ISSN 2738-7089 https://doi.org/10.11610/cybsec12bg

Информационен бюлетин за киберсигурност

Специален брой: Устойчивост и интегритет на информационното пространство – проект Код

Бюлетин Април 2024 Номер 12

Цели и обхват

Съдържание:

Настоящият брой на информационния бюлетин по киберсигурност има за цел да разшири обхвата си с един друг аспект на устойчивостта и интегритета на информационното пространство, а именно противодействието на дезинформацията. В тази връзка ще бъде представен проектът CoDE (Countering Disinformation Environment (Ecosystem) in Bulgaria), който е изследователски и цели пилотно изграждане на устойчива екосистема с капацитет за анализ на информационната среда и постигане на информационно превъзходство. В основата е изграждането на среда за OSINT (Open source intelligence) способност за работа на аналитици, но и на академия за подготовка на специалисти (с фокус на е-обучение и оценка от участниците на интегритета на средата, разкриване на дезинформация и противодействие с информационни операции и съвет към компетентните органи), както и акселератор за бързо технологично „узряване“ на добри идеи за използване на нови технологии (изкуствен интелект, машинно обучение и др.) и въвеждането им в реална експлоатация в екосистемата при бизнес модел, гарантиращ устойчивост.

Финансираща организация е Фондация „Америка за България“ по програмата за добро управление. Основа за изпълнение на проекта е мрежа между СУ „Св. Климент Охридски“ (Стопански Факултет, Философски Факултет, GATE Институт), ИИКТ-БАН, технологичните компании Identrics, Contipso, и Webcentric, и неправителствената организация Европейски софтуерен институт - Център Източна Европа (ЕСИ-ЦИЕ).

В настоящия брой е представена информация за всеобхватния подход за информационно превъзходство (CONOPS). Концепцията за подход „цялото общество в противодействие на дезинформацията и пропагандата“ се разглежда като програма от 6 взаимосвързани проекта. Представени са 2 от партньорите по проекта – Философски Факултет и GATE Институт.

Заедно с това е представен и проектът за Европейска обсерватория за цифрови медии (EDMO), чрез който се подкрепя независимата общност, бореща се с дезинформацията, и Подсиленият практически кодекс относно дезинформацията (Strengthened Code of Practice on Disinformation), който дава възможност на индустрията да се придържа към стандартите за саморегулиране за борба с дезинформацията.

Бюлетинът се публикува на български език на официалния сайт на проекта CoDE и Института по информационни и комуникационни технологии (ИИКТ) при Българска академия на науките (БАН) като академичен партньор.

Редактор на броя: **проф. д.н. Даниела Борисова**

Фокус на изданието:
Всеобхватен подход за информационно превъзходство

Концепцията за подход „цялото общество в противодействие на дезинформацията и пропагандата“ се разглежда като програма от 6 взаимосвързани проекта:

1. Разработка на базови инструменти за извличане на данни от информационната среда и първичната им обработка;
2. Построяване на знаниен граф и дълбочинен анализ на информационната среда с цел противодействие на дезинформацията и пропагандата;
3. Ускоряване на иновациите по инструментите чрез ефективен Test & Evaluation, Validation & Verification (TEVV) процес и сертификация за ползване в CoDE;
4. Разработване на електронни курсове и набор от обучения на аналитици за използване на инструментите, разработени в рамките на ориекти 1 и 2 за противодействие на дезинформация и пропаганда;
5. Надграждане на съществуващите способности в България чрез инструментите и обучените хора в CoDE за демонстрация чрез хакатони, учения и портфолио от нови, свързани с CoDE, проекти за постигане на позитивен ефект в обществото още в рамките на проекта;
6. Развитие на бизнес модел и добавяне на нови партньори за създаване на устойчива екосистема с ефективна стратегическа комуникация и вътрешна комуникация за интеграция на общността.

Концепцията за проекта и екосистемата за противодействие на дезинформацията и пропагандата е **първото ниво** на планиране и изисква изясняване на понятията, свързани с информационното превъзходство и оценка на текущото състояние в тази област в България, за което се провеждат серия от вътрешни семинари във ФФ-СУ, СФ-СУ, GATE, участващите технологични партньори и заключителна среща в ИИКТ, където се финализира и концепцията за управление на проекта. Съществена част от проекта е преходът от проектна организация към институционална организация с роли, които ще се изпълняват след края на проекта и които ще доведат до устойчивост чрез нови проекти и предоставяне на услуги, както и при възможност институционално финансиране на основната функция – развитие на способности (хора и технологии) за противодействие на дезинформацията.

Второто ниво е разработка на Концепция за противодействие на дезинформацията по модела „цялото общество“, което е нашето целево състояние (реализация на Всеобхватен подход за информационно превъзходство) и дефиниране на приноса на проекта CoDE с индикатори за успех. Това ниво включва и срещи с всички заинтересовани страни по подхода „цялото общество“ – университети, НПО, администрация, бизнес, международни партньори. На това ниво

се провежда и първата среща на Консултативния съвет за валидиране на оценка на ситуацията и визията за промяна, представена като Всеобхватен подход за информационно превъзходство.

