

ИНТЕРНЕТ, ТЕРОРИЗЪМ И НАЦИОНАЛНА СИГУРНОСТ

Богомил Шопов

INTERNET, TERRORISM AND NATIONAL SECURITY

Bogomil Shopov

Technologies reached their peak in the appearance of the global network The Internet. The use of the net for information exchange is increasing. Is it possible for the freely distributed information to be in favor of terrorism, how can we fight it and what measures may be taken to protect national security without violation of human rights.

Internet, terrorism, data retention, social networks, human rights, information, cyber crimes, cyber terrorism.

Интернет като среда е създаден преди много време, именно от военните в САЩ. Интернет като медия и среда за пренос на информация се доработва от потребителите на мрежата. Всеки един потребител допринася за развитието на световната мрежа.

В последно време се наблюдава използването на мрежата за разпространяване на терористични послания, обмен на информация и подобен род действия, имащи за цел подготовката на терористични актове или други заплахи за националната сигурност на една или много държави.

Всичко това е възможно поради факта, че Интернет е една преносна среда за всякаква информация. Както можете да намерите информация как да си сглобите бомба, така можете и да намерите информация как да спасите човешки живот или информация за издирваните престъпници от нашите или други служби.

Тогава къде минава тънката линия между тези два случая. Ситуацията е аналогична на всяка друга ситуация в нормалната практика – при извършване на престъпление, данните от Интернет комуникациите и от поведението на потребителите, за които е доказано, че е извършено престъпление или има съмнение за такова, може да бъдат използвани.

За тероризма обаче се налага превенция на престъпленията. Всички добре знаем, че за целите на националната сигурност в голяма роля е важна превенцията и анализа на терористичните мрежи с цел спиране на атаката още при подготовката и, а не разследването на пораженията след като този акт бъде

извършен.

Какво се предлага и защо то не е полезно?

Под натиска на САЩ, което те в последствие отричат започват да се създават механизми за наблюдения през Интернет и през всички средства в телекомуникацията.

Предложението за следене на информационния трафик ще разкрие кой на кого се е обаждал и изпращал имейли, какви сайтове са посещавали хората и дори къде са били с мобилните си телефони.

На телефонните компании и доставчиците на Интернет услуги ще бъде наредено да запазват цялата информация за трафика на клиентите си. Достъп до тези данни ще бъде даден на полицейските власти и разузнавателните агенции в Европа. Различни предложения в Брюксел съдържат различни периоди на пазене на информацията - от 6 месеца до 4 години.

Задържането на данни е агресивен метод, който се намесва в личния живот на 450 милиона души в Европейския съюз. Задържането на данни е политика, която безпрецедентно разширява правата на полицейско наблюдение.

В същото време нарушава много от инструментите, гарантиращи човешките права в Европа, като Директивите за защита на данните и Европейската конвенция за правата на човека.

Задържането на данни означава, че управляващите могат да се намесват в частния ви живот и личната ви кореспонденция, без значение дали сте заподозрян извършител на престъпление или не. Задържането на данни не е решение на проблемите с тероризма и престъпността.

През м. юли 2005 г. Европейският парламент прие доклад от члена на ЕП Александър Алваро относно плана за задължително задържане на данни. Заключение от доклада е, че предложението е прекомерна мярка. Също така, докладът поставя под въпрос необходимостта, ефективността и големите разходи за телекомуникационната индустрия и потребители.

Никъде в Европа не е проведено проучване, което да потвърди необходимостта от създаване на база данни от такъв мащаб и която да съдържа толкова поверителна информация, за нуждите на борбата с тероризма.

Нападенията срещу Лондон (атаките на метрото), които станаха причина за обсъжданията в директивата са нападения срещу човешките права. Защитаването на тези права е от особена важност, когато обществото и управляващите са изправени пред криза.

Възможно най-лошата реакция би била застрашаването на тези внимателно изработени права с панически отговор.

Отговор на тероризма под формата на масово наблюдение би довел до невероятен успех за извършителите на нападенията: цялостно подкопаване на нашите изконни ценности.

Кое е по-важно човешките права или спирането на терористичен акт?

Ако попитате специалистите, всяка информация е добре дошла. Ако попитате потребителите на Интернет или приносителите на мобилните телефони, събирането на информация за тях е нарушение на правата им за тайна на кореспонденцията и на правилото, че всеки е невинен до доказване на противното.

Пак стигаме до онази тънка линия, където двете понятия трябва да се засекът.

Никой не спори, че трябва да се лишим малко от своето си пространство в името на свободата и на сигурността си, но доколко всеки е готов насила да го направи?

Ако погледнем текущата ситуация в момента си личи недомислието – всеки един гражданин на България и Европа, ще бъде постоянно наблюдаван със специални разузнавателни средства, ще бъде следен къде се намира във всеки един момент, с кого си говори, кого познава и какво използва, само за да може, ако случайно реши да направи нещо лошо, информацията за него вече да е налице. От друга страна, би било божия благодат на хората работещи за сигурността да имат такава информация.

