Петко Димов

ПРИЛОЖЕНИЕ НА УЕБ ТЕХНОЛОГИИТЕ ЗА ЗАЩИТА НА НАЦИОНАЛНАТА СИГУРНОСТ

DIOMIRA
София 2018

Петко Димов

Приложение на уеб технологиите за защита на националната сигурност

София 2018

Съдържание

Увод

Знанието е сила, а интернет е най-голямото хранилище на човешкото знание! В Световната мрежа и в частност българското интернет пространство има много бази данни, уебсайтове и социални медии, където потребителите намират информация, комуникират един с друг и дори влияят на действията на обществото.

Използването на тези средства може да доведе до някои негативни ефекти за националната сигурност и неблагоприятни последици за интересите на държавата. Независимо от това, те предоставят и редица възможности за постигане на целите на дадената страна.

Целта на настоящата монография е да предостави актуална картина на потенциалните заплахи в Българското интернет пространство, да анализира влиянието им върху националната сигурност, възможностите на уеб технологии за предотвратяване или ограничаване на тези заплахи и да очертае основните сценарии за защитата на националната сигурност.

Изложението е структурирано в две части. В първата част са представени характеристиките и е предложена класификация на източниците на заплахи в интернет за националната сигурност. Във втората част се анализират интернет инструментите и възможностите за тяхното използване за защита на интересите на държавата.

1. Рискове и заплахи за националната сигурност в интернет

Съвременният човек живее в условия, характеризиращи се с бърз растеж и развитие на информационно-комуникационните технологии, които революционизираха начина по който хората, обществата и дори държавите взаимодействат помежду си. С навлизането на информационното общество ние все по-често общуваме, работим, играем, търгуваме, обучаваме се, управляваме и воюваме едни с други по начини, които не бяха възможни преди двадесет години. Днес ние не можем да си представим живота без интернет, който придобива толкова важно значение за съвременното общество, колкото електричеството, пътищата и водоснабдяването. Световната мрежа интернет се превърна в елемент на националната сигурност на страните!

Мрежовите информационни системи се използват за насърчаване на икономическото развитие, в научните изследвания, социално-културните отношения, за укрепване на военните и отбранителните системи, в електронното управление на правителствата, в новите типове медии, които преместват отразяването на действителността в интернет пространството.

Този нов свят изпълнен с цифрова информация става все по-зависим от употребата на мрежовите информационни системи и никак не е безопасен.

Заедно с положителните си страни, технологичното развитие доведе със себе си множество уязвимости и злонамерени заплахи

под формата на киберпрестъпления, кибертероризъм, кибератаки, кибервойни, опасност от изтичане на чувствителна информация или дезинформация и фалшиви новини, манипулиращи съзнанието на хората.

Всичко това налага постоянно да се наблюдава, анализира и прогнозира развитието на глобалната мрежа за да се неутрализират негативните ефекти за националната сигурност и неблагоприятни последици за интересите на държавата[1].

Успоредно с това задълбочените и актуални познания за интернет пространството предоставят забележителни възможности за постигне на националните цели, чрез ефективно разпространение на съдържание, подобряване на представянето на правителствените институции, укрепване на геополитическата позиция на държавата и нейното международно доверие.

1.1. Основни дефиниции в интернет

В публичното пространство съществува припокриване на понятията киберпространство, интернет пространство и информационно пространство, като често те се използват взаимнозаменяемо дори в официални документи, поради това се налага да се направят някои определения.

Според национална стратегия за киберсигурност „Киберустойчива България 2020“ **киберпространството** е интерактивна среда от електронни мрежи и информационна инфраструктура включително интернет, телекомуникационни мрежи, компютърни системи,

[1] Доктрина на въоръжените сили на Република България, София, 2017

вградени процесори и контролери, които се използват за създаване, унищожаване, съхранение, обработка, обмяна на информация, управление на обекти, системи и услуги за потребителите[2].

Световната мрежа интернет е глобална система от свързани компютърни мрежи, която служи за отдалечен достъп до голямо разнообразие от информационни ресурси и услуги. Към месец декември 2017 г. в нея има над 3,8 милиарда потребители, които всяка секунда правят по 2,3 милиарда търсения. Google е индексирала 1,3 милиарда уебсайта. Facebook има два милиарда активни потребители, като всеки един от тях има средно 130 приятели и всяко влизане в сайта му отнема средно по 23 минути[3]. По данни на Националния статистически институт за 2017 г. цели 67,3% от българските домакинства имат широколентов достъп до интернет, като 98 % от тях използват Google.BG за търсене на информация в световното интернет пространството[4].

