КОЛАБОРАТИВНА ЗАЩИТА: ПОДОБРЯВАНЕ НА НАЦИОНАЛНАТА КИБЕРСИГУРНОСТ ЧРЕЗ АНГАЖИРАНОСТ НА ГРАЖДАНСКОТО ОБЩЕСТВО

Красимир Маринов
Университет по библиотекознание и информационни технологии

COLLABORATIVE DEFENSE: ENHANCING NATIONAL CYBERSECURITY THROUGH CIVIL SOCIETY ENGAGEMENT

Krasimir Marinov

Abstract: *This paper discusses the essential role of civil society in reinforcing national cybersecurity strategies. It examines how collaboration between government entities and civil society can enhance defensive capabilities against cyber threats. It highlights the importance of developing innovative and effective strategies to counter cyber threats and explores the impact of artificial intelligence on national security. The report advocates for a balance between technological innovations and the protection of civil liberties, emphasizing the need for a multidisciplinary approach and public engagement in creating sustainable and adaptive cybersecurity solutions.*

Keywords: *civil society, national cybersecurity, collaboration, cyber threats, artificial intelligence.*

Въведение: В ерата на цифровата трансформация, пейзажът на киберсигурността става все по-сложен и ключов за националната сигурност. Разчитането на цифрови технологии както в частния, така и в публичния сектор е създало обширна, взаимосвързана мрежа, която, докато улеснява безпрецедентно нивата на комуникация и обмен на данни, също така отваря врати към нови уязвимости и заплахи. Тази нововъзникваща цифрова екосистема, която процъфтява благодарение на напредъка в технологии като облачните пространства, изкуствения интелект и „интернет на нещата" (IoT), изисква сложен и динамичен подход към киберсигурността.

Както технологията се развива, така се развива и природата и сложността на киберзаплахите. Тези заплахи вече не се ограничават до изолирани инциденти на кражба на данни или вандализъм. Те са еволюирали в по-сложни форми като държавно спонсориран кибершпионаж, мащабни атаки с откупен софтуер, засягащи критичната национална инфраструктура, и незабележими кампании за дезинформация, предназначени да дестабилизират общества. Честотата на тези атаки също нараства, което го прави належащ проблем за националната сигурност. Последствията от такива атаки могат да бъдат опустошителни, вариращи от икономически загуби до компрометиране на системата на национална сигурност и прекъсване на съществени обществени услуги. Нарастващата сложност и адаптивност на кибер-

заплахите налага по-инклузивен подход към стратегиите за национална отбрана, един, който активно включва гражданското общество.

Гражданското общество, състоящо се от индивиди, общности, бизнеси и неправителствени организации, играе ключова роля в изграждането на устойчива рамка за киберсигурност. Тяхното участие може да доведе до по-обстойно разбиране на киберзаплахите на ниво база и да насърчи култура на киберосведоменост и подготвеност. Сътрудничеството между правителството и гражданското общество може да доведе до иновативни решения, използвайки разнообразните гледни точки и експертиза, които тези групи носят. Това партньорство е съществено за разработването на проактивни и адаптивни стратегии за противодействие на динамичния характер на киберзаплахите. Следователно, преминаването към по-интегриран подход, включващ както традиционните правителствени инициативи, така и активното участие на гражданското общество, е съществено. Този колаборативен модел не само увеличава ефективността на националните стратегии за киберсигурност, но също така насърчава споделеното чувство за отговорност към поддържането на киберхигиена и устойчивост. Следва да разгледаме текущия пейзаж на киберсигурността, еволюцията на киберзаплахите, ограниченията на традиционните подходи към киберсигурността и критичната роля на гражданското общество в укрепването на националните отбранителни мерки за киберсигурност.

Участие на гражданското общество в средата на киберсигурност.

„Киберсигурността от много години е грижа и отговорност на всички участници в киберпространството. В стремежа да се намалят киберрисковете, към сигурността на технологиите бяха насочени мерки, които бяха смятани за крайни и достатъчни. Днес обаче се възприема, че процесът по осигуряване на киберсигурност изисква много повече от обикновен технически контрол, а именно човешки ориентиран подход и най-вече изграждане на култура на киберсигурност. Въпреки че ролята на формирането на култура за надеждно киберпространство е добре осъзната, изследванията, фокусирани върху културата на киберсигурността, все още са в начален стадий.“ Гражданското общество в контекста на киберсигурността обхваща широк кръг от неправителствени участници. Това включва индивиди, общности, неправителствени организации, академични институции, субекти от частния сектор и медиите. Всеки от тези участници внася уникални перспективи, умения и ресурси в областта на киберсигурността. Ролята на гражданското общество не е само в реактивните аспекти на справянето с киберзаплахите, но и в проактивното участие, което включва повишаване на осведомеността, допринасяне за разработването на политики и насърчаване на култура на киберсигурност. В областта на киберсигурността има множество примери, където етични хакери и изследователи от частния сектор са идентифицирали уязвимости в националните инфраструктурни системи, водещи до значителни подобрения в сигурността. Подобно на това, академичните институции са допринесли чрез изследвания и разработки, произвеждайки напреднали технологии и стратегии за киберсигурност.

