Тематичний Документ

НОВА РЕАЛЬНІСТЬ

Протидія Фінансуванню Самостійно Ініційованого Тероризму в Європі

Stephen Reimer та Matthew Redhead

Нова Реальність

Протидія Фінансуванню Самостійно Ініційованого Тероризму в Європі

Stephen Reimer та Matthew Redhead

Тематичний Документ RUSI, Травень 2021

RUSI EUROPE

Project craaft

Collaboration, Research & Analysis Against the Financing of Terrorism

RUSI Europe, що базується у Брюсселі, здійснює дослідження, сприяє обговоренню, просуває та інформує з усіх питань, пов'язаних з міжнародною обороною та безпекою в Європі та за її межами. RUSI Europe тісно співпрацює зі своєю міжнародною материнською організацією — RUSI, обмінюючись досвідом та розвиваючи зв'язки з міжнародними зацікавленими сторонами.

190 років незалежного аналізу в галузі оборони та безпеки

Королівський об'єднаний інститут оборонних досліджень (RUSI) — найстаріший у світі та провідний у Великій Британії аналітичний центр у сфері оборони та безпеки. Його місія полягає в тому, щоб інформувати, впливати та сприяти публічним дискусіям заради більш безпечного та стабільного світу. RUSI є науково-дослідним інститутом, що здійснює незалежний, практичний та інноваційний аналіз для реагування на сучасні складні виклики.

З моменту заснування у 1831 році RUSI спирається на підтримку своїх членів. Разом із надходженнями від дослідницької діяльності, публікацій та конференцій це дозволяє інституту вже 190 років зберігати політичну незалежність.

Цей проєкт профінансовано Фондом внутрішньої безпеки Європейського Союзу – Поліція

Опубліковано у 2021 році Королівським Об'єднаним Інститутом Оборонних Досліджень (RUSI)
Неофіційний переклад здійснено працівниками Міністерства фінансів України

Тематичний Документ RUSI, Травень 2021. ISSN 2397-0286 (Онлайн).

RUSI Європа
Avenue des Arts 46
1000 Брюссель
Бельгія
+32 (0)2 315 36 34
www.rusieurope.eu

Королівський Об'єднаний Інститут
Оборонних Досліджень
Whitehall
Лондон SW1A 2ET
Велика Британія
+44 (0)20 7747 2600
www.rusi.org
RUSI є зареєстрованою благодійною
організацією (No. 210639)

Зміст

Подяки

Автори висловлюють подяку своєму науковому асистенту Gabriel Mimoune, який підготував огляд неопублікованої літератури, що став основою для другого розділу цього документу, а також усім особам, які добровільно погодилися виступити експертами-інтерв'юерами в межах цього дослідження. Окрема подяка — анонімним рецензентам, чий зворотний зв'язок до проєкту першої версії документа був надзвичайно цінним. Автори також дякують Tom Keatinge, Alanna Putze та Kinga Redlowska за підтримку цього дослідницького проєкту, а також Isabella Chase за модерацію вебінару, під час якого було представлено деякі попередні результати дослідження. Це дослідження є частиною проєкту CRAAFT (Collaboration, Research and Analysis Against the Financing of Terrorism — Співпраця, дослідження та аналіз у сфері протидії фінансуванню тероризму).

Про Проєкт CRAAFT

Проєкт CRAAFT — це академічна дослідницька та мережева ініціатива, покликана зміцнити й покращити скоординовані спроможності ЄС та суміжних країн у сфері протидії фінансуванню тероризму. Проєкт фінансується за рахунок Фонду внутрішньої безпеки ЄС – Поліція та реалізується консорціумом під керівництвом RUSI Europe у співпраці з Амстердамським університетом, аналітичним центром GLOBSEC (Братислава) та Міжнародним центром з питань контртероризму (ICCT), розташованим у Гаазі. Докладніше: <projectcraaft.eu>.

Короткий Виклад

ЧИСЛЕННІ СМЕРТЕЛЬНІ ТЕРОРИСТИЧНІ атаки в Європі — від нападу на редакцію Charlie Hebdo у Парижі у 2015 році та вибуху на стадіоні Manchester Arena у 2016-му до збройного нападу ультраправого екстреміста в Ханау (Німеччина) на початку 2020 року — свідчать про те, що самостійно ініційований тероризм (іноді його також називають тероризмом одинаків або малих осередків) став серйозною загрозою безпеці континенту.

Значна частина сучасної «загальноприйнятої думки» щодо таких суб'єктів передбачає, що фінансування тероризму та боротьба з фінансуванням тероризму (ПФТ) не відповідають цій зростаючій загрозі. Повідомлення про атаки, які не потребували особливої підготовки чи фінансових ресурсів, сформували хибне уявлення, що діяльність терористів-одинаків не залишає жодної корисної фінансової інформації, яку можна використати в розслідуванні. Це створило значне занепокоєння серед фахівців з ПФТ у правоохоронних органах, чия роль полягає у використанні слідчих повноважень для попередження тероризму та виявлення терористів, а також серед представників фінансового сектору, чиї інструменти контролю спрямовані на виявлення та повідомлення про зловживання фінансовою системою тими, хто планує терористичні атаки. Існує природний страх: якщо приватний сектор не здатен надати релевантні фінансові розвіддані, правоохоронці не зможуть ефективно виконати свою роботу.

У зв'язку з цим Європейська комісія доручила RUSI Європа провести це дослідження в межах проєкту CRAAFT, яке має бути спрямоване на розв'язання двох пов'язаних питань:

1. Яким чином терористи, що здійснюють самостійно ініційовані атаки в Європі, здійснюють фінансову підготовку до нападів?
2. Як слід змінити систему з ПФТ, щоб ефективно реагувати на цю зростаючу терористичну загрозу?

Для відповіді на ці питання дослідницька команда проаналізувала наукову, аналітичну та медійну літературу; провела 37 напівструктурованих інтерв'ю з фахівцями; вивчила 106 випадків як здійснених, так і попереджених терористичних актів у Європі (2015–2020); провела глибинний аналіз трьох кейсів..

Ключові Висновки

Щодо питання 1:

- Планування атак терористами, що здійснюють самостійно ініційовані атаки, має фінансовий і комерційний вимір, який досі залишається недооціненим фахівцями.

- Такі терористи не обов'язково діють «невидимо» з фінансової точки зору та можуть використовувати ряд фінансових каналів та продуктів, включно з готівкою, цифровими платежами, а подекуди і новітні фінансові технології.
- Вони функціонують у досить широкій економічній екосистемі, а їх фінансова діяльність залишає певні комерційні сліди, які можуть бути помітними.

