УДК 327.8
DOI: 10.33663/1563-3349-2025-97-118

***Ю. В. СЕМЕНЮК***
***Ю. М. ЛИСЕЦЬКИЙ***

# ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО У СФЕРІ РОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ

*Досліджується державно-приватне партнерство у сфері розвідувальної діяльності. Розглянуто причини появи приватних розвідувальних компаній, історію їх виникнення та розвитку. Проаналізовано специфіку, особливості та напрями діяльності найвідоміших приватних розвідувальних компаній Сполучених Штатів Америки, Великої Британії, Ізраїлю, Об'єднаних Арабських Еміратів. Показано, що приватні розвідувальні компанії виступають виконавцями замовлень державних структур в якості здобувачів та обробників розвідувальної інформації, за допомогою якої держава дізнається про своє зовнішнє оточення та усвідомлює власні завдання у цій сфері. Доведено, що приватні розвідувальні компанії можуть бути використані для ведення політичної боротьби, і тому їхня діяльність повинна здійснюватися під контролем з боку держави на основі спеціально створеного законодавства.*

***Ключові слова:*** *розвідувальна діяльність, спецслужби, національна безпека, приватні розвідувальні компанії, інформаційно-аналітичні послуги.*

***Semenyuk Yurii, Lysetskyi Yurii.*** **Public-private partnership in the sphere of intelligence activities**

*The article explores public-private partnerships in the field of intelligence activities. It examines the reasons for the emergence of private intelligence companies, their history of origin and development. The specifics, features, and areas of activity of the most well-known private intelligence companies in the United States, the United Kingdom, Israel, and the United Arab Emirates are analyzed. It is shown that private intelligence companies act as contractors for government agencies, serving as collectors and processors of intelligence information through which the state gains insights into its external environment and understands its objectives in this sphere. Additionally, it is noted that*

---

© *СЕМЕНЮК Юрій Володимирович* – кандидат політичних наук, Національний університет оборони України; ORCID: 0000-0002-9415-4427; e-mail: snik71083@gmail.com

© *ЛИСЕЦЬКИЙ Юрій Михайлович* – доктор технічних наук, доцент, Воєнна академія імені Євгенія Березняка; ORCID: 0000-0002-5080-1856; e-mail: Yurii.Lysetskyi@snt.ua

*private intelligence companies can be used for political struggles, and therefore their activities should be carried out under state control based on specially developed legislation.*
***Key words:*** *intelligence activities, intelligence agencies, national security, private intelligence companies, information and analytical services.*

Нині зовнішня політика будь-якої держави базується на відомій їй інформації суспільно-політичного характеру, дослідженні ключових проблем у політичній та соціальній сфері, аналізі стратегій і тактик, здійсненні політичних та соціально-економічних перетворень. Одними з головних здобувачів та обробників цієї інформації є розвідувальні органи (РО), за допомогою яких держава дізнається про своє зовнішнє оточення та усвідомлює власні завдання у цій сфері. Відповідно цивільні та військові РО зосереджуються на пошуку, аналізі, використанні інформації, як секретної, так і одержаної із відкритих джерел (Open Source Intelligence, OSINT).

Впродовж тривалого часу держави прагнули зберігати за собою монопольне право на ведення розвідувальної діяльності. Проте упродовж першої половини 1990-х років з'явилися приватні структури, які надавали інформаційно-аналітичні послуги, що виходили за межі бізнес-розвідки не тільки великим корпораціям та приватним особам, а й державним структурам. Такі організації отримали назву «приватні розвідувальні компанії» (ПРК), і у цій специфічній сфері діяльності почало розвиватися державно-приватне партнерство. За приблизними даними, у понад 50 державах світу діють близько кілька сотень ПРК.

Вагомою причиною залучення ПРК до забезпечення зовнішньої складової частини національної безпеки було те, що приватні структури переважно еластичніші та ефективніші, ніж державні, зокрема в економічних відносинах. Крім того, такий «підряд» ПРК давав можливість знижувати державні видатки на утримання спеціальних служб, а також вирішувати деякі чутливі питання, приховуючи безпосередню причетність держави до них. ПРК пропонують свої послуги не лише державним органам, а й великим корпораціям та окремим споживачам. Тому дослідження діяльності ПРК та досвіду їх використання різними країнами є дуже актуальним.

Родоначальником у системі державно-приватного партнерства у сфері національної безпеки вважаються Сполучені Штати Амери-

ці, а першої ПРК – американський дослідницький центр глобальної політики RAND Corporation (Research ANd Development, RAND) [1]. Він був заснований 14 травня 1948 року в Санта-Моніка (Каліфорнія) Генрі Харлі Арнольдом, Дональдом Віллсом Дугласом та Кертісом Лемеєм як партнерство між американськими Військово-повітряними силами (ВПС) та компанією Douglas Aircraft для конструювання літаків, ракетної техніки та супутників. RAND Corporation вважається одним із перших у світі «мозковим центром», чи «інститутом політики» (think tank, policy institute), який надавав військові поради керівництву держави, міністерству оборони.

Історія виникнення RAND Corporation починається з часів Другої світової війни, колі в США була створена велика група переважно вчених та інженерів для реалізації війни на «технологічному фронті». У відносно короткий термін ця група створила такі новинки, як атомна бомба, радар, неконтактний підривач тощо. Також був розроблений і вдало застосований аналітичний метод дослідження операцій, що дозволило підвищити ефективність Протиповітряної оборони (ППО), бомбометання і військово-морських операцій.

Наприкінці війни, коли цей колектив став розпадатися, військові вирішили зберегти деяких із найбільш талановитих співробітників для продовження розвитку військових технологій. Генерал Генріх Г. Арнольд, командувач ВПС Армії Сполучених Штатів Америці, створив проєкт RAND із фінансуванням 10 млн доларів з метою довгострокового планування майбутньої зброї. У березні 1946 року компанія Douglas Aircraft отримала контракт на дослідження міжконтинентальної війни, використовуючи дослідження операцій. У травні 1946 року був випущений попередній проєкт експериментального космічного корабля, що облітає світ. 14 травня 1948 року RAND був зареєстрований як некомерційна корпорація відповідно до законів штату Каліфорнія, а 1 листопада 1948 року контракт Project RAND був офіційно переданий від Douglas Aircraft Company до корпорації RAND. Таким чином, проєкт RAND перетворився на незалежну некомерційну організацію RAND Corporation, початковий капітал для якої був наданий Фондом Форда (Ford Foundation).

Першою значною роботою RAND було дослідження, опубліковане як Preliminary Design of an Experimental World-Circling

Spaceship (попередній проєкт експериментального космічного корабля, який обертається навколо Землі). Незважаючи на те, що штучні супутники Землі на той час вважалися науковою фантастикою, у цьому документі 1946 року було вказано: «Супутниковий транспортний засіб з відповідною апаратурою можна вважати одним з найпотужніших наукових інструментів XX століття. Досягнення супутникового судна призведе до наслідків, порівнянних із вибухом атомної бомби ... ». Вдале пророцтво зміцнило престиж RAND Corporation. У середині 1957 року була спрогнозованоадата запуску першого супутника Землі, з помилкою лише у 2 тижні.

До кінця 50-х років наукова література визначає різницю між системним аналізом і дослідженням операцій, системним аналізом і системною інженерією, теорією рішень і дослідженням операцій тощо. Широко розглядаються проблеми застосування наукової методології до таких «неточних» сфер, як керівництво, прийняття рішень людиною, організація. Прикладом важливого досягнення RAND Corporation у розв'язанні цих науково-прикладних проблем є розробка і широке застосування Systems analysis (системного аналізу). Фахівці RAND Corporation виконали низку фундаментальних досліджень і розробок щодо системного аналізу, орієнтованих на вирішення слабоструктурованих проблем Міністерства оборони США. Створення у 1952 році надзвукового бомбардувальника B-58 було першою розробкою, що поставлена як система. Все це вимагало випуску наукової та навчальної літератури.

Перша книга із системного аналізу вийшла у 1956 році. Її видала RAND (автори А. Кан і С. Манн). Методологія системного аналізу була детально розроблена і представлена у I960 році. у книзі Ч. Хітча і Р. МакКін «Військова економіка в ядерне століття». У ній також наводиться додаток до методів кількісного порівняння альтернатив для вирішення проблем озброєння. Пізніше Дж. Хітч (помічник Міністра оборони США, Президент Каліфорнійського університету) описав системний підхід до вибору зброї у США.