Възможните приноси на различни сектори на гражданското общество са необятни. Обучението, заложено в университетите и изследователските институции са в челните редици на изследванията в областта на киберсигурността. Те допринасят чрез изследвания на ръба на технологията, разработване на напреднали инструменти за киберсигурност и обучение на следващото поколение професионалисти в об-

ластта на киберсигурността. Сътрудничеството между академията и правителството може да доведе до разработването на по-робустни политики и практики в областта на киберсигурността.

Неправителствени организации (НПО): НПО-тата могат да играят ключова роля в адвокатството, разработването на политики и кампаниите за осведоменост. Те могат да действат като посредници между правителството и обществеността, осигурявайки, че стратегиите за киберсигурност са инклузивни и съобразени с общественото благосъстояние.

- Частен сектор: Компаниите, особено тези в областта на технологиите и киберсигурността, притежават технически експертиза и ресурси, които са ценни за националните стратегии за киберсигурност. Тяхното участие може да варира от разработване на сигурна инфраструктура до споделяне на разузнавателна информация за нововъзникващи киберзаплахи. Освен това, бизнесите могат да насърчават най-добри практики за киберсигурност в своите организации, допринасяйки за по-сигурна обща цифрова среда.
- Медии: Медиите играят критична роля в разпространението на информация и повишаване на осведомеността относно въпросите на киберсигурността. Отговорното отразяване може да помогне за образованието на обществеността, насърчаване на най-добри практики за киберсигурност и насърчаване на по-информиран диалог относно националните политики за киберсигурност.
- Общности и индивиди: Местните общностни групи и индивидите са съществени за изграждането на култура на осведоменост за киберсигурността. Инициативите, ръководени от общността, могат да насърчават безопасните киберпрактики, увеличаване на бдителността срещу киберзаплахите и създаване на колаборативна среда за споделяне на информация и ресурси.

Според проф. Нейкова заинтересованите страни в киберпространството трябва да играят активна роля не само в защита на собствените си активи, но и извън границите на собствената си отговорност. Това е така, защото използваните приложения в киберпространството непрекъснато разширяват обхвата си от моделите бизнес потребител и потребител до форма на разнообразие от взаимодействия и транзакции. Изискванията към индивидите и организациите се разширяват, за да бъдат подготвени да реагират на възникващите рискове за сигурността и предизвикателствата за ефективна превенция и реакция при злоупотреби и усъвършенстване на криминалната обстановка.[2] Включването на гражданското общество в националните стратегии за киберсигурност не е просто полезно; то е необходимост във все по-взаимосвързания свят. Разнообразните приноси на тези различни сектори обогатяват пейзажа на киберсигурността, правейки го по-устойчив и адаптивен към развиващите се заплахи. Чрез ангажирането на гражданското общество, правителствата могат да използват широк спектър от експертиза и перспективи, водещи до по-обхватни и ефективни стратегии за киберсигурност.

Синергията между гражданското общество и правителството в киберсигурността е ключова за разработването на всеобхватни и устойчиви национални стратегии за отбрана. Това партньорство използва силите на двата сектора, комбинирайки гъвкавостта, иновациите и разнообразните перспективи на гражданското общество с авторитета, ресурсите и стратегическите способности на правителството. Пример за

участие на гражданското общество е Естонската академия за електронно управление: Тази инициатива включва сътрудничество между естонското правителство, гражданското общество и частния сектор, фокусирано върху разработването на цифрови решения за по-добро управление, включително здрави практики за киберсигурност. „Отвъд простата дигитализация, истинската цифрова трансформация включва значителна промяна в организационната култура и лидерството, както и споделена отговорност за този растеж. Накрая, вълната на цифровата трансформация не е само въпрос на оцеляване – а на процъфтяване.”[3].

Друг пример е Националният център за киберсигурност (NCSC) на Великобритания: NCSC сътрудничи с академични институции за сертифициране на магистърски програми по киберсигурност, гарантирайки, че учебната програма отговаря на националните нужди за сигурност: „Чрез Националната киберстратегия 2022, правителството призовава всички части на обществото да изиграят своята роля в укрепването на икономическите и стратегическите сили на Великобритания в киберпространството – това означава повече разнообразие в работната сила, уравновесяване на киберсектора във всички региони на Великобритания, разширяване на офанзивните и защитни кибервъзможности и приоритизиране на киберсигурността на работното място, в управителните заседателни и в цифровите вериги за доставки.”.[4]

Ползи от интегрирането на познания на гражданското общество.