Щодо питання 2:

- Система ПФТ має базові проблеми з виявленням фінансових розвідданих через зосередженість на застарілих моделях фінансування тероризму, що особливо критично у малих за масштабами, але складних загрозах, таких як самостійно ініційований тероризм.
- Навіть якщо приватний сектор надає якісно підготовлені фінансові дані, вони часто не узгоджені з оперативними пріоритетами або не використовуються належним чином.
- Чинні ініціативи зі збору інформації, які могли б виявити потенційно корисні фінансові дані щодо терористів, що здійснюють самостійно ініційовані атаки, не були повною мірою підтримані або використані державним сектором.
- Поточні форми співпраці з ПФТ не мають гнучкості й масштабу, необхідного для проактивного реагування на самостійно ініційований тероризм.

Рекомендації

- Надзвичайно важливо, щоб Europol, Eurojust та інші відповідні агенції на рівні ЄС співпрацювали з правоохоронними та розвідувальними органами держав-членів щодо збору й аналізу чутливої та публічно недоступної фінансової і комерційної інформації у справах, пов'язаних із самостійно ініційованим тероризмом. Це дозволить сформувати обґрунтоване розуміння поведінки під час підготовки атак і створити бібліотеку типологій, які допоможуть фінансовим установам краще розуміти логістику таких подій.

- Приватний сектор і агентства ЄС мають кращі перспективи виявлення підозрілої активності у випадках, коли не використовується готівка. Тому Європейська комісія має розглянути потенційні переваги обмеження готівкових розрахунків (або запровадження вимог до ідентифікації та верифікації клієнтів) під час купівлі окремих видів високоризикових товарів, таких як декоративна або ритуальна холодна зброя, чи хімічні речовини, що можуть використовуватись для виготовлення саморобних вибухових пристроїв.

- У межах своїх ширших повноважень у сфері ПВК/ФТ Європейська комісія повинна щороку переглядати разом з відповідними агенціями ЄС, чи охоплюють її Директиви з

ПВК усі новітні фінансові технології та платформи, які потенційно можуть використовуватися злочинцями і терористами.

- Європейська Комісія має розглянути можливість розробки переліку високоризикових товарів, які вже використовувались або потенційно можуть бути використані в самостійно ініційованому тероризмі чи інших нападах, щоб надавати продавцям орієнтири для прийняття рішень про доцільність продажу.

- Європейська Комісія має також оцінити, чи доцільно заохочувати окремі типи торговельних точок, що реалізують високоризикові товари, до впровадження добровільних механізмів повідомлення про підозрілі предмети, або ж охопити їх обов'язковими вимогами моніторингу та звітності з ПВК/ФТ.

- Європейська Комісія та відповідні органи ЄС мають провести консультації щодо забезпечення того, щоб фінансові установи та інші підзвітні суб'єкти генерували більш якісні та своєчасні фінансові розвіддані щодо самостійно ініційованого тероризму. Це може включати:
    - Розробку обґрунтованих типологій самостійно ініційованого тероризму, тематичних досліджень і супровідної інформації (базуючись на роботі відповідно до першої рекомендації), що передаватимуться урядам і відомствам держав-членів та підзвітним установам з приватного сектору.
    - Дослідження використання сучасних платформ моніторингу транзакцій для ПВК/ФТ, з метою кращого аналізу діяльності клієнта і того, як нові технології можуть використовуватися для наближення установ до моніторингу в режимі реального часу, для реагування на ризики, які загрожують життю.

- Європейська Комісія та відповідні органи ЄС повинні також розглянути шляхи кращої узгодженості ПФТ-розвідки з актуальними ризиками та ефективного розповсюдження її серед усіх відповідних учасників. Це може включати:
    - Створення механізмів пріоритезації та зворотного зв'язку щодо повідомлень про підозрілі операції у сфері ПФТ між державним і приватним секторами. Відповідальні державні органи можуть встановити конкретні вимоги до типу фінансової розвідки, яку вони хочуть отримувати (наприклад, стосовно потенційної діяльності терористів, що здійснюють самостійно ініційовані атаки), і оцінювати, наскільки ці вимоги виконуються.
    - запровадження вимоги, щоб усі розвідувальні служби, залучені до протидії тероризму, стали постійною і невід'ємною частиною каналів розповсюдження й зворотного зв'язку щодо повідомлень про підозрілі операції у сфері ПФТ.

- Європейська Комісія та відповідні агенції ЄС, зокрема Europol і AMLA, мають заохочувати національні правоохоронні органи та регуляторів, а також, опосередковано, і приватний сектор до використання новітніх технологій та інструментів аналітики даних загалом і в контексті самостійно ініційованого тероризму

зокрема. Найкращим підходом до цього є формування середовищ для співпраці, такі як партнерства для обміну фінансовою розвідкою.

- Європейська Комісія повинна розглянути, як підтримати таку співпрацю, зокрема шляхом перегляду та, за потреби, розширення правових меж щодо обміну даними у сфері ПФТ відповідно до законодавства про ПВК/ФТ і захист персональних даних.

- Європейська Комісія та відповідні агенції на рівні ЄС мають переглянути можливості для створення більш гнучких і оперативних механізмів обміну розвідданими з метою проактивної ідентифікації терористів, що здійснюють самостійно ініційовані атаки. Це може включати оцінку ймовірних витрат і операційних вигод від:
    - Прямого обміну даними або моніторингу транзакцій щодо ризиків ФТ урядовими структурами, як це реалізовано у Франції, або потенційно у співпраці з приватним сектором.
    - Створення приватно-публічних аналітичних «осередків злиття» розвідданих для обміну інформацією з питань ПФТ в режимі реального часу, зокрема щодо потенційних терористів, що здійснюють самостійно ініційовані атаки.

Слід зауважити, що ці рекомендації ґрунтуються на практичних можливостях з урахуванням поточних спроможностей для кращої протидії самостійно ініційованому тероризму. Водночас, будь-які реформи повинні брати до уваги й інші політичні аспекти — такі як фінансові витрати (і те, хто їх нестиме), а також можливі наслідки для захисту персональних даних в умовах поглибленої співпраці між державним і приватним секторами. Хоча певні ризики можна пом’якшити, запровадження більш адаптивної моделі ПФТ до загроз самостійно ініційованого тероризму вимагатиме зусиль та більш прицільного моніторингу окремих осіб. Остаточне рішення щодо впровадження таких змін має ґрунтуватися на загальносуспільному консенсусі щодо того, що очікувана оперативна вигода переважає пов’язані з цим витрати.