Третото ниво е разработване на пътя за реализация на Концепцията чрез детайлното описание на визията и плана за постигане на оптимален бизнес модел на център / мрежа за сътрудничество за споделени услуги в сферата на противодействие на дезинформацията, както и план за демонстрация на тази способност, подкрепени от двата основни стълба / инструмента за подхода – изграждането на Акселератор за инструменти по противодействие, както и подбор и обучение / сертификация на хора / екипи за противодействие.

Четвъртият заключителен етап, включва обсъждане с Консултативния съвет и интеграция на всички по-горе елементи в единна Концепция за развитие на ефективна, ефикасна и икономична екосистема за противодействие на дезинформация и пропаганда (и стратегическа комуникация).

Концепцията за Всеобхватен подход по същество дава рамка за постигане на информационно превъзходство (в когнитивния домейн), като използва добри практики от изградените системи за киберсигурност, които включват усилия за иновации, за обучение, за оперативно реагиране и обмен на информация, проактивни мерки за укрепване на устойчивостта на атаки и добавя специфични елементи за когнитивния домейн като стратегическа комуникация, развитие на критично мислене и медийна грамотност (хигиена). В контекста на членството в НАТО и ЕС е важно да се постигне това състояние на национално и на съюзно ниво, като модел е Регламент 887/2021 в сферата на киберсигурността. Търсенето на оптимален модел за България ще се подпомогне от сравнението на подходи в САЩ, Великобритания, Германия, Румъния и Украйна.

1. Инструменти „Данни и информация“

Осигуряване на инструменти за екипа от аналитици за събиране на данни и извличане на информация

Разграничават се 3 нива за създаване на информационно превъзходство в Интернет пространството:

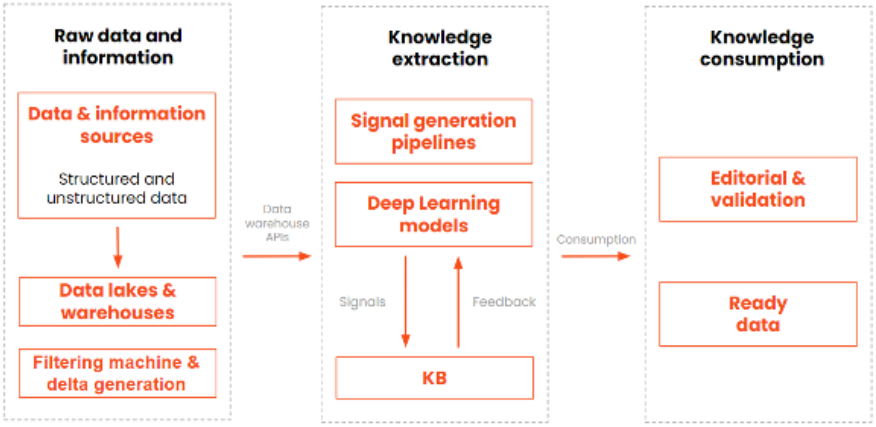
1) **Филтриране и блокиране** на сървъри, домейни, IP адреси, ключови думи и др. Такива техники за контрол над интернет пространството се прилагат от страни, като Китай;

2) **Създаване на правна и нормативна среда**, в която правителството може избирателно да откаже публичния достъп до информация в Интернет, ако и когато е “необходимо”. Видимата част на този вариант е в създаването на закони, които регулират “приемливото” уеб съдържание, както и закони срещу клеветата и обидата. Скритата част се състои в оказване на натиск върху доставчиците на интернет услуги и използването на Denial-of-Service (DDoS).

3) Трето ниво е т.нар. **контрол** 2.0. Целта тук не е да се отказва достъп до информация, а да се осъществява състезание за вниманието на аудиторията и да се разкрива дезинформацията в потока от друго съдържание. Тези действия могат да се ръководят от сложни методи за

интернет наблюдение и извличане на данни в информационните операции, които да бъдат внимателно насочени към деморализиране и дискредитиране на противниците.

Развитият бизнес на медиен мониторинг и анализ включва сериозна технологична екосистема от алгоритми и инструменти, позволяващи огромни количества данни да бъдат обработвани за секунди. Айдентрикс разполага с такава екосистема, със сегменти и решения от която участва в проекта CoDE. Автоматизираното агрегиране на медийни данни от интернет е процесът на събиране и организиране на тези данни по начин, който улеснява търсенето. Този процес включва следните стъпки:



1) Събиране на данни: Първата стъпка е да се съберат медийни данни от различни източници, включително уебсайтове, социални медии и новинарски организации;

2) Пречистване на данни: След като данните бъдат събрани, те трябва да бъдат пречистени, за да се премахне ненужната информация, като например реклами, спам, вътрешни елементи;

3) Индексиране на данни: След като данните бъдат пречистени, те трябва да бъдат индексирани, за да могат да бъдат търсени. Индексирането включва създаването на база данни, която свързва ключови думи и фрази с конкретни части от данните. Индексирането на медийни данни е от съществено значение за лесното и удобно търсене.

Данни OSINT: Компонент за агрегиране на сурови данни и информация.

Инструмент за откриване на данни AnnX-E(xtraction): Този инструмент е незаменим помощник, чрез който се намира и организира информацията, по удобен и ефективен начин. Основният сценарий за използване на инструмента „AnnX-E" е за извличане и филтриране на съдържание по теми и други метаданни.

