СПЕЦИФИЧНИ ПРОБЛЕМИ ПРИ РАЗСЛЕДВАНЕ НА КИБЕРПРЕСТЪПЛЕНИЯ

Доц. д.н. Драгомир Кръстев

Висше училище по телекомуникации и пощи

SPECIFIC PROBLEMS UNDER INVESTIGATION FOR CYBERCRIMES

Assoc. Prof. DSc. Dragomir Krastev

University of telecommunications and posts

Резюме: В доклада са разгледани специфичните проблеми при разследването на киберпрестъпления. Акцентът е поставен върху проблемите, свързани с анонимността, проследяването, атрибуцията, нетрайността на цифровите доказателства, както и с различията в законодателствата на отделните държави, свързани с разследването на киберпрестъпления.

Ключови думи: киберсигурност, киберпрестъпления, цифрови доказателства, разследване.

Abstract: The manuscript examines the specify problems when investigating cybercrime. Emphasis is placed on the problem of communication with anonymity, tracing back, attribution, non-discretion in digital evidence, as well as with differences in the legislation to separate the problem, to investigate cyber crimes.

Keywords: cybersecurity, cybercrime, digital evidence, investigation.

Doi: <https://doi.org/10.36997/ESDI2021.52>

Въведение

В началото на второто десетилетие на XXI в. все още няма действащи общовалидни процедури за разследване на киберпрестъпления. Всяка държава използва собствени протоколи за разследване. Съществуват обаче редица международни стандарти и добри практики, които могат да бъдат възприети от държавите при разследване на киберпрестъпления.

Изложение

През последните двадесет години са разработени редица методологии в тази област на криминалистиката. Така например през 2002 г. е предложен модел за цифрова криминалистика, базиран на опита на ФБР, наречен: „Абстрактен модел на цифрова криминалистика“. Именно този модел се използва най-често в практиката. Той се състои от девет стъпки:

- идентификация;
- събиране на цифрови доказателства;

- получаване на цифрови доказателства;
- запазване на цифрови доказателства;
- анализ и отчитане;
- допустимост на цифрови доказателства;
- оценка на цифрови доказателства;
- разглеждане на цифрови доказателства;
- вземане на решение относно допустимостта на цифрови доказателства.

В областта на киберпрестъпността използваните оперативни методи, софтуер и инструменти се променят непрекъснато и за кратко време. Затова протоколите, използвани от следствените органи, трябва да бъдат актуализирани постоянно (например чрез използване на специален софтуер за разследвания) в зависимост от еволюцията на киберпрестъпността.

В допълнение към обичайните методи за разследване, при дела за киберпрестъпления се използват някои специални техники. Най-често използваните, особено когато става дума за случаи на сексуална експлоатация на деца, са прихващането на съобщения, съхраняването на данни и разследването под прикритие.

Последното е особено полезно, когато разследването не може да се извърши с технически средства, а се осъществява чрез разполагане на служители под прикритие, които разследват форуми и блогове. Разследванията от този вид обаче дават задоволителни резултати само ако се провеждат в дългосрочен план.

Останалите специални техники за разследване се основават на новите технически възможности в онлайн борбата с компютърните престъпления, като например онлайн мониторинг или други техники, като блокиране на достъпа до хардуер и специални бит копирни машини, дистанционно претърсване и изземване (например когато правоприлагащите органи хакват онлайн подозрителен компютър вместо да го изземат по физически път), проследяването на IP адреси, търсене в интернет от открити източници, запазване на копие от носители на данни и от интернет (уебсайтове, регистрационни файлове и т.н.). Специални техники се използват и при мобилните устройства (напр. UFED).

Използването на специални техники за разследване обаче невинаги е предвидено в националните законодателства на държавите, членки на ЕС. В някои от тях за тази цел е необходимо разрешение от компетентен съд.

В тази връзка страните, членки на ЕС, които все още не са направили това, се насърчават да предвидят в националното си законодателство възможността за използване на специални техники за разследване с оглед улесняване разследванията на дела, свързани с киберпрестъпления.