Вступ

ЗГІДНО З ДАНИМИ EUROPOL, правоохоронного агентства ЄС, найсерйозніша терористична загроза для континенту походить від одинаків або малих осередків, які вдаються до насильства з власної ініціативи, без координації з боку більших організацій, і ця загроза йде як з боку ісламістських, так і ультраправих екстремістів[1]. Попри національні локдауни під час пандемії коронавірусу, ця загроза залишалася сталою. Так, протягом 2020 року атаки не припинялися, зокрема збройний напад у Відні в листопаді, внаслідок якого загинули четверо осіб і ще 20 були поранені[2] — ще один приклад того, що стало новою реальністю у сфері безпеки європейського суспільства.

Такі атаки часто приписують «одинакам» або «малим осередкам», які зазвичай складаються з двох або трьох осіб. Хоча цей термін не є хибним, він і не є оптимальним. У цьому дослідженні використовується більш точне поняття — "терористи, що здійснюють самостійно ініційовані атаки". Воно краще підкреслює головну особливість — операційну автономію таких осіб. Досі дослідження самостійно ініційованого тероризму зосереджувалися переважно на радикалізації та характеристиках, які відрізняють цих осіб від інших типів терористів. Основними темами попередніх досліджень були, зокрема, психічне здоров'я індивідів та високий рівень користування інтернетом.[3]

Натомість вивчення логістичних аспектів самостійно ініційованого тероризму, зокрема фінансування, залишається недостатньо розвиненим. Існують зрозумілі практичні причини цього: зростання загрози самостійно ініційованого тероризму є відносно новоим а дослідження діяльності організованих груп чи мереж (як-от «Аль-Каїда» чи Ісламська держава) часто є простішим і ймовірно більш результативним. Крім того, дослідження фінансової активності терористів, що здійснюють самостійно ініційовані атаки, гальмувалося через поширені припущення щодо її незначущості. На відміну від скоординованих атак з боку ісламістських угруповань, характерних до 2015 року, напади терористів, що здійснюють самостійно ініційовані атаки, як правило, були менш складними і значно дешевшими. Це викликає запитання: чи є взагалі поняття "фінансування тероризму" релевантним у цьому контексті?

Це питання має екзистенційне значення для глобального режиму з ПФТ. Цей режим, що виник після подій 11 вересня, використовує інструменти, закладені в рамковій системі ПВК, такі як замороження активів та подання повідомлень про підозрілі операції, для припинення переміщення коштів через міжнародну фінансову систему. Оскільки терористи, що здійснюють самостійно ініційовані атаки, зазвичай не отримують значного міжнародного

[1] Європол, 'Звіт про поточний стан та тренди тероризму у Європейському Союзі 2020', 23 червня 2020, стр. 19.
[2] DW, 'Терористична Атака у Відні: Поліція здійснює розслідування щодо 21 співучасника', 13 листопада 2020.
[3] Clare Ellis et al., 'Тероризм одинаків', Серія досліджень з протидії терористів одинаків. No. 11, Остаточний звіт, RUSI, квітень 2016, стр. viii–ix.

фінансування, важливість ПФТ у сучасних стратегіях боротьби з тероризмом дехто вважає сумнівною. Проте ці песимістичні припущення ґрунтуються на відносно обмежених даних про фінансову активність таких терористів.

Поточна ситуація є критичною та нестабільною. «Нова реальність» самостійно ініційованого тероризму вимагає системних змін по всій Європі для протидії фінансуванню тієї загрози, яку Європол вважає основною терористичною небезпекою для континенту. Метою цього документу є заповнення прогалини в колективному розумінні фінансової поведінки терористів, що здійснюють самостійно ініційовані атаки, різного ідеологічного спрямування, а також надання рекомендацій щодо того, як система ПФТ може бути адаптована до особливостей цієї загрози. Звіт спрямований на пошук відповідей на два взаємопов'язані дослідницькі питання:

1. Яким чином терористи, що здійснюють самостійно ініційовані атаки в Європі, готуються до нападів з фінансової точки зору?
2. Як має змінитися система ПФТ для ефективного реагування на цю терористичну загрозу?

Дослідження RUSI 2017 року заклало основу в цій сфері, проаналізувавши фінансування, пов'язане зі змовами 63 терористів-одинаків і малих осередків у Великій Британії та Франції в період із 2000 по 2014 роки[4]. Автори цього дослідження зазначили, що хоча збір і використання фінансових розвідданих щодо індивідуальної фінансової поведінки є складним завданням, такі дані можуть відігравати важливу роль у механізмах обміну інформацією між державним і приватним секторами, особливо після здійснення атак.[5]

Цей звіт покликаний розвинути напрацювання, зроблені у дослідженні 2017 року, зокрема шляхом розширення предмета аналізу на випадки самостійно ініційованих терористичних актів по всій Європі. Крім того, кілька прикладів фінансової та логістичної діяльності терористів, що здійснюють самостійно ініційовані атаки, за останні п'ять років (із моменту завершення попереднього дослідження) свідчать про те, що планування таких атак — особливо у випадках амбітних задумів із використанням саморобних вибухових пристроїв (СВП) — може залишати помітні фінансові сліди та ознаки комерційної діяльності. Хоча ці сліди, ймовірно, залишатимуться складними для виявлення та обміну в межах поточних ПФТ-процедур, результати дослідження дають обґрунтовані підстави вважати, що такого роду фінансова розвідка — за умови її поєднання з іншими видами розвідувальної інформації — може істотно підвищити ефективність заходів як на етапі до, так і після нападу. Потенціал використання такої інформації ще до нападу може бути реалізований за умови створення більш гнучких механізмів передачі розвідданих від приватного до державного сектору, що стане відходом від акценту на постфактум-аналізі, характерного для попереднього дослідження.

[4] Tom Keatinge та Florence Keen, 'Атаки терористів одинаків та маленьких терористичних осередків: Новий фронт у сфері ПФТ?', Тематичний документ RUSI (Січень 2017).
[5] *Ibid.*

У документі ці питання розглядаються в межах чотирьох розділів. Розділ I окреслює межі дослідження та методологічну основу. Розділ II присвячений еволюції розуміння фінансування самостійно ініційованого тероризму та купівельну поведінку. Розділ III аналізує, як до цього часу режим з ПФТ реагував на загрозу самостійно ініційованого тероризму. Документ закінчується пропозиціями щодо того, як фінансові розвіддані щодо самостійно ініційованого тероризму можна збирати та поширювати більш ефективно у майбутньому.

I. Методологія

У ДОСЛІДНИЦЬКІЙ РОБОТІ, що стосується будь-якого аспекту тероризму, чітке визначення термінів є фундаментальною основою, з огляду на складність дискусій навколо цієї тематики. Не менш важливо також забезпечити прозоре розуміння меж дослідження та способу збору даних, особливо з урахуванням того, що велика частина інформації у цій сфері є чутливою та зберігається в офіційних установах. У цьому розділі подано короткий опис підходу, застосованого у цьому документі до зазначених питань.

