ПРИНЦИПИ НА ДЕФАНЗИВНОТО КОНТРАРАЗУЗНАВАНЕ

ДОЦЕНТ Д-Р МИЛЕН ИВАНОВ

Резюме: *Статията разглежда основните принципи, на базата на които трябва да се изгражда системата на дефанзивното контраразузнаване. Изведени са основните им характеристики и е посочена връзката на тези принципи с конкретното им реализиране на практика.*

Ключови думи: *Контраразузнаване, разузнаване, операции, национална сигурност, саботаж, тероризъм, проникване.*

PRINCIPLES OF DEFENSIVE CONTRAASULATION

ASSOCIATE PROFESSOR MILEN IVANOV, PHD

Abstract: *The article discusses the basic principles on which the system of defensive counterintelligence should be built. Their main features are outlined and the link between these principles and their concrete implementation is outlined.*

Key words: *Counterintelligence, intelligence, operations, national security, sabotage, terrorism, penetration*

Транснационалният тероризъм, разпространението на оръжия за масово унищожение, проникванията в кибернетичното пространство, асиметричната и хибридната война, екстремистките движения и т. нар. „провалени държави“ представляват сериозни предизвикателства за предвидимия и стабилен международен ред. Способността да се отговори активно на тези предизвикателства е силно застрашена от разузнавателната дейност, провеждана от традиционни и нетрадиционни играчи на геополитическата сцена. Тези играчи – чужди специални служби, терористи, криминални предприятия, и нарушители в кибернетичното пространство, използват явни, тайни и нелегални дейности, за да се възползват и да навредят на интересите на държавата в сферата на националната сигурност.

Един от основните инструменти, с които разполага държавата, за да противодейства активно на тези заплахи е контраразузнаването. Когато то е успешно - допринася пряко за гарантиране на националната сигурност и служи като щит (предотвратява чуждо проникване в правителството, предоставя информация свързана със сигурността и реализира други защитни мерки) и меч (провежда офанзивни контраразузнавателни операции, за да моделира чуждите възприятия и разрушава способностите на чуждите разузнавания) в борбата със заплахите за сигурността на държавата.

Държавата постоянно се сблъсква със сериозни тайни или скрити заплахи. Контраразузнаването е този механизъм, чрез който се изучава природата на заплахата, придобива опит, и след това го използва, за да неутрализира или контролира тези заплахи чрез операции за проникване или по друг начин. Контраразузнавателната служба трябва да бъде осигурена със сериозни знания и умения, а вземаните решения да се съсредоточават върху главните цели. Ефективността на нейната дейност е от решаващо значение за функционирането на държавата като цяло.

Общоприетата теория на контраразузнаването посочва, че има четири основни принципа, на базата на които то трябва да функционира - възпиране, откриване, заблуда и неутрализиране усилията на противника да събира информация, независимо от причината, поради която се събира тази информация – разузнаване, подривна дейност, саботаж, тероризъм, разпрос-

транение на оръжия, конкурентна предимство и т н.

Тези принципи са част от „универсалната“ теория на контраразузнаването, като те могат да бъдат адаптирани и към различните сфери на контраразузнавателната дейност - военна, национална сигурност, правоприлагането и бизнеса. Така например, терминът „откриване“ може да се равнява на „идентифициране“ и т. н. В този смисъл, например, разузнаването може да включва планиране по отношение на различни цели – в областта на правоприлагането, националната сигурност, военна, бизнес и частни. Подривната дейност може да включва такива действия като бунт, предателство и радикализация. Саботажът може да се изразява в щети, прекъсване и възпрепятстване на услуги и процеси. Тероризмът може да включва актове на насилие и различни средства, чрез които политически или идеологически мотивирани групи да изразяват своите съобщения с актове на жестокост. Може да има и други, но с илюстративна цел този списък е достатъчно широк.

Тези четири принципа имат два основни фокуса - пасивна защита и активна защита, или казано по друг начин - дефанзивно контраразузнаване и офанзивно контраразузнаване.

Дефанзивното контраразузнаване започва с разглеждането на собствената организация за начина, по които тя може да бъде използвана от всеки вид чуждо разузнаване. Терминът „чуждо“ не винаги се отнася до друга международна сила. Той може да се отнася и до вътрешна група, която притежава войнстваща или бунтовническа идеология, или за някакъв вид транснационална организация, например такива на наркокартели или контрабандисти. Стратегическите оценки се правят, за да се предоставят възможности за осъществяване на последващи разследвания и операции.

