействие и управление на кампании за дезинформация.

На второ място, образованието и обучението на личния състав са от съществено значение както за държавните служители, така и за военнослужещите. Необходимо е да се провеждат информационни кампании, обучения за медийна грамотност и критично мислене. Това подготвя хората за прилагане и за противодействие на сложни комуникационни стратегии.

Инвестирането в технологии, които подпомагат анализа и разпространението на информация, е друго критично политическо измерение. Внедряването на усъвършенствани алгоритми за изкуствен интелект може да помогне за откриване на модели в дезинформацията и прогнозиране на конкурентни комуникационни стратегии.

Необходимо е във въоръжените сили да се изградят специализирани звена, които да се фокусират върху мониторинг, анализ и противодействие на дезинформация. Следва да се разработят ясни протоколи за идентифициране, опровергаване и неутрализиране на дезинформационни атаки. Специализираните звена трябва редовно да участват в съвместни учения за борба с дезинформацията и да обменят информация и добри практики.

От дипломатическа гледна точка съюзите и партньорствата, които позволяват споделянето на най-добри практики в стратегическите комуникации, могат драстично да подобрят позицията на колективната отбрана. Например стратегическият комуникационен център на НАТО за върхови постижения е платформа, където държавите членки си сътрудничат за разбиране и противодействие на пропагандата, като по този начин повишават колективната сигурност. Не на последно място, предоставянето на прозрачна и навременна информация от официалните канали е от съществено значение за подхранването на доверието в гражданското общество.

Създаването на политики също играе решаваща роля в борбата с дезинформацията. Законодателите по света започнаха да признават необходимостта от правни рамки, които могат да отговорят на разпространението на дезинформация, без да нарушават свободата на изразяване. Законодателни мерки като GDPR започнаха да се занимават с проблемите на поверителността на данните и разпространението на дезинформация от страна на социални медии чрез налагане на прозрачност и отчетност. Тези правни интервенции са основни компоненти на първоначалния набор от инструменти за управление на дезинформацията, тъй като създават структурирана среда, която ограничава капацитета на злонамерените участници да разпространяват подвеждащо съдържание.

Практическите съвети за противодействие от военнослужещите са:

– използвайте само официалните източници на Министерство на отбраната и Българската армия;

– не споделяйте непроверена информация за военни дейности;

– внимавайте какво публикувате в социалните мрежи;

– проверявайте фактите и при съмнение се консултирайте с прекия командир;

– бъдете особено внимателни при кризисни ситуации;

– докладвайте за съмнително съдържание.

В заключение, справянето с глобалната дилема с дезинформацията изисква многостранна и далновидна стратегия, която се адаптира към променящите се технологии и обществени тенденции. Бъдещето трябва да бъде подкрепено от солидни изследвания, технологични иновации, инициативи за сътрудничество, просветено регулиране и овластена, образована общественост. Само чрез такъв съгласуван и всеобхватен подход можем да се надяваме да защитим целостта на нашата информационна среда.

Опазването на целостта на информацията и противодействието на дезинформация изискват подход, основан на цялото общество и на много заинтересовани страни, който да интегрира дейностите на политиците, гражданското общество и частния сектор и да използва ефективно сътрудничеството с ЕС, САЩ и евроатлантическите институции. Функционалната институционална рамка трябва да има за цел да се справи с предлагането на проблемно съдържание (като фалшиви новини, конспиративни теории и подбуждане към насилие), но и с търсенето му, като приложи комбинация от възпиращи и превантивни мерки (фигура 14). Мерките следва да бъдат обединени в интегриран национален подход с няколко нива на защита, включващ не само институционален капацитет и процедури, но и инфраструктура за цифрова криминалистика и техническо ноу-хау, необходими за наблюдение на целостта на онлайн информационното пространство (Georgiev, Novosyolova 2023).

Ролята на медийните регулатори трябва да бъде засилена с мандат и капацитет за проследяване и ефективно санкциониране на присъствието на съдържание от санкционирани субекти. Това включва гарантиране на независимостта на медийните регулатори от политическа намеса и увеличаване на техните бюджети.

Технологичните предизвикателства, породени от възхода на новинарските уебсайтове, платформите на социалните медии и езиковите модели с изкуствен интелект (AI), които заедно могат да създават и разп-

ространяват съдържание в безпрецедентен мащаб, са сложни и безбройни. Доставчиците на онлайн информация работят в среда, която е много по-трудна за надзор в сравнение с тази на традиционните медии, не само защото законодателството изостава от технологичното развитие, но и поради самия мащаб и сложност на цифровата инфраструктура. Цифровизацията на производството и потреблението на знания поставя нови и непознати трудности пред публичните органи, отговорни за опазването на целостта на техните местни информационни пространства. За да се справят с предизвикателството, те трябва да приемат натрупания опит от субектите в частния сектор, гражданското общество и академичните среди, които през последното десетилетие анализират и практически се занимават с тези въпроси.

Създаването на основна линия на защита изисква разработването и внедряването на инфраструктура за цифрова криминалистика, която да открива и разследва кампании за дезинформация в почти реално време, както и участниците, които ги създават и разпространяват. На първично ниво това означава разгръщане на инструменти за медиен мониторинг и анализ на аудиторията, които могат да измерват обема и обхвата на повтарящите се наративи. Една по-усъвършенствана система би включвала и инструменти, анализиращи дигиталния състав на онлайн новинарските източници в големи количества и автоматично откриващи признаци на експлоатация и злоупотреба, като например неавтентична информация за контакт или собственост, промяна на предназначението на домейна и липса на политика за поверителност или общи условия за ползване, както и други добре документирани признаци на злонамерени намерения. Понататъшна стъпка ще бъде наблюдението на целостта на алгоритмите и монетизирането на съдържанието чрез реклами, като се гарантира, че те са в съответствие с националните и международните задължения.

Събраните от звената за цифрова криминалистика данни следва да се използват за изготвяне на оценки на заплахите за националната сигурност и оценки на риска, свързани с опасностите, които дезинформацията създава за критични въпроси на сигурността, като например външната политика, енергийната сигурност, и ангажиментите по ключови политики на ЕС от типа на DSA и пакетите от санкции срещу руски субекти. Тези усилия разширяват и допълват създадените от НАТО и ЕС механизми за цифрова сигурност, като например оперативните групи за стратегически комуникации и системата за бързо предупреждение на Европейската служба за външна дейност, мрежата от четиринадесет европейски центъра за наблюдение на цифровите медии, Съвета за търговия и технологии ЕС-САЩ, Центъра за високи постижения в областта на

стратегическите комуникации на НАТО и Европейския център за високи постижения за противодействие на хибридните заплахи (Hybrid CoE)

Достоверността на информацията може да бъде проверена чрез специализирани сайтове, наречени „фактчекъри“, където независими проверяващи от различни страни по света проверяват фактите, откриват фалшивите новини и дезинформацията и противодействат на вредата, която те нанасят. Такъв пример, който може да се използва у нас, е https://factcheck.bg [40]. Друг подобен ресурс в изграждането на който участват български екипи е страницата на Европейската обсерватория за цифрови медии (EDMO)[41], която се фокусира върху разпознаването и противодействието на дезинформацията в европейски мащаб.

В България действа и платформата на Фондация „Медийна грамотност за всеки“[42], която предлага образователни материали и инициативи за повишаване на медийната грамотност. Тези инструменти и платформи играят критична роля в изграждането на националното информационно пространство.

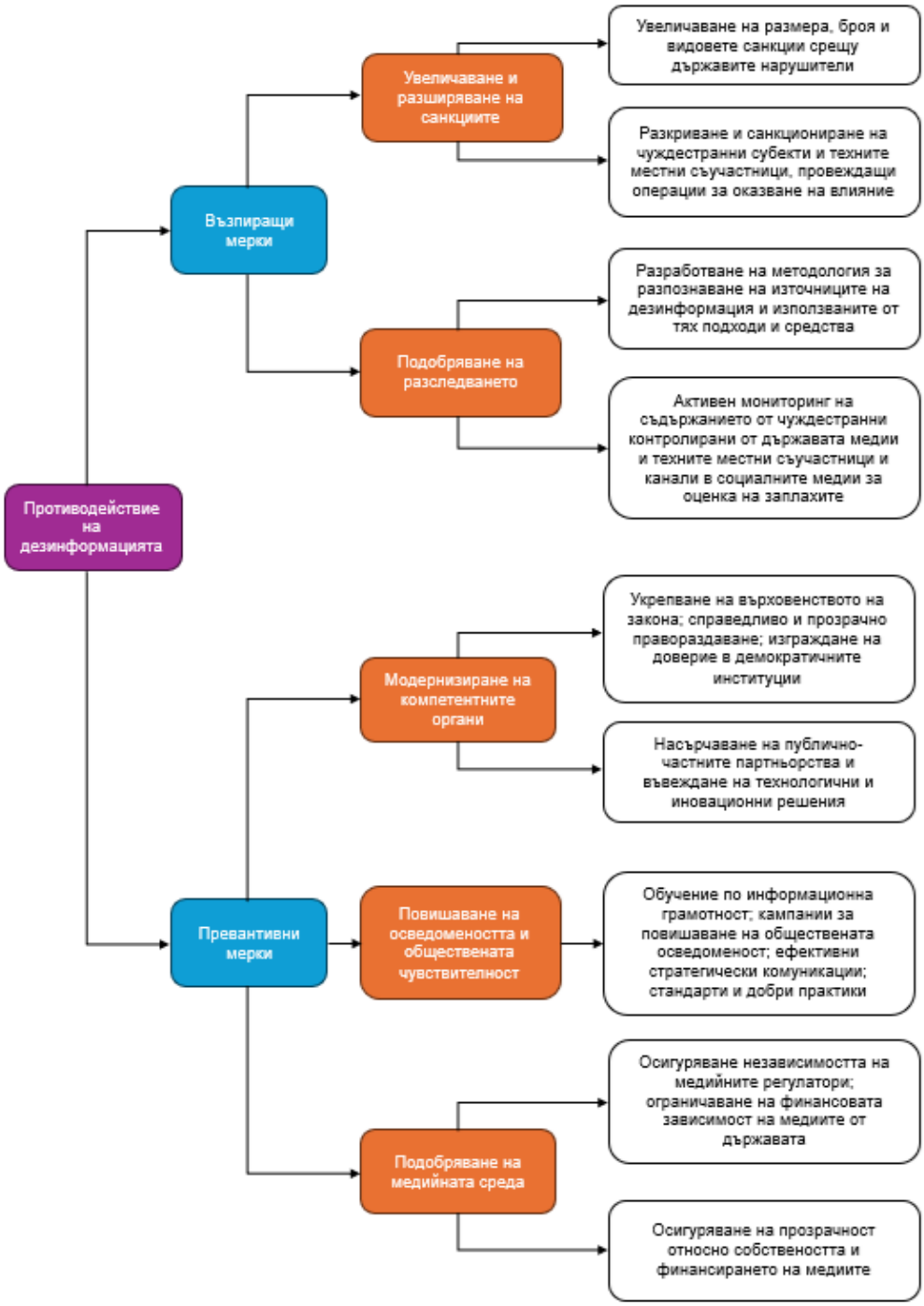
Националното когнитивно пространство е критичен елемент от сигурността и отбраната на всяка държава. В условията на нарастващи информационни заплахи мерките за повишаване на устойчивостта срещу дезинформация и стратегическите комуникации са основни инструменти за защита на обществото, но наред с технологичните методи най-сигурното оръжие а борба с дезинформацията остава образованието и медийната грамотност.

---

[40] Factcheck.bg. Платформа за проверка на факти. Асоциация на европейските журналисти – България, 2022. [Онлайн] Достъпно на: https://factcheck.bg.

[41] European Digital Media Observatory (EDMO) –Европейска обсервато-рия за цифрови медии (EDMO). [Онлайн] Достъпно на: https://edmo.eu

[42] Фондация „Медийна грамотност за всеки“. Образование за меди-ен свят, 2022. [Онлайн] Достъпно на: https://gramoten.li Даденият линк е към страницата на Коалиция за медийна грамотност.



Фигура 14. Мерки за противодействие на информацията

Отворени въпроси за самоподготовка

● Кои са основните принципи на стратегическите комуникации в националното когнитивно пространство?

● Каква е дефиницията за национално когнитивно пространство?

● Избройте методите за стратегически комуникации.

● Избройте мерките за изграждане на устойчивост срещу дезинформацията.

Глава шеста

ПРАКТИКА. ИЗГРАЖДАНЕ НА УСТОЙЧИВОСТ СРЕЩУ ДЕЗИНФОРМАЦИЯ

❖ Упражнения за създаване на стратегия за изграждане на когнитивна устойчивост. Решаване на примерни казуси от реални ситуации.

❖ Упражнения за разпознаване на фалшиви новини и дезинформация.

Практиката за разпознаване на чуждестранната когнитивна намеса е от изключителна важност. В упражнението се изисква обучаемите да приложат аналитичната рамка от Building Resilience and Psychological Defence (Palmertz et al. 2024), която предлага шестизмерен подход за оценка на чуждестранната когнитивна и информационна намеса в дадена страна или организация.

Рамка за анализ на чуждестранна когнитивна намеса

Рамката за анализ на чуждестранна когнитивна намеса включва шест измерения:

1. Оценка на риска.
2. Оценка на уязвимостта.
3. Механизми за отбрана.
4. Координация и сътрудничество.
5. Правна и политическа рамка.
6. Влияние и резултатност на действията.

За всяко от тези измерения могат да се формулират четири ключови въпроса и така се създава структуриран наръчник за оценка на чуждестранното влияние. Макар въпросите да са универсални, не е задължително да се дават отговори при липса на достатъчно стабилна основа в дадена държава. Тази рамка е примерна, защото е основно приложима за уязвимостите на демократични държави и институции, но може да

срещне несъответствия при използването ѝ в други политически контексти (Palmertz et al. 2024).

Занятието предлага обучаемите да работят в групи от 4 – 6 човека и да извършат анализ на когнитивната устойчивост на държавата, като използват анкетата на Палмерц за идентифициране и категоризиране на заплахите. След като попълнят анкетата, те трябва да анализират когнитивните заплахи и тяхното влияние върху обществото, и след това да предложат мерки за противодействие и формулиране на стратегия. За улеснение могат да използват таблица 2 по-долу.