У 1965 році з'явилася вельми ґрунтовна книга Е. Квейда «Аналіз складних систем для вирішення військових проблем». У ній представлені основи нової наукової дисципліни – аналізу систем. Книга спрямована на обґрунтування методів оптимального вибору при вирішенні складних проблем в умовах високої невизначеності. Ця книга є переробленим викладом курсу лекцій з аналізу систем,

прочитаних працівниками корпорації RAND для керівних фахівців Міністерства оборони та промисловості США.

Цього ж року вийшла книга С. Оптнера «Системний аналіз для вирішення ділових і промислових проблем», яка насичена великою кількістю нових ідей, дає повне і чітке уявлення про системний аналіз із характеристикою проблем ділового світу, сутності систем і методології вирішення проблем. Книга стала однією з перших виданих у нас праць, які висвітлюють стан цієї сфери в США. Навчальні дисципліни з теорії систем і системного аналізу є нормативними важливими елементами системи навчання у багатьох вищих навчальних закладах світу й України.

Як видно із назв книг, під час розробки методів системного аналізу для військової сфери з'ясувалося, що проблеми цивільні, проблеми фірм, маркетингу, аудиту та інші теж потребують обов'язкового застосування методології системного аналізу, системного підходу. Системний підхід перетворився на важливий метод пізнання, на відміну від спеціальних прийомів, характерних для розробки техніки XVI-XIX ст. Це був другий етап історичного розвитку системного підходу в техніці. Розроблено цілу низку вельми складних і тонких математичних методів, зокрема: лінійне програмування, динамічне програмування, визначення черговості проблем, нелінійне програмування, метод Монте-Карло, теорія ігор тощо. У 1957 році в США видана книга System Engineering. An introduction to the design of large-scale systems (Системна інженерія. Вступ до розробки великих складних систем) Г. Гуда і Р. Макола.

RAND Corporation провела значну роботу з вивчення проблем розповсюдження ядерної зброї, у ході якої здійснювався аналіз економічних, політичних і технічних аспектів створення ядерного потенціалу в різних країнах.

RAND Corporation перша серед американських установ почала розробляти науку «холодної війни» з використанням методів, які передбачають інтенсивне вивчення потенційного противника «з певної відстані». Також RAND Corporation є розробником концепцій «гнучкого реагування», «контрсили» та інших. Найбільш помітним внеском можна вважати Доктрину взаємного гарантованого знищення (Mutually Assured Destruction, MAD), розроблену під керівництвом тодішнього міністра оборони Роберта Макнамари на основі теорії ігор.

MAD – військова доктрина, згідно з якою застосування двома протиборчими сторонами зброї масового ураження призведе до повного знищення обох сторін, що робить безглуздими будь-які спроби застосування доктрини першого удару. Слово «mad» також означає «божевільний», «несамовитий», а термін MAD ввів Джон фон Нейман – геніальний математик, консультант корпорації RAND. Доктрина взаємного гарантованого знищення є наочним прикладом Рівноваги Неша, при якій жодна озброєна сторона не може ні почати безкарно конфлікт, ні роззброїтися у добровільному порядку.

В 1971 році група математиків з RAND Corporation на чолі з Ендрю Маршаллом розробила першу математично обґрунтовану «національну розвідувальну оцінку» (National Intelligence Estimates, NIE), яка містила систематизовані результати обробки розвідувальних та публічних даних, що отримані з різних джерел. Тепер NIE розробляє Національна рада з розвідки для федерального уряду. Це узгоджені судження всіх 18 складових розвідувального співтовариства США. Видатний аналітик Міністерства оборони США Ендрю Маршалл, якій передбачив низку важливих змін у світі, включаючи розпад СРСР, підвищення геополітичної ролі Китаю і широке використання робототехніки у військових операціях, у 1973 році був призначений керівником Управління загального аналізу Пентагону. На цій посаді він пережив «холодну війну», незліченні військові конфлікти і 10 президентських виборів.

Істотний внесок зробила RAND Corporation також у галузі Artificial Intelligence (штучний інтелект). Дослідники RAND розробили багато принципів, які використовувалися для побудови Інтернету. Досвід RAND Corporation у воєнній сфері привів до створення у США відомого у всьому світі DARPA, Defense Advanced Research Projects Agency (Агентства передових оборонних дослідницьких проєктів США). У свою чергу, вдалий досвід DARPA дав змогу створити відповідну структуру для IARPA, Intelligence Advanced Research Projects Activity (Національної розвідки США), а також подібну структуру в цивільних міністерствах (держагенціях), наприклад, ARPA-Ed – Агенство передових досліджень США у сфері освіти). Системний підхід привів до відкриття у 2018 році GARDA (Government Advant Research Development Agency) – Державного Агенства передових дослідницьких проєктів.

Нині RAND Corporation є одним із найавторитетніших дослідницьких центрів світу в усіх сферах державної політики та управління, національної безпеки та розвідки, від оборони та міжнародних відносин до освіти, охорони здоров'я, містобудівного планування та інфраструктури, транспорту, енергетики, охорони навколишнього середовища, права, демографії, зайнятості тощо. Водночас RAND підтримує тісні неафішовані зв'язки зі своїм основним замовником – Центральним розвідувальним управлінням (ЦРУ). Корпорація має близько 1700 працівників із 50 країн, які є фахівцями в найрізноманітніших галузях (економіка, психологія, медицина, освіта, інженерія, математика, комп'ютерні технології, міжнародні відносини тощо). Серед співробітників корпорації були таки відомі особи, як професор Френсіс Фукуяма, Державний секретар США Генрі Кіссінджер, міністр оборони і директор ЦРУ Джеймс Шлезінгер, заступник радника президента США з національної безпеки Джеймс Стейнберг, а до складу Ради директорів RAND входили колишні Державний секретар США Кондоліза Райс та міністр оборони США Дональд Рамсфельд. До реалізації різних проєктів корпорації долучалися 30 лауреатів Нобелівської премії.

RAND Corporation має офіси у США: Санта-Моніка (штат Каліфорнія), де розташована штаб-квартира та Вища школа Фредеріка С. Парді; Арлінгтоні (штат Вірджинія; Пітсбург, штат Пенсільванія); Бостоні (штат Массачусетс) і Вашингтоні. RAND також має американських дослідників, які живуть і працюють у понад 35 інших штатах та окрузі Колумбія. Крім того, вона має офіси в Кембриджі (Великобританія), Брюсселі (Бельгія); Роттердамі (Нідерланди) та Канберрі (Австралія). Замовниками досліджень RAND виступають уряди та урядові підрозділи різних країн, громадські організації, приватні компанії.

Rand Corporation яскраво характеризує книга, видана у 2008 році з назвою: Soldiers of Reason: The RAND Corporation and the Rise of the American Empire (Солдати розуму: The RAND Corparation і підгнсення американської імперії). Корпорація має за мету міждисциплінарне та кількісне вирішення проблем шляхом перекладу теоретичних концепцій з формальної економіки та фізичних наук у нові застосування в інших галузях, використовуючи та розробляючи прикладні наукові дослідження. Значна частина досліджень RAND включає проблеми національної безпеки. Багато подій, в

яких RAND відіграє певну роль, ґрунтуються на припущеннях, які важко перевірити через відсутність деталей роботи RAND для оборонних та розвідувальних органів.

Після розпаду СРСР, вже у нових геополітичних умовах, 1992 році у штаті Флорида колишніми співробітниками ЦРУ була створена CTC International Group. Імовірно, кадровий склад групи й спричинив обмежену відкриту інформацію про цю ПРК. У короткій рекламі на вебсайті зазначено, що компанія працює у сфері забезпечення безпеки та проведення розслідувань і надає практичну інформацію, щоб навчати клієнтів і допомагати їм приймати обґрунтовані рішення [2]. Очолювана колишніми офіцерами ЦРУ, CTC використовує цикл розвідки, щоб надати приватним клієнтам високоякісні розвідувальні дані, які уряд США використовує для прийняття рішень. Цілеспрямоване дослідження в поєднанні з професійним аналізом дає інтелект, а не просто «інформацію», яка відокремлює «приємно знати» від «необхідності знати». CTC надає розвідувальні дані генеральним директорам, юристам та іншим особам, які приймають рішення і яким потрібна точна, прогнозована та дієва розвідка. Адже знання справді є силою.

Спеціалізація CTC International Group – бізнес-аналітика, конкурентна розвідка, незалежна перевірка компаній, перевірка минулого, стратегічна розвідка, підтримка складних судових розглядів. Штат компанії налічує від 50 до 100 співробітників [3].