Информационното пространство се отнася до зоната на разпространение на информацията като цяло, чрез всички налични канали (телевизия, радио, вестници, списания, академични дебати и интернет), които въздействат на човешкото съзнание и затова е обект на информационна война[5]. "Терминът **информационна война** може да се определи като използване на информационни технологии и

[2] Национална стратегия за киберсигурност „Киберустойчива България 2020“, София: Министерски съвет, 2016.
[3] http://www.internetlivestats.com/ [прегледан 30.01.2018]
[4] Достъп на домакинствата в интернет [прегледан 30.01.2018] http://www.nsi.bg/bg/content/2808/достъп-на-домакинствата-до-интернет
[5] Alberts, D. S., Garstka, J. J., Hayes, R. E., & Signori, D. A. Understanding Information Age Warfare, 2001

съдържание, за да се повлияе на познанието на противника или целевата аудитория[6].

Разликата според въздействието на трите пространства е показана на фиг.1 и както се вижда върху интернет пространството се налагат характеристиките на останалите две.

Фиг. 1. Дефиниране на границите между киберпространство, интернет пространство и информационно пространство

Съответно **сигурността в интернет** се обуславя от понятията за киберсигурност и информационна сигурност. Заплахите в интернет пространството следва да са комбинация от киберзаплахи и информационни заплахи, а основните инструменти за влияние са уебсайтовете.

Уебсайтовете са места в мрежата, състоящи се от множество уеб страници с общ URL адрес, който често се състои само от името на домейна или IP адреса и пътя до основната директория в мрежа, базирана на протокола IP. Уебсайтовете са интернет базирани

[6] Theohary, C. A., Rollings, J., Terrorist Use of the Internet: Information Operations in Cyberspace, Congressional Research Service, Washington, 2001

приложения за масова комуникация, характеризиращи се с глобално разпространение и лекота на употреба, поради тяхната достъпност с помощта на програми наречени уеб браузъри. Съществуват различни видове уебсайтове в зависимост от тяхното предназначение, аудитория и съдържание. Те могат да бъдат: личен блог, корпоративен сайт, електронен магазин, новинарски сайт, форум, портал, търсачка, уикисайт или социална мрежа.

С появата на Уеб 2.0 започна да се използва терминът "**социални медии**", които се отнася до интернет базирани приложения, позволяващи на хората да комуникират и да споделят ресурси и информация [7] . Днес средностатистическия потребител може да създава уеб съдържание (видеоклипове, снимки, изображения, текстове, звуци и др.), което лесно се превръща от еднопосочното съобщение до двупосочен диалог в така наречените „нови медии.

Това позволява уебсайтовете и социалните медии да се превърнат в инструменти за масово и безконтролно публикуване на генерирано от потребителите съдържание от всякакъв вид, което е предназначено за обществено потребление [8] . Също така те позволяват на потребителя да управлява собствената си социална мрежа (организация, обкръжение) и собствената си социална идентичност или тази на групата, в която членува, което влияе на националната сигурност.

[7] Chief Information Officers Council (CIO), Guidelines for Secure Use of Social Media by Federal Departments and Agencies, Washington, 2009.

[8] US Air Force – Public Affairs Agency – Emerging Technology Division, Social Media and the Air Force, Arlington County, 2009.

Уебсайтовете и социалните медии боравят с информация и за разлика от традиционните медии, те могат напълно безплатно да я предоставят навсякъде по света, така че тя да се разпространи по подобие на биологичните вируси.

Информацията в интернет пространството се характеризира с три основни параметъра:

- Конфиденциалност – това са номерата на банкови сметки, лични данни, пароли, лична и служебна кореспонденция и всичко, което би трябвало да се вижда само от този, за които е предназначено.
- Достоверност – тя може да обхваща, както същността и целостта на данните, така и техния произход. Примери в тази посока има достатъчно много – фалшифициране на избори, умишлено манипулирани статистически данни, а във военната област – дезинформация на противника.
- Достъпност – информацията е ценна именно с това, че може да бъде използвана. Основен проблем за всяка информационна система е да се намери златната среда между нейната защита и използваемост. Именно това противоречие създава уязвимостите в информационните системи.

В крайна сметка уебсайтовете и социалните медии са информационни средства за връзка или комуникация и само поради това, че са "инструменти", те могат да представляват заплаха за национална сигурност или ресурс и възможност за защита на

стратегическите цели на държавата, в зависимост от начина, по който се използват, кой ги използва и по каква причина[9].

Интернет има следната картография:

Уеб 1.0 – това е най-старият, установен сегмент на мрежата. Той включва правителствени, корпоративни, обществени, лични, уебсайтове, блогове и др. Ресурсите на този сегмент от мрежата са лесно достъпни с помощта на търсачки (като Google, Bing, Yandex и т.н.).