Таблица 2

1. Оценка на заплахата	***СТЪПКА 1 Анализ***	***СТЪПКА 2 Оценка на влиянието***	***СТЪПКА 3 Действие, което трябва да се предприеме***
а) Кои са чуждите държави и актьори, намесващи се в политиката на държавата?			
b) Каква е специфичната тактика, техники и инструменти, които използват тези актьори при опита си да се намесват в политиката на държавата?			
c) Как нивата на заплаха и моделите на външно влияние се развиват в течение на времето?			
d) Какви нововъзникващи и бъдещи заплахи трябва да очаква и да се подготвя държавата?			
ЗАКЛЮЧЕНИЯ (Оценка на заплахите)			

2. Оценка на уязвимостта	***СТЪПКА 1 Анализ***	***СТЪПКА 2 Оценка на влиянието***	***СТЪПКА 3 Действие, което трябва да се предприеме***
а) Какви са основополагащите политически, социални и икономически фактори, които допринасят за уязвимостта на дадена държава при чужда намеса?			
b) Как се отразява влиянието на структурата на управлението на страната и демократичния процес върху външната намеса във вътрешните работи на държавата?			
c) Има ли особени социални разделения/въпроси или социални групи или организации, които нарочно или несъзнателно са били експлоатирани от чужди актьори с цел засилване на разногласията и манипулиране на общественото мнение?			
d) Как технологичната инфраструктура и мрежа на страната повлияват уязвимостта и на външно влияние?			
ЗАКЛЮЧЕНИЕ (Оценка на уязвимостта)			
3. Механизми за отбрана	***СТЪПКА 1 Анализ***	***СТЪПКА 2 Оценка на влиянието***	***СТЪПКА 3 Действие, което трябва да се предприеме***
а) Какви са съществуващите стратегии, политики и институции, чрез които се защитава държавата от външна намеса?			

b) По какъв начин отбранителните механизми засичат, предотвратяват и улесняват опитите за чужда намеса?			
c) Има ли пропуски или слабости в отбранителните способности на държавата, които трябва да бъдат адресирани?			
d) Как дадена държава се грижи за медийната грамотност, критичното мислене и устойчивост сред населението си с цел отблъскване на чужда намеса?			
ЗАКЛЮЧЕНИЯ (Механизми за отбрана)			
4. Координация и сътрудничество	***СТЪПКА 1 Анализ***	***СТЪПКА 2 Оценка на влиянието***	***СТЪПКА 3 Действие, което трябва да се предприеме***
a) Как съответните правителствени агенции, разузнавателни служби и служби за охрана координирано реагират на чуждата намеса във вътрешните работи?			
b) Как се развиват съвместните национални способности в рамките на спектъра на хибридните заплахи с цел идентифициране, анализ и противодействие на такива дейности?			
c) Каква е ролята на организациите на гражданското общество, медийните канали и ролята, която други недържавни актьори играят в подкрепа на отбраната срещу чуждо влияние?			

d) Как една държава може да участва в международно сътрудничество и обмен на добри практики, информация и разузнаване с международни партньори и съюзници?			
ЗАКЛЮЧЕНИЯ (Координация и сътрудничество)			

5. Правна и политическа рамка	***СТЪПКА 1 Анализ***	***СТЪПКА2 Оценка на влиянието***	***СТЪПКА 3 Действие, което трябва да се предприеме***
а) Какви правни рамки и регулации съществуват с цел отблъскване на външна намеса и защита на националната сигурност?			
b) Как тези закони и политики адресират комплексния характер на външното влияние и новите технологии, използвани от противниците?			
c) Има ли някакви законодателни пропуски или пропуски в политическите решения, на които трябва да се реагира с цел подсилване на отбраната срещу външно влияние/намеса?			
d) Как най-ефективно могат да се приложат и въведат в практика тези правни и политически мерки?			
ЗАКЛЮЧЕНИЯ (Правна и политическа рамка)			

6. Влияние и на постигане на резултат	*СТЪПКА 1 Анализ*	*СТЪПКА 2 Оценка на влиянието*	*СТЪПКА 3 Действие, което трябва да се предприеме*
a) Какво е измеримото влияние върху политическата стабилност на страната, общественото мнение и демократичния процес като се имат предвид второстепенни и непреднамерени ефекти на чуждото влияние ?			
b) Как отделната държава отговаря на определени специфични повтаряемости на чуждо влияние и какви са научените уроци?			
c) Как отбранителните механизми, които са използвани, показват ефективност в противодействието на външно влияние?			
d) Как гражданите на държавата възприемат ефективността на отбранителните мерки и тяхната увереност в способността на правителството?			
ЗАКЛЮЧЕНИЯ (Влияние и постигане на резултат)			

На база на рамката за анализ може да се изготви шаблон за анализ за всяко от шестте измерения като начална точка за насока, от която да се формулират допълнителни въпроси в зависимост от спецификата на средата и социалния контекст. Всеки аналитичен въпрос може да бъде анализиран чрез подход съставен от три стъпки:

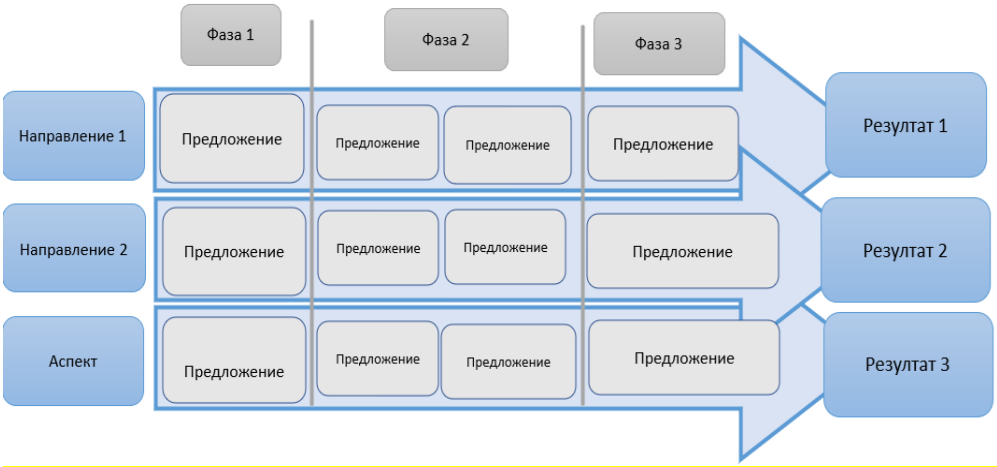
1) Анализ: отговор на поставения въпрос или посочване на проблема. Включва събиране на необходимите данни, информация и доказателства с цел осигуряване на задълбочено разбиране на ситуацията. В процеса трябва да се документират източниците, използвани при анализа. Тази първа стъпка поставя основата на следващите.

2) Оценка на влиянието – оценява се текущата значимост или влияние на обекта на анализ. Включва оценка на последиците върху различните участници, протичащите процеси и преследваните цели. Изследват се последиците и актуалността на анализираните фактори.

3) Действие – препоръка на специфични стъпки и стратегии с цел реакция на идентифицираните заплахи, уязвимости и възможности. Предложените действия трябва да се базират върху логична връзка между анализ и желани резултати, като се вземат предвид потенциалното влияние върху организацията или проекта. По този начин анализът ще бъде по-полезен при вземане на решение и бъдещото му прилагане.

Целта на този тристепенен подход е да се осигури цялостна и логична приемственост от цялата верига – от разбирането на проблема до оценяването на значимостта и предлагане на разумни решения. Оценката на всяко измерение приключва с обобщение на ключовата информация и на последиците и насочване към бъдещи аспекти и въпроси. По същия начин се оформят ключови действия и връзката между тях, насочване към цялостните перспективи, които трябва да се изведат в заключението.

След попълване на анкетата се анализират когнитивните заплахи и тяхното влияние върху обществото, в резултат на което биват предложени мерки за противодействие и формулиране на стратегия. Накрая групата представя своето решение в презентация и го защитава в дискусия с останалите участници в практическото занятие.



Фигура 15. Представяне на резултатите чрез матрица, схема или поточна диаграма

Примери и казуси от реални ситуации

Дезинформационните кампании са се превърнали в сериозен инструмент за манипулация на общественото мнение и подкопаване на доверието в институциите. Разглеждането на реални примери от нашата страна и световната практика позволява да се идентифицират общи модели и да се извлекат ценни уроци за противодействие.

Такива примери за използване на дезинформацията в хибридни конфликти можем да намерим в новините за Украйна след 2014 г., особено след започване на пълномащабна война, референдума за Брекзит (2016) и президентските избори в САЩ. Тези случаи подчертават ролята на дезинформацията като инструмент за влияние върху общественото мнение и дестабилизация на институциите.

Примери от България:

1. Дезинформацията около COVID-19.

Ситуация: По време на пандемията бяха разпространени фалшиви новини за задължителна мобилизация на армията за „тотален контрол над гражданите“. Това предизвика напрежение и недоверие сред обществото.

Урок: Липсата на бърза и прозрачна комуникация от официални източници допринесе за разпространението на слухове. Държавните институции трябва да реагират бързо с ясни и проверени съобщения, за да се ограничи паниката.

2. Фалшиви новини за военни учения.

Ситуация: Неправилно представени факти за учения на НАТО в България бяха използвани за създаване на негативни нагласи към армията и съюзниците.

Урок: Дезинформацията успя да подкопае престижа на институциите за сигурност. Важно е официалните източници да предоставят точна информация и да разясняват целите на ученията, за да предотвратят манипулации.

Международни примери:

1.Украйна – 2014 г.

Ситуация: Руската дезинформация изигра ключова роля в оправдаването на анексията на Крим и разпалването на конфликта в Източна Украйна. Фалшиви новини и снимки объркаха международната общност.

Урок: Дезинформацията може да бъде използвана за легитимиране на агресивни действия. Важно е да се идентифицират и опровергаят фалшивите новини в реално време.

2. САЩ – избори 2016 г.

Ситуация: Социалните мрежи бяха използвани за разпространение на дезинформация с цел манипулиране на обществените нагласи и подкопаване на доверието в демократичния процес.

Урок: Социалните платформи са мощно оръжие за разпространение на дезинформация. Необходимо е да се разработват механизми за автоматично маркиране на подозрително съдържание.

3. Военни операции в Сирия:

Ситуация: Фалшиви видеа и снимки бяха използвани за дискредитиране на международни мироопазващи мисии.

Урок: Визуалните материали са особено ефективни за манипулация. Важно е да се обучават военнослужещите и гражданите да разпознават манипулирано съдържание.

Чрез анализа на тези примери могат да се извлекат следните общи уроци:

– бърза реакция – времето е критичен фактор. Бързата реакция на официалните източници може да ограничи разпространението на дезинформация;

– прозрачна комуникация – ясните и проверени съобщения помагат за възстановяване на доверието;

– обучение и медийна грамотност – военнослужещите и гражданите трябва да бъдат обучени да разпознават и анализират дезинформация.

За да се приложат теоретичните знания на практика, в упражненията се разглеждат следните казуси:

Казус 1: Дезинформационна атака срещу военна операция.

Ситуация: В социалните мрежи се разпространява фалшива новина, че армията е извършила грешка по време на съвместно учение, което води до обществено недоволство.

Дискусия: Какви са непосредствените действия на армията? Как може да се провери източникът на информацията? Какви канали за опровержение са най-подходящи?

Казус 2: Вътрешна дезинформация в армията.

Ситуация: Разпространение на слух сред личния състав относно промяна в заповед, която може да доведе до напрежение и спад в морала.

Дискусия: Как да бъде идентифициран източникът на слуха? Каква е ролята на командния състав в успокояването на ситуацията? Как може да се предотврати бъдещо разпространение на подобни слухове?

Казус 3: Международна дезинформационна кампания.

Ситуация: Враждебна държава използва медии и социални мрежи, за да дискредитира ролята на България в НАТО.

Дискусия: Какви съвместни действия могат да бъдат предприети с партньори от НАТО? Как да се поддържа доверието на обществеността? Как да се подобри разпознаването на подобни кампании?

Възможни действия и решения

На базата на разгледаните казуси и дискусиите могат да се предложат следните действия:

– интегриране на обучение по критично мислене и медийна грамотност – военният и цивилният персонал трябва да бъдат обучени да разпознават и анализират дезинформация;

– създаване на симулационни упражнения – практическите тренировки помагат за развиване на умения за реакция при дезинформационни атаки;

– поддържане на активна и прозрачна комуникация: Официалните източници трябва да предоставят точна информация и да реагират бързо на слухове.

Разглеждането на реални казуси и извличането на уроци от тях са от съществено значение за изграждането на устойчивост срещу дезинформацията. Чрез комбинация от бърза реакция, прозрачна комуникация и обучение на персонала Българската армия може ефективно да се противопостави на дезинформационните заплахи и да поддържа доверието на обществото.

Проучването на казуси предоставя безценна дълбочина на разбиране за това как дезинформацията се замисля, конструира и разпространява чрез комуникационни модели. При изследването на тези казуси могат да бъдат анализирани пътищата, използвани за насочване към аудитории, манипулиране на общественото мнение и въздействие върху социалната и политическа среда.

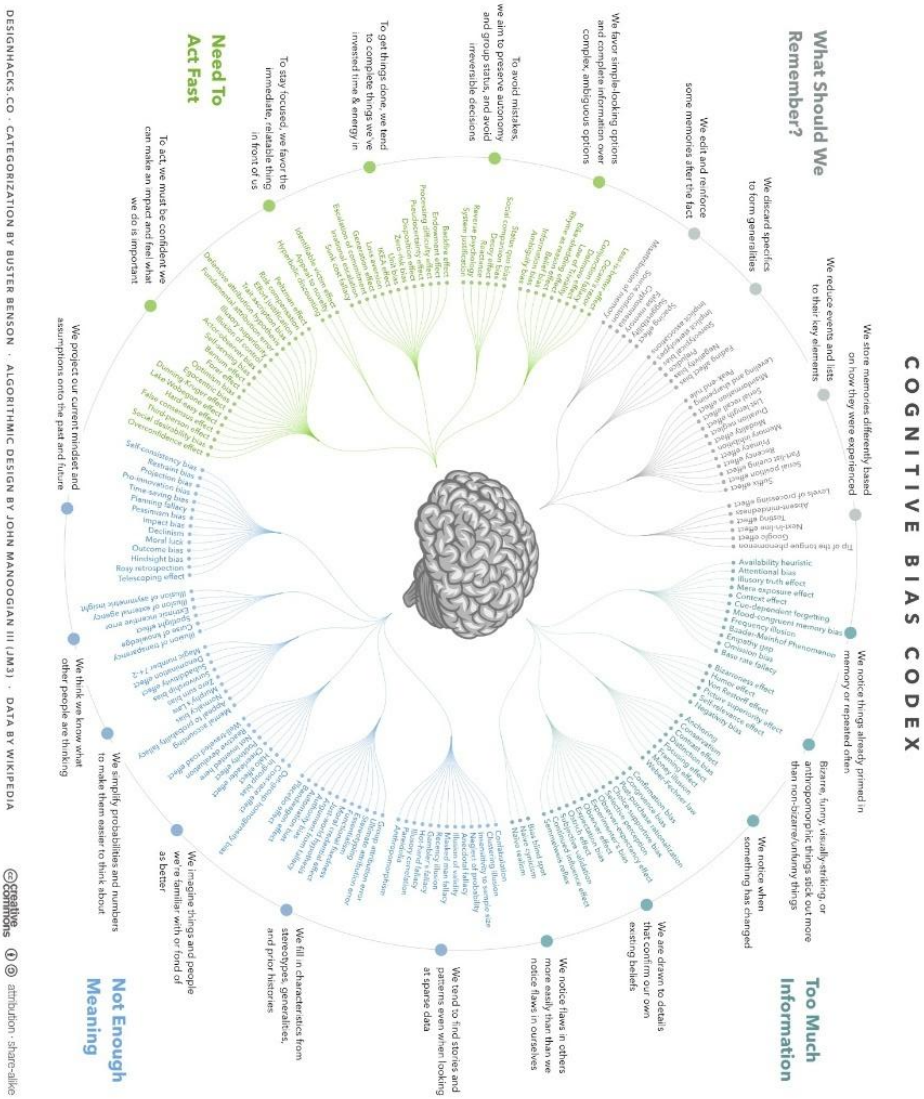
Важен пример представлява дирижираната кампания за дезинформация по време на президентските избори в Съединените щати през 2016 г. в която бяха използвани сложна комбинация от технологични и психологически тактики за умишлено разпространение на невярна информация. Това е образец за адаптация на традиционния комуникационен модел, при който изпращачът целенасочено създава съобщения с намерението да измами получателя, а съобщението е фино настроено, за да използва съществуващите обществени разделения.

Друг интересен пример е разпространението на дезинформация около избухването на пандемията от COVID-19. Фалшивите разкази за произхода на вируса, ефикасността на маските и за ваксините се разпространяваха с изумителна скорост. Уникални характеристики на тази кампания за дезинформация бяха скоростта и обхватът на разпространение, улеснени от взаимносвързан цифров пейзаж, илюстриращ как съвременните комуникационни модели трябва да вземат предвид виралността, активирана от платформите на социалните медии.