Инструмент за дизайн и анотиране на информационни набори AnnX-A(nnotation): Чрез този инструмент обучени анализатори извличат знание от информацията. Основният сценарий за използване на инструмента „AnnX-A" е да послужи за обогатяване (анотиране) на вече извлечено и филтрирано медийно съдържание (информационни набори), разпределянето на задачи към различни анализатори и организиране на различни методи за анализ.

Инструмент за проследяване и измерване на ангажираността на потребителите към събития, отразени в медиите – EventVista: Този онлайн инструмент за автоматична категоризация на новини дава общ преглед на тенденциите и нововъзникващи тематични наративи, както и задълбочено проследяване в показателите, които ги определят, напр. тема, хора, организации, сантимент и др. Основният сценарий за използване на инструмента „EventVista" е за откриване на нови или формиращи се дезинформационни кампании.

Инструмент Risk inteligence platform: Тази онлайн платформа за фирмено разузнаване за региона на Югоизточна Европа е базирана на иновативна технология за entity linkage. Основният сценарий за използване на инструмента „Risk inteligence platform" е да даде възможност на анализаторите на дезинформационни кампании, след като локализират определени актьори, да проследят свързаността им с различни компании и публични политически личности.

Инструмент AI models: След като анотираните информационни набори са разработени в AnnX и бъдат организирани в структурирани експорти, започва обучението и тестването на алгоритми за дълбоко обучение за автоматизирана оценка и прогнозиране и анализ на различни наративи, тоналност, обобщена тема. Тези алгоритми използват най-добрите модели от "арсенала" на Айдентрикс и са дообогатени с анализираните вече в проекта данни, анотирани от експерти по домейни. Целта на тези модели за дълбоко самообучение е, след като бъдат обучени, в крайна сметка да действат като първо ниво на анализ. Основният сценарий за използване на инструментите от тип „AI models" е за автоматизирано обогатяване на OSINT данните с цел по-качествена филтрация.

2. Инструменти „Наблюдение, ориентация, решение, действие"

Формиране и анализ на графи на знанията за разбиране и подпомагане на вземане на решения за необходимите действия

Платформата за ситуационна осведоменост и анализ (Intelligence and Analytics Platform, IAP) в рамките на проекта CoDE има за цел да отговори на предизвикателствата за анализ на информационното пространство, като използва интегрирани набори от оперативно съвместими инструменти за работа с най-съвременните техники, включително графи на знанието и графи на социални мрежи / анализ на социалните мрежи, за да осигури цялостен поглед върху разпространението на информацията и дезинформацията.

1) Графите на знанието (Knowledge Graph, KG) или „знанийни графи" са колекции от взаимосвързани точки от данни, представляващи различни обекти и връзките между тях. Те са структурирани така, че да имитират начина, по който хората обработват информация, което ги прави особено полезни за анализ на сложни данни.
2) Социалните графи (Social Network Graph, SNG) подпомагат главно илюстрирането на връзките по различни признаци и взаимодействията между различните участници в рамките на мрежата. Те са фокусирани върху социалните аспекти в набора от данни и често представляват екстраполация на съществуващи графи на знанието.

3) Анализът на социалните мрежи (Social Network Analysis, SNA) на фундаментално ниво е клъстерирането и разбирането на сложните взаимоотношения в социалните мрежи. Този анализ включва подробно картографиране и изследване на начина, по който индивидите, групите и организациите си взаимодействат и оказват влияние върху по-широката екосистема от зависимости.

В контекста на динамично еволюиращия информационен пейзаж тези технологии се използват от експерти за разкриване на разнообразни зависимости в информационната екосистема и най-вече в областта на разпознаването на дезинформацията и изследването на моделите на разпространение на фалшива информация. Някои ключови приложения на KGs и SNGs включват:

1) **Извличане на данни** като например обекти (хора, организации, събития), връзки и атрибути от неструктуриран текст (т.е. SNA).
2) **Разпознаване на субекти** и понятия, свързани с дезинформацията, като източници на фалшиви новини, влиятелни лица и теми.
3) **Картографиране на взаимоотношенията** чрез установяване на връзки между субекти въз основа на споменавания, препратки, референции, групови принадлежности и други взаимодействия в данните, които може да са директни или индиректни.
4) **Темпорален анализ** за описване на ключовите събития по време, с цел проследяване развитието на субектите и техните взаимоотношения във времето.

Предвид тези приложения, когато става въпрос за SNA в контекста на противодействието на дезинформацията, можем да говорим за някои ключови възможности, които такъв анализ би могъл да предостави на екипите от медийни изследователи, а именно: 1) Ранно известяване; 2) Идентифициране на източника; 3) Анализ на влиянието; 4) Проверка на съдържанието; 5) Алгоритмично откриване; 6) Споделяне на ключови знания и информация.

3. Акселератор на инструменти за информационно превъзходство

Среда за повишаване на технологичното ниво на готовност на необходими инструменти и интеграцията им

Отправната точка в работата по проекта е осведомеността относно софтуерните решения, които се предлагат от страна на партньорите, както и други налични инструменти. По принцип тези решения са предназначени за автоматизация на ръчните дейности, за предоставяне на специализирана информация в помощ на работещите в сферата и за подпомагане на вземането на решения, които обслужват работата. Софтуерните решения за борба с дезинформацията могат да се класифицират в няколко групи в зависимост от различни технически критерии.

