SocioBrains

ISSN 2367-5721 (online), JOURNAL HOMEPAGE: WWW.SOCIOBRAINS.COM
Publisher: SMART IDEAS – WISE DECISIONS, Ltd., Sofia, Bulgaria

ISSUE 76, DECEMBER 2020

CYBERTERRORISM - DEFINITON AND FORMS

Abstract: Cyber-attacks are increasing at an alarming rate around the world. They are often being linked to the widely publicized and popularized threat of cyberterrorism. However, cyberterrorism is a relatively young field of research and the terminology, much like its parent term, 'terrorism', is still not adequately defined or congruently applied. The article suggest a definition for the term "cyberterrorism" and examines its two basic forms – hybrid cyberterrorism and direct cyberterrorism.

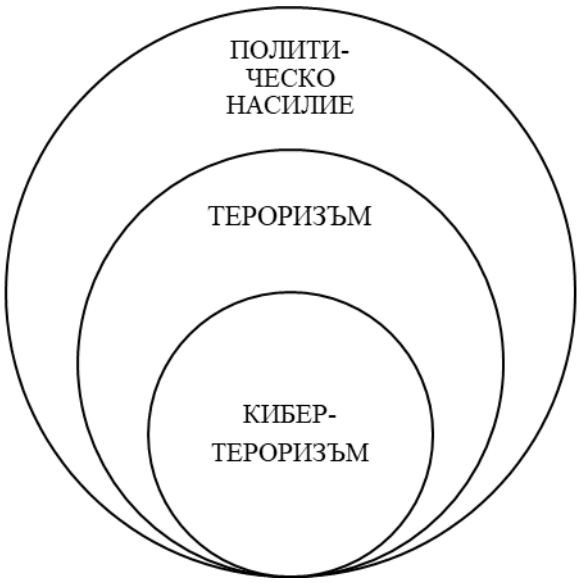
Author information:

Zdravko Kuzmanov
Chief assist. prof. PhD
in Management of Security Systems Department
at Konstantin Preslavsky University of Shumen
✉ z.kuzmanov@shu.bg
Bulgaria

Keywords:
cyberterrorism, global threat, hybrid cyberterrorism, direct cyberterrorism

Понятието **„кибертероризъм**“ е комплексно и комбинира две концепции: *„кибер“* - отнасящо се за киберпространството и *„тероризъм“,* произлизащ от *„терор“* – насилие, извършено от индивид, група или правителствена/неправителствена организация, с цел сплашване на обществото и постигане на политическа цел. Терминът „кибертероризъм“ се използва за първи път през 1980 г. от Бари Колин, който го определя като *действие, отнасящо се до използването на киберпространството за извършване на терористични актове.* Понятието започва да става популярно сред експертите по киберсигурност през 90-те години, когато информационните и комуникационни технологии се развиват и разпространяват по целия свят.

Въпреки, че няма общоприета дефиниция за кибертероризма, той се приема за пресечната точка между тероризма и киберпространството. Той не бива да бъде разглеждан като отделно явление, а като ***продължение на политическото насилие, тероризма и терористични актове*** (Фигура 1) ***и тактики в киберпространството или като предварително организирано посегателство върху комуникационните и информационни ресурси на дадена страна с цел блокиране, унищожение или нарушение на целостта на жизненоважни системи, базирано на социална, политическа или идеологическа основа.*** Под киберпространство разбираме всяка електронна форма за пренос, съхранение и обработка на информация.



Фигура 1. Явлението „кибертероризъм“

Според редица експерти по телекомуникации и национална сигурност, кибертероризмът следва да се третира като една от най-важните заплахи и предизвикателства на 21-ви век. Следователно е необходимо да се идентифицира причината за проявлението на този феномен и да се обясни защо терористите избират да действат в киберпространството. Най-очевидните ***причини*** за по-голямата популярност на кибертероризма спрямо традиционните форми на тероризъм включват: [1]

- По-широко въздействие;
- По-ниски цени и лесен достъп до интернет;
- Минимален риск за предварително разобличаване на планирана атака;
- Възможност за внезапни и непредвидими действие срещу напълно неподготвени жертви;
- Извършва се напълно анонимно, което позволява разпространението на дезинформация;
- Затрудняване при определяне на разликите между реална и виртуална заплаха;
- По-малък риск самите терористи да бъдат афектирани от атаките;
- Избягване на допълнителни щети, които могат да бъдат използвани като част от пропагандата за въздействие върху общественото мнение.

За да се разработи ефективен подход за борба с кибертероризма следва да се разграничат двете му основните форми – хибриден кибертероризъм и директен кибертероризъм (Фигура 2).