Уеб 2.0. е така наречената мрежа от социални платформи, като Facebook и Twitter. Съдържанието в този сегмент на интернет се създава най-вече от самите потребители, затова те се наричат социални медии и в тях делът на видео и фото съдържанието нараства с ускорени темпове. Днес почти всички уебсайтове са обвързани с останалите социални платформи и публикуваното в тях съдържание автоматично се разнася в социалните мрежи.

Уеб 3.0 се пови през последните години като "мрежа от мобилни приложения", в което потребителите просто установяват връзка между притурката си и ресурса (услуга, портал и т.н.) чрез интернет.

Невидим интернет - са ресурси, които не са индексирани от търсачките. Според наличната информация около 90% от цялото научно, техническо, технологично, финансово, икономическо и обществено съдържание се намира в него. Обемите на невидимия интернет непрекъснато нарастват.

[9] Smirnov, M. Information War in the Internet. The Conflict which Cannot Be Won. Master thesis by Radboud University Nijmegen, 2015

Невидимия интернет има и т.н. **тъмна мрежа**, която се използва от различни видове престъпници, чрез софтуер наречен Tor. Понастоящем той се използва главно за незаконни дейности, престъпления в киберпространство, трафик на наркотици, оръжия и за осъществяване на целенасочени действия за подкопаване на държавния суверенитет.

Интернет на нещата. Това са вградени информационни блокове, свързани чрез интернет, с контролни центрове на различни обекти от физическия свят. Така, например, към световната мрежа са свързани всевъзможни домакински уреди, производствени линии, системи за управление на водите, за отопление, електропренасяне и така нататък.

Специален сегмент е така наречената **мрежа от пари**. Световната тенденция е намаляването на оборота на плащанията в брой и прехода към електронни пари във всичките им форми и системи от рода на „Биткойн“.

По този начин цифровата среда на интернет пространството има сложно картографиране, където отделни сегменти се развиват сами, независимо от общите тенденции.

За понятието **информационни технологии** има редица дефиниции, много от които се обединяват около предназначението, а именно „група от технологии за събиране, обработка, съхранение и разпространение на информация“. За това те се състоят от компютри, мрежи, мобилни и сателитни комуникации, телевизия, радио и автоматизирани системи за управление.

При използването им в информационни операции с военно предназначение спокойно можем да кажем, че те са „**информационно оръжие**“, с което целенасочено да се активират, унищожават, блокират или създават определени процеси, мрежови ресурси (сайтове, компютри) и социални групи в интересуващата ни информационната система. На 9 октомври 2017 в Букурещ Парламентарната асамблея на НАТО прие резолюция, в която се констатира "превръщането на информацията в оръжие". В нея се посочва, че интернет технологиите "могат да доведат до раздробяване и поляризиране на обществото, да предоставят по-голяма видимост на радикални мнения и фалшиви новини“.

Потребителите на интернет на първо място са отделни лица, които използват такива инструменти за комуникация, споделяне на информация и различно съдържание, взаимодействие с другите хора, развитие на личността и укрепване на тяхната социална идентичност. Според някои изследователи, отделните индивиди използвайки интернет, могат да задоволят всичките си основни потребности с изключение на физиологичните нужди като: пиене, хранене или сън[10]. А именно това са следните видове потребности от пирамидата на Маслоу:

- потребност от сигурност: поради това, че потребителят взаимодейства и комуникира главно с контактите на собствената си мрежа породени от предишни отношения (социални, професионални, културни и др.);

[10] Riva, G. I social network, il Mulino. Bologna: Universale Paperworks, 2010.

- потребности от принадлежност: потребителят има възможност да комуникира и да споделя съдържание, като постоянно се сблъсква с контактите на своята мрежа;
- потребност от уважение: освен избора на контакти, които да се включат в неговата собствена мрежа, потребителят може да бъде избран и от други потребители, което повишава самочувствието му;
- потребност от самореализация: потребителят може да опише профила си по желания от него начин и да получи искания за съвет или помощ от неговите контакти.

Тези лица могат да използват интернет не само за личните си цели, но и за целите на организацията от която са част. Следователно, организираните групи (в най-широкия смисъл на термина: държави, неправителствени организации, компании, движения, терористични групи и т.н.) са потенциални участници в информационните отношения.

Исторически, интернет се формира като свободна среда за информационно взаимодействие в резултат на което се получава парадоксална ситуация. Ключови сфери за всяка държава, като търговията, финансовите транзакции, политическата и социалната активност в голяма степен се изместиха към интернет пространството, като в същото време в него не се признават някои принципи на международното право.

Нарастващата роля и значимост на информационно-комуникационните технологии е основа за появата на нови заплахи и рискове, свързани с възможности за компрометиране на системи за управление и нерегламентирано манипулиране на данни в тях.