Визначення

Одним із основних викликів для цього дослідження стало визначення термінів «терорист одинак» та «тероризм малих осередків»[6], і, відповідно, пошук всеохопного поняття, яке б охоплювало обидва явища. Визначення «одинак» є особливо неоднозначним: навіть якщо напад здійснюється одноосібно, виконавець рідко є повністю ізольованим від ширших екстремістських чи радикальних середовищ[7]. Один із шведських посадовців, опитаний у межах дослідження, зауважив: «одинаки» і «малі осередки» — це не частина групи або мережі, але й не повна ізоляція від зовнішнього середовища[8]. Визначення цієї загрози лише за кількістю учасників (зазвичай три або менше) також є незадовільним, адже воно не виключає, що «малі осередки» можуть діяти під контролем або за прямими вказівками від групи чи мережі, а також «великі осередки» з чотирьох і більше осіб, які можуть бути повністю автономними.

У зв'язку з цим у цьому звіті використовується поняття «терористи, які здійснюють самостійно ініційовані атаки», запропоноване Меттью Фельдманом[9]. Воно стосується осіб, які здійснюють ініціювання, планування та виконання атаки самостійно. Це поняття охоплює осіб, які мають зв'язки з ширшими екстремістськими мережами, водночас визнаючи, що вони демонструють певну оперативну автономію. Звісно, визначення самостійно ініційованого тероризму не є абсолютно чітким. Завжди існуватимуть «пограничні» випадки, у яких складно достеменно оцінити рівень особистої самостійності виконавців.

---

[6] У цьому дослідженні використовується визначення терористичних актів, закріплене в Декларації Генеральної Асамблеї ООН 1994 року «Про заходи з ліквідації міжнародного тероризму», згідно з яким терористичні акти — це «злочинні дії, вчинені з наміром або розрахунком викликати стан терору серед широкої громадськості, окремої групи осіб або конкретних осіб з політичною метою». Див. ООН, Декларація про Заходи з Ліквідації Міжнародного Тероризму, грудень 1994 року, https://legal.un.org/avl/ha/dot/dot.html

[7] Paul Gill, *Терорист одинак: Поведінковий Аналіз* (Абінгдон: Routledge, 2015), с. 11–15; Bart Schuurman та ін., «*Планування та Підготовка Атак Терориста Одинака: Аналіз на Основі Даних*», Journal of Forensic Sciences (Випуск 63, № 4, 2018), с. 1191–1200; Bart Schuurman та ін., «*Кінець Одинокого Вовка: Типологія Якої не Мало Бути*», Studies in Conflict & Terrorism (Випуск 42, № 8, 2019), с. 771–778.

[8] Інтерв'ю автора у форматі відеоконференції з представниками Служби безпеки Швеції, 2 липня 2020 року.

[9] Щодо обговорення обмеженості концепції «одинаків», що й стало передумовою до формування розуміння самостійно ініційованого тероризму, можна ознайомитися у: Gerry Gable та Paul Jackson, «Одинаки: Міф чи Реальність», Searchlight, 2011, http://nectar.northampton.ac.uk/6014/1/Gable20116014.pdf; Matthew Feldman, «Порівняльний Тероризм Одинаків: Шлях до Евристичного Визначення», Democracy and Security (Випуск 9, № 3, 2013).

У цьому документі застосовано широкий підхід, включено як атаки, що були підготовлені та здійснені без безпосереднього керівництва чи підтримки, так і ті, що могли бути підбурені ззовні.

Сфера охоплення

Цей документ досліджує фінансові аспекти планування останніх самостійно ініційованих терористичних атак в Європі та ефективність чинних заходів ЄС із ПФТ для виявлення та припинення таких приготувань. Підготовлений за підтримки Європейської комісії з метою розробки потенційних реформ у сфері ПФТ, він розглядає випадки з усього політичного спектра, зокрема ідеології, натхненні релігією, такі як ісламістський екстремізм, а також як успішні, так і зірвані напади. Документ зосереджується на плануванні атак у межах ЄС та сусідніх держав (Великої Британії, Норвегії та Швейцарії). Щоб забезпечити актуальність цього дослідження для сучасної моделі діяльності терористів, що здійснюють самостійно ініційовані атаки, проаналізовано матеріали 106 випадків, що мали місце в період з 1 січня 2015 року до 30 листопада 2020 року. Хоча обрані часові рамки певною мірою є умовними, цей період охоплює час, коли Європол визнав особливе значення діяльності одинаків та малих осередків.[10]

Збір та Аналіз Даних

Проєкт тривав з січня по грудень 2020 року, а дослідницький процес складався з наративного огляду наявної англомовної академічної та політичної літератури, опублікованої станом на кінець червня 2020 року.

Було проведено напівструктуровані інтерв'ю з метою оцінки поточного рівня знань про фінансову діяльність терористів, що здійснюють самостійно ініційовані атаки, та ефективність заходів ПФТ. Респондентів обирали з чотирьох категорій зацікавлених сторін, залучених до питань тероризму та ПФТ: дослідники; державні службовці; представники правоохоронних органів; фахівці приватного сектору з питань дотримання вимог ПВК/ПФТ.

Representatives from each of these different categories were identified in four 'target' countries: France; Germany; the UK; and Sweden. France, Germany and the UK were chosen because they were subject to the largest number of relevant attacks in the period of study, while Sweden was included because of its significant terrorism research community. Initial expectations were that two interviews per category in each country would be completed, totalling 32 interviews.

Представників кожної категорії було визначено у чотирьох «цільових» країнах: Франція, Німеччина, Велика Британія та Швеція. Перші три країни було обрано через найбільшу кількість релевантних атак у період дослідження, а Швецію – через значну дослідницьку спільноту з питань тероризму. Початково планувалося провести по два інтерв'ю в межах категорії у кожній країні, тобто загалом 32 інтерв'ю.

[10] Європол, Звіт щодо Поточної Ситуації та Тенденцій Тероризму в Європейському Союзі (TE-SAT) 2016 (Гаага: Офіс Європейської Поліції, 2016), с. 5

Через труднощі, спричинені пандемією коронавірусу, організувати інтерв'ю в усіх категоріях і країнах не вдалося, а в чотирьох випадках респонденти через робоче навантаження обрали письмовий формат відповіді. Де було можливо, додаткові інтерв'ю проводилися з фахівцями інших європейських юрисдикцій. Загалом було проведено 33 усні та 4 письмові інтерв'ю.