Социалните медийни платформи разширяват дезинформацията чрез алгоритми, които са предназначени да увеличат ангажираността на потребителите, често за сметка на фактическата точност. Тези управлявани от алгоритми комуникационни модели създават ехо камери, засилващи пристрастията на потребителите, което води до плодородна почва за процъфтяване и увековечаване на дезинформацията. Такъв тип среда предизвиква традиционните представи за линейния комуникационен процес, тъй като обратната връзка и участието на потребителите на социални медии усложняват комуникационната диаграма.

Анализът на кампании за дезинформация относно изменението на климата, като тези, които поставят под съмнение научния консенсус, разкрива използването на комуникационни модели, разчитащи на авторитета на привидно достоверни източници. При разглеждането на тези казуси трябва да се признае ролята на психологическите принципи, като пристрастието към потвърждението, за успеха на кампаниите за дезинформация. Хората имат склонност да предпочитат информация, която потвърждава съществуващите им вярвания – фактор, който архитектите на дезинформация използват при проектирането на своите комуникационни стратегии.

Всеки от тези случаи служи като таблица с инструкции за изследователи, преподаватели и политици, за да разберат по-добре и по този начин да разработят по-ефективни инструменти и стратегии за противодействие на дезинформацията. Продължаващото проучване на тези случаи също помага за напредъка на теоретичните парадигми, които могат да бъдат прагматично преведени в образование за медийна грамотност и кампании за обществена осведоменост.



Фигура 16. Класификация на когнитивните предразсъдъци
Източник: JOHN MANOOGIAN III, 2016. *Cognitive Bias Codex*. Достъпно на: https://archive.org/details/cognitive-bias-codex_202202

Разпространението на дезинформация не е ново явление, но дълбокото въздействие на технологичния напредък върху комуникационния

модел изисква постоянен контрол. Тези казуси са предвестници на сложността и потенциалната вреда, която крие неконтролираното разпространение на дезинформация, като подчертават необходимостта от многостранен подход за справяне с проблема.

Установяване на факти в постистинска среда

Понятието „постистина“ отразява ситуация, при която емоциите и личните вярвания често засенчват обективните факти при формирането на общественото мнение (Higgins 2016). В този контекст първата стъпка е разграничаването между факт и мнение. Фактът е обективна реалност, която може да бъде потвърдена с доказателства, докато мнението е субективно твърдение, отразяващо вярвания или преценки. Пред лицето на дезинформацията това ясно разграничение се размива, тъй като невярната информация често се представя подвеждащо като факт, което прави задачата за установяване на истински факти трудна.

Днешният процес на проверка на фактите включва не само директен преглед на наличните данни, но и критично изследване на източниците на информация. Учени като Левандовски, Екер и Куук (Lewandowsky, Ecker & Cook 2017) твърдят, че за ефективно установяване на факти хората трябва да оценят достоверността на източниците, да сверят информацията с множество реномирани бази данни и да останат бдителни към пристрастия, които могат да повлияят върху тълкуването. Тези стъпки са основни, за да се гарантира, че всеки цитиран в научен дискурс факт може да издържи на проверка.

Предизвикателството обаче не приключва с установяването на фактите. Начинът, по който се съобщават те, е също толкова важен. Самото предоставяне на коригираща информация невинаги е достатъчно, за да промени създадените убеждения. Ефектът на продължаващото влияние показва, че дезинформацията може да остане в паметта на хората и да продължи да влияе върху разсъжденията дори след коригиране.

Ролята на съобщенията при разпространението на дезинформация е ключов фактор за нейното въздействие и успешното ѝ проникване в обществото. Завладяващите и последователни наративи, които се вписват в по-широки социални и културни контексти, е по-вероятно да бъдат приети и разпространявани. Особено силно влияние оказват истории, които подкрепят манталитета „ние срещу тях“, като засилват разделението и предубежденията в обществото (Harsin 2015).

Фронталните групи и астротурфингът играят ключова роля в разпространението на дезинформация чрез манипулативни съобщения. Понятието фронтални групи се използва за организации, които изглеждат

независими и представляват интересите на обществото, но всъщност са създадени и финансирани от частни интереси със скрити цели. Те често се използват за разпространение на дезинформация с цел създаване на легитимност и заблуда на обществеността.

Астротурфингът е техника, при която се симулира подкрепа от широката общественост за определени идеи, продукти или каузи. Чрез астротурфинг се създава впечатление за масово движение, което прикрива истинските цели на инициаторите. Съобщенията от такива групи са подготвени така, че да имитират истинска загриженост на общността, но крайната им цел е да подведат и нарушат общественото разбиране (Lyon & Montgomery 2013).

Отворени въпроси за самоподготовка

- Какви са трите подхода за борба с дезинформацията?
- Кои елементи включва критичното мислене?
- Какви са стъпките на алгоритъма за разпознаване на фалшиви новини?

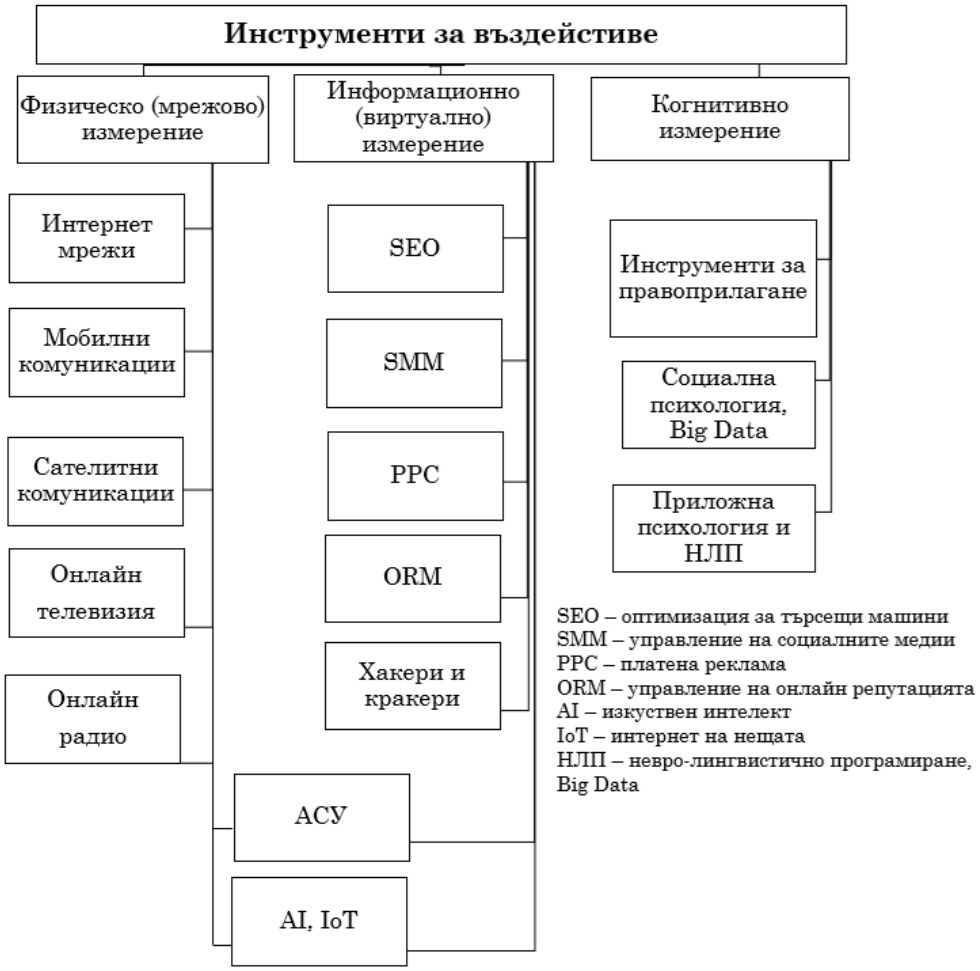
Глава седма

РАБОТА С ДИГИТАЛНИ ИНСТРУМЕНТИ ЗА ПРОВЕРКА НА ФАКТИ И БОРБА С ДЕЗИНФОРМАЦИЯТА

- Работа с дигитални инструменти за проверка на факти и борба с дезинформацията.
- Алгоритъм за разпознаване на дезинформацията в Българското интернет пространство.

Усилията за справяне с дезинформацията включват множество заинтересовани страни, включително политици, технологични компании и гражданско общество. Именно в този контекст се разкрива значението на дигиталните инструменти за проверка на фактите не само за идентифициране и коригиране на неистини, но и за обучение и овластяване на хората да различават надеждната информация от дезинформацията. Този преглед поставя началото на по-задълбочено изследване на това как цифровите инструменти могат да подкрепят критичната оценка на информацията и да помогнат за смекчаване на неблагоприятните ефекти от дезинформацията върху обществото.

Ако разгледаме внимателно възможните сфери на конфронтация и петте бойни полѐта, навсякъде може да се види присъствието на информационния компонент. Като се позоваваме на описаните вече определения и методи за мрежова конфронтация, се вижда, че съвременните информационни конфликти се основават на високотехнологични мрежови средства, специални манипулации на предоставяното съдържание, набор от социалнопсихологически инструменти и техники, използвани за имплицитно въздействие на индивиди или групи хора. Моделът на Изследователската програма за командване и управление към Министерството на отбраната на САЩ посочва, че действията имат три измерения: *физическо, информационно и когнитивно измерение, като следствие от това можем да определим три вида инструменти на дезинформацията* (Dimov 2018).



Фигура 17. Инструменти за медийно въздействие (Dimov 2018)

Във физическото измерение информацията се възприема като сигнали, които могат да се приемат и предават от различни технологични устройства – мрежи, компютърни системи, мобилни комуникации, телевизия, радио, сателитни комуникации и т.н. (Kluban, Kurban & Lyubovec 2016). В информационното измерение информацията се възприема като съдържание, което се създава, обработва и споделя и хората лесно могат да манипулират информационните послания и управленски решения. Това е информацията, която срещаме всеки ден като потребители или създатели на съдържание в уебсайтовете и социалните мрежи, под формата на текстове, видео, аудио съобщения и др. Използват се технологии за манипулиране на съдържанието, включващи *оптимизация на сайтове*

за търсещите машини (SEO), управление на социални медии (SMM), контекстна и платена реклама (PPC), управление на онлайн репутацията, хакерски атаки и други дейности, изискващи експертен персонал.

В когнитивното измерение се води война за човешките умове и колективното поведение (Alberts, Garstka, Hayes, Signori 2001). Неговите съставни части са нематериални – лидерство, морал, сплотеност на подразделенията, ниво на подготовка, осъзнаване на обстановката и обществено мнение. Когнитивното измерение е свят на *нормативните и психосоциалните техники, социалната психология, приложната психология и невролингвистичното програмиране*, които влияят на поведението и комуникационните процеси на социалните групи или индивидите. Тук е мястото на анализа на голямо количество данни (Big Data), които обогатяват изследванията в социалните науки и получаването на нова информация (Chen, Yu 2018).

Технологични инструменти за борба с дезинформацията

Първоначално отговорността за проверка на фактите беше основно в обсега на редакциите и журналистическите организации, но с появата на World Wide Web и последвалата експлозия в генерираното от потребителите съдържание този модел стана неустойчив. Нуждата от автоматизирани или полуавтоматизирани инструменти за проверка на фактите стана очевидна.

Първото поколение цифрови инструменти за проверка на факти представляват обикновени уебсайтове, предлагащи такива услуги. Организации като FactCheck.org, стартирана през 2003 г., и PolitiFact, стартирана през 2007 г., започнаха да предоставят на обществеността ресурси за проверка на политически изявления и твърдения. Тези платформи използваха достъпността и скоростта на интернет, за да достигнат до по-широка аудитория, насърчавайки по-информиран публичен дискурс.

Едновременно с това академични институции и технологични компании започнаха да изследват изчислителни методи за подпомагане на процеса на проверка. Разработването на алгоритми, способни да кръстосват данни и да оценяват надеждността на източниците, се превърна във фокусна точка. Иновациите, невролингвистичното програмиране и машинното обучение оттогава позволиха автоматизирането на определени аспекти на проверката на фактите, позволявайки анализ на големи обеми данни с нарастваща точност.

Съвременният пейзаж на дигиталните инструменти за проверка на факти е разнообразен, включващ комбинация от проекти с отворен код,

патентован софтуер и инициативи за сътрудничество. Инструменти като автоматизираната машина за проверка на факти на Full Fact и алгоритъмът ClaimBuster, предназначени да идентифицират фактически твърдения, които си струва да бъдат проверени в големи набори от данни, илюстрират тази тенденция. Освен това усилия като Fake News Challenge стимулират усъвършенстването на инструменти, които оценяват истинността на новинарските истории чрез насърчаване на сътрудничеството между технолози и експерти по темата.

Образователен инструмент за борба с дезинформацията

Образователните инициативи са основен инструмент за повишаване на устойчивостта срещу дезинформацията, като развиват умения за медийна грамотност и критично мислене. Тези два аспекта са взаимносвързани и се допълват, за да предоставят на военнослужещите и обществото необходимите инструменти за разпознаване и противодействие на дезинформацията.

В предишната глава разгледахме медийната грамотност, която дава способността да се анализира, оценява и интерпретира информацията, като от гледна точка за борбата с дезинформацията тя включва уменията:

– за разпознаване на фалшиви новини – обучение за идентифициране на фалшиви новини чрез анализ на източници, проверка на факти и разбиране на контекста;

– откриване на фалшиви профили – насочване на вниманието към признаци на фалшиви акаунти като липса на лична информация, подозрителна активност или използване на автоматизирани скриптове;

– анализ на визуално съдържание – обучение за разпознаване на манипулирани изображения и видеа, като се използват инструменти за обратна проверка на източниците.

Практическото обучение по медийна грамотност може да се осъществява чрез организиране на симулации и игри, в които участниците трябва да разпознаят и реагират на дезинформационни атаки, както и да използват специализирани инструменти за проверка на факти, като FactCheck.org или Google Reverse Image Search.

Алгоритъм за разпознаване на фалшивите новини

Една новина в социалните медии може да бъде определена като достоверна, частично достоверна и недостоверна. За да успеем да ги различим по-лесно, можем да използваме онлайн инструмент за разпознаване на фалшивите новини, например на страницата Postvai.com[43]. Инструментът може да подпомогне откриването на белези за фалшифициране, но последната преценка остава за човека, който го използва. За да различим истината от лъжата в интернет, с помощта на предложения алгоритъм ние трябва да си отговорим на следните седем въпроса:

1. Кой е източникът?

Отправна точка при оценката на една новина е определянето на типа на нейния източник – дали е първичен, вторичен, или анонимен.

● В интернет това започва с визуална оценка на цялостния дизайн на сайта. Трябва да видим дали е направен професионално, или в него има прекалено много реклами.

● Проверява се дали страницата използва безплатен домейн от типа .ml, .ga, .tk и т.н. Изглежда ли, че URL адресът на уеб страницата е достоверен? Следва да се обърне внимание на адресите, които са направени, за да изглеждат официални. Някои от тях могат да подведат интернет потребителите за името на домейн, което имитира официалния уебсайт на призната организация (пример: cnn.com.de, а не cnn.com). Ако URL адресът изглежда подозрителен, потърсете организацията в Google, за да намерите истинския адрес. Оригиналната страница на организацията обикновено се появява в горната част на списъка с резултати, докато тази с фалшивия адрес ще излезе много по-назад.