1) **Задачи, които могат да се решават с използването на софтуерни решени**я – проверка на факти, идентифициране на насоченост към определена социална група, откриване на скрити цели, проследяване на събития, формиращи процес на внедряване на идеи, формулиране на цялостни изпълнения на сценарии за въздействие (narrative) и други;

2) **Процедурна пълнота от гледна точка на практиката в борбата с дезинформацията, поддържани от тях** – поддръжка на конкретна стъпка, решаване на отделна задача, изпълнение на цялостен сценарий и др.;

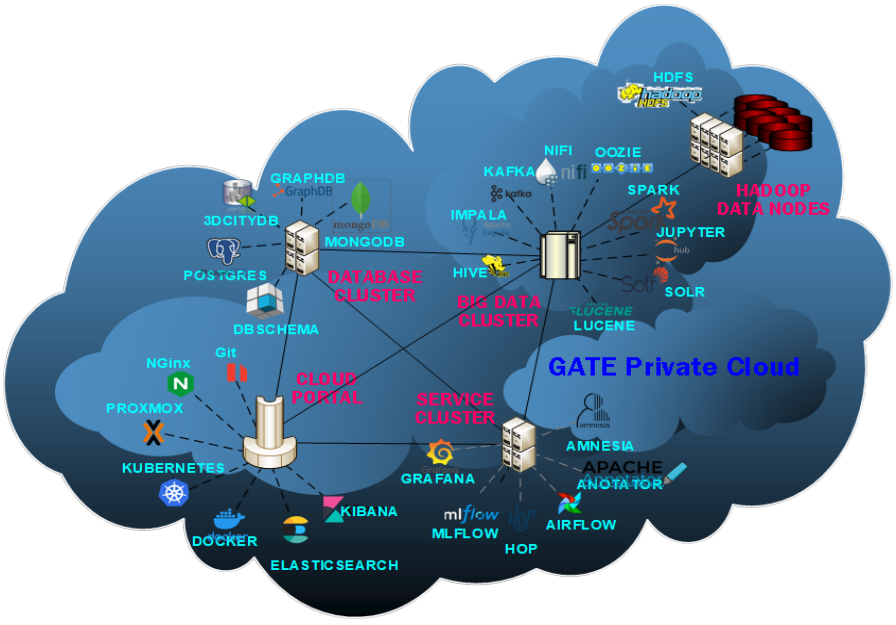
3) **Начин на работа със софтуерните решения от крайните потребители** – самостоятелно използване на персонално устройство в режим на връзка с централизиран източник на поддръжка в Интернет (клиент-сървър), чрез получаване на готово решение по заявка, чрез контакт с външен експерт, използващ софтуерното решение в организацията, предоставяща консултантски услуги и др.;

4) **Изисквания към техническата подготовка на потребителите** – краен потребител, извършващ специфична задача без познание за работата на софтуера и без експертиза за цялостни решения в борбата с дезинформацията, експерт в областта, познаващ цялостните сценарии за работа в борбата с дезинформацията и технически експерт, поддържащ работата на проблемните експерти;

5) **Организация на начина на предоставяне на услугите**, които се предлагат на специалистите в борбата с дезинформацията и други;

На основата на направената класификация на предлаганите от участниците в проекта софтуерни решения, тяхната оценка може да се направи по различна методология:

1) **Експертна оценка** на инфраструктурно решение за поддържане на работата по борбата с дезинформацията. Такива решения са: а) системата за колаборативна работа на Webcentric, и б) платформата за данни на GATE, която може да се използва за различни цели – разработка, тестване и хостване на решения в областта на борбата с дезинформацията;



2) **Софтуерно тестване на продуктите предлагащи автоматизация** на отделни задачи в борбата с дезинформацията;

3) **Софтуерно тестване на системи за автоматизация** на работата по борбата с дезинформацията, предназначени за използване в конкретни организации;
4) **Проверка и анализ на данните,** генерирани с помощта на предлаганото софтуерно решение;
5) **Валидиране на концептуалните модели,** реализирани в софтуерните решения;
6) **Верификация на процедурите за работа**, поддържани от софтуерните решения;
7) **Качествено и количествено оценяване на предлаганите услуги**;
8) **Определяне на степента на технологична зрялост** на софтуерните решения.

Използването на института GATE като основа за акселератор на инструменти (платформи, услуги, пакет от данни) в сферата на анализ на информационното пространство, противодействие на дезинформацията и постигане/поддържане на информационно превъзходство създава солидна основа на операторите за работа с иновативни компании за каталогизиране и интегриране на най-подходящите инструменти за различни кампании, адекватно обучение на аналитиците да ползват тези инструменти общо и в конкретни сценарии (последното е задача на Академията в екосистемата CoDE).

4. Академия за информационно превъзходство

Подготовка на аналитици за работа по концепцията и с инструментите в програмата

В рамките на CoDE се предвижда създаването на Академия за противодействие на дезинформация, която включва разработването на 8 обучителни пакета, адаптирани към различни целеви групи, както и провеждането на 3 хакатона, като част от пакета за демонстрация на способността на екосистемата.