Однією з найбільш відомих та авторитетних ПРК є Strategic Forecasting, Inc. (Stratfor), заснована 1996 року політологом Джорджем Фрідманом [4]. Він на початку 1980-х років почав проводити дослідження з проблематики радянсько-американських відносин. У 1994 році при Університеті штату Луїзіана він заснував Центр геополітичних досліджень, який спеціалізувався на стратегічному прогнозуванні. Протягом 1996–2015 рр. – очолював Stratfor.

На матеріали Stratfor посилаються авторитетні ЗМІ, зокрема CNN, Bloomberg, Associated Press, Reuters, The New York Times, Time та BBC. У 2001 році газета «Barron's» назвала Stratfor «тіньовим ЦРУ». Поступово за своєю впливовістю серед корпорацій і державних організацій та популярністю серед журналістів ця ПРК витіснила RAND. Принципова відмінність Stratfor від RAND полягає в тому, що Stratfor першою створила загальносвітову агентурну

мережу, яка зорієнтована насамперед на корпорації та корпоративний підхід.

Співробітники Stratfor збирають та аналізують інформацію про події у світі, акцентуючи на безпекових питаннях та геополітичних ризиках. Інформацію вони отримують не лише зі ЗМІ та інших відкритих джерел, а й з власних джерел. Фактично це агентурна розвідка (Human Intelligence, HUMINT). На підставі зібраних відомостей аналітики Stratfor роблять економічні та геополітичні прогнози. Штат компанії налічує близько 100 співробітників.

Крім дослідників різних наукових галузей, Stratfor залучає до роботи експертів із відповідним практичним досвідом. Так, у 2004–2020 рр. віцепрезидентом компанії з питань антитероризму та корпоративної безпеки був Фред Бартон, колишній співробітник Секретної служби США, а пізніше – заступник начальника відділу боротьби з тероризмом Служби дипломатичної безпеки Державного департаменту США. У 2013–2018 рр. віцепрезидентом з питань митної розвідки був Брет Бойд, колишній офіцер Командування спеціальних операцій США.

У 2012 році Stratfor опинилася в центрі скандалу, організованого міжнародною організацією WikiLeaks, яку заснував австралійський журналіст Джуліан Ассанж. Він виклав у відкритому доступі понад 5 млн електронних повідомлень цієї компанії і звинуватив її у відстеженні діяльності міжнародних активістських організацій за дорученням клієнтів ПРК, зокрема компаній «The Dow Chemical Company» та «The Coca Cola Company», а також спецслужб США. У викрадених хакерами матеріалах були згадки й про контакти Stratfor з ізраїльською національною розвідслужбою Моссад. Після скандального витоку даних компанія була змушена запевняти своїх клієнтів, що посилить заходи безпеки, також запропонувала двотижневу безкоштовну передплату на нові розсилки. Зважаючи на напівпублічний характер агентурної мережі компанії, її часткове розкриття не призвело до великих втрат цієї мережі чи до втрати репутації ПРК.

У 2015 році Дж. Фрідман став засновником і керівником нової ПРК – Geopolitical Futures (GPF). Аналіз відкритих публікацій компанії та висловлювань цього провідного експерта свідчить про певні зміни в його політичних симпатіях, що, можливо, й спону-

кало Дж. Фрідмана піти зі Stratfor, а також про непослідовність у стратегічних прогнозах [5].

У травні 2000 року була створена The Arkin Group LLC (TAG) [6]. Засновники цієї ПРК – колишній начальник глобальних операцій ЦРУ та відомий нью-йоркський юрист Стенлі Аркін. TAG спеціалізується на міжнародному кризовому управлінні, стратегічній розвідці, слідчих дослідженнях та вирішенні бізнес-проблем, що здійснюється у спосіб використання стратегічної інформації, прогностичного аналізу й даних HUMINT.

Джек Девайн – партнер-засновник та президент The Arkin Group LLC є 32-річним ветераном ЦРУ. Він обіймав посади виконувача обов'язків директора та заступника директора з операцій ЦРУ за межами США з 1993 по 1995 рік, де здійснював нагляд над тисячами співробітників ЦРУ, які брали участь у секретних місіях по всьому світу. Крім того, у 1992 -1993 роках Девайн обіймав посаду начальника Латиноамериканського відділу і був головним менеджером секретних проектів ЦРУ в Латинській Америці. У період з 1990 по 1992 рік Девайн очолював Центр боротьби з наркотиками ЦРУ, який відповідав за координацію та побудову тісної співпраці між усіма основними правоохоронними органами США та інших країн у відстеженні світових наркоторговців та злочинних організацій. З 1985 по 1987 рік очолював Афганську оперативну групу ЦРУ, яка успішно протистояла радянській агресії у регіоні. 1987 року за це досягнення був відзнач ений нагородою ЦРУ «Заслужений офіцер».

Міжнародний досвід Девайна в уряді США включав відрядження до Латинської Америки та Європи. За більш як 30 років роботи в ЦРУ він брав участь в організації, плануванні та виконанні великої кількості секретних проєктів практично у всіх галузях розвідки, включаючи аналіз, операції, технології та управління. Девайн нагороджений медаллю «За видатні заслуги у розвідці» Агентства та кількома почесними нагородами. Він визнаний експерт у питаннях розвідки і писав статті-огляди для The Washington Post, The Wall Street Journal, The Financial Times, Foreign Affairs Magazine, The World Policy Journal, Politico та The Atlantic Monthly. Він також виступав як гість у National Press Club, CNN, CBS, NBC, MSNBC, Fox News, CSPAN, Bloomberg News, а також на каналах History та Discovery, PBS, NPR та ABC Radio.

У приватному секторі Девайн раніше працював у Kohl's Cyber Security Advisory Group, SAP National Security Services (NS2) Advisory Board, CyberCore Advisory Board та Secretary of Navy Advisory Board. Він проживає в Нью-Йорку і є членом Ради з міжнародних відносин, володіє іспанською та італійською мовами. Книга Девайна «Good Hunting! An American Spymaster's Story», бестселер New York Times, була опублікована у червні 2014 року. Вона присвячена його кар'єрі в Агентстві та ролі таємних операцій у минулому та майбутньому.

Команда TAG об'єднує фахівців із найкращих американських університетів та аспірантських програм і має досвід роботи в ключових державних установах США, міжнародних організаціях і провідних консалтингових фірмах. У своїй діяльності ПРК спирається на широкі національні та міжнародні мережі регіональних і функціональних експертів, у тому числі спеціалістів із розвідки, правоохоронних органів, дипломатів і політиків, промислових, бізнес- і фінансових аналітиків, провідних науковців, журналістів і спеціалізованих експертів із судової експертизи та безпеки. Спеціалізація TAG: бізнес-аналітика, незалежна перевірка компаній, криміналістичні розслідування, стратегічне кризове консультування, аналіз політичних ризиків, безпека та готовність. Місія ПРК – використовувати стратегічну розвідку та прогнозний аналіз, щоб дозволити клієнтам мінімізувати ризики та максимізувати виплати під час прийняття важливих бізнес-рішень. Вона виконала сотні завдань у кожному регіоні Земної кулі. TAG відрізняється індивідуальним підходом та індивідуальними послугами. Для кожного завдання ПРК створює унікальний план гри для досягнення конкретних цілей клієнта. Незважаючи на те, що вона покладається на широкий спектр слідчих, криміналістичних, комунікаційних і безпекових інструментів, відмінними рисами методології TAG є обґрунтований аналіз і добре отримані людські дані.

У лютому 2009 року з'явилася ще одна американська ПРК – The Chertoff Group [7]. Це спеціалізована консалтингова компанія фірма, яка є світовим лідером у сфері безпеки та управління ризиками. Засновниками та основними співробітниками стали колишні високопосадовці США: Майкл Чертофф, міністр внутрішньої безпеки (2005–2009); Майкл Вінсент Хейден, чотиризірковий генерал, директор АНБ (1999–2005), перший заступник директо-

ра національної розвідки (2005–2006), директор ЦРУ (2006–2009); Чед Світ, керівник штабу Міністерства внутрішньої безпеки (2005–2009), колишній співробітник ЦРУ; Чарльз Аллен, заступник міністра внутрішньої безпеки з питань розвідки та аналізу (2005–2009), колишній помічник директора ЦРУ; Джей Коен, контрадмірал, заступник міністра внутрішньої безпеки з питань науки і технологій (2006–2009). Команда визнаних експертів The Chertoff Group з різноманітним досвідом у сфері безпеки в приватному та державному секторах допомагає організаціям керувати кібернетичними, фізичними, регуляторними та геополітичними ризиками. Завдяки практиці розвитку бізнесу вона допомагає своїм клієнтам отримати конкурентну перевагу та прискорити зростання.