Дефанзивните контраразузнавателни операции до голяма степен се състоят от реактивни и превантивни мерки, като се търсят слабостите и уязвимостите в дадена организация, които биха могли лесно да бъдат използвани, и се търсят начини за изграждане на защита за тези недостатъци. Това се прави чрез първоначални оценки, които анализират данни от многобройни разузнавателни източници и дисциплини, за да се създадат ефективни системи за възпиране на организации или хора, които са заплаха за националната сигурност. Дефанзивното контраразузнаване се състои и от разследвания на нарушения на сигурността и на дейността на държавните служители; като се търсят на конкретни деяния или проблеми, които могат да показват, че те са заплаха за сигурността, като например високо ниво на дълг, компрометиращи семейни взаимоотношения, психологически разстройства, или връзка с потенциално опасни групи[1].

Кенет Деграфенрайд заявява: „Една страна трябва първо да знае какво се опитва да защити. Какви са тези ценности, тайни и институции, които се нуждаят от защита? В едно свободно общество има много от тях. Предвид крайния характер на неговите контраразузнавателни ресурси, какви са най-ценните му тайни? Това изисква анализ и вземане на решения.“[2]

Дефанзивното контраразузнаване има няколко основни принципа, на базата, на които то се изгражда. Тези принципи са залегнали в основата на философията и логиката на всяка дейност и система в този вид контраразузнаване и тяхното познаване ще позволи да си обясним по-добре начина който то трябва да функционира.

Необходимост да бъде там (need-to-be-there). В системата за сигурност, която е основата на дефанзивното контраразузнаване трябва да бъде създадена логична обосновка, която да позволява на определени хората да имат достъп до район, зона, сектор, сграда или помещения където се обработва, анализира или съхранява чувствителна информация. Този принцип е известен като „приятелски достъп“, и това е средство, което се използва там където противникът се опитва да получи достъп чрез измама, а не чрез сила. Той изисква достъпът до тези зони да бъде ограничен до работниците, служителите и посетителите, които са известни или имат определени срещи. Всички други посетители трябва да бъдат внимателно проверени и тяхната самоличност установена преди влизането. С хората, които извършват доставки, включително доставки на поща и работници по поддръжката, трябва да се действа по същия начин. Достъпът до всички обекти трябва да бъде

ограничен на основата на забраната да се намират там без да има необходимост от това. Ако трафикът на посетители и персонал на дадена структура е тежък, се използва система от специално проектирани лични карти, носени над връхните дрехи на служителите или специални униформени жилетки със съответните обозначения и баджове. Системата за издаване и ползване трябва да е така организирана, че лесно и бързо да се установява дали дадено лице е приятел или враг.

Необходимост да се знае (Need to know). Най-добрият вариант за дефанзивното контраразузнаване е ако противникът никога не е наясно, че някъде съществува чувствителна информация. Това означава, че първото нарушение на сигурността е налице, когато противникът разбере, че съществува ценна информация. Ако това, все пак се случи, всичко, което може да се направи в този момент е да се засилят защитните мерки на контраразузнаването и/или провеждане на офанзивни контраразузнавателни операции. Затова, ако дадена информация притежава някаква степен на чувствителност, нейното съществуване трябва да се пази в тайна за всички, освен тези, които трябва да знаят.

Същото важи и за хората, които са носители на тайна информация по силата на служебното си положение. Самият факт, че противникът научи, че дадено лице е секретоносител, то той ще стартира своята програма за активно насочване (targeting) на своите сили и средства, за да получи логичен достъп до това лице и чрез него до интересуващата го информация. Това налага самият факт, че определено лице има достъп до тайни да се пази в тайна. Това е и един от основните дефекти на действащия сега Закон за защита на класифицираната информация. Публичността на списъка на длъжностите и задачите изискващи достъп до класифицирана информация и липсата на защита на издадените разрешения за достъп до класифицирана информация улесняват сериозно разузнавателното проникване на чуждите специални служби до нашите тайни, като подпомага техния разузнавателен цикъл и планирането на операциите.

Противодействие на наблюдението (Counterreconnaissance). Този принцип е свързан предишния и има за цел да не се позволява на противника да получи необходимото му знание за информацията или операциите. Той има за цел да се предотврати провежданото от него наблюдение (reconnaissance). В този си смисъл, тази дейност е повече от предотвратяване на физическото разузнаването на целта, и в зависимост от случая ще бъде приложена по отношение на дадена част от критичната инфраструктура. Задача е да се пречи на сканирането на околната среда, което служи за откриване на потенциални признаци, които да показват, каква е активността на обекта в зависимост от дадени събития. Например, стратегически разузнавателни анализатори използват метод, известен като "сканиране на околната среда", който има за цел да се получат данни на макроравнище. Ако в анализа на тези данни анализаторите заключават, че са налице индикатори, че противникът може да участва в определени дейности, представляващи интерес, то тогава лесно се стига и да конкретно знание да ситуацията.