Огляд літератури та інтерв'ю доповнювалися аналізом наявних англомовних матеріалів у національних друкованих та телевізійних ЗМІ у країнах, що підпадали під сферу охоплення. У результаті було виявлено 106 випадків самостійно ініційованого тероризму у 14 юрисдикціях,[11] хоча цей перелік, імовірно, не є вичерпним. Багато зірваних атак не висвітлюються у ЗМІ, а коли терористів було вбито під час нападу, судові процеси не завжди відбуваються, або підпадають під юридичні обмеження щодо оприлюднення інформації.

[11] Австрія, Бельгія, Велика Британія, Данія, Італія, Латвія, Нідерланди, Німеччина, Норвегія, Польща, Фінляндія, Франція, Хорватія та Швеція

II. Фінансування та Забезпечення Ресурсами

Загроза самостійно ініційованого тероризму зростає в Європі вже понад десятиріччя. Наприклад, Петтер Несер встановив, що у період між 2008 та 2014 роками кількість таких атак у Європі зросла на 40%, і щорічні оперативні звіти Європолу свідчать про продовження цієї тенденції.[12]

Як зазначив Ерік Прайс у своєму огляді літератури з питань фінансування тероризму за 2001–2013 роки, академічні дослідження того часу здебільшого зосереджувалися на фінансовій діяльності організованих груп і мереж,[13] тоді як ґрунтовна база знань щодо фінансової поведінки та стратегій забезпечення ресурсами самостійно ініційованого тероризму лише починала формуватися.[14]

Відповідно до сучасного консенсусу, терористи, що здійснюють самостійно ініційовані атаки, незалежно від ідеології, найчастіше використовують власний заробіток або позикові кошти для фінансування чи забезпечення підготовки атак, а у разі нестачі легальних джерел можуть вдаватися до дрібної злочинної діяльності.[15] Літературні джерела вказують, що через обмежені можливості більшості таких осіб атаки, як правило, є відносно скромними, а отже — простішими у фінансуванні та ресурсному забезпеченні.

Дані за останні п’ять років у Європі переважно підтверджують ці оцінки. Водночас існують помітні приклади, коли плани були значно масштабнішими та потребували тривалої підготовки. Це означає, що у багатьох випадках обсяг фінансової розвідки щодо підготовки атак буде обмеженим, але існують і ситуації, коли інформації може бути значно більше. Чим амбітнішими є плани терориста, що планує самсотійно ініційовану атаку, тим більше фінансових даних ймовірно виникне. Крім того, варто пам’ятати, що багато реальних і потенційних задумів такого типу, які вдалося зірвати, демонстрували прагнення та можливості до проведення операцій, масштаб яких перевищував рівень дрібних атак.

---

[12] Див. : Europol, *European Union Terrorism Situation and Trend Report 2019* (Гаага: Europol, 2019).

[13] Для огляду літератури з питань фінансування тероризму за період 2001–2013 рр. див.: Eric Price, ‘Literature on the Financing of Terrorism’, *Perspectives on Terrorism* (т. 7, № 4, 2013), с. 112–130; Financial Action Task Force (FATF), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations*; Резолюція Ради Безпеки ООН № 1373 від 28 вересня 2001 р., S/RES/1373.

[14] Див., наприклад: Emilie Oftedal, *The Financing of Jihadi Terrorist Cells in Europe* (К’еллер: Norwegian Defence Research Establishment, 2015); Michael Freeman, ‘The Sources of Terrorist Financing: Theory and Typology’, *Studies in Conflict & Terrorism* (т. 34, № 6, 2011), с. 461–475; Rajan Basra і Peter Neumann, ‘Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus’, *Perspectives on Terrorism* (т. 10, № 6, 2016), с. 25–40; Petter Nesser, Anne Stenersen і Emilie Oftedal, ‘Jihadi Terrorism in Europe: The IS-Effect’, *Perspectives on Terrorism* (т. 10, № 6, 2016); Schuurman та ін., ‘Lone Actor Terrorist Attack Planning and Preparation’.

[15] Freeman, ‘The Sources of Terrorist Financing’.

Фінансування Тероризму

Після подій 11 вересня 2001 року існувало поширене припущення, що терористичні мережі, такі як Аль-Каїда, переказують кошти через фінансову систему для підтримки діяльності своїх бойовиків у всьому світі — підхід «згори вниз», коли кошти надходили разом з інструкціями безпосередньо з центру мережі. Оскільки державне спостереження та міжнародна співпраця виявилися дедалі ефективнішими у зниженні можливостей і руйнуванні командних структур організованих груп, окремі елементи цих рухів перейшли від безпосереднього керування атаками до стимулювання автономної діяльності через соціальні мережі та інтернет.[16] Моделі фінансування пройшли схожий шлях розвитку. Як зазначає Емілі Офтедал на основі дослідження, що охоплювало період з 1994 по 2013 рік, плани, що залежали від міжнародного фінансування, почали занепадати одразу після 11 вересня.[17]

Офтедал також вважає, що ця тенденція значною мірою збереглася і в поведінці окремих терористів, адже основні групи та мережі ослабли, а фінансування надходить переважно з буденних і легальних джерел, зокрема зарплат, заощаджень, кредитів і державних соціальних виплат.[18] Атаки залишаються малозатратними та відносно простими у фінансуванні — 80% самостійно ініційованих атак терористів-ісламістів у Європі, досліджених Офтедал, коштували менше ніж 10 000 доларів США, що свідчить про відсутність значного фінансового «сліду» під час підготовки.[19]

Хоча досліджень фінансування екстремістів ультраправого спрямування поки що менше, наявні дані свідчать, що й вони здебільшого отримували кошти з відносно непримітних джерел.[20] За даними Барта Шуурмана та його колег, чиє дослідження охоплювало ультраправий та ісламістський самостійно ініційований тероризм, лише 13% терористів намагалися отримати зовнішню фінансову підтримку для здійснення атаки.[21] Наприклад, Андерс Брейвік, який у липні 2011 року здійснив напад із використанням вантажівки з вибухівкою та стрілецькою зброєю в Осло та на острові Утойя, Норвегія,[22] для підготовки свого нападу використав власні заощадження, отримані від продажу фальшивих онлайн-дипломів та інших інвестицій.[23]