До складу Chertoff Group входять:

• інвестиційно-банківська дочірня компанія Chertoff Capital, яка надає консультації щодо злиття та поглинання (M&A, Mergers and Acquisitions) компаніям у сфері оборонних технологій, державних послуг і ринків кібербезпеки;

• Merchant Banking Practice, що має підтверджену історію консультування щодо майже 8 мільярдів доларів у закритих транзакціях M&A, надає інтегровані інвестиційні банківські послуги та інвестиції капіталу для швидкозростаючих, орієнтованих на місію компаній у сфері національної безпеки, кібербезпеки та уряду ринки технологій;

• дочірня компанія MC2 Investment Management, LLC, яка пропонує капітал для зростання через фонд прямих інвестицій MC2 Security Fund, що здійснює інвестиції в акціонерний капітал компаній, котрі швидко розвиваються та мають високий потенціал у сфері кібербезпеки, національної безпеки, оборонних технологій та державних послуг. Фонд безпеки MC2 здійснює інвестиції безпосередньо або через компанії спеціального призначення, такі, як MC2 Titanium, LLC.

The Chertoff Group обслуговує підприємства зі списку Fortune 500 у різних секторах, а також малий і середній бізнес зі спеціальними потребами. Робота експертів і фахівців ПРК ґрунтується на передбаченні того, що буде далі, застосуванні передового досвіду та демонстрації цінності. Її досвічена команда допомагає організаціям керувати кібернетичними, фізичними, транспортними та геополітичними ризиками; розвивати стійкість; орієнтуватися в

змінних нормативних вимогах і вимогах відповідності; і відкривати можливості для ведення бізнесу та створення цінності.

The Chertoff Group є однією з небагатьох професійних компаній у світі, яка отримала статус БЕЗПЕКИ відповідно до Закону Міністерства внутрішньої безпеки США за перевірену методологію консультування з управління ризиками безпеки. Вона розробила власну методологію, щоб дати можливість організаціям оцінювати, пом'якшувати та контролювати ризики фізичної та кібербезпеки для своїх людей, об'єктів і технологічних активів, а також для бізнес-операцій, які вони підтримують.

Місія The Chertoff Group полягає в застосуванні свого досвіду у сфері безпеки, технологій і політики, щоб допомагати клієнтам створити стійкі організації, отримати конкурентну перевагу та прискорити зростання. Для цього вона має такі можливості:

♦ 360-градусний огляд ризиків безпеки

• глобальне середовище ризиків безпеки;

• бізнес-ринки та інвестиційні можливості технологій безпеки та безпеки;

• політична та нормативна взаємодія;

♦ інтегрована консультативна модель повного життєвого циклу

• управління ризиками безпеки;

• стратегії органічного та неорганічного зростання;

• події транзакційної ліквідності;

• інвестування в акціонерний капітал.

Конкурентними перевагами The Chertoff Group є: перевірена методологія консультування з управління ризиками безпеки; продемонстрований успіх у зниженні загального ризику безпеки; (прибрав) надання клієнтам можливості вимірювати та повідомляти про ефективність своїх програм управління ризиками; прагматичний підхід, заснований на досвіді операторів безпеки та розробників політики; можливість перетворити знання безпеки на створення цінності для клієнтів; наявність міцної глобальної мережі стратегічних відносин і надійних партнерів: доступ до великих обсягів капіталу зростання та синдикатів інвесторів.

Оскільки використання ПРК у розвідувальній діяльності США мало й деякі побічні ефекти, то у серпні 2009 року в Національному прес-клубі відбулася експертна дискусія, учасники якої обговорили цю проблему з керівниками The Chertoff Group та The Arkin

Group. Експертів насамперед цікавили відповіді на два запитання: чи загрожують інтересам національної безпеки та майбутньому розвідувального співтовариства така приватизація; проблема «переманювання» значної кількості співробітників розвідки до приватних фірм, де вони використовують свої професійні знання та навички. Під час дискусії наводилися дані про те, що розвідувальні служби США передоручають виконувати частину своїх традиційних функцій «підрядникам», на оплату роботи яких витрачаються значні кошти, наприклад ЦРУ витрачає понад 30 % річного бюджету. Крім того, ПРК «переманили» дві третини високопоставлених співробітників Міністерства внутрішньої безпеки, які мають широкі контакти в різних колах, значний професійний досвід та знання про механізм роботи державних органів.

Особливо напружені дискусії точилися навколо проблеми секретних програм ЦРУ, в рамках яких, наприклад, приватна військова компанія Blackwater USA (із січня 2010 року – Academi) 2004 року отримала контракт на фізичну ліквідацію лідерів Аль-Каїди. За даними американських ЗМІ, метою такого кроку було виведення співробітників ЦРУ з-під можливої кримінальної відповідальності в разі провалу операції чи інших непередбачених обставин.

Учасники дискусії дійшли висновку, що дії «підрядників», яких наймають федеральні органи, повинні відповідати таким же жорстким моральним та юридичним нормам, що й дії співробітників розвідувального співтовариства. Вирішальним чинником під час наймання ПРК чи окремих осіб є їхня унікальна кваліфікація або навички, на оволодіння якими може піти багато часу. Крім того, до «підрядників» звертаються зазвичай тоді, коли виникає тимчасова потреба в знаннях і вміннях у певній сфері. У цих випадках наймання спеціалістів заощаджує час і ресурси, оскільки «підрядники» не є постійними співробітниками, їх можна легко замінити за потреби. Це особливо актуально, коли законодавці ставлять перед розвідувальним співтовариством завдання, що потребують значних витрат, але при цьому скорочують бюджет.

Як зазначив керівник The Arkin Group Дж. Девін, наприкінці 1990-х років Конгрес скоротив бюджет ЦРУ на 25 %. Це означало, що на момент терактів 11 вересня 2001 року людські та матеріальні ресурси цього розвідувального органу були недостатні для швид-

кого й ефективного виконання його функцій. Задля вирішення проблеми керівництво вдалося до масового використання «підрядників». Проте їм передавалися не всі функції, відповідно всередині ЦРУ розроблялися концепції завдань та здійснювався менеджмент і контроль за їх виконанням. Водночас Дж. Девін заперечив, що американська розвідка практикувала наймання ПРК для ліквідації терористів (принаймні за час його 32-річної служби в ЦРУ).

Генерал М. Хейден (The Chertoff Group) закликав не проводити межу між державними органами та представниками приватного бізнесу, значна частка яких готова ризикувати без грошової винагороди, щоб допомогти забезпечувати національну безпеку. Він також наголосив, що відсутність вичерпних даних про осіб та компанії, які працюють за урядовими контрактами у сфері розвідки та безпеки, зумовлена необхідністю захисту джерел інформації. Такий підхід має бути зрозумілий, зокрема представникам ЗМІ, котрі виявляють до цього питання підвищений інтерес.

Нині Велика Британія є лідером у наданні приватних послуг розвідувального характеру на Європейському континенті. За оцінками експертів, кілька років тому бюджет галузі ПРК, розташованих лише в Лондоні, наближався до 20 млрд доларів США. Варто охарактеризувати роботу деяких відомих ПРК, що діють на теренах Великої Британії.

SCL Group (Strategic Communication Laboratories) – приватна британська компанія поведінкових досліджень та стратегічних комунікацій, була зареєстрована в Companies House 20 липня 2005 року Найджелом Оуксом, який був її генеральним директором [8]. Компанія позиціонувала себе як «глобальне агентство з управління виборами». Керівники та власники компанії мали тісні зв'язки з Консервативною партією, британською королівською сім'єю, британськими військовими, Міністерством оборони США та НАТО, а серед її інвесторів були деякі з найбільших спонсорів Консервативної партії.