Информацията е полезна, но тя трябва да бъде събирана по-друг начин и с други средства. Тоталното наблюдение със сигурност не е решение на проблема за нито една от двете страни, най-малко, че е невалидна за борбата с тероризма.

Защо ли? Защото терористичните групи, няма да използват традиционните канали за комуникация, няма да се съобразяват с изискванията за регулация на Интернет, няма да разкрият данните си, така както всеки, които си мисли, че не е наблюдаван ще направи.

Терористите са умни хора с много средства. Кодирането на комуникацията в Интернет с необратим механизъм е много лесно. Използването на техники за прикриване на местоположението е също достъпно.

Тогаво какво се оказва? Предложените мерки за борба срещу тероризма не са срещу него, а срещу всички останали и пак стигаме до извода, че отговор на тероризма под формата на масово наблюдение би довел до невероятен успех за извършителите на нападенията: цялостно подкопаване на нашите изконни ценности.

Тогава какво да направим?

Използването на информацията за поведението на потребителите в Интернет може да е наистина полезна. Така се разкриват голям брой престъпления. Всички помним заплахата към Президента на Република България преди няколко години през Интернет. Тогава 'шегаджията' беше заловен още преди да стане от компютъра си в 'анонимен' клуб.

Всички помним и заловените банди от кибер-престъпници от Варна и София? Е, как става това.

След като е налице престъпление или разследване по евентуално престъпление МВР има правото с прокурорска заповед да изисква информация от доставчиците на Интернет и други съобщителни услуги тези данни, които те пазят в рамките на 24 часа. Информацията не е лична, а предоставя набор от IP адреси, които могат да бъдат проследени до определено физическо местоположение.

Като имаме информацията от местоположението, характера на престъплението и другите данни, можем да направим поведенческа карта на евентуалния престъпник и да знаем къде и как да го заловим. Всичко това, разбира се, зависи много от вида на престъплението, понякога трябва да се действа бързо и проследяването на Интернет-дейността на извършителя е достатъчна, а понякога, когато трябва да се разкрие цяла схема, се предполага и използване на други методи, като social networking.

Само преди месеци в Турция, използвайки такива методи са намерили престъпник по сложно дело в което друг начин не е имало. Въведена е информация от стари дела, където е имало свързани лица и така е направена диаграма за връзките между лица, които не са били свързани преди, но са поддържали връзки с един или повече хора от предишно гледаните дела.

Според световната енциклопедия "Уикипедия",
"Социалната мрежа е социална структура от възли (представляващи предимно отделни хора или организации), свързани по специфични типове възли като идеи, виждания, финансови облаги, приятелство, традиции, хипервръзки и други.

В нейната най-проста форма социалната мрежа представлява карта на връзките между всички релативни възли, които са изучавани. Тези концепции обикновено се представят чрез социална мрежова диаграма, където възлите са точки, а връзките са линии."

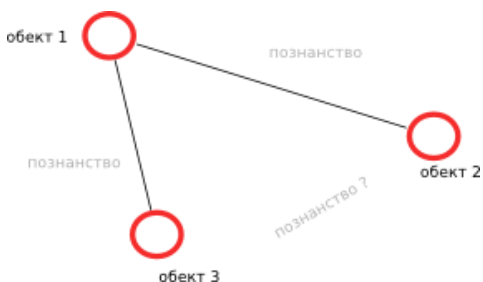
Намирането на връзка между два или повече обекта, винаги е била трудната част в планирането на поведенческия модел на дадена част от определена

логика.

Ако имаме човек, който познава друг човек, можем да кажем, че той се отнася към първия с определено отношение, това е ниво едно на поведенчески модел



Ако същия човек, има отношение към друг човек или обект, то може да се предположи, че вероятността обект1 и обект 3 косвено да се познават, което дава предпоставки да се следи и неговия поведенчески модел, за да бъде използван в анализа. Това отново е първо ниво:



Ако разполагаме с повече данни, можем добре да знаем връзката между елементите и да можем да определим възлите на отговорност между отделните елементи. Можем да имаме информация, която да използваме в последствие за нещо друго.

Използването на повече от един вид информация за връзка на обект с обект или на група обекти с група обекти, може да се приеме като ниво 2, когато освен първичната информация се добавя и вторична такава.

Имаме информацията, имаме модела имаме и вторични и третични данни и престъплението е разкрито. Знаем, че не става лесно, но е начин да се борим с тероризма в световната мрежа по разумен начин, които едновременно пази гражданите и помага на експертите. Сигурен съм, че има много такива начини, за това да се намери идеалната среда между сигурността и гражданските права, защото все пак сигурността и правата на гражданите са именно цел на службите за национална сигурност и те трябва да защитават гражданите.

Богомил Борисов Шопов - "Електронна граница".

телефон: 0897 615128

bogomil@spisanie.com, <http://bogomil.info>