---

[16] Петтер Несер, *Islamist Terrorism in Europe* (Лондон: Hurst, 2018), с. 267; інтерв'ю автора у форматі відеоконференції з колишнім співробітником британської розвідки, 20 травня 2020 року.
[17] Офтедал, *The Financing of Jihadi Terrorist Cells in Europe*, с. 15.
[18] *Ibid.*
[19] *Ibid.*, с. 24. У цьому дослідженні Офтедал проаналізувала фінансування 40 терористичних осередків, які планували напади в Європі у період з 1994 по 2013 роки.
[20] Див. Tom Keatinge, Florence Keen та Kayla Izenman, *Fundraising for Right-Wing Extremist Movements: How They Raise Funds and How to Counter It*, *RUSI Journal* (Том 164, № 2, 2019), сс. 10–23; Bethan Johnson, *Financing Right-Wing Extremism and Terrorism*, *Project CRAAFT Research Briefing* (№ 5).
[21] Schuurman та ін., *Lone Actor Terrorist Attack Planning and Preparation*, с. 1196. Шурман та колеги дослідили планування та підготовку атак 55 одинаків у Європі та Північній Америці у період з 1986 по 2015 роки.
[22] Schuurman та ін., «End of the Lone Wolf»; інтерв'ю авторів у форматі відеоконференції з Флоренс Кін, 1 травня 2020 року.
[23] Torgeir Husby та Synne Sørheim, «Rettspsykiatrisk erklæring 1» [«Судово-психіатричний висновок 1»], 11 серпня 2011 року, с. 77, https://www.vg.no/spesial/2011/22-juli/psykiatrisk_vurdering/, дата звернення: 20 квітня 2020 року.

Джерела Фінансування

Аналіз випадків за період 2015–2020 років, проведений у межах цього дослідження, підтвердив результати, отримані Офтедал, Несером та іншими дослідниками, щодо важливості легальних, хоча й неправомірно використаних, джерел фінансування атак самостійно ініційованого тероризму. Частина такого зловживання включає шахрайство, зокрема використання доходів, позик і державних соціальних виплат, а також продаж особистих речей і збір коштів серед знайомих.[24] Обмежена доступність публічних даних не дозволяє здійснити кількісний аналіз поширеності кожного джерела фінансування, однак дослідження випадків демонструє різноманітні канали, які використовують такі терористи:

- **Дохід**: Мохамед М., який заклав вибуховий пристрій у Ліоні у травні 2019 року, ймовірно, придбав його складові за кошти, зароблені на онлайн-викладанні IT через приватну навчальну платформу.[25] В іншому випадку Мохаммед Рехман та його дружина Сана Ахмед Хан були засуджені у 2015 році за планування теракту в Лондоні з використанням 11 кг речовин для виготовлення вибухівки, які були придбані на зарплату Хан (додатково до коштів, отриманих за швидкими позиками).[26]
- **Кредити та позики**: Амеді Кулібалі, який на початку 2015 року здійснив серію збройних нападів в Іль-де-Франс, частково профінансував свою діяльність за рахунок споживчого кредиту на 6 000 євро, отриманого у 2014 році за підробленими документами.[27] В іншому випадку Салман Абеді, виконавець вибуху на стадіоні Manchester Arena, ймовірно, використав частину студентської позики для фінансування своїх операційних витрат.[28]
- **Державні виплати**: Основним джерелом доходу Салмана та Хашема Абеді були державні соціальні виплати, що надходили на банківський рахунок їхньої матері у Великій Британії, до якого вони мали доступ, поки вона перебувала у Лівії. Рахунок отримував житлову допомогу, податкові пільги та допомогу на дітей на суму понад 500 фунтів стерлінгів на тиждень упродовж двох періодів протягом семи років, доки сім'я жила між Великою Британією та Лівією.[29]

[24] Oftedal, *The Financing of Jihadi Terrorist Cells in Europe*, с. 7.
[25] Інтерв'ю авторів у форматі відеоконференції з представником французьких правоохоронних органів, 9 липня 2020 року.
[26] Berkshire Live, «Reading Terror Plotters Husband and Wife May Never be Released» [«Подружжя, яке планувало теракт у Редінгу, можливо, ніколи не вийде на волю»], 30 грудня 2015 року, https://www.getreading.co.uk/news/reading-berkshire-news/reading-terror-plotters-husband-wife-10667833
[27] Basra та Neumann, «Criminal Pasts, Terrorist Futures», с. 35.
[28] BBC News, «Manchester Arena Bomb Parts "Bought By Brothers Using Mum's Card"» [«Частини для бомби в Manchester Arena "куплені братами за карткою матері"»], 10 лютого 2020 року; John Scheerhout, «All the Evidence in the Manchester Arena Trial, Day by Day» [«Усі докази у справі Manchester Arena по днях»], *Manchester Evening News*, 20 серпня 2020 року, https://www.manchestereveningnews.co.uk/news/hashem-abedi-evidence-manchester-arena-18790131
[29] *Ibid.*

- **Особисті пожертви**: У невеликій кількості випадків потенційні терористи, що планували здійснити самостійно ініційований напад, також шукали фінансову підтримку серед ідеологічних соратників. Наприклад, у відео, оприлюдненому після своєї атаки, Кулібалі заявив, що пожертвував кілька тисяч євро Саїду та Шеріфу Куаші, аби вони могли завершити підготовку до збройного нападу на редакцію *Charlie Hebdo*.[30] Адель Керміш, один із двох нападників із ножами у церкві в Нормандії в липні 2016 року, за повідомленнями, також просив гроші у друзів перед атакою.[31]
- **Продаж особистого майна**: Мохамед Лахуайє-Бухлель, який у липні 2016 року здійснив наїзд вантажівкою у Ніцці, купив вогнепальну зброю за 1 400 євро та орендував вантажівку для атаки за готівку, отриману від продажу власного автомобіля за 3 000 євро.[32]

Поряд із зловживанням легальними фінансами, постійним джерелом підтримки операційної діяльності багатьох ісламістських екстремістів, особливо у Франції, залишаються кошти отримані незаконним шляхом. Багато з терористів, які здійснюють самостійно ініційовані напади, належать до так званого «покоління ІДІЛ» (*Generation ISIS*) – групи молодих екстремістів, світогляд яких сформувався переважно під впливом мобільних технологій та соціальних мереж, і які часто поєднують джихадистський та дрібнокримінальний спосіб життя.[33] Наприклад, брати Куаші змогли придбати зброю частково за рахунок прибутків від наркоторгівлі та незаконної торгівлі контрафактними товарами,[34] а Аюб Ель-Хаззані, який у серпні 2015 року намагався здійснити збройний напад у потязі між Брюсселем та Парижем, мав попередні судимості й принаймні частково фінансувався за рахунок злочинної діяльності, зокрема пограбувань та продажу наркотиків.[35]

[30] *L'Express*, «Amedy Coulibaly a pu financer ses attentats par un crédit à la consommation» [«Амеді Кулібалі міг профінансувати свої напади за рахунок споживчого кредиту»], 1 квітня 2015 року, https://www.lexpress.fr/actualite/societe/amedy-coulibaly-a-pu-financer-ses-attentats-par-un-credit-a-la-consommation_1640488.html

[31] Ben Farmer та ін., «France Church Attack: Second Normandy Priest Killer Named» [«Напад на церкву у Франції: названо ім'я другого вбивці священика у Нормандії»], *The Telegraph*, 27 липня 2016 року.