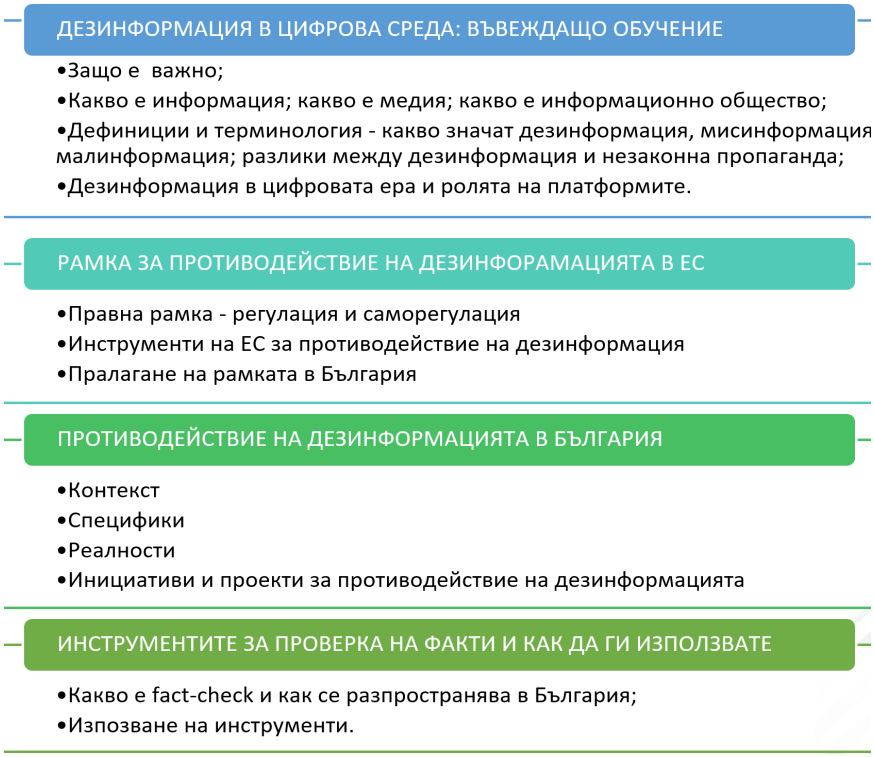
В рамките на CoDE са идентифицирани 5 целеви групи: 1) студенти, 2) ученици; 3) обучители, преподаватели, учители; 4) изследователи, журналисти, факт-чекъри, експерти от неправителствения сектор и 5) служители на администрации. На база на разработената карта на заинтересовани страни, ангажираните с противодействие на дезинформацията в България, ще бъде изпратена покана за участие в обученията на различните целеви групи, като желаещите да се включат в обученията ще получат достъп до обученията и съдържанието за целевата група, от която са част.

Специфичен подбор с конкурс ще се извърши в рамките на проекта за набиране на участници, които искат да станат обучители и да се ангажират по-тясно с провеждане на обученията, веднъж след като те самите преминат през такова.

Първоначалният план е обучението да премине през следните етапи:

1) **Подбор и регистрация**;
2) **Базови обучения** – за повишаване на базовите им компетенции за разпознаване и противодействие на дезинформация и за анализ на информационната среда, както и на познанията им за

терминологията в областта и правната рамка за противодействие на дезинформацията в ЕС;



3) **Специализирани обучения** – достъп до конкретни инструменти, разработени от технологичните партньори в проекта, което да подобри уменията за последващо участие в хакатоните и практическите упражнения;
4) **Хакатони и практически упражнения**;
5) **Сертификация**;
6) **Партньорства** – сътрудничество с академия, институции (вкл. МС и НС, Министерство на образованието, Министерство на електронното управление, Министерство на външните работи, Министерство на отбраната, Министерство на вътрешните работи, Министерство на културата, неправителствени организации и бизнес сектора за подкрепа и разширяване на обхвата на инициативата у нас, както и изграждане на партньорства с подобни центрове за обучение в други страни.

В рамките на Академията ще бъдат подготвени и сертифицирани за участие в хакатони, учения, целеви проекти/операции около 150 специалиста от различни университети, НПО, училища и други доброволци, които ще имат и достъп до обучение и използване на инструментите на CoDE. От обучените специалисти ще бъдат набирани доброволци за включване в отделни „проекти“ на CoDE (хакатони, учения, демо и реални информационни операции за противодействие на дезинформация и пропаганда).

В рамките на CoDE се предвижда разработването на интерактивни онлайн обучения за изграждане на устойчива екосистема за противодействието на дезинформацията в България.

5. Демонстрация на способността за информационно превъзходство (оценка на As-Is през 2023 и преди: къде сме?)

Интеграция на ползите от всички проекти в полза за екосистемата и потребителите / обществото чрез оценка и поддържане интегритет на информационното пространство

Финансиращата организация очаква с проекта CoDE да се изгради устойчива екосистема от участници с фокус на академичната общност и НПО, с участие на бизнеса и администрацията за реализиране на основни ползи за обществото като:

1) **Повишаване на нивото на разбиране на заплахата от дезинформация и пропаганда** и съответно необходимостта от изграждане на способност за устойчивост;
2) **Подобряване на програмите за обучение в университетите и училищата** по въпроси на анализа и оценката на информационната среда и развитието на способности за постигане на информационно превъзходство над опитите за зловредно влияние;
3) **Повишаване на иновативността и конкурентоспособността** на български фирми, ангажирани с развитие на средства за анализ, оценка на информационната среда и противодействие на дезинформация;
4) **Създаване на ефективна и ефикасна среда за взаимодействие** на всички заинтересовани страни за постигане на синергия в усилията за информационно превъзходство;
5) **Мотивиране за използване на управленски и бизнес практики** за устойчивост на екосистемата за противодействие на дезинформация и пропаганда;
6) **Принос към усилията в НАТО и ЕС**, позициониране на България като лидер в ЮИЕ по противодействие на дезинформацията и пропагандата;
7) **Подобряване на средата за реформи и инвестиции в България** чрез намаляване на зловредното влияние на дезинформацията и пропагандата в обществото и институциите.

