

Киберсигурност

СИЛИТЕ ЗА СПЕЦИАЛНИ ОПЕРАЦИИ В КОНТЕКСТА НА КИБЕРРАЗУЗНАВАНЕТО

ПОДП. Д-Р ХРИСТО АЛЕКСАНДРОВ ГЕОРГИЕВ

Главен асистент в катедра „Сухопътни войски”. Завършил Националния военен университет „Васил Левски”, специалност „Разузнаване“ през 2005 г. Служил като офицер както в парашутния полк в град Сливен, така и в 68-ма бригада „Специални сили”.

Резюме: В статията са разгледани взаимовръзките между кибер разузнаването и силите за специални операции, обърнато е особено внимание на същността и пресечните им точки. Разгледан е и процесът по разузнаване от открити източници, като неизменна част от дейността на силите за специални операции



Ключови думи: сили за специални операции, национална сигурност, киберразузнаване, разузнаване от открити източници.

SPECIAL FORCES IN THE CYBER INTELLIGENCE CONTEXT

HRISTO GEORGIEV

Abstract: The article examines the interrelationships between cyber intelligence and special forces, paying particular attention to their nature and intersections. The process of open-source intelligence

as an integral part of the operation of special operations forces is also examined.

Key words: Special Forces, national security, cyber intelligence, open source intelligence.

В контекста на съвременните заплахи, които са неделима част от функционирането на държавните системи, необходимостта от своевременна разузнавателна информация се превръща в жизненоважен елемент за функционирането на система за национална сигурност на която и да е държава. Тази така важна информация може да бъде довивана в различни домейни, като един от най-обширните и силно наситени с информация може да бъде определен именно кибер домейна. Имайки предвид неговите същностни характеристики, основния инструмент с който може да се реализират дейности по добиване на информация в него е киберразузнаването.

Това е „процес по придобиване, обработка, анализиране и разпространение на информация,

която идентифицира, проследява и предвижда заплахи, рискове вероятности за тяхното реализиране в кибердомейна, с цел намирането на пътища за тяхно противодействие.“¹

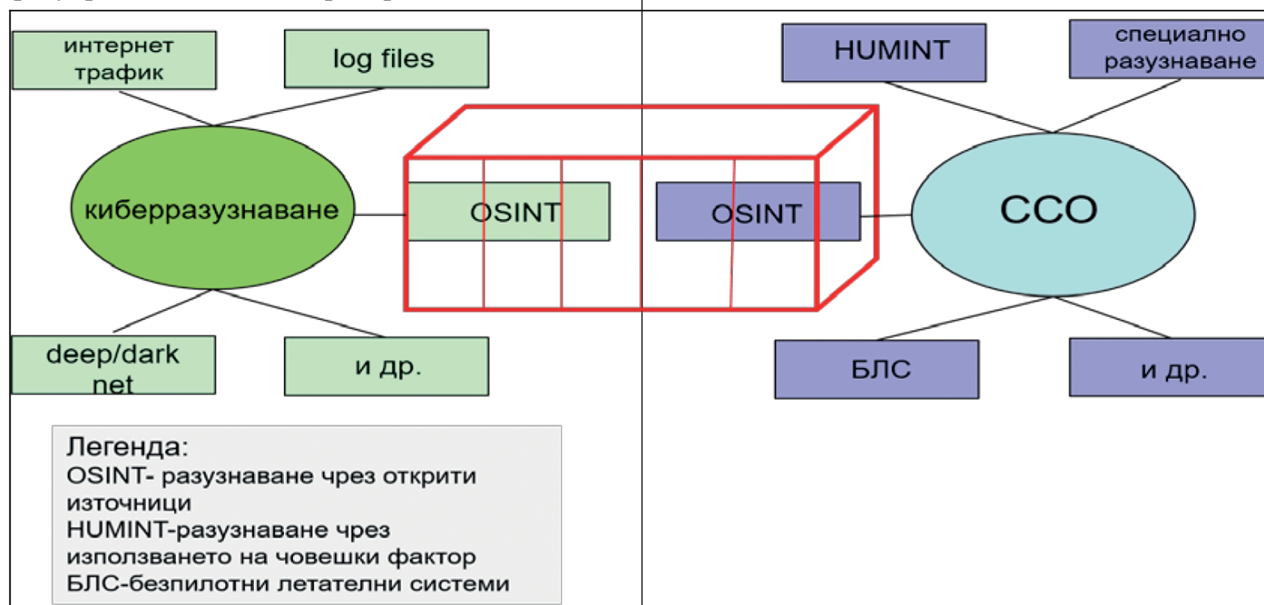


Основната структура която е с първостепенна отговорност към киберразузнаването на национално ниво е Държавна агенция национална сигурност. Разбира се на държавно ниво има и други структури, които са ангажирани с този процес. Едни от тях са именно разузнавателните отдели във видовете въоръжени сили и съвместното командване на специалните операции. Именно обвързаността на последното с киберразузнаването е предмет на настоящия анализ.