● Страниците „За нас“ и „Контакти“ посочват ли съществуващо име, адрес, телефони и имейл, които лесно могат да бъдат проследени в международния регистър на домейни от типа DomainBigData? Посочени ли са целта и мисията на сайта? Ако има линкове на страницата, къде ви отвеждат?

● Можем да върнем сайта назад във времето с инструменти като Archive.org и да видим дали има подозрително или изтрито съдържание.

● Трябва да проверим за регистрирани стари злоупотреби в сайтове, които събират подобни нарушения, като Медийно око, MyWot,

[43] *Ръководство за борба с фалшивите новини*. Достъпно на: https://postvai.com/fakenews/.

Decodex и раздела на Нова TV за фалшивите новини. Могат да бъдат потърсени всякакви доклади, идентифициращи страницата като сайт за фалшиви или истински новини.

● Много важен момент е да разгледаме кода на сайта за съществуващи идентификатори от типа на Google Analytics, които можем да проследим. Днес в интернет почти не съществуват сайтове без такъв инструмент за обратна връзка, а те обикновено са свързани с реални акаунти. Без да разбираме от код, можем да направим проверка с помощта на инструмента SpayOnWeb, с който да разберем за други свързани сайтове на неговия собственик (Ivanov, Dimov 2020).

2. Кой е авторът?

● Кой е написал статията? Подписан ли е текстът? Автор, който е инвестирал време в написването на добре проучена статия, обикновено иска да се появи името му.

● Ние трябва да проучим идентичността на автора, като реално, физическо лице и какъв дигитален отпечатък е оставил той в интернет. За целта можем да направим бързо търсене в Google по намерените имейли, телефони или други открити данни. Още по-лесно е да използваме онлайн инструменти от рода на WebMii или други специализирани търсачки на хора, които ще покажат на едно място всички негови връзки в социалните мрежи и допълнителни резултати от няколко търсещи машини на едно място.

● Какви са неговите умения като експерт? По какви въпроси пише най-често? Изследвайте автора, намерете неговата професия, квалификация и други статии, които е написал. Научете кои социални мрежи използва и какво публикува в тях? Работи ли за реномирана организация? Другите му статии добре ли са документирани? Пристрàстен ли е към някоя политическа сила или друга идея и т.н.

3. Какво е съобщението?

● Представя ли статията различни гледни точки? Текстовете в новините трябва да бъдат безпристрастни и да отразяват различни гледни точки по темата. В противен случай читателите трябва да имат предвид, че имат достъп само до част от истината и написаното може да крие пристрастия.

● За целта трябва да започнем с бърз преглед на заглавията за нискокачествени и сензационни измислици, да проверим има ли много правописни грешки. Добре проучените статии обикновено се четат и се препрочитат преди публикуването.

● След това с помощта на инструменти за плагиатство можем да проверим уникалността на текста. Ако той е копиран от друго място, инструментите ще ни покажат първоизточника. Защо да вярваме на човек, който е копирал от друг източник?

● Съобщението балансирано ли е и подписано ли е с името на автора, авторът цитира ли източници в подкрепа на коментарите му? Надеждни ли са тези източници? Поддържат ли твърденията на автора?

● Накрая можем да проверим в интернет какво казват вече доказани експерти по темата.

4. Какво е снимано?

Валидацията на използваните изображения е много важен момент в проверката на дадена новина. Ако открием белези за фалшифициране на използваните снимки, информацията няма как да бъде вярна.

● Разгледайте изображението, вижте има ли неестествени пропорции, цветове или съмнителни детайли.

● Направете обратно търсене за подобни изображения в интернет, за да видите къде са използвани те и първата дата на тяхното публикуване. Така можете да разберете кой е първоизточникът.

● С инструментите Image Verification Assistant или http://fotoforensics.com/ може да бъде проверено дали са нанасяни технически поправки за фалшифициране на снимката и да се види EXIF информацията на файла. Често в него остават данни за камерата, която го е заснела, дори името на нейния собственик.

● Изображението може да бъде засечено с други източници, които потвърждават местоположението и времето. Това са например номера, табели, знаци, терен, облекло. По този начин могат да бъдат идентифицирани несъответстващите детайли (Ivanov, Dimov 2020).

5. Какво е видеото?

Не бива да се забравя, че видеоклиповете и снимките може да са редактирани, за да служат за целите на автора. Тук важат същите правила като за снимките.

● Анализирайте медийния контекст на видеоклипа в InVID Analysis или направете обратно търсене на извлечени изображения от клипа с помощта на инструментите, посочени в приложението.

● Разгледайте акаунта, от който са публикувани видеото и коментарите под него. Вижте има ли описания на клипа, други социални профили и имат ли разлика с метаданните на файла с Metadata2go.

● Потърсете още видеоканали в YouTube по ключова дума със SocialBlade и дали може да намерите свързана информация в тях.

● Анализирайте събраната информация, времето и мястото, за което става въпрос в клипа (Ivanov, Dimov 2020).

6. Кога и къде?

Кога са публикувани статията, снимката или видеоклипът? Публикация без дата може да съдържа информация, която вече не е актуална или впоследствие е опровергана или дискредитирана. Имайте предвид, че датата може да е променена, за да се създаде впечатлението, че новините са по-актуални, отколкото са всъщност. Ако например във видеоклип се твърди, че действията се развиват в гр. Алепо (Сирия) на определена дата и на кадрите виждаме, че е дъждовно, можем да проверим дали в този град е валяло на посочената дата с помощта на услугата WoframAlfa. За да определим дали ни лъжат за мястото на събитието, можем да използваме услугите Google Earth или Street View. С тяхна помощ можем да видим реален изглед от терена на събитието и дали дадената улица, място или сграда изглеждат по същия начин като на съответния клип или снимка. Ако в изображението има някаква табела или друг надпис на непознат за нас език, можем да използваме някой инструмент за конвертиране от изображение към текст (Optical Character Recognition (OCR), след което да го преведем с Google Translate.

7. Защо?

Накрая трябва да се запитаме защо се публикува това съобщение. Каква е целта на тази статия – да информира или да манипулира? Бъдете критични, дори скептични по отношение на информацията, която получавате, като си отговорите на следните три основни въпроса:

– Можете ли да се доверите на източника и автора?;

– Открихте ли подозрителни белези за фалшифициране на съдържанието на текста, изображенията и видеоклиповете?;

– Верни ли са отговорите на въпросите кога и къде на посоченото от автора?

Отговорите на тези въпроси ще ви дадат възможност да определите дадената информация като достоверна, частично достоверна или недостоверна. Най-важното в случая е да се запитате убеждава ли ви статията в нещо и в какво. След това си задайте въпроса защо някой иска да ви убеди да приемете това конкретно мнение. Кой има интерес към това, което мислите? Помислете също кой има полза от фалшивата новина и защо. (Ivanov, Dimov 2020).

Характеристики на сайтовете по отношение на тяхната надеждност като източници на информация

Интернет пространството непрекъснато се развива и разширява. Ежедневно се появяват нови сайтове и се публикува актуално съдържание. За да може потребителят да се ориентира в този океан от информация и да намери най-полезната за него, се ползват специализирани сайтове, наречени „търсещи машини“ или накратко „търсачки“. Чрез тях с въвеждането на няколко ключови думи се предоставя списък с множество сайтове, страници и ресурси, които отговарят на зададените критерии за търсене.

Всъщност процесът е много по-сложен и остава скрит за потребителя. Въпреки че всяка търсеща машина използва собствени алгоритми за търсене и извеждане на информация, тази задача се извършва в няколко основни етапа:

– събиране на информация – периодично се обхожда интернет пространството и се събира наличната информация;

– анализ на събраната информация – алгоритмите на търсещите машини по определени правила и критерии обработват събраната информация и „разбират“ за какво се отнася тя;

– оценка на събраната информация – на базата на определени параметри и характеристики се прави оценка доколко тази информация и нейният източник са актуални, достоверни и пълни;

– предоставяне на получената информация – в зависимост от запитването на потребителя, неговото поведение и други характеристики (например географското му местоположение, езика, устройството, което ползва, и др.) се извеждат най-подходящите според търсещата машина резултати.

От гледна точка на борбата с дезинформацията и фалшивите новини по-подробно ще бъде разгледан третият етап – оценката на информацията и нейният източник. На коя позиция ще бъде изведен даден сайт или страница при търсене по определени ключови думи зависи от множество характеристики, които могат да бъдат разделени в две основни групи – технически характеристики и съдържание на сайта. Към техническите характеристики спадат скоростта на зареждане, спазване на стандартите и добрите практики, възможност за ползване на различни устройства и др. Докато изграждането на сайт, който да покрива напълно или в много голяма степен тези изисквания, е сравнително лесна задача, то създаването на ново, качествено, актуално и достоверно съдържание е много по-труден и продължителен процес.

На базата на събраната, обработена и анализирана информация търсещите машини дават цифрови оценки на всеки сайт, чрез които се определя качеството на неговото съдържание. Основните оценки са:

● Google PageRank (PR) – цифрова стойност от 0 (нула, най-ниска стойност) до 10 (най-висока стойност). Изчислява се на базата на множество параметри, сред които наличие на нова информация, уникално съдържание, връзки от и към други страници с висок рейтинг, и др. Сайтовете с висок PR се приемат за източник на надеждна, достоверна и проверена информация, докато тези с нисък вероятно съдържат фалшиви новини, дезинформация и/или дублирано съдържание.

● Domain Authority (DA) е параметър за класиране в търсачките, разработен от софтуерната компания Moz, предвиждащ колко вероятно е даден уебсайт да се класира в страниците с резултати от търсачките (SERPs). Резултатите варират от 1 до 100, като по-високите съответстват на по-голяма вероятност за класиране. Параметърът се изчислява чрез оценка на множество фактори, включително свързване на основни домейни и общ брой връзки в един резултат от DA.

● Page Authority (PA) е параметър, също разработен от Moz, който предвижда колко добре ще се класира конкретна страница на страниците с резултати от търсачките (SERP). Резултатите за авторитет на страницата се определят по логаритмична скала от 0 до 100. По този начин е значително по-лесно да се увеличи стойността от 20 на 30, отколкото от 70 на 80.

● Trust Flow (TF) е метрика на потока, предоставена от Majestic – популярен инструмент за SEO и анализ на връзки. Той може да има стойности от 0 до 100 и оценява възприетата надеждност на уебсайта от качеството на обратните връзки. Резултат от потока на доверие 10 не означава, че имате 10 обратни връзки или 10 надеждни обратни връзки, а по-скоро дава контекст на качеството на вашия обхват, PR и подобни дейности. Заедно показателите Citation Flow и Trust Flow образуват алгоритъма Majestic Flow Metrics. Обобщено – представлява качеството на връзките, които сочат към страници от вашият сайт.

● Citation Flow (CF) също е алгоритъм разработен от Majestic. Този показател изразява оценка от 0 до 100 и има за цел да изобрази колко авторитетен може да бъде даден уебсайт според това колко сайтове се свързват с него. В допълнение, потокът от цитирания също определя тежестта или авторитета на връзките, които вашият сайт има и може да предаде. Потокът от цитирания сам по себе си не е достатъчен, за да се определи авторитета на даден уебсайт, и той ще работи заедно с много други аспекти на SEO, за да се получи представа за надеждността, екс-

пертизата и авторитета на сайта. Обобщено, това е резултат, който отразява количеството връзки, които сочат към даден уебсайт, без да се интересува дали връзката е с добро или лошо качество. Уеб страница с по-висок Trust Flow от Citation Flow обикновено има връзки с добро качество, което представлява параметъра Trust Ratio (TR) = TF/CF.

● Topical Trust Flow (Topical TF) – резултатите на Majestic Topical Trust Flow са между 0 и 100, дадени на категории, за да се определи нишата или сектора на даден URL адрес или домейн. Колкото по-висок е резултатът в дадена категория, толкова повече връзки в тази категория отиват към URL адреса. Topical Trust Flow може да се използва за определяне на тематичната релевантност на връзките, сочещи към даден URL адрес, като същевременно се разбере колко влиятелен ще бъде определен URL адрес в дадена категория за връзки или трафик.

● Domain Rating (DR) е алгоритъм разработен от Ahrefs и показва силата на профила на обратната връзка на уебсайта в сравнение с останалите в база данни по 100-точкова скала.

В интернет има множество инструменти за проверка на характеристиките на сайтовете по отношение на тяхната надеждност като източници на информация чрез тези и множество други параметри. Важно е да познаваме тези инструменти, да ги ползваме и да можем правилно да анализираме получените резултати. Когато имаме съмнения за достоверността на дадена информация или на базата на събраните данни трябва да вземем важно решение, то тяхното ползване е силно препоръчително, а ако не сме сигурни в оценката на данните следва да се обърнем към специалист.

Отворени въпроси за самоподготовка

● Избройте основните видове инструменти за въздействие в интернет.

● Кои са седемте стъпки на алгоритъма за разпознаване на фалшиви новини?

● Какви видове източници разпознавате?

Глава осма

ПРАКТИКА. РАЗПОЗНАВАНЕ НА ТРОЛОВЕ, БОТОВЕ И ФАЛШИВИ ПРОФИЛИ

❖ Как да проверим изображение или видео за оригиналност.

❖ Разпознаване на тролове, ботове и фалшиви профили.

❖ Работа с инструменти за събиране на информация от открити източници.

Често в дейността по управление на онлайн репутацията и провеждането на информационни операции се използват т.нар. тролове или агенти за влияние. В интернет жаргона под думата „трол“ се разбира *човек, който публикува провокативни коментари по дадена тема с цел да смути автора или да разстрои нормалната дискусия в даден форум, като насочи темата в определена посока*. Дейността на подобен човек се нарича „тролене“. Това е деструктивен феномен, започващ от обикновено развлечение за сметка на по-неопитните потребители, стигащ до нивото на информационна война (Theohary, Rollins 2011). Днес съществуват цели институции за тролинг, които организират платени групи хора с цел агитация и манипулиране на резултатите в Интернет и общественото мнение.

Обикновено, троловете „работят“ в две направления. Едното е чрез провокация и обиждане на съвсем непознати хора, а второто е добре планирана разработка с цел отмъщение на конкретен човек или група чрез използване на различни слухове, клевети и компромати.

Трябва да се прави разлика между хейтър и трол. Докато първите са природно негативни и просто изразяват омраза към всичко, то вторите са по-скоро хитри манипулатори.

Най-общо троловете се делят на два вида – прости и сложни. Простите тролове, използват явни обиди и целенасочено нарушават правилата на форумите, а сложните работят на границата на нарушенията.

Стратегии за тролене по света и у нас

Все по-често започва да се говори за воденето на информационна война и нуждата от създаване на кибер подразделения във въоръжените сили. При модерните конфликти те със сигурност не могат да се лишат от използването на тролове за моделиране на общественото мнение.

1. *Западна школа за тролене*. В западния свят платеният тролинг е отдавна развит, дори му се обръща специално внимание от държавните институции. Въоръжените сили на Великобритания създават специално интернет подразделение за „психологически атаки" наречено „Бригада 77" , чиято численост може да достигне до 2000 обучени трола. В Съединените щати военните провеждат операция „Искрен глас" за разработване на специален тролски софтуер – Ntrepid, чрез който един оператор ще може да борави с 10 различни акаунта.

Голяма част от англоговорящите тролове и групите Anonymous се раждат в сайта 4chan.org. Той е безплатен, не изисква регистрация или акаунт, постоянно се обновява и няма база данни, което води до прекалена разкрепостеност. Там най-вече се качват картинки наречени „мемове" и демотивиращи плакати. Един такъв мем е главата на трола – едно безформено, разкривено лице, което често ядосва останалите потребители на форумите. Друг такъв сайт е Urban Dictionary и българския „Всичко за 1 лев" – нещо като пародия на Wikipedia за тролове.