У 1990 році Найджел Оукс, який мав досвід роботи у сфері телевиробництва та реклами, заснував Behavioral Dynamics Institute (BDI) – Інститут поведінкової динаміки як дослідницький центр для стратегічної комунікації [9]. Оукс вважав, що для зміни громадської думки слід застосовувати академічні ідеї, отримані психологами та антропологами в BDI, і це буде успішнішим, ніж традицій-

ні методи реклами. Вивчення масової поведінки та того, як її змінити, призвело до створення Strategic Communication Laboratories (SCL Group) – Лабораторій стратегічної комунікації, а BDI став її некомерційною філією SCL Group. Серед інвесторів у SCL Group був банкір Пол Девід Ешбернер Нікс, чий син Олександр Нікс мав стати близьким соратником Оукса. Одним із колишніх директорів є лорд Івар Маунтбеттен. Серед інвесторів компанії були Джонатан Марланд, Барон Марланд і Роджер Габб, великий спонсор Консервативної партії, який був зареєстрований як такий, що має значний контроль над компанією станом на 2018 рік.

Після початкового комерційного успіху SCL Group розширила свою присутність на військових та політичних аренах. Вона стала відома передбачуваною участю у військових дезінформаційних кампаніях із брендингу в соціальних мережах та таргетування виборців. SCL Group почала фокусуватися на виборах у країнах, що розвиваються, залучалася їх військовими та політиками для вивчення та маніпулювання громадською думкою та політичною волею. Для цього ПРК використовувала те, що називалося «психологічними операціями», щоб отримати уявлення про мислення цільової аудиторії. Вона проводила інтелектуальний аналіз даних та аналіз даних про свою аудиторію. Грунтуючись на результатах, націлювала комунікації спеціально на ключові групи аудиторії, щоб змінити поведінку відповідно до вимог своїх замовників. На початок 1990-х років ПРК брала участь у психологічній війні у військових контекстах як підрядник для американських і британських військових під час війни в Афганістані та війни в Іраку.

У 2005 році на виставці Defence and Security Equipment International (DSEI) – найбільшій виставці військових технологій у Сполученому Королівстві, SCL Group продемонструвала свої можливості в «операціях впливу», показавши, як можна допомогти організувати складну кампанію масового обману громадськості такого великого міста, як Лондон. SCL Group стверджує, що її методологію було схвалено, серед іншого, агенствами уряду Сполученого Королівства та федерального уряду Сполучених Штатів.

Згідно з інформацією на її веб-сайті, з 1994 року SCL Group взяла участь у понад 25 міжнародних політичних та виборчих кампаніях та впливала на вибори в Італії, Латвії, Україні, Албанії, Румунії, Південній Африці, Нігерії, Кенії, Маврикії, Індії, Індоне-

зії, Філіппінах, Таїланді, Тайвані, Колумбії, Антигуа, Сент-Вінсенті та Гренадінах, Сент-Кітсі та Невісі, Тринідаді та Тобаго.

У 2013 році SCL Group заснувала дочірню компанію Cambridge Analytica, яка спеціалізується на наданні консалтингових послуг у політичній сфері, використовуючи при цьому технології глибинного аналізу даних, зокрема із соціальних мереж для розроблення стратегічної комунікації в мережі Інтернет під час виборчих кампаній [10]. Ці технології засновані на алгоритмах, опрацьованих співробітником Кембриджського університету Міхалом Косінським, які дозволяють створювати психологічні портрети користувачів вебресурсів.

Ця ПРК була створена для участі у виборчому процесі у Сполучених Штатах та брала участь у 44 виборах до Конгресу США, Сенату США та виборах на рівні штатів на проміжних виборах 2014 року. У 2015 році компанія брала участь у попередніх виборах президента Республіканської партії на виборах 2016 року, насамперед на підтримку Теда Круза.

Cambridge Analytica значною мірою фінансувався мільярдером-хедж-фондом Робертом Мерсером, основним прихильником Круза, а потім Дональда Трампа. За повідомленням газети The Guardian, Cambridge Analytica сформувала глобальну мережу своїх джерел, «пустивши коріння» в 68 країнах світу.

Вважається, що саме Cambridge Analytica 2016 року допомогла урядові переконати населення Великої Британії проголосувати на референдумі за вихід із Європейського Союзу. В опублікованому через кілька років «Звіті про Росію», підготовленому Комітетом з питань розвідки та безпеки парламенту, йшлося про факти можливого втручання Росії у референдум щодо Брекзиту. В розслідуванні фігурувала й Cambridge Analytica. Варто зазначити, що у 2017 році до послуг цієї компанії звертався російський Сбербанк задля покращення системи оцінювання кредитоспроможності (кредитних ризиків) клієнтів.

У 2018 році Cambridge Analytica опинилася в центрі міжнародного скандалу: стало відомо, що компанія незаконно отримала доступ до даних 87 млн користувачів Facebook, працюючи на виборчу кампанію президента США Дональда Трампа. Крім того, британський телеканал «Channel 4» оприлюднив запис розмов із менеджерами ПРК, з яких можна дійти висновку, що співробітни-

ки СА вдаються до хабарів для дискредитації політичних діячів. Скандал призвів до того, що мережа Facebook закрила доступ до будь-яких послуг для Cambridge Analytica, а сама компанія опинилася під слідством урядів (виправив) Великобританії та США. Відтоді компанія була розформована та куплена Emerdata Limited. У 2019 році Федеральна торгова комісія (FTC) подала адміністративну скаргу на Cambridge Analytica за неправомірне використання даних, одночасно уклавши мирові угоди з її колишнім генеральним директором Олександром Ніксом та розробником додатків Олександром Коганом, в яких вони погодилися видалити незаконно отримані дані.

У 2020 році Олександр Нікс підписав дискваліфікаційне зобов'язання, ухвалене Алоком Шармою, державним секретарем з бізнесу, енергетики та промислової стратегії 14 вересня 2020 року. Починаючи з 5 жовтня 2020 року Олександр Нікс дискваліфікований на сім років від виконання обов'язків директора або прямої чи непрямої участі без дозволу суду в просуванні, формуванні або управлінні британською компанією.

ПРК Emerdata Limited була заснована у серпні 2017 року групою людей, пов'язаних із Cambridge Analytica. Emerdata, директором за даними та головою материнської компанії Cambridge Analytica SCL Group, яка припинила свою діяльність 1 травня 2018 року [11]. Її штаб-квартира в Лондоні знаходиться в тій самій будівлі, що й Cambridge Analytica. Було зазначено, що компанія пропонує аналогічні послуги, що й SCL Group та Cambridge Analytica.

До ради директорів Emerdata увійшли співробітник Frontier Services Group Джонсон Чун Шун Ко, гонконзький бізнесмен, пов'язаний з Еріком Прінсом (засновником Blackwater), інвестор Cambridge Analytica Ребекка Мерсер і генеральний директор Cambridge Analytica Олександр Нікс. У січні 2018 року Emerdata Limited залучила 19 мільйонів доларів від міжнародних інвесторів і широко обговорювалася в ЗМІ. Її зображували як потенційного наступника Cambridge Analytica. У травні 2018 року Найджел Оукс, засновник SCL Group, британської філії Cambridge Analytica, визнав, що наміром Emerdata було придбати Cambridge Analytica і SCL, але сказав, що ці плани були покинуті, що Emerdata та її частка, що належить дочірній компанії Firecrest Technologies Ltd.

яка була створена колишнім генеральним директором Cambridge Analytica Олександром Ніксом, будуть ліквідовані.

У липні 2019 року з'ясувалося, що Emerdata повністю придбала ці компанії, сплачувала юридичні рахунки компаній SCL в умовах процедур банкрутства, розслідувань та судових позовів по обидва боки Атлантики, а також заплатила мільйони, щоб придбати те, що залишилося від компаній, доки вони перебували у процесі ліквідації.

У контексті дослідження інтерес становить діяльність кількох ізраїльських ПРК. Psy-Group була заснована у 2014 р. Рої Бурштейном колишнім підполковником ізраїльської армії, який очолював спеціальний підрозділ розвідки при уряді країни, і він став генеральним директором цієї ПРК [12]. Власником був Джоел Замель – австралійський єврей, який розбагатів на видобутку корисних копалин. Серед радників – колишній заступник директора Моссада Рам Бен-Барак, а також Яаков Амідрор – колишній голова Ради національної безпеки при канцелярії Біньяміна Нетаньяху. Юридичний радник компанії – Даніель Рейзнер.

Psy-Group займалася управлінням сприйняттям в Інтернеті, кампаніями з впливу/маніпулювання у соціальних мережах, дослідженнями опозиції, пастками-медовиками та таємними заходами на місцях для клієнтів. Psy-Group інколи називали «приватною службою Моссад».