Информационното превъзходство се състои от елементи, които формират обхвата и съдържанието му, използват се за изграждане и поддържане на способности, използването им в операции и интеграцията му в системата за национална сигурност. Информационното превъзходство като компонент на националната сигурност се характеризира с: цел, операции за постигането ѝ, способности. Важни елементи на това превъзходство са партньорствата, управлението на промяната и демократичният контрол, които обхващат всички елементи от цел до способности. Ние не действаме сами, а като част от по-големи организации, при постоянни промени – от отделните организации през държавата до съюзи, в които членуваме, и до ООН като глобална организация в сферата на сигурността и развитието. Всичко, свързано със сигурност, в свободния свят изисква строг (демократичен) контрол от представители на гражданите за гарантиране на целесъобразно и законно използване на силата.

Структура за изграждане на информационното превъзходство

Проектът CoDE е изследователски, затова включва стратегически инициативи и управление на риска с практическа насоченост чрез демонстрация на постиженията в реална среда. В този смисъл Концепцията включва изследвания и демонстрации (отделни и интегрирани) на следните компоненти (стратегически инициативи):

1) Академия за информационно превъзходство;
2) Акселератор за инструменти на информационното превъзходство;
3) Инструменти за структуриране, обработка и първичен анализ на потоци от данни;
4) Инструменти за създаване на графи на знанието и дълбочинен анализ;
5) Процеси, организация, бизнес модел и план за OSINT хъб и мрежова организация за сътрудничество за постигане на информационно превъзходство;
6) Демонстрация на горните елементи по отделно и интегрирано при провеждане на реални операции за информационно превъзходство по избрани теми / опонент.

6. Бизнес модел на платформа за информационно превъзходство

Създаване на среда за взаимодействие в екосистемата и при ползване на услугите ѝ

В България екосистемата за борба с дезинформацията и фалшивите новини все още не е достигнала своята зрялост. Макар страната да е изложена на негативно информационно влияние от поне десетилетие и риска, заплахата от информационни операции и хибридни атаки да бяха ясно очертани във Визия 2020 „България в НАТО и Европейската отбрана“ (рамков документ на СС-МС за участие на българската делегация на срещата на върха в Уелс през септември 2014), то основните елементи и компоненти на екосистемата започват да се оформят след 2019 г. и особено след Ковид-19 кризата и последвалата я вълна от дезинформация през 2020 г.

Има дефицити в правната рамка за борба с дезинформацията, като основната нормативна регламентация идва по линия на членството на страната в Европейския съюз – Законодателния акт за цифровите услуги (Digital Services Act, DSA) и Акта за цифровите пазари (Digital Markets Act,

DMA). Националното законодателство все още изостава, като няма ясно регламентирана нормативна рамка за осъществяването на дейности за борба с дезинформацията.

От търговска гледна точка, частните компании в екосистемата оперират хибридни бизнес модели. Макар те да предоставят „суровините“ за генериране на информационните услуги за борба с дезинформацията (входни данни, аналитични платформи и инструменти), те не зависят от нейното успешно развитие. В екосистемата се оформят определени аналитични центрове сред неправителствените организации и някои университети. Работата по аналитични дейности за борба с дезинформацията в тези центрове се финансира или чрез външни проекти или в рамките на по-ограничени вътрешни бюджети. Усилията и резултатите (бази данни, аналитични инструменти, крайни изводи, научени уроци от проведени дейности) са сравнително слабо координирани и следва да бъдат фокусирани за постигане на по-висока ефективност. Основната активност на екосистемата за борба с дезинформацията е концентрирана в София. Крайните потребители на продуктите на екосистемата най-често са отделни индивиди. Потребителите в България имат сравнително ниско ниво на медийна грамотност, сравнено с това в останалите страни-членки на ЕС.

Екосистемата за борба с дезинформацията не е стандартен пазар. При нея не е водещо търсенето на крайните потребители (гражданите, държавните институции, академичната общност и в определени случаи търговски субекти) на услугите, които тя предлага, и в този смисъл е малко вероятно тя да може да функционира на чисто пазарен принцип. Въпреки това производителите на тези (a priori допуснати за необходими) аналитични услуги имат своите разходи, вкл. за данни, разработване и поддържане на инструменти и труд. Това предполага, че те имат разходи без конкретни насрещни приходи и по този повод съществуват следните начини на финансиране:

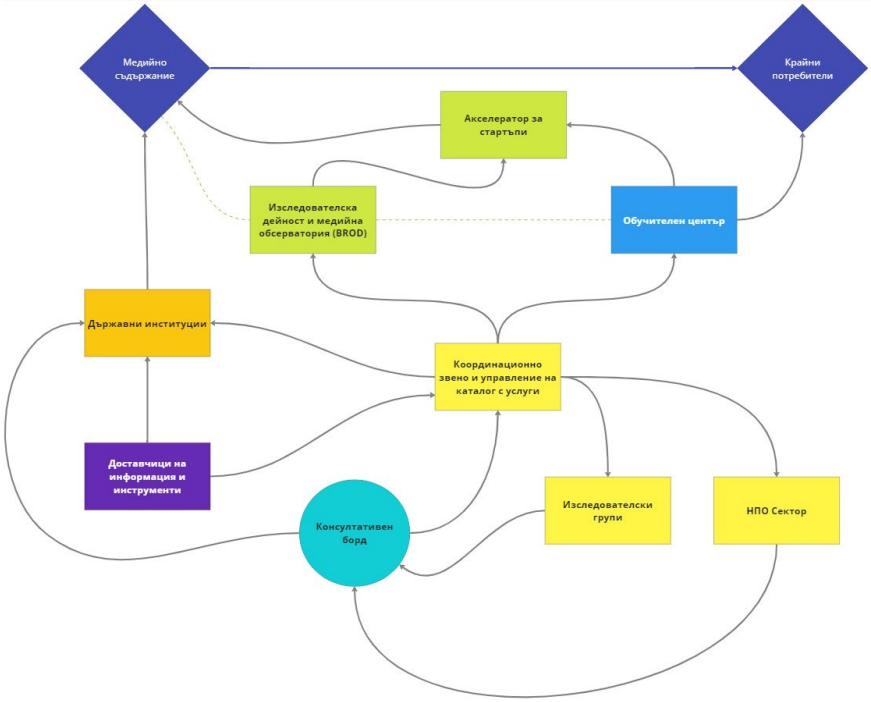
1) Крос-субсидиране на доставчиците на услуги за борба с дезинформацията от други техни печеливши дейности;
2) Отделяне на безвъзмездни средства по линия на вече съществуващи бюджети (държавни, общински, на конкретни публични институции);
3) Проектно финансиране от източници в публичния сектор, НПО сектора и частния сектор;
4) Финансиране чрез потребителите на услуги – частни и публични, вкл. чуждестранни потребители.

Силни страни	Слаби страни
✓ Изследователски групи с опит в областта (GATE, СУ, НБУ, ЦИД, БАН и др., вкл. в НПО). ✓ Развит ИТ сектор, който може да предостави аналитичен и изчислителен капацитет.	✓ Ниско ниво на медийна грамотност. ✓ Липса на значително търсене на такива услуги от обществеността. ✓ Нужда от усъвършенстване на нормативната рамка.

✓ Специализирани доставчици на информационни услуги. ✓ Наличие на граждански активисти с опит и интерес по темата.	✓ Липса на национална стратегия и координация за борба с дезинформацията. ✓ Липса на институционализирано устойчиво финансиране. ✓ Ограничени програми в университетите и вътрешни проекти в академичната общност. ✓ Недостатъчно разбиране на оперативните аспекти на борбата за информационно превъзходство.
Възможности	**Заплахи**
✓ Ръст на външното финансиране на проектен принцип, вкл. по програми на НАТО и ЕС. ✓ Интеграция с други екосистеми за борба с дезинформацията в съседни страни (пр. по линия на EDMO мрежата). ✓ Създаване на съвместни консорциуми за координирани действия. ✓ Предоставяне на аналитичен и научен капацитет на външни партньори и клиенти. ✓ Ползване на уникален опит придобит от правителствени и частни организации в Украйна.	✓ Висока активност при генерирането на дезинформация, което да доведе до претоварване и демотивация на участниците. ✓ Промяна на политиките за финансирана на донорските организации. ✓ Усилване на политическата нестабилност в страната и липса на ангажимент към темата от отговорните институции. ✓ Повишаване на мотивацията и ресурсите на нашите опоненти в сферата на информационно-психологически специални операции. ✓ Зловредно използване на технологията на Изкуствения интелект.

В подобни случаи се наблюдават пазарни провали – т.е. чисто пазарното предоставяне на услугата е невъзможно в достатъчно количество и е обичайно такива пазарни провали да се адресират чрез държавна намеса или регулация. В настоящето състояние на екосистемата е видно, че липсват ключови връзки между институциите от една страна и доставчиците на продукти и услуги, медиите, академичните среди и крайните потребители от друга.

За функциониране на екосистемата като доставчик на публични блага, чиято стойност не е напълно възприета от потребителите, е необходимо значителна институционална намеса от гледна точка на финансиране на екосистемата, контрол върху производството на информационни услуги и регулация на медийното съдържание. В този смисъл в екосистемата следва да се допусне a priori стойността от дейностите по борба с дезинформацията, тъй като тя няма да бъде изведена и не може да бъде монетизирана на пазарен принцип. Това е така тъй като предложението за стойност тук не е насочена към крайните потребители – то е предложение за създаване на колективна обществена стойност и доставката на тази стойност може да бъде финансирана само чрез колективни средства.



Основни връзки в структурата на управление на екосистемата

Рискът от прекомерната държавна намеса и произтичащата от това неефективност и заплаха от цензуриране на съдържание следва да се балансира от децентрализирана структура на екосистемата, която да бъде координирана от широк кръг заинтересовани страни чрез добра система за ръководство на мрежова организация за сътрудничество.