- Подобрена разузнавателна информация за заплахи и реакция: Гражданското общество, особено частният сектор и академичните институции, могат да предоставят уникални прозрения за нововъзникващи киберзаплахи, подобрявайки способността на правителството да реагира по-ефективно на тези заплахи.
- Иновации и технологично развитие: Сътрудничеството с гражданското общество отваря вратата към иновативни решения и напреднали технологии, които могат значително да подобрят националната инфраструктура за киберсигурност.
- Публична осведоменост и ангажиране: Участието на гражданското общество гарантира, че киберсигурността не е само правителствен въпрос, но и обществен. Чрез ангажиране на обществеността, правителството може да насърчи култура на осведоменост за киберсигурност, водеща до по-добра превенция и ограничаване на киберзаплахите.
- Разнообразни перспективи и инклузивно формиране на политики: Участието на гражданското общество гарантира, че политиките за киберсигурност са всеобхватни, вземайки предвид разнообразните нужди и перспективи на различните сектори на обществото.
- Изграждане на доверие: Прозрачното сътрудничество между правителството и гражданското общество може да изгради обществено доверие в националните стратегии за киберсигурност, което е съществено за тяхното успешно изпълнение.

Синергията между гражданското общество и правителството в киберсигурността е мощна сила. Като приемат колаборативни модели и учат от успешни примери, правителствата могат значително да подобрят своите стратегии за киберсигурност. Интегрирането на нововъведенията и ресурсите на гражданското общество води до по-солидни, иновативни и инклузивни национални отбранителни рамки, по-добре

подготвени да се справят с предизвикателствата на развиващия се пейзаж на киберзаплахите. Тази глава подчертава значението на тези синергии и предоставя пътна карта за изграждане на ефективни партньорства в киберсигурността.

Влиянието на изкуствения интелект върху гражданското общество: Последици за националната сигурност.

Появата на изкуствения интелект (ИИ) доведе до трансформации във всички аспекти на обществото, включително значителни ефекти върху гражданските свободи, социалните норми и икономическите структури. С увеличаването на сложността на технологиите на ИИ, тяхното приложение в системите на националната сигурност поражда критични въпроси относно неприкосновеността на личния живот, етичното управление и баланса между защитата на гражданите и опазването на гражданските свободи. Ролята на ИИ в гражданското общество е едновременно всеобхватна и нюансирана, влияеща на различни области, включително заетостта, здравеопазването, образованието и социалната взаимодействие. Способността на ИИ да обработва огромни количества данни е революционизирала предоставянето на услуги и процесите на вземане на решения. Въпреки това, тази способност също така въвежда предизвикателства, свързани с неприкосновеността на личния живот, сигурността на данните и потенциала за системни предразсъдъци, които биха могли да засилят социалните неравенства.

Въвеждането на изкуствения интелект (ИИ) в сферите на националната сигурност носи със себе си обещанието за по-ефективно предотвратяване на заплахи, подобряване на аналитичните способности и оптимизиране на отбранителните операции. Технологиите на ИИ могат да анализират големи обеми от данни за идентифициране на потенциални заплахи за сигурността, подобрявайки времевите рамки и точността на реакциите. Разработването на автономни системи за отбрана също предлага възможности за минимизиране на риска за човешки живот в конфликтни зони.

Въпреки това, нарастващата зависимост от ИИ в контекста на националната сигурност поражда значителни притеснения относно гражданските свободи и неприкосновеността на личния живот. Технологиите на изкуствения интелект (ИИ) представляват ярък пример за двойната употреба – способността на една и съща технология да носи значителни ползи за обществото, докато едновременно с това представлява потенциални рискове за сигурността и стабилността. Наблюдението, подсилено от ИИ, може да доведе до непропорционално навлизане в личния живот на гражданите, като същевременно създава възможности за злоупотреба и надзор, който надхвърля законните цели за сигурност. Освен това, прозрачността и отчетността на алгоритмичните системи са от съществено значение за предотвратяване на дискриминация и гарантиране на справедливост, особено когато те влияят на правосъдните решения и оценката на заплахи.

Стратегии за балансиране на националната сигурност и гражданските свободи включват:

- **Установяване на ясни регулаторни рамки:** Разработването на строги законодателни и регулаторни рамки, които определят границите на използването на ИИ в националната сигурност, е критично за защитата на гражданските свободи.