2. *Руска фабрика за тролове*. В нашумяло интервю с известния руски блогър Марат Буркхард"[44] той твърди, че организация за „Интернет изследвания" работи като огромна фабрика за тролове. Там са били заети около 200 – 300 човека, разделени в украински отдел, английски отдел за бомбардиране на CNN и BBC, Фейсбук отдел, за останалите социални мрежи, местни и регионални сайтове, новинарски, за създаване на демотивиращи колажи, отдел за видео клипове. Първоначалната заплата на един човек е била около 700 долара за норма от 135 коментара при 12-часова работна смяна.

3. *Стратегия „Злодей, снимка, линк"*. При манипулиране на общественото мнение троловете работят в групи от по трима души по метод, наречен „Злодей, снимка, линк". Първият човек е „злодей", той играе ролята на съмняващ се в написаното критикар. Вторите двама започват спор с него от рода, че „всичко написано е вярно, ето виж…" и единият слага снимка, а другият поставя линк към специално написана статия в подкрепа на аргументите им. Във всеки от коментарите са длъжни да включват подбрани

[44] VOLCHEK, D.; SINDELAR, D., 2015. One Professional Russian Troll Tells All. *Eurasinet*. Достъпно на: https://eurasianet.org/one-professional-russian-troll-tells-all.

ключови думи, които трябва да излязат на челните места в търсачките и опорни точки за коментиране. Във фирмата за целта е имало подбрани каталози с регионални сайтове и за една смяна е трябвало да прекосят цялата страна по азбучен ред чрез метода „Злодей, снимка, линк“, като коментират статии по определени опорни точки, например войната в Украйна, Путин и т.н.

Решаване на примерна задача:

Тема: *Натовски войници се бият за Украинската армия*.

Ключови думи: *Война в Украйна; Русия; НАТО; наемници*.

Необходими са 3 трола, 1 статия, 3 коментара, 1 снимка или видео, 1 линк.

Работата започва след специален пост, публикуван в социалната мрежа LiveJournal, че чужди наемници се бият на страната на Украинската армия в със специално разработено видео, показващо двама американски войници. Появява се злодея и оспорва написваното, като казва, че не е ясно какво са правили там американските войници, включвайки в поста си задължителните ключови думи. Идва вторият трол и потвърждава статията, като добавя линк към втора статия, в която пише за американските войници. Следващият трол със снимката обвинява американците в лицемерие и добавя демотивиращ колаж за акцент.

Тънкости – винаги единият трол е лош, другият му противоречи, а третият е умерен, но изразява желаната от поръчителя позиция. Освен това, когато спорят помежду си, по-лесно си изкарват нормата от постинги. Още по-добре е, когато се включи някой почтен потребител на интернет форум, тогава той им помага, без да знае за това.

Български принос в стратегията за тролене в социалните мрежи

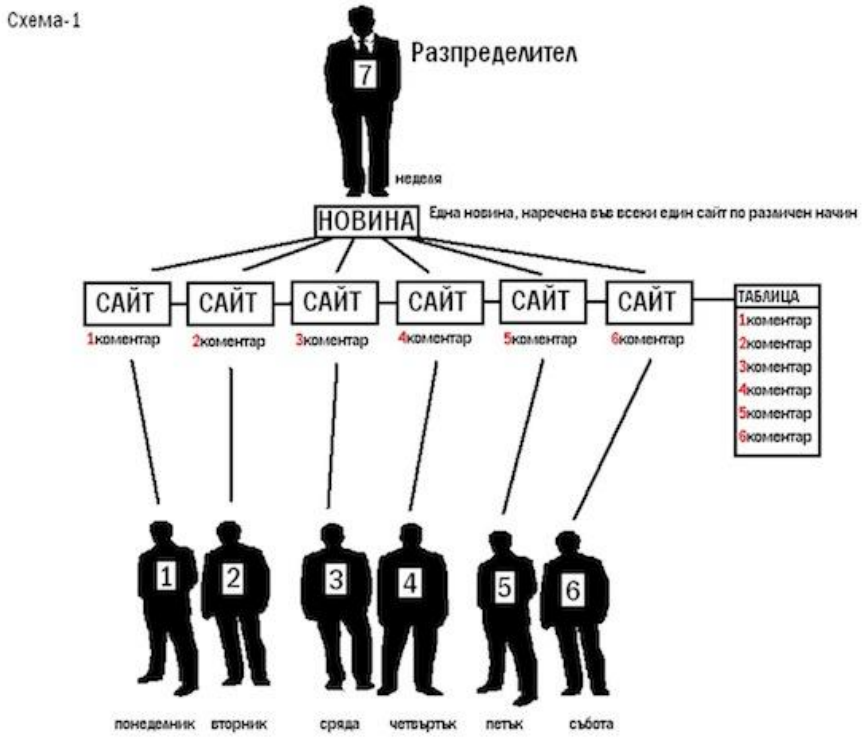
В българската практика има няколко примера за използване на стратегии, свързани с тролене в социалните мрежи и манипулиране на общественото мнение. Тези практики обикновено се свързват с политически интереси и външни влияния.

Например през 2014 г. разследване на сайта Биволъ разкри, че българската рекламна агенция Leadway Media Solutions е предоставяла услуги за публикуване на коментари в социални мрежи и форуми. Тези коментари често се използвали за манипулиране на общественото мнение и подкрепа на определени политически позиции.

През 2013 г. назначението на Делян Пеевски за шеф на ДАНС предизвика масови протести в България. Организацията на протестите чрез социалните мрежи, особено чрез Facebook групата „ДАНСWithMe“, показа

как социалните медии могат да бъдат използвани за мобилизиране на обществото. Въпреки това, по-късно се появиха твърдения, че някои политически сили са се опитали да манипулират общественото мнение чрез онлайн платформи, разпространявайки антипротестни послания и конспиративни теории.

Една от най-използвани в България е *схемата за тролинг 6 х 7* – на шест сайта от седем човека. Всеки трол има номер, отговарящ на ден от седмицата 1 – понеделник, 2 –вторник и прочие. Номер 7 е „разпоредител“ неговата работа е всяка неделя да избира една публикация, повтаряща се в шест специално избрани посещавани сайта и да я даде на другите 6 трола за коментари. Тяхната работа е да коментират в съответния ден от седмицата под всеки един от шестте сайта. С други думи, всеки коментира под всеки един сайт и се получава 6 х 6 = 36 коментара.



Фигура 18. Схема за тролене[45]

[45] *Наръчник за интернет тролове*. Достъпно на: https://postvai.com/cyber/trol-trolene.html.

Троловете използват няколко **основни техники**, които може да бъдат обобщени така:

● Клонирането е най-често използваният трик. Всеки трол задължително „се клонира“ чрез създаване на няколко акаунта от различен компютър и започва да води ожесточена дискусия със самия себе си. По този начин много бързо може да блокира дадена тема във форум, блог или социална мрежа.

● Стоварването на десант с обучена група от тролове, която влиза организирано в нарочен форум и със своите клонинги е в състояние да го превземе за кратко време. При спам над 75% от публикациите, трафикът на сайта буквално спада до нулата.

● Плувки, куки и мрежи – това са различни средства за създаване на провокативни съобщения, които могат да се хвърлят във вече открита тема или да са първи пост в нова тема. Обикновено се маскират като невинен въпрос, но съдържат една или повече „куки“, за които после да се хванат троловете.

● Потъване и различни маневри. Често тролът публикува нещо и „потъва“ за известно време, през което наблюдава реакциите, търпимостта и нивото на захапване, намесата на администратора и др. При благоприятна среда подгрява темата със свои клонинги и след това се прави на жертва.

● Засада. Тролът следи даден блог, например на президента, и когато излезе нова публикация, веднага започва да му намира грешки, да доказва, че лъже и цели да го изкара от равновесие.

Практическо упражнение за разпознаване на трол или бот

Социалните мрежи се превърнаха в много важен информационен компонент в живота на човека. Те стават основен канал за получаване на новини, обсъждане, обмяна на мнения и разпространяване на информация.

Един такъв широко използван канал винаги е интересен както за бизнеса, така и за нуждите на държавата, защото той може да бъде употребяван за манипулиране на целевата аудитория. При провеждане на информационни операции този канал може да служи за масово разпространение на съобщенията и поради това че аудиторията в него може да бъде разнообразна, той се нуждае от автоматизиране на процеса. Именно за удовлетворяването на тази нужда се използват ботове.

Ботовете са компютърни програми, автоматично изпълняващи някои действия, които на теория трябва да бъдат изпълнени от хора. Например коментират постовете на други хора, харесват постове и изпращат съобщения. В информационните операции ботовете се използват за разпространяване на целева информация. Те имитират виртуални личности и често се контролират от тролове. Поради тази причина е много трудно да се определи кой акаунт е бот и кой е на човек. Затова следва представяне на признаците, по които това може да се направи. Признаците могат да се класифицират като статични и поведенчески.

1.*Статични признаци*. Това са тези, които включват характеристиките на дизайна на профила. Например един такъв признак е, че съответният профил няма име на човек. Друг признак е да няма публикации с история в профила, а само коментари под публикации на други хора. Съдържанието на снимките също са от значение, но е трудно да се формулира такава оценка.

Друг начин на оценка е да бъде съпоставена датата на раждане с датите за начало и край на образование. Също така може да се провери дали датата на създаване на профила е много близка до дадения момент за коментиране на събитието, за което е създаден. Много често може да се видят групи ботове, които са в една и съща общност с близки дати на създаване (направени от един човек за една и съща цел). Друг интересен показател е съотношението между времето на съществуване на акаунта (датата на създаване) и на неговата дейност (брой публикации или коментари). Ако акаунтът е регистриран преди няколко дни, но вече има няколко хиляди коментара, е по-вероятно да е бот.

Броят на приятелите също е интересен индикатор. Липсата на приятели, макар и виртуални и най-вече на активно комуникиране (коментари) не е съвсем обичайно човешко поведение.

2. *Поведенчески черти*. Участието на акаунта в неестествено популяризиране на различни материали също може да ни насочи, че това е бот. В някои случай акаунтите се наемат, а в други могат да бъдат хакнати. Един от основните признаци за това е скоростта на коментиране – обикновен потребител не може да остави коментари в първата секунда след публикацията. При автоматизирания софтуер често се случва коментари от различни акаунти да бъдат от едно и също IP.

Не всички ботове са злонамерени или политически. Автоматизираните акаунти могат да публикуват например поезия, фотография или новини, без да създават ефект на изкривяване.

В следващите редове се теоретизира и класифицира събраният от авторите опит за разпознаване на фалшивите профили и автоматизирани

ботове. Във всички случаи е важно да се отбележи, че не може да се разчита на единични и точни фактори за идентифициране на поведение, подобно на бот. Разпознаването е базирана на натрупания опит комбинацията от фактори, като най-важните от тях са дейност, анонимност и усилване.

1. Дейността е най-важният и най-очевидният индикатор, че профилът е автоматизиран. Има профили, които са толкова активни, че не е възможно човек да извърши толкова действия за толкова кратко време. Дейността може лесно да се изчисли, като се раздели броя на публикациите по броя на дните, в които профилът е бил активен. Показателят за подозрителна дейност варира, изследователите от Оксфорд предлагат преминаването на границата от повече от 50 активности на ден да се счита за подозрителна. Например през 2017 г. у нас стана известен случаят с 20-годишния Адриан Димитров от Шумен, който за две години е навъртял над 85 000 публикации във Facebook на политическа тематика. Това не е типично човешко поведение, поради което за целта явно е използван софтуер.

2. Анонимността е вторият ключов показател, която показва профилът. Колкото по-малко лична информация има за съответния човек, толкова по-вероятно е това да е бот. Например, ако вместо снимка на човека се използва някакъв предмет или символ за аватар в акаунта. По този начин акаунтът изобщо не дава никаква лична информация. Друг белег е когато аватарът и фонът са неспецифични спрямо местоположението, например аватарът е китаец в Ямбол, който има приятели от Африка.

3. Третият ключов индикатор е усилването. Една от основните роли на ботовете е да стимулират сигнала от други потребители чрез повторно споделяне, харесване или цитиране. Поради това историята на профила на типичния бот ще се състои от поредица чужди цитати, думи и новинарски заглавия, без оригинални публикации. Най-ефективният начин да се установи този модел е да се направи машинно сканиране на голям брой постове. Ботнет мрежите са друг начин за усилване на една и съща публикация от голям брой акаунти, с което се постига същият ефект. Разликата спрямо представените примери е, че при тях това се прави само с един акаунт. Ботмрежите могат бързо да бъдат идентифицирани, когато се използват за усилване, ако акаунтът, който е публикувал поста, обикновено не е активен.

Общото съдържание публикувано в профила също може да е признак. Вероятността акаунтите да принадлежат на една мрежа може да

бъде потвърдена, като се гледат публикациите им. Ако всички те публикуват едно и също съдържание или тип съдържание едновременно, те вероятно са програмирани да го правят.

Най-примитивните ботове са особено лесни за идентификация, защото създателите им не са си направили труда да сложат аватар. Особено явно е когато имат поредица от приятели без аватар, както е показано на снимката фигура 19.



Фигура 19. Акаунти (примери)

Много често ботовете използват откраднатa или споделена снимка. За да проверите заподозрения акаунт, направете обратно търсене на снимката на профила.



Фигура 20. Профили (примери)

● Ако в името след знака „@“ има думата „бот“ или поредица цифри и букви без ясен смисъл от рода на @LlPPvhAlk или @admh132kn2 и други, генерирани от алгоритъм имена.

● Може името на акаунта да не съвпада с името на екрана, може да има мъжки имена с женски образи, както е показно на снимките.

● Може да показват съдържание на арабски, английски, испански, френски език и суахили, като е малко вероятно толкова езици да се владеят от един и същи човек.

● В реалния живот всеки, усвоил толкова езици, вероятно има не би прекарвал времето си предимно в YouTube или Facebook.

● Един класически индикатор е рекламата и търговското съдържание. Акаунтите, които показват предимно реклами, особено ако те са на няколко езика, са най-вероятно членове на търговски ботмрежи, наети от потребители, които искат да разширят или да рекламират своите постове.

● Софтуер за автоматизация може да се разпознае по наличието на къси URL в поста, като ift.tt. Те се използват предимно за проследяване на трафика на конкретна връзка и са индикатор за автоматизация. Това е вид софтуер, произведен от фирмата ifttt.com, който позволява на потребителите да автоматизират своите постове според редица критерии, например всяка публикация с даден хаштаг. Друг пример е съкращението ow.ly, bit.ly или tinyurl.com.

● Споделянията и харесванията са окончателен индикатор, че това е работа на робот. Някои ботове са програмирани да го правят. В такива случаи броят на споделянията и харесванията ще бъде почти идентичен за поредицата от акаунти. Броят на профилите, които са извършили действията, също може да съвпадат за една и съща изследвана новинарска публи-

кация или политическо съобщение. Най-важно е потребителите да осъзнават, че акаунтите могат да бъдат фалшиви, което прави потребителите помалко податливи на манипулация от тях.