Силите за специални операции (ССО) са „инструмент който се използва за постигането на стратегически или ясно дефинирани оперативни цели.“² Тези цели са постигат чрез провеждането основно на различни видове специални операции. Но ССО в мирно време са част и от един неспирен процес на водене на разузнаване с цел ранно предупреждение и идентифициране на потенциал-

на разузнаването информация и достъпът, до които е условно свободен.

От друга страна едни от основните задачи по разузнаването които се спускат към видовете въоръжени сили и ССО в частност са свързани именно с реализирането на дейности в киберсреда, чрез воденето на разузнаване чрез открити източници. Ето защо на първо място може да се формулира твърдението, че именно информацията и разузнаването за което са обект могат да бъдат определени като свързващото звено между киберразузнаването и силите за специални операции. На следващо място обаче може да се потърси и допирателна по отношение на общата цел за водене на OSINT, а именно за идентифицирането на потенциални рискове и заплахи за националната сигурност в касаещия обем.



ни рискове и заплахи за националната сигурност. Но къде може да бъде открита невидимата нишка, която обединява и свързва силите за специални операции и киберразузнаването. Ако се разгледат способите за водене на киберразузнаване може да се дефинират няколко основни направления за реализирането му, като разузнаване свързано с интернет трафика, log files, deep и dark web.³ Един от тях се явява и разузнаването чрез открити източници (Open Sorce Intelligence – OSINT). Открити (явни) източници на информация са всички елементи от заобикалящата ни среда (обкръжение), които са носители на представляваща интерес за нуждите

Фиг. 1 Области за разузнаване при ССО и киберразузнаване

За да се детайлизира и затвърди обвързаността между ССО и киберразузнаването е необходимо да се нагледа по-подробно разузнаването от открити източници. Това е “комплекс от съгласувани действия и мероприятия, провеждани от органите за разузнаване на всички нива, съдържащ систематично и целенасочено добиване на информация от открити източници, нейното обработване за получаване на своевременна, достоверна и пълна разузнавателна информация и раз-

пространението ѝ с подходящи средства и форма до упълномощените потребители.”⁴

Откритите източници се използват за получаване на разузнавателна информация в следните по-важни информационни области:

- военнополитическа - важни текущи и дългосрочни военнополитически решения и дейности в национален, двустранен и многостранен аспект, състояние и тенденции в развитието на военно-политическата обстановка и др;
- военна - състав, организация, дислокация (базиране), въоръжение, военни доктрини, планове и схващане за използване, оперативна подготовка и др. на въоръжените сили на отделните страни, характеристика на реални и потенциални театри на военните действия, биографични данни за политическото и военното ръководство на страните и др;
- военно-икономическа - състояние и тенденции за развитие на икономиката, основни икономически показатели, брутен вътрешен продукт, военен бюджет и неговото разпределение, военна промишленост;
- военно-техническа - нови технологии и въоръжения, оръжия на нови принципи, тактико-технически характеристики на образци въоръжение и бойна техника и др.;
- сигурност - борба с тероризма, наркотрафика, нелегалния трансфер на хора, въоръжение, технологии и др.

Добиването на информация от открити източници се извършва преди всичко с използването на легални и етични способности. Познаването на качествата и свойствата на откритите източници е условие за тяхното ефективно използване в интерес на информационната дейност, тъй като позволява насочване на усилията за добиване на информация на разузнавателните щабове към точно определени видове открити източници.

Създаването и поддържането на стройна разузнавателна библиотека (картотека, база данни) с по-важните характеристики на конкретни открити източници съществено ускорява и улеснява процеса на добиване на информация. От гледна точка на използването на откритите източници в информационната дейност на разузнавателните щабове могат да бъдат определени техните по-важни отличителни свойства и качества, които съ-

щевременно служат за критерии при определяне на различните видове открити източници.

В зависимост от **характера на информацията, вида и особеностите на функциониране и способите** на разпространение откритите източници се разпределят най-общо в четири основни категории:

- средства за масова информация (осведомяване);
- специализирани издания;
- електронните компютърни мрежи;
- библиотеки и архивни фондове.

Предвид специфичните особености и характерни черти на отделни открити източници във всяка една категория може да съществуват различни групи и подгрупи открити източници на информация.