У 2016 році ПРК запустила проект «Метелик», покликаний боротися з BDS на території американських університетів. Psy-Group запропонувала своїм спонсорам підірвати зсередини стабільність організацій, які просувають бойкот Ізраїлю. Співробітники компанії шукали в соціальних мережах та у відкритому доступі, а також у так званій «темній мережі» (Dark Web) інформацію, що ганьбить активістів BDS або покликану посіяти розбрат у лавах BDS-рухів.

Як приклад журналісти The New Yorker наводять публікації фотографії мусульман, які розпивають алкоголь або змінюють своїх дружин. Результати роботи Psy-Group завжди публікувалися таким чином, щоб їх не можна було пов'язати ні з фірмою, ні з її замовниками. Загалом у проєкт, за даними The New Yorker, було вкладено 2,5 мільйона доларів, і боротьба з BDS поширилася на 10 великих американських університетів.

Psy-Group була фінансово пов'язана з Групою компаній «Метрополь», керівником якої є російський мільйонер Михайло Слепенчук, колишній депутат Державної думи рф від партії «Єдина Росія». Свого часу Psy-Group надавала послуги російським олігархам Олегу Дерипасці та Дмитру Риболовлєву, заступникові керівника Служби загальної розвідки Саудівської Аравії генерал-майору Ахмеду аль-Ассірі (причетному до вбивства журналіста Джамаля Хашоґджі) та корумпованому президентові Габону Алі Бонго Ондімбі. Крім того, у червні 2016 році Дж. Замель брав участь у Петербурзькому міжнародному економічному форумі, який проводиться за участю президента рф.

У 2016 році ця ПРК співпрацювала з британською Cambridge Analytica під час виборчої кампанії президента США Дональда Трампа. Джоел Замель зустрічався з Дональдом Трампом-молодшим та Джаредом Кушнером, пропонуючи їм розпочати інтернет-кампанію зі знищення політичної репутації суперників Трампа (співробітники Psy-Group як мінімум один раз провели таку операцію напередодні парламентських виборів в одній з європейських країн). В рамках цієї кампанії використовувалися такі методи: проникнення в цільову аудиторію в соціальних мережах спеціально створених фейкових учасників; поширення оманливої інформації через вебсайти, що імітували новинні портали; дискредитація політичних опонентів завдяки організації вручення хабарів чи звинувачень у сексуальних домаганнях. Діяльність Psy-Group пізніше стала частиною розслідування ФБР та Спеціального комітету в справах розвідки Сенату щодо можливого втручання росії в президентські вибори у США.

У 2017 році ПРК провела кампанію з дезінформації проти українського Центру протидії корупції (ЦПК), спрямовану проти голови правління Віталія Шабуніна та виконавчої директорки організації Дар'ї Каленюк. Організована PSY Group кампанія з дискредитації членів ЦПК призвела до того, що як мінімум два відео на YouTube розповсюджували неправдиву інформацію про українських активістів. Два повністю фейкові «випуски англомовних новин» були розміщені на каналі Storozh Ukraina і мають понад 20000 переглядів, що свідчить про розкручування відео через рекламу. Storozh Ukraina – ще одне анонімне об'єднання громадян, які «викривають» антикорупціонерів.

У березні 2017 року високопосадовці Саудівської Аравії, близькі до наслідного принца Мухаммеда бін Салмана, пропонували кільком ПРК за 2 млрд доларів організувати низку замовних убивств. Зокрема, йшлося про командувача спецпідрозділом «Аль-Кудс» Корпусу стражів Ісламської революції Ірану генерала Касема Сулеймані. На зустрічі були присутні вищезгадані заступник керівника Служби загальної розвідки Саудівської Аравії генерал-майор Ахмед аль-Ассірі та Дж. Замель, який нібито відмовився від такої пропозиції. Але слід зазначити, що К. Сулеймані був ліквідований 3 січня 2020 року точковим авіаударом ВПС США. За деякими даними, інформацію про місцезнаходження генерала американській стороні надала служба Моссад.

У 2018 році, після того, як діяльністю Psy-Group зацікавилася комісія спеціального прокурора Роберта Мюллера, Дж. Замель був змушений її закрити, і окремі співробітники перейшли до компанії Black Cube, діяльність якої пов'язана зі справою Харві Вайнштейна та зі збором компромату на Барака Обаму. Натомість сам Дж. Замель залишається керівником Групи компаній «Zamel», до складу якої входить ПРК Wikistrat, заснована 2010 року в США [13]. У 2014–2017 рр. її директором зі стратегічного розвитку був колишній співробітник ізраїльської розвідки Шая Гершковіц. Напрям діяльності Wikistrat: геостратегічний консалтинг з використанням краудсорсингу (залучення широкого кола осіб для використання їхніх творчих здібностей, знань та досвіду на кшталт субпідрядної роботи на добровільних засадах із застосуванням інформаційних технологій).

ПРК White Knight Group, яка фактично є правонаступницею Psy-Group, була заснована у 2017 році [14]. Спеціалізація цієї ПРК: кампанії у соціальних мережах, акції впливу, управління виборчими кампаніями. Група також є активним інвестором у транснаціональні інфраструктурні проєкти, включно зі сферою розвитку штучного інтелекту та сектором кібербезпеки, особливо для компаній Центральної та Східної Європи. Подібні до Psy-Group методи: онлайн-управління сприйняттям, вплив через соціальні мережі, маніпулятивні кампанії, стратегічна дезінформація (наприклад, підготовка фейкових новин чи пропагандистської продукції), політичні кампанії з використанням соціальних медіа

та штучного інтелекту. Те ж саме використовують інші ізраїльські ПРК – Archimedes Group та Black Cube [15, 16].

Тактика діяльності Archimedes Group, орієнтованої на низку африканських держав, Латинську Америку та Південно-Східну Азію, дуже нагадує тактику інформаційної війни, яку часто використовують уряди окремих країн, зокрема росії. Зі свого боку, Black Cube прослуховувала неурядові організації Угорщини напередодні виборчої кампанії навесні 2018 року з метою зібрати компромат для передачі штабу прем'єр-міністра країни Віктора Орбана.

Деякі ПРК спеціалізуються на технічному забезпеченні розвідувальної діяльності. Однією з них є ізраїльсько-американська Verint Systems Inc., яка існує з 1994 року, штат оцінюється у 5–10 тис. співробітників [17]. 2017 року вона купила невелику ПРК «Terrogence», створену в 2005 році колишнім офіцером контррозвідки «Шин Бет» Шаєм Арбелем [18]. Обидві компанії активно укладають контракти з урядом США щодо забезпечення АНБ та інших спецслужб новітніми шпигунськими технологіями. Серед таких технологій – сервіс «Face-Int», призначений для розпізнавання облич, заснований на базі даних багатьох тисяч осіб, які підозрюються в протиправній діяльності. ПРК «Terrogence» активно відстежувала та збирала в Інтернеті інформацію про терористів та інших осіб, які становили загрозу національній безпеці (зокрема, у сфері безпеки авіаперевезень, імміграції тощо). Джерелами таких даних називалися мережі YouTube, Facebook, а також різні відкриті та закриті форуми. У квітні 2018 року інформація про сервіс «Face-Int» зникла із сайту Terrogence, проте можна вважати, що компанія і досі продовжує надавати такі послуги, а як джерела інформації використовує більше ресурсів, ніж офіційно було відомо. Точно невідомо, на базі якої технології сервіс «Face-Int» отримує зображення облич, але опис програми нагадує один із проєктів АНБ США, розкритий Едвардом Сноуденом у 2014 році. Ця спецслужба за три роки існування проєкту зібрала 55 тис. якісних знімків розпізнаних облич. Схоже, що Terrogence порушує політику Facebook, згідно з якою заборонено використання для стеження за користувачами даних, отриманих із соціальної мережі. Не дозволяється також використання будь-яких автоматизованих методів збирання інформації, наприклад ботів.

Немає свідчень про те, що американський уряд може використовувати сервіс «Face-Int», проте відкриті дані свідчать про наявність у компанії «Terrogence» принаймні двох державних контрактів із ВМС США на загальну суму майже 150 тис. доларів. Ця сума еквівалентна річній передплаті на два сервіси цієї ПРК – «Mobius» та «TGAlertS». Сервіс «Mobius» є добіркою матеріалів із різних соціальних мереж та платформ про останні тренди щодо вибухових пристроїв, створених терористами, та способів їх застосування, а «TGAlertS» містить оперативну інформацію про деякі важливі події, отриману співробітниками Terrogence з Інтернету.