Други белези на фалшивите профили могат да бъдат:

– профилът е създаден наскоро и веднага е започнал да бълва информация;

– непрозрачни профили (без снимка, без достъп до история на публикации, без достъп до приятелите). Трябва да имаме предвид, че само това не е достатъчно доказателство, че един профил е фалшив, защото има хора, които напълно скриват данните си;

– фалшивите профили имат хиляди приятели, а според статистиката един български потребител на Facebook има среден брой от 229 приятели в профила си, само 7% от които е виждал лице в лице;

– фалшивите профили, направени с политическа или рекламна цел, нямат споделени лични публикации в профила или в групи;

– фалшивите профили много по-често са млади жени – може да се провери с търсене по снимка (за напреднали – EXIF информация);

– тагването на снимки е около 100 пъти по-често от нормалните профили;

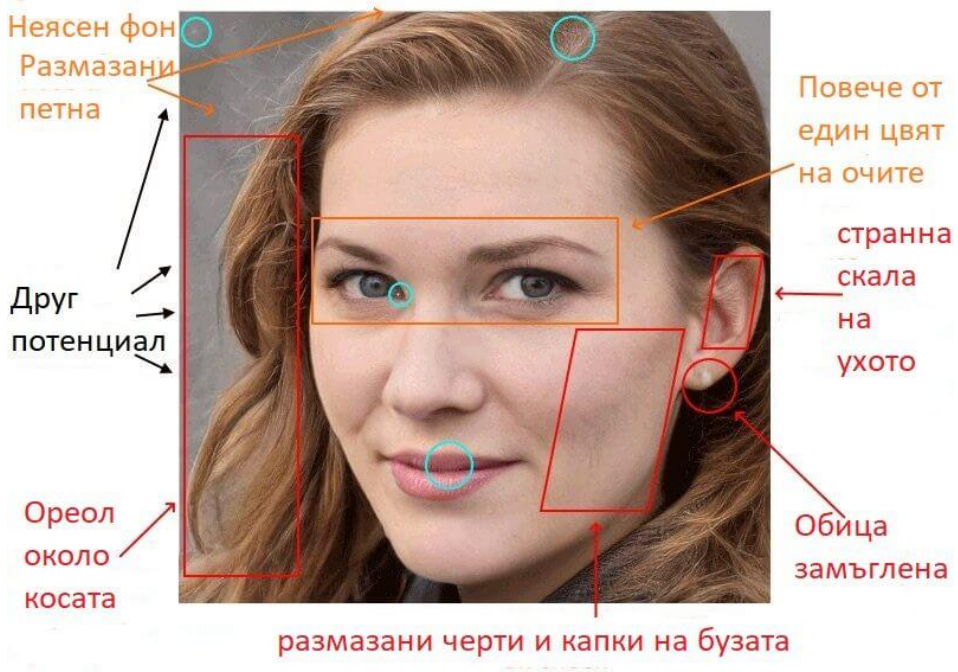
– слабо поддържан профил – последен пост от преди няколко месеца, обикновено нямат време или желание да поддържат всичките фалшиви профили;

– несъответствие в личните данни на профила – например млад човек, който е професор в Оксфорд;

– при търсене на името в Google (сложено в кавички), ако при поредки имена от типа на Трендафил Каракашев няма резултати или излезе само Facebook профила, е доста вероятно това да е фалшива самоличност. При разпространени имена като „Георги Георгиев“ няма смисъл да се прави такова търсене.

Ботовете и фалшивите профили съществуват, за да повлияят на реалните потребители. Като противодействие на фалшивите профили те може да се докладват такива на администраторите на страницата. За да бъдат премахнати, е нужно това бъде направено от множество реални профили. Най-голям успех има, ако профилът се представя за друг Facebook профил, който си има собствен официален Facebook профил. Най-често това се прави с известни личности. Популярен е скандалът, който избухна в LinkedIn с Пол Уинфрий, бившият заместник-директор на съвета по вътрешната политика на президента Доналд Тръмп, който се разглеждаше за ръководна длъжност във Федералния резерв. Той беше уличен за връзка с шпионин, представящ се с фалшив профил в същата социална мрежа под псевдонима Кейти Джоунс. „Тя“ дори използва изцяло фалшива снимка

създадена от изкуствен интелект. Както е видно от фигура 21, това е снимка на профила на около 30-годишна жена със синьозелени очи, коса с цвят на мед и загадъчна усмивка. На фигурата са показани някои белези, по които можем да познаем, че снимката е фалшива.



Фигура 21. Белези за разпознаване на фалшива снимка

Може да направите кратък тест на уменията за разпознаване на фалшивите лица от истинските със следните онлайн инструменти:

– От тази връзка може да създавате собствени фалшиви профили: https://thispersondoesnotexist.com. Влизането в страницата генерира различно изображение на личност, която не съществува в реалността.

– А на този адрес може да тествате способността си да разпознавате истинско лице от фалшив профил: http://www.whichfaceisreal.com/.

В днешния технологичен свят вместо изпращане на таен агент на живо много по-евтино е създаването на изкуствен профил и изпращане на молби за приятелство до 30 000 държавни служители. Например, такъв е случаят с пенсионираният служител на ЦРУ Кевин Малори, който е осъден на 20 години затвор за предаване на подробности за секретни операции в Пекин на връзка, която е започнала в Linkedin.

За разлика от Facebook, който акцентира върху семейство и приятели, в Linkedin се намират хора, търсещи работи, което ги предразполага

за нуждите на разузнаването. Неслучайно от компанията заявяват, че през първите месеци на 2019 г. са изтрили няколко хиляди фалшиви акаунти.

Упражнение за разпознаване на методи за манипулиране на аудиторията

1. Представяне на нерелевантни данни, така че вниманието на всички да бъде отклонено от обсъждан въпрос. Например в политически дебат, защитавайки собствените си политики по отношение на обществената безопасност, говорещият казва „Работих усилено, за да помогна за премахването на престъпната дейност. Това, от което се нуждаем, е икономически растеж, който може да дойде само от чрез икономиката“.

2. Дискредитиране позицията на противника, като ги обвиняваме в лицемерие, без да опровергаваме пряко аргументите му. Например, една нация отклонява критиките към неотдавнашните нарушения на правата на човека, като насочва към историята на робството в САЩ.

3. Причинно-следствено прехвърляне на вина, породено от сложни процеси. Пример: „Президентът Тръмп е на поста си от месец и цените на газта скачат до небето. Покачването на цените на газа е заради президента Тръмп“.

4. Умишлено неясно или сложно говорене. Използване на думи, които не са конкретни, така че публиката да има свои собствени интерпретации.

5. Цитиране на експерт – „Според експерта Х нашата външна политика е най-добрата на Земята. Така че ние сме в правилната посока“. Това е мнение, но не доказателство, защото експертът може да се използва в подкрепа на доказателство.

6. Черно-бяла заблуда, с която казвате на публиката какво да направи, като елиминирате всички други опции. Пример: Трябва да сте комунист или демократ. Ти не си демократ. Следователно, трябва да си комунист.

7. Етикетиране. Обозначаваме обекта с прякор, назоваващ нещо, от което целевата аудитория се страхува или мрази.

8. Емоционално зареден език. Пример: „Колко глупави и дребнави неща са станали в Народното събрание!“.

9. Преувеличение или свеждане до минимум. Например: да направим нещата по-големи, по-добри или „най-доброто от най-доброто“ и обратното – да ги направим маловажни, като да кажете, че обидата е само шега.

10. Посяване на съмнение. Пример: Кандидат-кмет говори за опонента си и пита готов ли е да бъде кмет.

11. Използване на страха и предразсъдъците – „Трябва да спрем бежанците, тъй като те са терористи“.

12. Използване на лозунги, които включват стереотипи – „Да направим Америка велика отново!“.

13. Използване на думи, които омаловажават критиката или клишета, завършващи с мисъл. Например: Това е просто здрав разум; Нищо не е постоянно, освен промяна; По-добре късно, отколкото никога; Никой не е съвършен, и аз не съм.

14. Убеждаване на публиката да не одобри идея с подсещането че тя е популярна сред други, които мразим – „Знаете ли кой друг е правил това? Хитлер!“.

15. Повторение на едно и също послание отново и отново, така че в крайна сметка публиката да го приеме.

Упражнения за разпознаване на фалшиви новини

1. За проверка на разбирането на понятията „информация“ и „източник“ посочете за всяко едно от твърденията дали е информация, или мнение.

а) Националният футболен отбор на България е изключително слаб.

Да, това е факт. **Не**, това е мнение.

б) Мачът между България и Англия завърши 0:6.

Да, това е факт. **Не**, това е мнение.

в) Равнището на регистрираната безработица продължава да намалява, достигайки 5,6% през август, показват данни на административната статистика на Агенцията по заетостта. Отчита се минимално понижение от 0,1 процентни пункта спрямо юли 2018 г. и от 1,1 процентни пункта на годишна база.

Да, това е информация. **Не**, това не е факт.

Отговори

а) Не, това е мнение, без аргументи.

б) Да, това е факт, проверяем от всички.

в) Да, това е факт, проверяем от всички.

2. За всяко от тези твърдения посочете дали идват от първичен или вторичен източник.

а) Моят брат ми каза, че миналия четвъртък видял полицейски служител да бие нарушител.

б) Чух от журналист, който е много запознат с темата, че г-жа Иванова ще се кандидатира за президентските избори.

в) В четвъртък сутринта бях на улицата, когато видях кола, която не успя да направи завой и се заби в стената на мола.

г) Г-н Борисов заяви пред БТВ, че възнамерява да намали данъците.

Отговори:

а) Вторичен източник: показанията се докладват от посредник.

б) Вторичен източник: информацията се съобщава от посредник, който не е ясен.

в) Първичен източник: Авторът е този, който казва, че е присъствал на събитието.

г) Първични и вторични източници: ако видим видеото на изявлението на г-н Борисов, то е първичен източник, тъй като имаме пряк достъп до онова, което казва. Ако пък ви разкажат онова, което е казал г-н Борисов, това е второстепенен източник.

3. Ето два откъса от статия. Кой от тях ви се струва надежден и защо?

а) „В понеделник сутринта по Националното радио кметът на Русе г-жа Иванова беше попитана дали възнамерява да продължи проекта за големия футболен стадион. Строителството трябва да започне през следващите месеци, но проектът е много критикуван. В сайта *Petition.com* беше подписана петиция от 3000 интернет потребители, които искат проектът да бъде изоставен, защото би бил твърде скъп. „Не мога да ви кажа днес какво ще е решението ми“, каза г-жа Иванова. „Ще направим равносметка на ситуацията, за да сме сигурни, че разходите са били правилно изчислени, за да знаем дали критиките са оправдани, или не. След като това бъде направено, ще можем да решим спокойно дали да продължим със строителството.“

б) „Г-жа Иванова видимо е напълно некомпетентна. Тя дори не е в състояние да каже дали е „за“ или „против“ проекта на големия футболен стадион в Русе. Тя каза по радиото, че не е в състояние да реши, защото не знае нищо за това. Честно казано, този кмет е наистина некомпетентен.“

Отговори:

Първият откъс предоставя определени факти и конкретни изявления на г-жа Иванова, които могат да бъдат проверени чрез слушане на нейното изявление по радиото. Статията също се стреми да е балансирана, защото предоставя и аргументите на противниците на проекта. Авторът не дава становище, а отчита информация.

Вторият откъс е с много по-предубеден текст, изпълнен с квалификации. Авторът реално взема страна по проекта, но е невъзможно всеки, който не познава темата, да разбере аргументите му или тези на противниците, без да види фактите.

Отворени въпроси за самоподготовка

- Дайте определение за трол.
- Опишете кои стратегии за тролене са ви известни.
- Избройте техниките за тролинг.
- Какво е определението за бот?
- Кои са основните признаци за разпознаване на ботове?

Примерен изпитен тест

Дисциплината „Противодействие на дезинформацията“ завършва с изпитен тест. Крайната оценка за дисциплината се оформя като сума от средната оценка от текущия контрол с теглови коефициент 0,2 и оценката от изпитния тест с теглови коефициент 0,8, като резултатът се закръглява с точност до единица.

$$КО = 0,2*О_{тк} + 0,8*О_{т}$$

където КО е крайната оценка за дисциплината;

– $О_{тк}$ е средната оценка от контрола по време на практическите упражнения;

– $О_{т}$ е оценката от изпитния тест.

Примерни въпроси за теста

1. Какви са основните характеристики на дезинформацията и как тя се различава от други форми на информационно разстройство?

a) Дезинформацията е съзнателно разпространявана подвеждаща информация, докато другите форми не включват злонамереност.

b) Дезинформацията винаги е правилна, но неправилно интерпретирана.

c) Дезинформацията е резултат от липса на проверка на фактите.

d) Дезинформацията се разпространява единствено чрез държавни институции.

2. В кои измерения и по кои канали се разпространява дезинформацията?

a) Физическо, информационно и когнитивно измерение; социални медии, новинарски сайтове и телевизия.

b) Единствено в когнитивното измерение; чрез устна комуникация.

c) Информационно измерение; само чрез печатни медии.

d) Физическо измерение; единствено чрез телевизия.

3. Кои са основните фактори, правещи хората и обществата уязвими към дезинформация?

a) Висока степен на медийна грамотност и критично мислене.

b) Липса на критично мислене, ехо камери и когнитивни пристрастия.

c) Технологично развитие и достъп до факти.

d) Недоверие към медии и държавни институции.

4. Кои методи и подходи могат да се използват за разпознаване на дезинформация?

a) Проверка на източниците, анализ на авторите и съдържанието.

b) Доверие само на новини от социалните медии.

c) Използване на алгоритми за потвърждение на пристрастията.

d) Следване на популярните мнения в интернет.

5. Посочете основните направления, по които дезинформацията влияе върху националната сигурност:

a) Засилване на междукултурните връзки и стабилност.

b) Подкопаване на доверието в институциите, поляризация и манипулиране на обществени настроения.

c) Увеличаване на доверието към правителствените източници.

d) Насърчаване на сътрудничество между различни социални групи.

6. Кога влиза в сила Директивата НИС-2 и какъв е крайният срок за въвеждането ѝ в националното законодателство на държавите членки?

a) Влиза в сила през 2023 г. с краен срок до 2025 г.

b) Влиза в сила през 2024 г. с краен срок до 2026 г.

c) Влиза в сила през 2023 г., с краен срок до 2024 г.

d) Влиза в сила през 2025 г., с краен срок до 2026 г.

7. Кои са основните елементи на Акта за цифрови услуги?

a) Ограничаване на достъпа до всички социални медии.

b) Повишаване на прозрачността, премахване на незаконно съдържание и защита на потребителите.

c) Въвеждане на нови такси за използване на онлайн платформи.

d) Забрана за създаване на ново съдържание в интернет.

8. Кои са четирите стълба на Плана за действие на ЕС срещу дезинформацията?

a) Оборудване на армията, обучение на преподаватели, глобална комуникация, засилване на регулациите.

b) Подобряване на откриването, засилване на устойчивостта, работа с платформи, международно сътрудничество.

c) Усъвършенстване на образованието, контрол на социалните мрежи, криминализиране на дезинформацията, насърчаване на журналистиката.

d) Финансово подпомагане на медии, блокиране на съдържание, обучение на гражданите, забрана на социалните медии.

9. Какво въвежда Директива 2019/790 относно авторското право в цифровия единен пазар?

a) Забрана за публикуване на всякакви новини без авторско право.

b) Прозрачност и възнаграждение за авторите и изпълнителите на цифрово съдържание.

c) Намаляване на изискванията за авторско право.

d) Ограничение за достъпа до научни публикации.

10. Избройте техники за критичен анализ на публикувана новина в социалните медии.

a) Проверка на източника, кръстосана проверка с други новини, анализ на емоционалния тон.

b) Следване на най-популярните публикации.

c) Доверие само на новини, препоръчани от приятели.

d) Проверка единствено на заглавията.

11. Как алгоритмите на социалните медии влияят върху разпространението на дезинформация?

a) Те ограничават разпространението на подвеждаща информация.

b) Те насърчават ехо камери, като популяризират съдържание, което съвпада с интересите на потребителите.

c) Те премахват съдържание, което не е популярно.

d) Те улесняват достъпа до проверени източници.