[32] Інтерв'ю авторів у форматі відеоконференції з представником французьких правоохоронних органів, 9 липня 2020 року.

[33] Інтерв'ю авторів у форматі відеоконференції з Пітером Нойманом, 4 травня 2020 року; інтерв'ю авторів у форматі відеоконференції з колишнім старшим співробітником правоохоронних органів Великої Британії, 4 червня 2020 року; інтерв'ю авторів у форматі відеоконференції зі співробітником ПФР Швеції, 3 липня 2020 року; інтерв'ю авторів у форматі відеоконференції з Ніколасом Райдером, 24 квітня 2020 року.

[34] Union des Fabricants (UNIFAB), «Contra-Façon et Terrorisme: Rapport 2016» [«Контрафакт і тероризм: звіт 2016»], с. 16, https://www.inpi.fr/sites/default/files/rapport-a-terrorisme-2015_fr.pdf; Oftedal, *The Financing of Jihadi Terrorist Cells in Europe*, с. 63.

[35] Peter Neumann, «Don't Follow the Money: The Problem with the War on Terrorist Financing» [«Не йдіть за грошима: проблема війни з фінансуванням тероризму»], *Foreign Affairs*, липень/серпень 2017 року, с. 98; Louise Shelley, «"ISIS" Members Depend on Petty Crime to Function in Europe» [«Члени "ІДІЛ" залежать від дрібної злочинності для діяльності в Європі»], *New York Times*, 20 листопада 2015 року; Angelique Chrisafis, «Life of Paris Attacker Omar Ismail Mostefai: From Petty Crime to Radicalisation» [«Життя паризького нападника Омара Ісмаїла Мостефаї: від дрібної злочинності до радикалізації»], *The Guardian*, 16 листопада 2015 року.

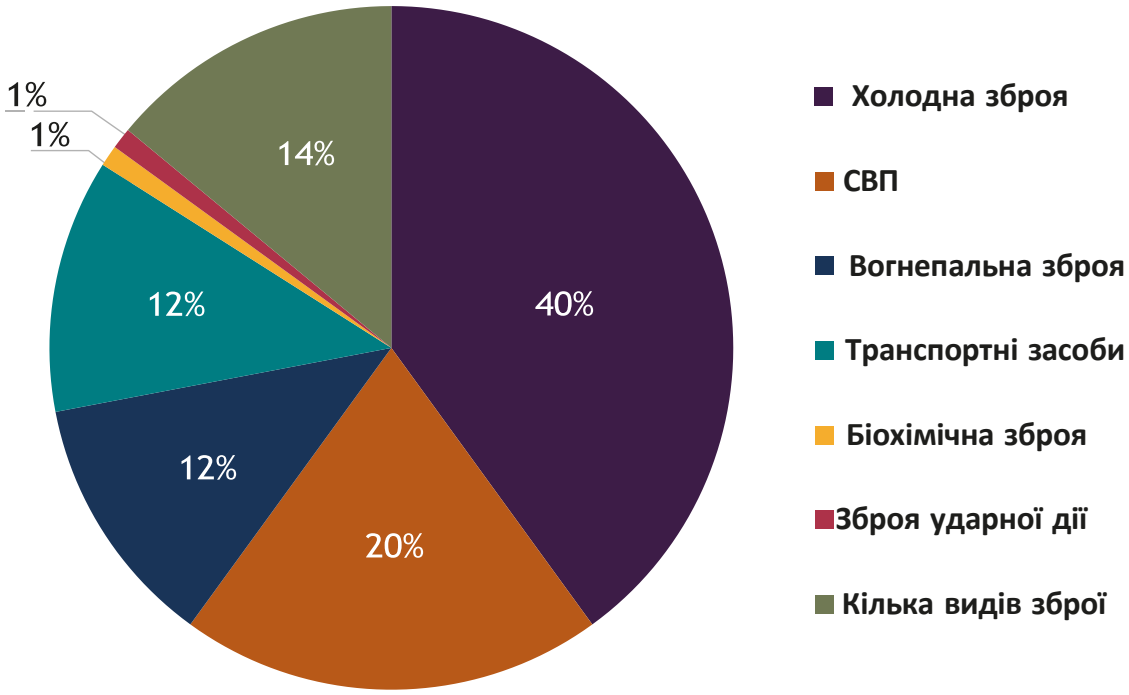
Напади, Логістика та Канали Постачання

Вибір зброї є одним із найважливіших рішень, пов'язаних із фінансуванням, яке повинен ухвалити терорист, що планує здійснити самостійно ініційовану атаку, і більшість використовує один із чотирьох типів (див. рисунок 1) або їх комбінацію – холодну зброю, таку як ножі чи мачете, вибухові пристрої (СВП), транспортні засоби або вогнепальну зброю.[36] У 40% випадків основною зброєю є холодна зброя, у 20% – СВП, у 12% – транспортні засоби та у 12% – вогнепальна зброя. Останні самостійно ініційовані атаки терористів з числа ультраправих екстремістів демонструють особливий інтерес до вогнепальної зброї, як це видно з інцидентів у Галле та Ханау в Німеччині у жовтні 2019 року та лютому 2020 року відповідно (див. нижче).[37]

[36] Едвін Баккер та Беатріс де Грааф, «Lone Wolves: How to Prevent This Phenomenon?» [«Одинокі вовки: як запобігти цьому явищу?»], International Centre for Counter-Terrorism – The Hague, Expert Meeting Paper, листопад 2010 р.

[37] Олівер Муді, «Germany Synagogue Attacker Used Gun Manual from UK Enthusiast Philip Luty» [«Нападник на синагогу в Німеччині використав інструкцію зі зброї від британського ентузіаста Філіпа Люті»], *The Times*, 11 жовтня 2019 р.; Джастін Гагглер, «Tobias Rathjen: Hanau's Disturbed Far-Right Gunman Not on Any German Police Watchlists» [«Тобіас Ратжен: психічно нестабільний стрілець з Ханау, пов'язаний із крайнім правим рухом, не перебував у жодних поліцейських списках спостереження у Німеччині»], *The Telegraph*, 20 лютого 2020 р.

Рисунок 1: Основні Види Зброї, Які Використовують Терористи для Самостійно Ініційованих Атак в Європейських Державах, Січень 2015 – Листопад 2020



Джерело: Дослідження авторів, див. Додаток для отримання додаткової інформації

Так само, як і фінансування, забезпечення ресурсами та логістичні потреби кожного типу атаки різняться (створюючи різні «сліди» у фінансовій чи комерційній діяльності), патерни у випадках за останні п'ять років свідчать, що існує й різноманіття способів, у які нападники використовують свої кошти для підготовки та здійснення атаки.