Устойчивото функциониране на екосистемата е обвързано и с наличие на устойчиво финансиране. Оценяваме общият размер на пазара за борба с дезинформацията на стойност от под 2 млн. лева, което не е достатъчно за поддържането нито на дейностите, нито на координационните структури. При целева стойност от 10 млн. лева, следва да се планира достигането им в средносрочен план от 3 до 5 години.

Потенциално разпределение на потоците би било както следва:

5) 50% фиксирани бюджети в държавни институции (5 млн. лева) за дейности, свързани с борбата с дезинформацията. Те следва да включват както поддържане на експертен капацитет, така и разходи за външни продукти и услуги.
6) 30% нарочно национално проектно финансиране (3 млн. лева), насочено към различни сегменти от екосистемата (изследователи, НПО, партньори).
7) 20% (2 млн. лева) проектно и ад хок финансиране от различни финансиращи организации, вкл. по линия на неправителствените организации и директно финансиране от Европейската комисия.

Подобно разпределение, но и съвместен контрол осигурява и че различните финансиращи страни развиват умения да работят заедно, изграждат доверие и синергия, с което се осигурява и по-добро цялостно управление на екосистемата.

Нашият партньор: Институт GATE

Институтът GATE – Големи данни в полза на интелигентно общество е първият високотехнологичен център за научни изследвания и иновации в областта на големите данни и изкуствения интелект в България и Източна Европа. Той е създаден през 2019 г. като основно структурно звено на Софийския университет в партньорство с Технологичния университет Чалмърс и Чалмърс Индустри Техник, Швеция.

GATE има за цел да създаде уникална среда и инфраструктура за приложни научни изследвания в най-съвременните технологични области – големи данни и изкуствен интелект, като се превърне в глобално конкурентен дигитален хъб за иновации и прилагането им в решаване на проблеми в областта на „Градове на бъдещето“, „Дигитално здравеопазване“, „Умна индустрия“ и „Интелигентно правителство“.

През 2021 г., в отговор на нарастващата обществена потребност от справяне с различни форми на дезинформация, GATE добави към своето портфолио изследванията в областта на откриването на дезинформация.

Проектът „Големи данни за интелигентно общество“ (GATE) се финансира по мярката WIDESPREAD-2018-2020 TEAMING Phase 2 на програма „Хоризонт 2020“ и по Оперативна програма „Наука и образование за интелигентен растеж“ 2014-2020, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Повече за GATE може да намерите тук.

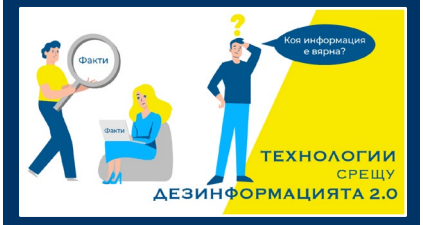
Нашият партньор: Философски факултет на СУ „Св. Климент Охридски“

Философският факултет е един от центровете на българската хуманитарна наука от основаването на Софийски университет „Св. Климент Охридски“ през 1888 г. По брой студенти, преподавателска, библиотечна, материално-техническа и информационна осигуреност факултетът е сред най-големите научни средища в Югоизточна Европа в областта на общественото и хуманитарното знание. В него преподават над 180 висококвалифицирани професори, доценти и асистенти и учат около 3000 студенти от 25 страни в трите образователни степени – бакалавър, магистър и доктор.

Мисията на колегията от преподаватели, студенти и служители е да изучава, изследва, развива и препредава човешкия опит в социалната и политическата сфера чрез висока научна и практическа квалификация. Философският факултет действа като институция от национално значение и формира ядрото на българската хуманитарна интелигенция.

Повече за Философския факултет на СУ „Св. Климент Охридски“ може да намерите тук.

Конференции и събития



На 7 ноември 2023 г. в София се проведе второто издание на конференцията "Технологии срещу дезинформацията". Фокусът на събитието е върху различните методологии, целящи идентифициране на пропагандни процеси, както и начините, с които новите технологии могат да помогнат в борбата с дезинформацията.

Запис на конференцията може да се види тук.

Връзки към проекти и документи

EDMO
European Digital Media Observatory

The Strengthened Code of Practice on Disinformation 2022

- EDMO – European Digital Media Observatory. Проектът за Европейската обсерватория за цифрови медии (EDMO) е проект, чрез който се подкрепя независимата общност, бореща се с дезинформацията. EDMO ще предоставя техническа подкрепа и съвети на Групата на европейските регулатори за аудиовизуални медийни услуги (ERGA) за наблюдение на политиките на онлайн платформите съгласно Кодекса за поведение във връзка с дезинформацията и/или бъдещите регулаторни рамки.
- Strengthened Code of Practice on Disinformation – Новият кодекс обединява по-разнообразен набор от заинтересовани страни от всякога, като им дава възможност да допринесат за широкообхватни подобрения, като поемат точни ангажименти, свързани с тяхната област. Такива ангажименти включват демонетизиране на разпространението на дезинформация; гарантиране на прозрачност на политическата реклама; засилване на сътрудничеството с лицата, проверяващи фактите; и улесняване на достъпа на изследователите до данни.

Редакционен съвет

Публикуването на настоящия брой на бюлетина се реализира с финансовата подкрепа на проект **CoDE: Среда (екосистема) за противодействие на дезинформацията в България**