12. Как съвременните технологии могат едновременно да улеснят разпространението на дезинформация и да помогнат противодействието срещу нея?

a) Те не оказват влияние върху разпространението на дезинформация.

b) Те създават канали за разпространение, но и механизми за проверка на фактите.

c) Те напълно елиминират дезинформацията чрез автоматизация.

d) Те ограничават достъпа до информация.

13. Какво е медийна грамотност?

a) Способността за четене и писане.

b) Умението за анализ, оценка и създаване на медийно съдържание.

c) Разбирането на техническите аспекти на комуникационните технологии.

d) Познаването на основните медийни закони.

14. Кои са основните методи за анализ на медийно съдържание?

a) Контекстуален анализ, проверка на факти и оценка на източника.

b) Ретуширане на изображения и монтаж на видеа.

c) Сравнение с други източници и отхвърляне на новините от социалните медии.

d) Редактиране и писане на новини.

15. Кои са основните характеристики на социалните медии, които дават приоритет на съдържанието?

a) Случайно разпределение на публикациите.

b) Алгоритми, базирани на интереси, емоционално въздействие и честота на взаимодействия.

c) Хронологичен ред на публикациите.

d) Рекламиране чрез телевизия и радио.

16. Какви правила трябва да се следват при споделяне в социалните медии?

a) Споделяне само на информация с одобрението на администраторите.

b) Проверка на източника, избягване на сензационност и уважение към аудиторията.

c) Споделяне на всяка информация, която изглежда интересна.

d) Избягване на съдържание, което изисква потвърждение.

17. Какво разбирате под „замърсяване на информационното пространство“?

a) Замърсяване на околната среда чрез използване на технологии.

b) Пренасищане на медийното пространство с подвеждаща или фалшива информация.

c) Липсата на информация по важни теми.

d) Прекалена употреба на дигитални устройства.

18. Кои са трите подхода за борба с дезинформацията?

a) Дигитална грамотност, регулации и проверка на факти.

b) Блокиране на интернет достъпа, цензура и наказания.

c) Промотиране на истинските новини.

d) Създаване на повече фалшиви новини за разсейване на дезинформацията.

19. Какво е определението за трол?

a) Лице или бот, който умишлено провокира или манипулира в онлайн дискусии.

b) Потребител, който изразява своето мнение.

c) Софтуер за управление на социалните медии.

d) Тип алгоритъм за популяризиране на съдържание.

20. Кои стратегии за тролинг са ви известни?

a) Провокации, разсейване и създаване на полемика.

b) Разпространение на истински новини.

c) Насърчаване на етични дискусии.

d) Избягване на конфликтни теми.

21. Кои са техниките за тролинг?

a) Лична атака, отклоняване от темата и създаване на спам.

b) Проверка на факти и привличане на експерти.

c) Опити за намаляване на напрежението в дискусиите.

d) Оценка на качеството на съдържанието.

22. Какво е бот?

a) Софтуерна програма, която автоматично изпълнява задачи онлайн.

b) Човек, който работи в социалните медии.

c) Устройство за събиране на данни от интернет.

d) Технология за създаване на видеосъдържание.

23. Кои са основните признаци за разпознаване на ботове?

a) Нереалистично честота на публикации, липса на лични данни и шаблонни отговори.

b) Прекомерно взаимодействие с приятели.

c) Участие само в групови дискусии.

d) Поддържане на реалистични и смислени разговори.

24. Кои елементи включва критичното мислене?

a) Анализ, синтез, оценка и вземане на решения.

b) Емоционални реакции и субективни оценки.

c) Самоанализ и отклоняване от мненията на другите.

d) Фокус върху бързото вземане на решения.

25. Кои са стъпките на алгоритъма за разпознаване на фалшиви новини?

a) Идентифициране на източника, проверка на фактите и сравнение с надеждни медии.

b) Четене и споделяне на съдържанието.

c) Търсене на мнения от социалните медии.

d) Оценка на популярността на новината.

26. Кои са основните принципи на стратегическите комуникации в националното когнитивно пространство?

a) Последователност, прозрачност, интеграция и адаптивност.

b) Скриване на информация и контрол на медиите.

c) Ограничаване на комуникацията с международни партньори.

d) Активна цензура на социалните медии.

27. Какво е национално когнитивно пространство?

a) Сферата на влияние, в която държавата защитава своите комуникационни канали и създава възприятия.

b) Физическото пространство, в което се разпространяват информационни съобщения.

c) Среда за разпространение на държавни пропагандни материали.

d) Зоната за технически комуникации на армията.

28. Кои са методите за стратегически комуникации?

a) Пропаганда, публична дипломация, социални медии и връзки с обществеността.

b) Тайни операции и шпионаж.

c) Цензура и блокиране на медийни канали.

d) Само анализ на конкуренцията.

29. Кои са мерките за изграждане на устойчивост срещу дезинформация?

a) Образование, повишаване на медийната грамотност, прозрачност и ефективни регулации.

b) Намаляване на достъпа до интернет.

c) Избягване на критично мислене и доверие само на държавните медии.

d) Ограничаване на международното сътрудничество.

Отговори:

1a, 2a, 3б, 4a, 5b, 6c, 7b, 8b, 9b, 10a, 11b, 12b, 13b, 14a, 15b, 16b, 17b, 18a, 19a, 20a, 21a, 22a, 23a, 24a, 25a, 26a, 27a, 28a, 29a

ЗАКЛЮЧЕНИЕ

Днес, в информационната епоха масово се използват високоинтелигентни средства за манипулиране на информацията във всички аспекти на модерния начин на живот. Дезинформацията се превърна в един от основните проблеми на нашето време и важен аспект на националната сигурност. Нещо повече, това е формата на войната на бъдещето. Война зад войната. Като хора свързани със сферата на сигурността и отбраната имаме отговорност да бъдем информирани и бдителни. Нашата устойчивост към дезинформация е част от защитата на България.

В съвременната информационна епоха високоинтелигентните средства за манипулиране на информацията се използват масово във всички аспекти на модерния начин на живот. Дезинформацията се превърна в един от основните проблеми на нашето време и важен аспект на националната сигурност. Нещо повече, това е формата на войната на бъдещето – война зад войната. Хората, работещи в сферата на сигурността и отбраната, имат отговорност да бъдат информирани и бдителни. Тяхната устойчивост към дезинформация е част от защитата на България.

Предложеният курс от лекции предоставя базови знания за разпознаване на дезинформацията, изграждане на когнитивна устойчивост и медийна грамотност при анализ на информацията в области на държавното управление. Настоящият учебник може да бъде използван от студенти или военнослужещи, изучаващи дисциплината „Противодействие на дезинформацията“, докторанти от областта на висшето образование „Сигурност и отбрана“ в професионално направление „Национална сигурност“, както и за повишаване на личната информационна култура на широката аудитория.

* Запомнете: **Винаги проверявайте фактите, преди да споделите!**

ЛИТЕРАТУРА

ГЕОРГИЕВ, А., 2022. Етика и технологии: Риск и отговорност при развитието на изкуствения интелект. *Философски преглед*, бр. 1 – 2, стр. 34 – 48.

ГЕОРГИЕВ, В., 2022. Изкуствен интелект и етично поведение. В: *Сборник с доклади от международната научна конференция „Изкуственият интелект в сферата на сигурността – предимства и заплахи“, Том 1*, стр. 249 – 254. Пловдив: изд. Комплекс ВУСИ.

ГЕОРГИЕВ, Г.; НОВОСЬОЛОВА, Т., 2023. *Дезинформационна буря. Хибридни заплахи от неконвенционални оръжия в България и в Румъния*. София: Център за изследване на демокрацията. Достъпно на: https://csd.eu/fileadmin/user_upload/publications_library/files/2024_2/Disinformation-Storm_Publication_BG.pdf.

ГЕРАСИМОВ, В. 2013. Ценность науки предвидения. *Военно-промышленный курьер*, № 8 (476). Достъпно на: https://web.archive.org/web/20220316074248/https://vpknews.ru/articles/14632.

ДИМИТРОВ, Д., 2018. Операции за влияние: механизъм на действие и противодействие. *Военен журнал*, бр. 2.

ДИМОВ, П., 2018. *Приложение на уеб технологиите за защита на националната сигурност*. София: Диомира.

ИВАНОВ, Е.; ДИМОВ, П., 2020. *Фалшивите новини*. София: Военна академия „Г. С. Раковски“.

ИГНАТОВ, И., 2024. Медийната грамотност като част от дигиталните компетентности. *Национална сигурност*, бр. 17.

МАКИАВЕЛИ, НИКОЛÒ, 2006. *Принцът*. София: Захарий Стоянов.

САВОВА, Л., (преводач) 1991. *Христоматия по интелектуална собственост, патенти, търговски марки, авторско право*. София: Институт за изобретения и рационализации ИНРА.

СЕРАФИМОВА, М., 2025. *Практическо ръководство на публичната комуникация в сигурността и отбраната. Българският опит*. София: Издателство „Ваньо Недков“.

СТОЙКОВ, М., 2018. *Експертна оценка на институционалните способности за противодействие на хибридни заплахи*. София: Военна академия „Г. С. Раковски“.

СУН ДЗЪ 2022. *Изкуството на войната*. София: Фама.

ХИТЛЕР, А., 2001. *Моята борба*. София: Апостроф.

ЦАКОВА, И., 2014. *Интернет право.бг. Кратък курс лекции*, стр. 252 – 277. София: Парадигма.

POSTVAI.COM. Ръководство за борба с фалшивите новини. https://postvai.com/fakenews/ [прегледан 4.02.2020].

POSTVAI.COM. Ръков*одство за борба с фалшивите новини*. https://postvai.com/fakenews/.

ALBERTS. D; GARSTKA, J.; HAYES, R.; SIGNORI, D., 2001. *Understanding Information Age Warfare*. Washington D.C.: Command and Control Research Program.

BERGSTRÖM, A. & JERVELYCKE BELFRAGE, M., 2021. *News in a Post-Truth Era: Journalism and the Decline of Public Trust*. Routledge.

BENNETT, W.L.; LIVINGSTON, S., 2018. The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions. *European Journal of Communication*, vol. 33, no. 2, pp. 122 – 139. [онлайн] Налично на: https://doi.org/10.1177/0267323118760317 [Последно посетен: 31.05.2025].

BIESTA, G., 2013. *The Beautiful Risk of Education*. Routledge.

BRETAG, T. & MAHMUD, S., 2009. Self-plagiarism or Appropriate Textual Re-use? *Journal of Academic Ethics*, Vol. 7, No. 3, pp. 193 – 205.

CANTRIL, H.; HAZEL, G.; HERTA H., 1940. *The Invasion from Mars: A Study in the Psychology of Panic with the Complete Script of the Famous Orson Welles Broadcast*. Princeton, New Jersey: Princeton University Press.

CHEN, SH., YU, T. (eds), 2018. *Big Data in Computational Social Science and Humanities.* Springer, Cham. https://doi.org/10.1007/978-3-319-95465-3_1

CHIEF INFORMATION OFFICERS COUNCIL (CIO), 2009. *Guidelines for Secure Use of Social media by Federal Departments and Agencies*. Washington.

CIALDINI, R. 2008. *Influence: Science and Practice*. Boston: Allyn and Bacon.

CLAVERIE, B. 2025. Cognitive warfare: the new battlefield exploiting our brains. Polytechnique Insights, February 5. Available at: https://www.polytechnique-insights.com/en/columns/geopolitics/cognitive-warfare-the-new-battlefield-exploiting-our-brains/

CORNISH, P., LINDLEY-FRENCH, J., YORKE, C., 2011. *Strategic Communications and National Strategy*. London: Chatham House. ISBN: 9781862032552.

CROSS, M., 2014. *Social media security: leveraging social networking while mitigating risk*. Syngress.

EUROPEAN COMMISSION, 2022. *Strengthened Code of Practice on Disinformation*. [Онлайн] Налично на: https://digital-strategy.ec.europa.eu

FUKUYAMA, F. 1995. *Trust: The Social Virtues and the Creation of Prosperity*. New York: Free Press.

HARSIN, J. 2015. Regimes of Posttruth, Postpolitics, and Attention Economies. *Communication, Culture & Critique*, Vol. 8, No. 2, pp. 327 – 333. DOI: 10.1111/cccr.12097.

HIGGINS, K. 2016. Post-truth: a guide for the perplexed. *Nature*, Vol. 540, p. 9. DOI: 10.1038/540009a

HOWARD, R. M., 2007. Understanding "Patchwriting": The Importance of Disciplinary Contexts. *Writing Program Administration*, Vol. 30, No. 1-2, pp. 99 – 118.

KLUBAN, O.M., KURBAN, O.V., LYUBOVEC, G.V., 2016. Suchasni komunikacijno-kontentni procesy v bezpekovij sferi. Kyiv: VIKNU.

KRUGER, J., DUNNING, D. 1999. Unskilled and Unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of personality and social psychology*, Vol. 77, No. 6, pp. 1121 – 1134. DOI:10.1037/0022-3514.77.6.1121.

LEWANDOWSKY, S.; ECKER, U.; COOK, J., 2017. Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era. *Journal of Applied Research in Memory and Cognition*, Vol. 6, No. 4, pp. 353 – 369.

LYON, T. & MONTGOMERY, A., 2013. Astroturfing and Front Groups in Public Policy. *Journal of Consumer Policy*, Vol. 36, No. 3, pp. 283-305

NEWMAN, N.; FLETCHER, R.; KALOGEROPOULOS, A.; LEVY, D.; NIELSEN, R., 2018. *Reuters Institute. Digital News Report*. Reuters Institute for the Study of Journalism.

NYHAN, B. И REIFLER, J. 2010. When Corrections Fail: The Persistence of Political Misperceptions. *Political Behavior*, Vol. 32, No. 2, pp. 303 – 330. https://doi.org/10.1007/s11109-010-9112-2.

O'NEIL, C., 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown Publishing Group.

PAMMENT, J., 2020. *Strategic Communication in EU External Relations: From Information to Engagement*. Palgrave Macmillan.

PAUL, R.; ELDER, L., 2006. *The Miniature Guide to Critical Thinking: Concepts and Tools*. Dillon Beach, CA: Foundation for Critical Thinking

PALMERTZ, B.; BJÖRN, M.; WEISSMANN, N.; MIKAEL, J. 2024. *Building Resilience and Psychological Defence: An Analytical Framework for Countering Hybrid Threats and Foreign Influence and Interference*. Lund University, Psychological Defence Research Institute. Available from: https://mpf.se/download/18.7bb35f1818ec664dc7a4664/1712909687772/building-resilience-and-psychological-defence.pdf.

PURDY, J. P., 2009. When the Tenets of Composition Go Public: A Study of Writing in Wikipedia. *College Composition and Communication*, Vol. 61, No. 2, pp. 351 – 373.

RADOSLAVOV, D. Strawman Strategy For Countering Russian Information Perations And Cognitive Warfare In Bulgaria, 2022

SCANLON, P. M. & NEUMANN, D. R., 2002. Internet plagiarism among college students. *Journal of College Student Development*, Vol. 43, No. 3, pp. 374 – 385

SNOWDEN, P., 1915. Woman and War. *Journal of Proceedings and Addresses of the Fifty-Third Annual Meeting and International Congress on Education*. Oakland, California.

SUNSTEIN, C. R., 2019. *On Freedom*. Princeton University Press.

SUTHERLAND-SMITH, W., 2010. Retribution, Deterrence and Reform: The Dilemmas of Plagiarism Management in Universities. *Journal of Higher Education Policy and Management*, Vol. 32, No. 1, pp. 5 – 16.