При извършване на кибератака е необходима техническа оценка (цифров анализ на материалите, иззети по време на операции, като вируси по търсачките, възстановяване на заличени данни и т.н.), за каквато в някои държави се отправя искане към частния сектор, тъй като има добър експертен опит и работи с по-добро оборудване и при по-малко разходи. Освен това е необходимо да се направи оценка на последиците за инфраструктурите от евентуални атаки и да се изгради всеобхватна ситуационна осведоменост и оценка на атаката, в това число използваните методи и средства.

Понятието „киберпрестъпност“ не може да бъде асоциирано със или отнесено към едно общо и единствено определение. То изразява или представя не толкова единичен престъпен акт, а по-скоро съвкупност или сбор от незаконни действия и поведения в киберпространството. В практиката това понятие се използва за определяне на широк спектър от правонарушения, включително традиционните компютърни правонарушения, а също така и мрежовите престъпления.

Предвид горепосочените аргументи, процесът на разследване на киберпрестъпления се характеризира с редица проблеми, които са характерни само за този вид престъпна дейност, на които следва да се отдели специално внимание.

Анонимизирането позволява на хората да участват в дейности, без да разкриват самоличността и/или действията си пред другите. Има няколко метода за анонимизиране, използвани от киберпрестъпниците. Един от тези методи е използването на прокси сървъри. Прокси сървърът представлява междинен сървър, който се използва за свързване на клиент (т.е. компютър) със сървър, от който клиентът изисква ресурси (Maras 2014, p. 294). Анонимизаторите или анонимните прокси сървъри скриват идентификационната информация на потребителите, като маскират техните IP адреси и ги заменят с други такива.

Киберпрестъпниците могат да използват и анонимни мрежи за криптиране на трафика, и скриване на адреса на *„уникалния идентификатор, присвоен на компютър от доставчик на интернет услуги (ISP), когато е свързан към мрежата“* (Ibid, p. 294), за да скрият своята онлайн активност и местоположение. Добре проучени примери за анонимни мрежи са Tor, Freenet и Invisible Internet Project (Invisible Internet Project, известен като I2P). Тези анонимни мрежи не само маскират идентифициращите данни на потребителите, но и хостват уебсайтовете на техните ресурси, използвайки възможностите на техните „скрити услуги, което означава, че тези сайтове могат да бъдат достъпни само от лица в тези анонимни мрежи. По този начин тези анонимни мрежи се използват за достъп до сайтове в Darknet или Dark Web.

Атрибуцията е друго препятствие, което затруднява разследването на киберпрестъпността. Целта на атрибуцията е да се разкрие киберпрестъпление на конкретно цифрово устройство, потребител на устройство и/или други извършители на киберпрестъпления (Lin, 2017). Използването на инструменти, които увеличават анонимността, може да затрудни идентифицирането на устройствата и/или лицата, отговорни за киберпрестъпността.

Процесът на атрибуция се усложнява допълнително от използването на заразени от зловреден софтуер зомби компютри (ботнети) или цифрови устройства, контролирани от инструменти за отдалечен достъп (т.е. зловреден софтуер, който се използва за създаване на задна врата на заразено устройство, за да позволи на дистрибутор на злонамерен софтуер достъп и системи за контрол). Тези устройства могат да се използват без знанието на потребителя, чието устройство е заразено, за извършване на киберпрестъпления.

Проследяването представлява процесът на проучване на незаконни дейности за идентифициране на източника на киберпрестъпление. Прави се обратно проследяване при разследване и разкриване на дадено киберпрестъпление (Pihelgas, 2013, pp. 31 – 60). Конкретно се търси информация за престъплението

чрез изследване на регистрационните файлове (дневници на събития, показващи активност на файловата система), които могат да помогнат за разкриване на информация за киберпрестъпление.

Цифровите доказателства са крехки и краткотрайни и неправилното боравене може да доведе до тяхното изменение. Поради нестабилността на доказателствата трябва да се следват определени протоколи, за да се гарантира, че данните не се променят, докато се обработват (т.е. по време на достъп до данни, събиране, опаковане, прехвърляне и съхранение). Тези протоколи описват стъпките, които трябва да се предприемат при работа с цифрови доказателства.