Хоча основним напрямом діяльності Terrogence є співпраця з розвідслужбами та правоохоронними органами для боротьби з тероризмом, проте у профілях колишніх співробітників компанії у LinkedIn можна знайти згадки про «роботу з громадською думкою для урядових клієнтів» та використання «методів роботи в соціальних мережах для вивчення політичних та соціальних груп».

Ще одним напрямом діяльності ПРК, подібних до Terrogence, що викликає занепокоєння громадськості, є створення різних «чорних списків». У 2018 році Verint запустила іншу програму розпізнавання облич – «FaceDetect», яка уможливлює ідентифікацію людини, незважаючи на її національність, будь-які перешкоди, старіння об'єкта, маскування, і миттєво вносить дані до реєстру осіб, які розшукуються. Основною проблемою подібних реєстрів, котрі створюють держави, є алгоритм потрапляння до них конкретних людей та сфера застосування зібраних даних.

У лютому 2021 р. Amnesty International повідомила, що Verint Systems надала Службі національної безпеки Південного Судану обладнання для перехоплення каналів зв'язку. Цю спецслужбу звинувачують у переслідуванні, залякуванні, свавільному затриманні та, у деяких випадках, насильницькому зникненні, навіть убивствах політичних противників режиму.

Об'єднані Арабські Емірати (ОАЄ) також мають свою ПРК DarkMatter Group (DarkMatter), яка заснована 2014 році емірацьким бізнесменом Фейсалом аль-Баннаі, засновником постачальника мобільних телефонів Axiom Telecom и сином генерал-майора поліції емірату Дубай [19]. Ця ПРК позиціонувала себе як компанія з комп'ютерної безпеки, що займається виключно оборонними заходами, але деякі експерти стверджують, що DarkMatter

причетна до «наступальних» заходів, тобто зламу комп'ютерних мереж, кібернетичних атак, незаконного отримання доступу до даних в мережі Інтернеті, зокрема в інтересах уряду ОАЄ. В тому ж 2014 році розпочала свою діяльність у Фінляндії дочірня компанія DarkMatter – Zeline 1. Свій штат вона формувала з колишніх співробітників АНБ та офіцерів технічних підрозділів Армії оборони Ізраїлю, пропонуючи їм до 1 млн доларів у рік.

Публічний старт DarkMatter відбувся у 2015 році на 2-му щорічному саміті Arab Future Cities. На той час компанія рекламувала такі можливості, як мережева безпека та усунення помилок, а також обіцяла створити новий «захищений» мобільний телефон і позиціонувала себе як «цифрову оборонну та розвідувальну службу» для ОАЕ.

У 2016 році з'явилися повідомлення про те, що компанія CyberPoint, яка працювала на уряд ОАЕ, уклала контракт з італійською компанією-розробником шпигунського ПЗ Hacking Team, що підірвало репутацію CyberPoint як фірми, що займається кібербезпекою. ОАЕ незадоволені тим, що покладаються на американського підрядника, замінили CyberPoint на DarkMatter, яка стала підрядником проєкту Raven замість компанії CyberPoint. Цей проєкт був конфіденційною ініціативою, покликаною допомогти владі ОАЕ стежити за урядами інших країн, терористами та політичними противниками. До його команди входили колишні агенти розвідки США, які застосовували свою підготовку для зламання телефонів та комп'ютерів, які належать жертвам проєкту Raven. Операція проводилася в переобладнаному особняку в передмісті Абу-Дабі в Халіфа-Сіті, яке називалося «Вілла». Проєкт Raven виник у 2008 році як Відділ досліджень, експлуатації та аналізу розвитку (DREAD), створений Річардом А. Кларком через його консультативну групу з безпеки Good Harbor Consulting як підрозділ королівського двору ОАЕ Мохамеда бін Заїда Аль Нахайяна. До кінця 2010 року Good Harbor відійшов від DREAD, поступившись контролем Карлу Гамтоу, співзасновнику та генеральному директору CyberPoint. З 2014 до 2016 року CyberPoint постачала проєкту Raven підрядників, навчених у США. Після цього проєкт Raven розширив своє стеження, включивши до неї американців, що потенційно залучали її американських співробітників до протиправної поведінки. Наприклад, DarkMatter зламав електронне

листування між першою леді Мішель Обамою та колишнім міністром Катару щодо поїздки Мішель Обами та Конана О'Браєна до Катару в листопаді 2015 року. Обама та О'Брайєн відвідали авіабазу Аль-Удейд, на якій розміщується передова штаб-квартира Центрального командування США та 83-а експедиційна авіагрупа Королівських ВПС. Крім того, авіабаза служила штаб-квартирою Центрального командування ВПС США під час воєн в Іраку та Афганістані. DarkMatter був дуже зацікавлений у зламі комп'ютерів Катару, щоб отримати та прочитати його електронні повідомлення, оскільки вважалося, що Катар підтримує Братів-мусульман. Після публікації статті The Intercept від 24 жовтня 2016 року, де розкривається стеження DarkMatter, Самер Халіфе, фінансовий директор DarkMatter, перевів деяких громадян США з DarkMatter до нової компанії Connection Systems.

Того ж року проєкт Raven купив інструмент під назвою Karma. Karma могла віддалено експлуатувати Apple iPhone у будь-якій точці світу, не вимагаючи жодної взаємодії з боку власника iPhone, доки було вказано ім'я користувача, таке, як Apple ID, адреса електронної пошти, пов'язана з телефоном, або номер телефону. Оперативники проєкту Raven могли переглядати паролі, електронні листи, текстові повідомлення, фотографії та дані про місцезнаходження зі скомпрометованим iPhone. Серед людей, чиї мобільні телефони були навмисно зламані за допомогою Karma, були Емір Катару шейх Тамім бін Хамад Аль Тані, Хамад бін Халіфа Аль Тані, а також його брат та кілька інших наближених; Надя Мансур, дружина ув'язненого активіста з прав людини з ОАЕ Ахмеда Мансура; британський журналіст Рорі Донагі; прем'єр-міністр Лівану Саад Харірі; Лауреат Нобелівської премії з Ємену Тавакуль Карман (лідер Арабської весни); сотні інших користувачів айфонів у Європі та на Близькому Сході, включаючи уряди Катару, Ємену, Кувейту, Оману, Сербії, Лівану, Ірану та Туреччини.

Також у 2016 році DarkMatter шукала експертів із розробки смартфонів у Оулу (Фінляндія) та найняла кількох фінських інженерів. Вона розробила модель смартфона під назвою Katim, що в перекладі з арабської означає «тиша». У 2021 році кіберактивність DarkMatter була передана компанії Digital14 із штаб-квартирою в Абу-Дабі, яка поширювала захищену систему зв'язку «Katim». Digital 14 позиціонує себе як одну з провідних компаній з кібер-

безпеки на Близькому Сході, що обслуговує клієнтів із державних, енергетичних, транспортних, фінансових та медичних секторів.

На початку 2018 року оборот DarkMatter становив сотні мільйонів доларів. Відомо, що 80 % контрактів ПРК припадає на урядові структури ОАЕ, включно з Агентством радіотехнічної розвідки (SIA), раніше відомим як Національне управління електронної безпеки (NESA). Ця спецслужба є розвідувальною агенцією ОАЄ – аналогом АНБ, яка створена в 2011 році за допомогою США у відповідь на ймовірне кібершпигунство з боку Ірану.

У 2018 році Фейсал аль-Баннаї підтвердив, що DarkMatter дуже тісно співпрацювала з урядом ОАЕ та була конкурентом ізраїльської фірми NSO Group. З січня 2016 року по листопад 2019 року завдяки своїм експертам – колишньому співробітнику АНБ Марку Байєру, а також Райану Адамсу та Деніелові Геріці, які працювали у військових та розвідувальних колах США, значно покращило послуги, які DarkMatter надавала уряду ОАЕ.

У січні 2020 року, на підставі матеріалів розслідування ФБР, зокрема щодо DarkMatter, за такими злочинами, як послуги цифрового шпигунства, участь у вбивстві Джамаля Хашоггі та позбавлення волі іноземних дисидентів Конгрес США ухвалив закон, запропонований у 2019 році конгресменом Максом Роузом із Нью-Йорка. Закон вимагає від розвідувального співтовариства щорічно оцінювати загрози національній безпеці, що можуть виникати через діяльність колишніх співробітників розвідки, які після звільнення зі служби працюють на іноземні фірми, організації та уряди.