- **Подобряване на прозрачността и отчетността:** Въвеждането на механизми за прозрачност и отчетност, които позволяват надзор над използването на ИИ от страна на службите, гарант за националната сигурност на страната, може да помогне в изграждането на доверие и гарантирането на отговорно използване.
- **Засилване на етичните стандарти:** Разработването и прилагането на етични стандарти за използването на ИИ в националната сигурност трябва да вземат предвид необходимостта от защита на гражданските свободи и неприкосновеността на личния живот.
- **Подкрепа за международно сътрудничество:** Сътрудничеството на международно ниво за разработването на общи принципи и стандарти за използването на ИИ в националната сигурност може да спомогне за създаването на глобален консенсус относно етичните и правните норми.

Тези стратегии подчертават необходимостта от балансиран подход, който признава значението на националната сигурност, докато активно защитава основните граждански права и свободи. В крайна сметка, успехът в управлението на ИИ в контекста на националната сигурност ще зависи от способността да се навигира в сложната динамика между технологичните иновации, етичните императиви и демократичните принципи. днешната ера на технологичен прогрес, регулирането на изкуствения интелект (ИИ) стои в основата на усилията за създаване на сигурно и справедливо общество. Задачата пред законодателите е да намерят деликатния баланс между използването на ИИ в целях на национална сигурност и защитата на демократичните ценности, като едновременно с това гарантират прозрачността, отчетността и общественото участие.

Пример за това е прилагането на ИИ в системите за видеонаблюдение, което може значително да подобри сигурността в обществените пространства. В същото време, без подходящи регулации, съществува риск тези системи да бъдат използвани за непропорционален надзор и нарушаване на неприкосновеността на личния живот. Създаването на законодателство, което изисква ясно определяне на случаите за използване, съгласувано с правата на човека и етичните стандарти, е пример за стремежа към баланс между сигурността и личните свободи.

Международното сътрудничество също играе важна роля в регулирането на ИИ. Пример за това са глобалните инициативи като Глобалния пакт за ИИ (Global Partnership on AI), които събират държави, научни общности и частния сектор за разработването на общи принципи и стандарти за етично използване на ИИ. Такива инициативи демонстрират значението на споделянето на най-добри практики и разработването на съгласувани подходи към предизвикателствата, които ИИ поставя на глобално ниво.

Гражданското общество играе не по-малко важна роля в надзора над развитието и използването на ИИ. Неправителствени организации като „Access Now" или „Amnesty International" активно участват в дебатите за ИИ, насочвайки вниманието към въпроси, свързани с правата на човека и етичните аспекти на технологичния прогрес. Те също така призовават за създаването на регулаторни рамки, които да осигуряват отчетност и прозрачност от страна на компаниите и правителствата.

Заключение

Докладът подчертава критичната роля на гражданското общество в укрепването на националната киберсигурност чрез колаборативен подход. Акцентира се върху значението на сътрудничеството между различни сектори, включително правителството, частния сектор, академичните среди и неправителствените организации, за разработването на иновативни и ефективни стратегии срещу киберзаплахите. Освен това, разглежда се влиянието на изкуствения интелект върху националната сигурност и необходимостта от баланс между технологичните иновации и защитата на гражданските свободи. В крайна сметка, докладът подчертава силата на колективните усилия и важността на обществената ангажираност за създаването на устойчива и адаптивна киберсигурност.

References/Литература

1. Денчев С. „Информация и сигурност“, Академично издателство „За буквите - О писменехь“, 2019, (ISBN:978-619-185-369-4);
2. Neykova, M. CYBERSECURITY OR THE LACK THEREOF. University of economics and innovation in Lublin, Free University of Varna, 2018, ISSN 2367-4555;
3. https://www.forbes.com/sites/forbeshumanresourcescouncil/2023/08/14/thriving-not-surviving-digital-transformation-lessons-from-estonia/?sh=550580aa7157;
4. https://www.ncsc.gov.uk/news/government-publishes-blueprint-to-protect-uk-from-cyber-threats;
5. Чилова Н. „Финансова инспекция“. София: Издателски комплекс на УНСС, 2017, 234 стр. ISBN 978-954-644-928-3
6. Нейкова, М. Гражданското общество – фактор на сигурността в държавата, 2018;
7. Манев, Е. „Анализ на определение на понятието национална сигурност” Analysis of definitions of the concept National Security Article №1; Юридически сборник Бургаски свободен университет т.XXVII 2020 г.;
8. Нейкова, М. Понятието „национална сигурност” – съвременни аспекти. Юридически сборник 2017 г., Бургаски свободен университет;
9. Нейкова, М. Относно необходимостта от промяна на стратегията за Национална сигурност на Република България, МК, БАН-УНИБИТ, 2017.