Основната категория, която касае кибер домейна е разбира се „**електронните компютърни мрежи**“. Те представляват “мрежа от свързани компютри, разположени на различни места от пространството посредством използването на стандартизирани правила за обмен на информация.”⁵

В зависимост от **обхвата на функциониране и разпространение на информацията** електронните компютърни мрежи могат да бъдат:

- световни (глобални) компютърни мрежи;
- континентални компютърни мрежи;
- регионални компютърни мрежи;
- национални компютърни мрежи;
- ведомствени компютърни мрежи;
- местни (локални) компютърни мрежи.

По отношение на **правото на достъп и работата със съхраняваната информация** електронните компютърни мрежи се разделят на:

- електронни компютърни мрежи със свободен достъп – официалните и популярни електронни компютърни мрежи с некомерсиално предназначение, които са със свободен достъп на всички граждани;
- електронни компютърни мрежи с ограничен достъп – това са предимно специализирани библиотеки и архиви на различни министерства, служби и ведомства, които съдържат предимно специфична, а в много случаи служебна и класифицирана информация, а дос-

тъпът е позволен в зависимост от правото на достъп на съответните потребители;

- електронни компютърни мрежи със смесен достъп – това са специфични компютърни мрежи на различни учреждения, организации, служби и ведомства, които съдържат, както официални и популярни материали, така и ведомствени и / или специфични и класифицирана информация. Особеното при тях е, че достъпа до отделни мрежи и информационни масиви е свободен, ползването на други се осъществява срещу заплащане на различни такси, а ползването на трети се позволява само на определени категории потребители.

Безспорно интернет е най-големият открит източник на информация в света. Обемът на информацията, съхраняваща се в интернет е динамична, постоянно променяща се величина и е невъзможно да бъде определен с точност. Интернет е средство (среда) за достъп до почти всички споменати открити източници. Чрез нея може да се следят всякакви печатни средства за масова информация, да се гледа телевизия и слуша радио и едновременно с това да се извършва запис на съответното предаване (емисия), да се открият и поръчат специализирани издания, да се издирят представляващи интерес за разузнаването на ССО теми и въпроси, както и много други дейности.

Освен това понастоящем няма по-бърз и удобен начин за следене на откритите източници от Интернет. За това допринасят и предлаганите срещу заплащане услуги от много частни фирми, компании и агенции, които осъществяват периодично (ежедневно, непрекъснато или при поискване) предоставяне на всякакъв вид информация от различни области и сфери, която представлява интерес за съответния клиент. Следва да се има предвид обаче, че информацията в Интернет е неструктурирана, в много случаи непълна, неточна или подвеждаща, а в много случаи и умишлено дезинформираща и заблуждаваща. Ето защо при добиване на информация от Интернет е необходимо съответните специалисти от ССО да притежават необходимите познания, специфични умения и опит за пресяване на релевантна, актуална и достоверна информация, която да удовлетворява необходимите потребности.

Използването на интернет налага коренно нов подход обаче при добиването и обработването на снетата информация. Като правило това изисква осигуряване с най-съвременни технически средства за обработване, съхраняване и последващо търсене на сведения и данни в разузнавателната библиотека и неминуемо води до принципно нова организация на работата в структурите за разузнаване. Поради така изложените съображения всички разузнавателни служби и по-сериозни информационни агенции, ведомства, организации, средства за масова информация, фирми и др. подобни създават свои специализирани звена (структури) за следене на открити източници в Интернет и добиване на необходимата им информация.

От всичко описано до тук може да се заключи, че киберразузнаването ще бъде все по-застъпено по отношение разкриването на рискове и заплахи за националната сигурност на страната, поради нарастващата активност и обем на кибер домейна. На следващо място силите за специални операции в своята ежедневна разузнавателна дейност използват способности прилагани от киберразузнаването, за да изпълнят поставените им задачи по добиване на информация. Ето защо формулирането на идеята за воденето на киберразузнаване от ССО в интерес на националната сигурност няма нужда от апробация поради своята истинност. Разбира се приноса на ССО трябва да се разглежда като част от цялостната изградена мрежа от структури на държавно ниво имащи отговорност за воденето на ефективно киберразузнаване в интерес на националната сигурност.

БЛАГОДАРНОСТИ

Докладът е написан благодарение на финансиране от Министерство на образованието и науката в изпълнение на Националната стратегия за развитие на научните изследвания 2017 – 2030 по Национална научна програма „Сигурност и отбрана“, приета с решение на Министерски съвет № 731 от 21 октомври 2021 г.

1. Начев, Й, Конкурентно разузнаване, София, 2007 г.
2. Доктрина за специалните операции, София, 2021.
3. <https://www.fortinet.com/resource>
4. <https://www.sans.org/blog/what-is-open-source-intelligence>
5. <https://bg.khanacademy.org/computer-network>