Реалистични политики и процедури. Мерките за противодействие трябва да бъдат гъвкави и да съответстват на риска. Те не трябва да се превърнат в твърд набор от политики и процедури. Вместо това, те трябва да бъдат гъвкави и адаптивни към промените в изискванията на сигурността. Тези които ги прилагат ще трябва да се съобразяват с много фактори, преди да се приложат конкретни мерки за противодействие. Въпреки това, трябва да бъдат преценени важни въпроси, когато се изгражда или се подобрява дефанзивната контраразузнавателна програма. Те включват, но не се ограничава до финансовите ограничения и желанието на служителите да следват предложените процедури. Така например в частния бизнес няма смисъл при изразходването на големи суми пари за безопасни и алармени системи за откриване, ако ползата не е оправдана, или те водят до финансови проблеми на организацията. По същия начин, персоналът може да се изкуши да заобиколи процедурите за сигурност, ако ги счита за прекалено сложни или отнемат много време.

Синергичен подход. Мерките за противодействие трябва да се разглеждат като модулна структура, което е в състояние

да се адаптира, изцяло или частично в зависимост от резултатите от процеса на планиране на контраразузнаването. Важният въпрос е, че принципите на дефанзивното контраразузнаване се наблюдават и се извършват периодични преоценки, за да се провери дали стандартите за сигурност се използват. Мерките за противодействие може да бъде видени и в синергичния ефект - комбинацията на цялото е по-голяма от сумата на отделните компоненти.

Ранно откриване. Проникването чрез взлом и кражбите не са необичайно явление за правителствени агенции или фирми. Много случаи показват, че в реалността взломяването не е само метод за придобиване на парични средства и ценни материални активи, но също така е и техника за събиране на информация.

В дейността на разузнаването тази техника се нарича black bag operation или black bag jobs. Тя се осъществява чрез тайно или скрито физическо проникване в структури, за да се получи информация за дейността на разузнаването.[3] Това обикновено включва и влизане с взлом в забранени райони. Някои от тактиките, техниките и процедурите, свързани с този вид операции са: разбиване на ключалки, разбиване на сейфове, подправяне на ключове, взимане на пръстови отпечатъци, фотографиране, електронно наблюдение (включително аудио и видео наблюдение), манипулиране на кореспонденция, подправяне на документи и множество други свързани с тях умения. Терминът „черна чанта“ произлиза от малката черна чанта, в която в миналото крадците носели своите инструменти.[4]

Дефанзивните контраразузнавателни операции до голяма степен се състоят от реактивни и превантивни мерки, които започват, като се потърсят слабостите и уязвимостите в дадена организация, които биха могли лесно да бъдат използвани, и намиране на начини за изграждане на защита за тези недостатъци. Това се прави чрез първоначални оценки, които анализират данни от многобройни разузнавателни източници и дисциплини, за да се създадат ефективни системи за възпиране срещу организации или хора, които са заплаха за националната сигурност.

Контраразузнавателната теория в България се намира е преходен етап между неосъзнатите докрай остатъци от руско-съветската теория по темата и нуждата от адаптиране на съвременните теория на водещите западни държави и трансформацията на НАТО. Тази твърде неизгодна за страната ни позиция се комбинира и с липсата на сериозен научен потенциал и изследователско звено, което да анализира практиката и да адаптира опита към съвременните теории, като предаде научените уроци от тази адаптация на следващите генерации контраразузнавачи. Формулирането на базовите принципи на контраразузнавателната дейност е необходимо, за да станат те основа за успешната реализация на тази държавна дейност на стабилна правова основа, която да подпомогне тя да функционира успешно и да се гарантира спазването на основните права на човека.

1 Joint Publication (JP) 2-01.2, Counterintelligence and Human Intelligence Support to Joint Operations, 5 July 2017.

2 Kenneth deGraffenreid, The Cox Report: the unanimous and bipartisan report of the House Select Committee un U.S. national security and military commercial concerns with the People's Republic of China. Regenery Publishing. ISBN 0-89526-262-2.

3 Tallinn government surveillance cameras reveal black bag operation, https://intelnews.org/2008/12/16/04-11/, (02.03.2019)

4 The CIA Code Thief Who Came in from the Cold, https://www.matthewaid.com/post/32043919336/the-cia-code-thief-who-came-in-from-the-cold, (07.03.2019)