Различията в разпоредбите на законодателството на различните държави в областта на киберпрестъпността, липсата на международни стандарти по отношение на изискванията за представяне на доказателства (както по отношение на допустимостта на доказателствата в съда, така и по отношение на международната отговорност на държавата), механизми за предоставяне на взаимна правна помощ по дела, свързани с киберпрестъпността, навременното събиране, съхраняване и обмен на цифрови доказателства между държавите също представлява пречка за разследванията на киберпрестъпления.

За някои видове киберпрестъпления, особено политически мотивираните, като цяло **липсва воля сред държавите за сътрудничество** в такива случаи. Разследващите киберпрестъпления експерти са изправени и пред предизвикателства от технически характер. Така например много цифрови устройства използват собствени операционни системи и софтуер, които изискват специализирани инструменти за идентифициране, събиране и съхраняване на цифрови доказателства. Освен това следователите може да не разполагат с необходимото оборудване и инструменти за цифрова криминалистика, за да разследват правилно киберпрестъпността, включваща цифрови устройства. Други пречки пред разследванията в областта на киберпрестъпността включват ограничената способност на правоприлагащите органи да провеждат такива разследвания. В страни, в които съществуват национални специализирани звена, те разследват само ограничен брой случаи на киберпрестъпления. Широкото използване на информационни и комуникационни технологии в наказателни разследвания прави тази практика неефективна. Обучението за национални служители на правоприлагащите органи в неспециализирани полицейски области и нетехнически специализирани звена (напр. престъпления, свързани с наркотици, организирана престъпност, престъпления срещу деца), киберпрестъпления, разследвания в областта на ИКТ и цифрова криминалистика е един от начините за укрепване на националния капацитет. В допълнение, тези ограничени възможности за правоприлагане се влошават допълнително от нетрайните професионални знания на разследващите киберпрестъпления (Harkin, D, Ch. Whelan, and L. Chang, 2018, p. 530).

Заклучение

Неоспорим е фактът, че информационните и комуникационните технологии се развиват непрекъснато и с бързи темпове. В тази връзка експертите, които се занимават с разследване на киберпрестъпления, трябва непрекъснато да повиша-

ват своята квалификация, да следват развитието на технологиите, да са в крак с киберпрестъпниците, да са наясно с техните мотиви, цели, тактики и методи за извършване на престъпления. Освен това националните служби за сигурност са изправени пред проблема с т.нар. „изтичане на мозъци“, когато висококвалифицирани и опитни следователи, специализирани в киберпрестъпността, напускат тези органи и се прехвърлят в частния сектор, където им се предлагат по-високи възнаграждения за техните знания, умения и способности.

Сериозни са и проблемите, свързани с техническата обезпеченост на специализираните в разследване на киберпрестъпления държавни органи. Перманентно препятствие при разследването и разкриването на киберпрестъпления са и различията в националните материални и процесуални наказателни закони на отделните държави, а в някои отделни случаи и липса на добра воля за участие в разследвания на ниво национални държави.

Литература:

1. **Harkin, D, Ch. Whelan, and L. Chang** (2018). The challenges facing specialist police cyber-crime units: an empirical analysis. *Police Practice and Research*, Vol. 19(6), 530.
2. **Lin, H.** (2017). Attribution of Malicious Cyber Incidents. Hoover Institution, Aegis Paper Series No. 1607.
3. **Maras, M.-H.** (2014). Computer Forensics: Cybercriminals, Laws, and Evidence. Jones and Bartlett, 40 – 41.
4. **Pihelgas, M.** (2013). Back-tracing and Anonymity in Cyberspace. In Katharina Ziolkowski (ed.). *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy* (pp. 31 – 60). NATO Cooperative Cyber Defence Centre of Excellence.

За контакти:

Доц. д.н. Драгомир Кръстев
Висше училище по телекомуникации и пощи
drago.krastev@gmail.com