TAYLOR, F. (Ed.), 1995. *The Goebbels Diaries 1939 – 1941*. New York: G. P. Putnam's Sons.

TECHAU, J., 2011. What makes communication strategic? Preparing military organizations for Battle of Ideal. *NATO Research Paper*, No. 65.

THEOHARY, C.A.; ROLLINS, J., 2011. *Terrorist Use of the Internet: Information Operations in Cyberspace*. Washington: Congressional Research Service. https://sgp.fas.org/crs/terror/R41674.pdf.

TZU, S., 2003. 2003. *The Art of War*. Griffith, S. (Translation). Oxford University Press.

VAN DER LINDEN, S.; LEISEROWITZ, A.; ROSENTHAL, S. & MAIBACH, E., 2017. Inoculating the Public against Misinformation about Climate Change. *Global Challenges*, Vol. 1, No. 2.

VOSOUGHI, S., ROY, D., & ARAL, S. 2018. The spread of true and false news online. *Science*, Vol. 359, No. 6380, pp. 1146 – 1151.

WANYANA, R., 2025. Cognitive Warfare: Does it Constitute Prohibited Force? *EJIL: Talk! Blog of the European Journal of International Law*. Достъпно на: https://www.ejiltalk.org/cognitive-warfare-does-it-constitute-prohibited-force/.

WARDLE, C.; DERAKSHAN, H., 2017. Information Disorder: Toward an interdisciplinary framework for research and policymaking. *Harvard Kennedy School. Shorenstein center of Media, Politics snd Public Policy*. Достъпно на: https://shorensteincenter.org/information-disorder-framework-for-research-and-policymaking/.

WINEBURG, S. & MCGREW, S. 2019 Lateral Reading and the Nature of Expertise: Reading Less and Learning More When Evaluating Digital Information. *Teachers College Record*, vol 121, no 11, pp. 1–40. [онлайн].

Налично на: https://journals.sagepub.com/doi/10.1177/ 016146811912101102 [Последно посетен: 31.05.2025].

ZUBOFF, S., 2019. *The Age of Surveillance Capitalism*. New York: PublicAffairs.

REFERENCES

ALBERTS. D; GARSTKA, J.; HAYES, R.; SIGNORI, D., 2001. *Understanding Information Age Warfare*. Washington D.C.: Command and Control Research Program.

BENNETT, W.L.; LIVINGSTON, S., 2018. The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions. *European Journal of Communication*, vol. 33, no. 2, pp. 122 – 139. [online]. Available on: https://doi.org/10.1177/0267323118760317. [Last visited: 31.05.2025].

BERGSTRÖM, A. & JERVELYCKE BELFRAGE, M., 2021. *News in a Post-Truth Era: Journalism and the Decline of Public Trust*. Routledge.

BIESTA, G., 2013. *The Beautiful Risk of Education*. Routledge.

BRETAG, T. & MAHMUD, S., 2009. Self-plagiarism or Appropriate Textual Re-use? *Journal of Academic Ethics*, Vol. 7, No. 3, pp. 193 – 205.

CANTRIL, H.; HAZEL, G.; HERTA H., 1940. *The Invasion from Mars: A Study in the Psychology of Panic with the Complete Script of the Famous Orson Welles Broadcast*. Princeton, New Jersey: Princeton University Press.

CHEN, SH., YU, T. (eds), 2018. *Big Data in Computational Social Science and Humanities.* Springer, Cham. https://doi.org/10.1007/978-3-319-95465-3_1

CHIEF INFORMATION OFFICERS COUNCIL (CIO), 2009. *Guidelines for Secure Use of Social media by Federal Departments and Agencies*. Washington.

CIALDINI, R., 2008. *Influence: Science and Practice*. Boston: Allyn and Bacon.

CLAVERIE, B., 2025. Cognitive warfare: the new battlefield exploiting our brains. *Polytechnique Insights*. Available on: https://www.polytechnique-insights.com/en/columns/geopolitics/cognitive-warfare-the-new-battlefield-exploiting-our-brains/

CORNISH, P.; LINDLEY-FRENCH, J.; YORKE, C., 2011. *Strategic Communications and National Strategy*. London: Chatham House. ISBN: 9781862032552.

CROSS, M., 2014. *Social media security: leveraging social networking while mitigating risk*. Syngress.

DIMITROV, D., 2018. Operatsii za vliyanie: mehanizam na deystvie i protivodeystvie. *Voenen zhurnal*, no. 2. [In Bulgarian].

DIMOV, P., 2018. *Prilozhenie na web tehnologiite za zashtita na natsionalnata sigurnost*. Sofia: Diomira. [In Bulgarian].

EUROPEAN COMMISSION, 2022. *Strengthened Code of Practice on Disinformation*. [online]. Available on: https://digital-strategy.ec.europa.eu

FUKUYAMA, F., 1995. *Trust: The Social Virtues and the Creation of Prosperity*. New York: Free Press.

GEORGIEV, A., 2022. Etika i tehnologii: Risk i otgovornost pri razvitieto na izkustvenia intelekt. *Filosofski pregled*, vol. 1 – 2, pp. 34 – 48. [In Bulgarian].

GEORGIEV, G.; NOVOSYOLOVA, T., 2023. *Dezinformatsionna burya. Hibridni zaplahi ot nekonventsionalni orazhia v Bulgaria i v Rumania*. Sofia: Tsentar za izsledvane na demokratsiyata. Available on: https://csd.eu/fileadmin/user_upload/publications_library/files/2024_2/Disinformation-Storm_Publication_BG.pdf. [In Bulgarian].

GEORGIEV, V., 2022. Izkustven intelekt i etichno povedenie. In: *Sbornik s dokladi ot mezhdunarodnata nauchna konferentsia „Iz-kustveniyat intelekt v sferata na sigurnostta – predimstva i zaplahi“*, vol. 1, pp. 249 – 254. Plovdiv: VUSI. [In Bulgarian].

GERASIMOV, V., 2013. Tsennosty nauki predvidenia. *Voenno-promiyshleniyy kuryer*, no. 8 (476). Available on: https://web.archive.org/web/20220316074248/https://vpknews.ru/articles/14632. [In Russian].

HARSIN, J., 2015. Regimes of Posttruth, Postpolitics, and Attention Economies. *Communication, Culture & Critique*, Vol. 8, No. 2, pp. 327 – 333. DOI: 10.1111/cccr.12097.

HIGGINS, K., 2016. Post-truth: a guide for the perplexed. *Nature*, Vol. 540, p. 9. DOI: 10.1038/540009a

HITLER, A., 2001. *Moyata borba*. Sofia: Apostrof. [In Bulgarian].

HOWARD, R.M., 2007. Understanding "Patchwriting": The Importance of Disciplinary Contexts. *Writing Program Administration*, Vol. 30, No. 1-2, pp. 99 – 118.

IGNATOV, I., 2024. Mediynata gramotnost kato chast ot digi-talnite kompetentnosti. *Natsionalna sigurnost*, Vol. 17. [In Bulgarian].

IVANOV, E.; DIMOV, P., 2020. *Falshivite novini*. Sofia: Voenna akademia „G. S. Rakovski". [In Bulgarian].

KLUBAN, O.M., KURBAN, O.V., LYUBOVEC, G.V., 2016. *Suchasni komunikacijno-kontentni procesy v bezpekovij sferi*. Kyiv: VIKNU.

KRUGER, J.; DUNNING, D., 1999. Unskilled and Unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of personality and social psychology*, Vol. 77, No. 6, pp. 1121 – 1134. DOI:10.1037/0022-3514.77.6.1121.

LEWANDOWSKY, S.; ECKER, U.; COOK, J., 2017. Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era. *Journal of Applied Research in Memory and Cognition*, Vol. 6, No. 4, pp. 353 – 369.

LYON, T. & MONTGOMERY, A., 2013. Astroturfing and Front Groups in Public Policy. *Journal of Consumer Policy*, Vol. 36, No. 3, pp. 283-305

MAKIAVELI, NIKOLÒ, 2006. *Printsat*. Sofia: Zahariy Stoyanov. [In Bulgarian].

NEWMAN, N.; FLETCHER, R.; KALOGEROPOULOS, A.; LEVY, D.; NIELSEN, R., 2018. *Reuters Institute. Digital News Report*. Reuters Institute for the Study of Journalism.

NYHAN, B. & REIFLER, J., 2010. When Corrections Fail: The Persistence of Political Misperceptions. *Political Behavior*, Vol. 32, No. 2, pp. 303 – 330. https://doi.org/10.1007/s11109-010-9112-2.

O'NEIL, C., 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown Publishing Group.

PALMERTZ, B.; BJÖRN, M.; WEISSMANN, N.; MIKAEL, J., 2024. *Building Resilience and Psychological Defence: An Analytical Framework for Countering Hybrid Threats and Foreign Influence and Interference*. Lund University, Psychological Defence Research Institute. Available on: https://mpf.se/download/18.7bb35f1818ec664dc7a4664/1712909687772/building-resilience-and-psychological-defence.pdf.

PAMMENT, J., 2020. *Strategic Communication in EU External Relations: From Information to Engagement*. Palgrave Macmillan.

PAUL, R.; ELDER, L., 2006. *The Miniature Guide to Critical Thinking: Concepts and Tools*. Dillon Beach, CA: Foundation for Critical Thinking.

POSTVAI.COM. *Rakovodstvo za borba s falshivite novini*. https://postvai.com/fakenews/.

PURDY, J.P., 2009. When the Tenets of Composition Go Public: A Study of Writing in Wikipedia. *College Composition and Communication*, Vol. 61, No. 2, pp. 351 – 373.

RADOSLAVOV, D., 2022. Strawman Strategy for Countering Russian Information Perations and Cognitive Warfare in Bulgaria.

SAVOVA, L., (transl.), 1991. *Hristomatia po intelektualna sobstvenost, patenti, targovski marki, avtorsko pravo*. Sofia: Institut za izobretenia i ratsionalizatsii INRA. [In Bulgarian].

SCANLON, P.M. & NEUMANN, D.R., 2002. Internet plagiarism among college students. *Journal of College Student Development*, Vol. 43, No. 3, pp. 374 – 385.

SERAFIMOVA, M., 2025. *Prakticheskо rakovodstvo na publichnata komunikatsia v sigurnostta i otbranata. Balgarskiyat opit*. Sofia: Izdatelstvo „Vanyo Nedkov“. [In Bulgarian].

SNOWDEN, P., 1915. Woman and War. *Journal of Proceedings and Addresses of the Fifty-Third Annual Meeting and International Congress on Education*. Oakland, California.

STOYKOV, M., 2018. *Ekspertna otsenka na institutsionalnite sposobnosti za protivodeystvie na hibridni zaplahi*. Sofia: Voenna akademia „G. S. Rakovski“. [In Bulgarian].

SUN DZA, 2022. *Izkustvoto na voynata*. Sofia: Fama. [In Bulgarian].

SUNSTEIN, C.R., 2019. *On Freedom*. Princeton University Press.

SUTHERLAND-SMITH, W., 2010. Retribution, Deterrence and Reform: The Dilemmas of Plagiarism Management in Universities. *Journal of Higher Education Policy and Management*, Vol. 32, No. 1, pp. 5 – 16.

TAYLOR, F. (Ed.), 1995. *The Goebbels Diaries 1939 – 1941*. New York: G. P. Putnam's Sons.

TECHAU, J., 2011. What makes communication strategic? Preparing military organizations for Battle of Ideal. *NATO Research Paper*, No. 65.

THEOHARY, C.A.; ROLLINS, J., 2011. *Terrorist Use of the Internet: Information Operations in Cyberspace*. Washington: Congressional Research Service. https://sgp.fas.org/crs/terror/R41674.pdf.

TSAKOVA, I., 2014. *Internet pravo.bg. Kratak kurs lektsii*, pp. 252 – 277. Sofia: Paradigma. [In Bulgarian].

TZU, S., 2003. 2003. *The Art of War*. Griffith, S. (Translation). Oxford University Press.

VAN DER LINDEN, S.; LEISEROWITZ, A.; ROSENTHAL, S. & MAIBACH, E., 2017. Inoculating the Public against Misinformation about Climate Change. *Global Challenges*, Vol. 1, No. 2.

VOSOUGHI, S.; ROY, D. & ARAL, S., 2018. The spread of true and false news online. *Science*, Vol. 359, No. 6380, pp. 1146 – 1151.

WANYANA, R., 2025. Cognitive Warfare: Does it Constitute Prohibited Force? *EJIL: Talk! Blog of the European Journal of International Law*. Available on: https://www.ejiltalk.org/cognitive-warfare-does-it-constitute-prohibited-force/.

WARDLE, C.; DERAKSHAN, H., 2017. Information Disorder: Toward an interdisciplinary framework for research and policymaking. *Harvard Kennedy School. Shorenstein center of Media, Politics snd Public Policy*. Available on: https://shorensteincenter.org/information-disorder-framework-for-research-and-policymaking/.

WINEBURG, S. & MCGREW, S., 2019 Lateral Reading and the Nature of Expertise: Reading Less and Learning More When Evaluating Digital Information. *Teachers College Record*, vol. 121, no 11, pp. 1–40. [online]. Available on: https://journals.sagepub.com/doi/10.1177/016146811912101102 [Last visited: 31.05.2025].

ZUBOFF, S., 2019. *The Age of Surveillance Capitalism*. New York: PublicAffairs.

ДОПЪЛНИТЕЛНИ ИЗТОЧНИЦИ

ВЪЛЧАНОВА, З., 2023. Над 400 административни регистъра трябва да станат електронни до март 2025 г. *Инвестор.бг*. [Онлайн]. Достъпно на: https://www.investor.bg/a/516-politika/383218-nad-400-administrativni-registara-tryabva-da-stanat-elektronni-do-mart-2025-g. [Прегледан на 19.03.2025].

ЕВРОПЕЙСКА КОМИСИЯ, 2018. Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите. *Европейски подход за борба с дезинформацията, разпространявана онлайн*. Достъпно на: https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:52018DC0236.

МИНИСТЕРСТВО НА ОТБРАНАТА, 2023. *Наръчник по стратегическа комуникация*. София: Министерство на отбраната.

НАРЕДБА за минималните изисквания за мрежова и информационна сигурност. ПМС № 186 от 26.07.2019 г.

ЦЕНТЪР ЗА ИЗСЛЕДВАНЕ НА ДЕМОКРАЦИЯТА, 2023. *Resisting Foreign Influence in the Digital Age.* CSD Report,

JOINT PUBLICATION 1-02: Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms (Washington, DC: Government Printing Office, 8 November 2010. As Amended Through 15 July 2011).

JOINT PUBLICATION 1-02: US Department Of Defense Dictionary of Military and Associated Terms. February 2018.

JOINT PUBLICATION 1-02: US Department Of Defense Dictionary of Military and Associated Terms. February 2018.

LIVERMORE, D., 2018. China's "Three Warfares" In Theory and Practice in the South China Sea. *Georgetown Security Studies Review*. [Online]. Available on: https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/.

MD, 2012. MC 422/4. Military formation Operations.

Петко Стефанов Димов
Ивайло Иванов Игнатов
Христина Николаева Добрева

ПРОТИВОДЕЙСТВИЕ НА ДЕЗИНФОРМАЦИЯТА

Българска
Първо издание

рецензенти: доцент д-р Елислав Иванов
капитан I ранг доц. д-р Тодор Димитров

редактор: Катерина Антонова
предпечатна подготовка: Георги Кирилов

формат 70x100/16

Военна академия „Георги Стойков Раковски“
София, бул. Евлоги и Христо Георгиеви, № 82

https://rndc.bg/publishing

ISBN: 978-619-7711-69-1