У 2021 році Луджайн аль-Хатлул подала позов до окружного суду США в Орегоні проти трьох колишніх офіцерів розвідки та армії США, які проводили хакерські операції від імені ОАЕ. Згідно з позовом троє чоловіків – Марк Байєр, Райан Адамс і Деніел Геріке – працювали на DarkMatter і допомагали співробітникам служби безпеки Еміратів витягувати дані з її iPhone. Злам призвів до арешту аль-Хатлул в ОАЕ та видачі до Саудівської Аравії, де її затримали, ув'язнили і катували.

14 вересня 2021 року Марку Байєру, Райану Адамсу та Денієлу Геріке були пред'явлені звинувачення в порушенні законів США, пов'язаних із комп'ютерним шахрайством та неналежним експортом технологій. Вони погодилися на відстрочення судового переслідування в обмін на: сплату штрафів у розмірі 750 000, 600 000 та

335 000 доларів США протягом трьох років відповідно на загальну суму 1,68 мільйона доларів США; підтримку розслідувань ФБР та Міністерства юстиції; розрив зв'язків із будь-якими розвідувальними та правоохоронними органами ОАЕ; підпорядкування заборони на послуги, включаючи оборонні статті, що підпадають під Міжнародні правила торгівлі зброєю (International Traffic in Arms Regulations, ITAR), та майбутню роботу з експлуатації комп'ютерних мереж; відмова від своїх допусків до секретної інформації у США та будь-якої іноземної організації; прийняття довічної заборони майбутніх допусків до секретної інформації зі США.

У грудні 2021 року американські законодавці закликали Міністерство фінансів та Державний департамент ввести санкції проти DarkMatter, NSO Group, Nexa Technologies та Trovicor. У листі, підписаному головою фінансового комітету Сенату Роном Уайденом, головою комітету з розвідки Палати представників Адамом Шиффом та 16 іншими законодавцями, містилося прохання про запровадження глобальних санкцій Магнітського, оскільки компанії звинувачували у сприянні порушенням прав людини.

Підсумовуючи, можна зробити висновки, що для будь-якої держави стратегічно важливою є обізнаність з подіями та процесами, які відбуваються поза її межами, але можуть становити інтерес для вироблення тактики і побудови стратегії для відповідного реагування. Діяльність ПРК є вагомою з цієї точки зору. ПРК часто випереджають спецслужби у створенні та застосуванні новітніх технологій у своїй діяльності. Ці організації виступають не тільки виконавцями замовлень державних структур, а й є об'єктами, котрі становлять розвідувальний інтерес для інших країн для отримання інформації, якою вони володіють. ПРК можуть бути використані для ведення політичної боротьби. Тому їхня діяльність повинна здійснюватися під контролем з боку держави на основі спеціально створеного законодавства. Україні варто вивчати зарубіжний досвід функціонування ПРК та використовувати його для зміцнення національної безпеки держави.

**1.** Приватні розвідувальні компанії: іноземний досвід залучення приватного сектору до виконання завдань розвідки. URL: https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/pryvatni-rozviduvalni-kompaniyi-inozemnyy-dosvid-zaluchennya. **2.** Погляд з України на американську корпо-

рацію «солдатів розуму» RAND Corporation. URL: https://dss-bi.blogspot.com/2019/01/rand-corporation.html. **3.** CTC International Group. URL: https://ctcintl.com/. **4.** Strategic Forecasting Inc. URL: https://stratfor.com/ **5.** Geopolitical Futures (GPF). URL: https://geopoliticalfutures.com/welcome/ **6.** The Arkin Group. URL: https://thearkingroup.com/ **7.** The Chertoff Group. URL: https://thearkingroup.com/ **8.** Strategic Communication Laboratories. URL: https://www.devex.com/organizations/strategic-communication-laboratories-41754 **9.** Behavioral Dynamics Institute. URL: https://behavioraldynamicsinc.com/ **10.** Cambridge Analytica. URL: https://uk.wikipedia.org/wiki/Cambridge_Analytica (дата звернення 20.08.2024). **11.** Emerdata Limited. URL: https://en.wikipedia.org/wiki/Emerdata_Limited (дата звернення 26.08.2024). **12.** Psy-Group. URL: https://en.wikipedia.org/wiki/Psy-Group (дата звернення 30.08.2024). **13.** Wikistrat. URL: https://en.wikipedia.org/wiki/Wikistrat **14.** White Knight Group. URL: http://www.whiteknight.asia (дата звернення 30.08.2024). **15.** Archimedes Group. URL: https://en.wikipedia.org/wiki/Archimedes_Group **16.** Black Cube. URL: https://www.blackcube.com/ **17.** Verint Systems Inc. URL: https://en.wikipedia.org/wiki/Verint_Systems **18.** Terrogence Ltd. URL: https://www.bloomberg.com/profile/company/1251707D:IT **19.** DarkMatter Group. URL: https://en.wikipedia.org/wiki/DarkMatter_Group.

***References***

**1.** Privatni rozviduvalni kompanii: inozemnii dosvid zaluchena privatnogo sektoru do vikonany zavdan rozvidki. Retrieved from https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/pryvatni-rozviduvalni-kompaniyi-inozemnyy-dosvid-zaluchennya. **2.** Poglyd z Ukraini na amerikancky korporatsiy "soldativ rozymy" RAND Corporation. Retrieved from https://dss-bi.blogspot.com/2019/01/rand-corporation.html **3.** CTC International Group. Retrieved from https://ctcintl.com/. **4.** Strategic Forecasting Inc. Retrieved from https://stratfor.com/. **5.** Geopolitical Futures (GPF). Retrieved from https://geopoliticalfutures.com/welcome/. 6. The Arkin Group. Retrieved from https://thearkingroup.com/. **7.** The Chertoff Group. Retrieved from https://thearkingroup.com/. **8.** Strategic Communication Laboratories. Retrieved from https://www.devex.com/organizations/strategic-communication-laboratories-41754. **9.** Behavioral Dynamics Institute. Retrieved from https://behavioraldynamicsinc.com/ **10.** Cambridge Analytica. Retrieved from https://uk.wikipedia.org/wiki/Cambridge_Analytica. **11.** Emerdata Limited. Retrieved from https://en.wikipedia.org/wiki/Emerdata_Limited. **12.** Psy-Group. Retrieved from https://en.wikipedia.org/wiki/Psy-Group **13.** Wikistrat. Retrieved from https://en.wikipedia.org/wiki/Wikistrat. **14.** White Knight Group. Retrieved from http://www.whiteknight.asia. **15.** Archimedes Group. Retrieved from https://en.wikipedia.org/wiki/Archimedes_Group. **16.** Black Cube. Retrieved from https://www.blackcube.com/. **17.** Verint Systems Inc. Retrieved from https://en.wikipedia.org/wiki/Verint_Systems. **18.** Terrogence Ltd. Retrieved from https://www.bloomberg.com/profile/company/1251707D:IT.

**19.** DarkMatter Group. Retrieved from https://en.wikipedia.org/wiki/DarkMatter_Group.

***Semenyuk Yurii, Lysetskyi Yurii.*** **Public-private partnership in the sphere of intelligence activities**

Today the foreign policy of any state is based on the socio-political information known to it, the study of key problems in the political and social sphere, the analysis of strategies and tactics, the implementation of political and socio-economic transformations. Intelligence agencies are one of the main collectors and processors of this information, with the help of which the state learns about its external environment and realizes its own tasks in this area. Accordingly, civilian and military intelligence agencies focus on obtaining, analyzing, and using information, both classified and obtained from open sources. For a long time, states sought to retain the monopoly right to conduct intelligence activities. However, during the first half of the 1990s, private structures appeared that provided information and analytical services that went beyond business intelligence not only to large corporations and private individuals, but also to government structures. Such organizations were called «private intelligence companies» and public-private partnerships began to develop in this specific field of activity. According to approximate data, there are several hundred private intelligence companies operating in more than 50 countries of the world. A significant reason for their involvement in ensuring the external component of national security was that private structures are mostly more flexible and efficient than state ones, particularly in economic relations. In addition, such «contracting» of private intelligence companies made it possible to reduce state expenses for the maintenance of special services, as well as to solve some sensitive issues, hiding the direct involvement of the state in them. Therefore, their activities should be conducted under state control based on specially designed legislation. Ukraine should study the international experience of private intelligence companies and leverage it to strengthen the state.

***Key words:*** intelligence activities, intelligence agencies, national security, private intelligence companies, information and analytical services.