Фигура 2. Форми на кибертероризма

Хибридният кибертероризъм включва използването на Интернет за терористични дейности като пропаганда, пресичане, радикализация, набиране на средства, извличане на данни, комуникация, обучение и планиране за действителни терористични атаки:

- ***Пропаганда и психологическа война.*** Интернет се използва от терористи и терористични организации за управление на терористична пропаганда чрез информационна война с цел разпространение на идеология, осъществяване на психологическа война, както и да се радикализират и привличат нови членове по целия свят чрез терористични уебсайтове, онлайн списания и социални мрежи като *Facebook, Twitter, Istagram, Youtube* и други. ДАЕШ разполага със седем медийни агенции (най-известната от които *„Amaq”*) под свое влияние и 37 медийни офиси, действащи в различни държави. Ал-Кайда сформира медиен канал, познат като *„As-Sahab”* и Глобален Ислямски медиен фронт *(„GIMF”),* както и онлайн списания, чрез които подсилват своята пропаганда. От 2015 г. насам терористичните организации използват приложението *„Telegram”* заради криптираното му и безопасно използване. Пример за терористична психологическа война, е Обединения кибер халифат, който се отъждествява с ДАЕШ и е част на хакерския отдел на „Ислямска държава“, който през юли 2016 г. разпространи няколко плаката със заплаха за САЩ и Египет;
- ***Комуникация и работа в мрежа.*** Терористичните групи са използвали платформи за социални медии и системни приложения за шифровани съобщения (като *Kik, SuperSpot, Wickr, Whatsapp, Gajim*), онлайн чат игри, кодирани съобщения или стеганография за скрити дискусии, директни и частни комуникационни цели (което включва работа в мрежа с други членове на групата, взаимодействие с новобранци и поддръжници) и планиране и координация на

физически атаки, както и планиране на хакване операции. Например „*VoIP“* телефонни услуги са били използвани по време на атаките в Мумбай през 2008 г;

- ***Събиране на финансови средства.*** Финансирането на дейности, свързани с тероризма (придобиване на оръжия или подкрепа на военните усилия) се извършва чрез дарение през социални платформи и блогове за диалог, както и чрез използването на биткойн цифрова валута. Такива кампании са *„Въоръжете ни“* на *„Джихад за Аллах“,* имаща за цел въоръжаването на муджихадини с оръжия и боеприпаси, ракети, бомби, физическа подготовка и насърчаване на шариата, както и кампанията „Вашите синове на ваше разположение“ с цел спонсориране на семейство муджахид със 100 щатски долара на месец;
- ***Извличане на данни, набиране и обучение на кадри.*** Терористите използват Интернет за извличане на данни и събиране на информация за определени места и хора, както и потенциални цели за атаки. Днес ДАЕШ и много други организации използват социалните мрежи за подбор на индивидуални лица за целите на радикализирането. Вербовчиците идентифицират потенциални индивиди чрез мониторинг на Фейсбук профили. Организациите използват мрежата за разпространение на обучителни материали за извършване на физически атаки, инструкции за обучения на новите членове и поддръжници за придобиване на умения за киберзащита и подобряване на нападателните способности.

Директният кибертероризъм се отнася до преки атаки срещу кибер инфраструктура на жертвата (като компютри, мрежи и съхраняваната в тях информация) за постигане на политическо, религиозно и идеологическо влияние. [2] Директният кибертероризъм може да бъде допълнително диференциран на деструктивен и пробивен:

- ***Деструктивният кибертероризъм*** е манипулирането и корупцията на информационната система, инсталирането на функции за повреда или унищожаване на виртуални и физически активи. Най-популярното оръжие е на деструктивния кибертероризъм е използването на компютърни вируси и червеи (*„trojans”* и *„ransomware”*);
- ***Пробивният кибертероризъм*** се описва като извършване на системен пробив с цел сваляне на уебсайтове, прекъсване на системи, неоторизирано въвеждане или копиране на данни или нарушаване на мерките за сигурност за поемане на контрол над определени инфраструктурни компоненти. Пробивните кибер атаки са насочени към системи, които подпомагат функционирането на държавната администрация, вътрешната сигурност, отбрана, телекомуникации, енергийния и воден сектор, финансови услуги и спасителни служби.

Може да се заключи, че с развитието на дигитализацията и разпространението на информационните технологии в обществото заплахите на кибертероризма тепърва ще се увеличават. Те имат потенциала да се превърнат в най-сериозния невоенен инструмент на мека сила в света. Кибертерористите непрекъснато търсят нови решения и подобряват своите IT умения. Рискът, свързан с транснационалните хакерски дейности не бива да бъде подценяване поради разрушителното въздействие, което може да има върху международната сигурност и публичния ред.

References:

1. **Majdan, P.,** Cyber terrorism as a modern security threat, The WSB University in Poznan Research Journal, 2017
2. **Zerzri, M.,** The threat of cyber terrorism and recommendations for countermeasurs, Center for applied rolicy research (CAP), CAperspectives on Tunisia No. 04-2017