Деякі підготовчі дії тривають протягом тривалого часу, що підтверджується прикладами терористів, які мають схильність накопичувати широкий спектр небезпечних предметів, не всі з яких можуть бути використані під час однієї атаки. Так, у домі Шеріфа Шекатта, який у грудні 2018 року здійснив вибух на різдвяному ярмарку у Страсбурзі, було знайдено великий арсенал зброї та гранат — більше, ніж потрібно для однієї атаки. Так само, за повідомленнями, Мохамед М зібрав матеріали, яких вистачило б на кілька, і навіть потужніших, СВП, ніж та, яку він заклав.[38] У деяких випадках особи, які не планують негайного нападу, можуть накопичувати зброю. У грудні 2018 року в Ньюкаслі був заарештований Фатах Мохаммед Абдулла за

[38] Інтерв'ю авторів у форматі відеоконференції з представником французьких правоохоронних органів, 9 липня 2020 року.

підбурювання двох осіб у Німеччині до здійснення атаки. Під час обшуку його житла поліція виявила, що він також мав запас зброї, яку можна було використати для нападу, зокрема феєрверки, детонатор, складаний ніж, балаклаву та 200 грамів сірчаного порошку.[39]

Однак частіше підготовка до нападу, яка головним чином пов'язана з придбанням зброї, здійснюється у короткі терміни. Хоча чіткого усталеного патерну для цього немає, різні типи нападів зазвичай демонструють спільні риси у своїй підготовці.

Холодна Зброя

One of the common assumptions about edged weapons is that attackers simply use knives they already have at home. However, it is not always clear that they do. For example, Safia S, who attacked a police officer with a knife in Hanover in February 2016, used a standard kitchen knife that German officials interviewed for this project believed *could* easily have come from her own home, but may have been bought specifically.40 Moreover, in other instances some attackers purchase edged weapons specifically for an attack. For example, the knives used in Khalid Masood's attack in Westminster in March 2017, and the three-man attack on the areas around London Bridge in June 2017, were purchased from major supermarkets.41

Одним із поширених припущень щодо використання холодної зброї є те, що нападники просто застосовують ножі, які вже мають удома. Проте не завжди зрозуміло, що це дійсно так. Наприклад, Сафія S, яка напала на поліцейського з ножем у Ганновері в лютому 2016 року, використала звичайний кухонний ніж, який, на думку німецьких фахівців, опитаних у рамках цього дослідження, цілком міг бути з її власного дому, але водночас міг бути придбаний спеціально.[40] Крім того, в інших випадках деякі нападники купували холодну зброю саме для здійснення атаки. Так, ножі, використані Халідом Масудом під час нападу у Вестмінстері в березні 2017 року, а також у нападі трьох осіб у районі Лондонського мосту в червні 2017 року, були придбані у великих супермаркетах.[41]

Нападники з ультраправого крила також купували символічну зброю у спеціалізованих магазинах. Наприклад, Антон Лундин Петтерссон, який здійснив напад у школі в Тролльгеттані, Швеція, у жовтні 2015 року, спеціально придбав репліку меча вікінгів та японський ритуальний ніж разом з предметами нацистської атрибутики для використання у своєму нападі.[42]

[39] Королівська прокурорська служба (Crown Prosecution Service), «Прихильник "Даіш" засуджений до ув'язнення за планування теракту з використанням 8 000 сірників», 26 червня 2020 року, https://www.cps.gov.uk/cps/news/daesh-fanatic-jailed-masterminding-8000matches-terror-attack

[40] Письмове листування авторів з німецькими посадовими особами, 8 жовтня 2020 року.

[41] Макс Гілл, «Терористична атака на Вестмінстерському мосту» (Лондон: The Stationery Office, 2018), с. 43; BBC News, «Слідство щодо нападу на Лондонському мосту: нападник "купив рожеві ножі в Lidl"», 29 травня 2019 року.

[42] Аса Ерландссон та Рейд Мелой, «Напад у шведській школі в Тролльгеттані», *Journal of Forensic Sciences* (Том 63, № 6, 2018).

Транспортні Засоби

Здавалося б логічним припустити, що транспортні засоби легко купити через високий рівень власності автомобілями в Європі. Однак транспортні засоби, використані в атаках протягом останніх п'яти років, зазвичай були більшими комерційними автомобілями, такими як фургони та вантажівки, ймовірно через їхню здатність спричинити більше жертв. Власність на такі транспортні засоби поширена значно менше, і в низці випадків – під час нападу на набережній у Ніцці в липні 2016 року, нападу біля мечеті Фінсбері в червні 2017 року та нападу на Лондонському мосту також у червні 2017 року – нападники отримували транспортні засоби, орендуючи їх у комерційних компаній. Коли це виявлялося неможливим, або через відсутність коштів, або через відсутність необхідних документів для проходження перевірки під час оренди, нападники у деяких випадках просто викрадали транспортні засоби, як це сталося у Стокгольмі у квітні 2017 року, коли Рахмат Акілов направив викрадену вантажівку на універмаг.[43] Як і у випадку нападів із застосуванням холодної зброї, фінансові та організаційні потреби під час підготовки атак із використанням транспортних засобів є обмеженими.

Саморобні Вибухові Пристрої (СВП)

Хоча такі атаки й залишаються відносно «дешевими», їх виконання однозначно потребує більше часу та заходів із закупівлі. Дивує те, що чимало осіб, які намагалися виготовити хімічні СВП, змогли відкрито й безперешкодно придбати необхідні компоненти, здебільшого в інтернеті, з огляду на те, що багато з цих складових є досить буденними. Так, брати Абеді придбали більшість інгредієнтів для вибухівки, використаної під час атаки в Манчестерській арені, через Amazon,[44] так само, як і Ахмад Гассан, який у вересні 2017 року встановив СВП у поїзді лондонського метро на станції Парсонс-Грін. Показово, що Гассан використав подарунковий сертифікат Amazon, який він виграв у школі, щоб купити перекис водню.[45] Інші великі онлайн-майданчики, зокрема eBay, також фігурували у кількох випадках, а деякі терористи, що здійснювали самостійно ініційовані атаки, зверталися навіть до спеціалізованих онлайн-постачальників. Так, праворадикал Анвар Дріуїш із Мідлсбро був заарештований у серпні 2019 року після того, як замовив онлайн 10 кг аміачної селітри в компанії Aqua Plants Care.[46]

Хоча онлайн-покупки відігравали важливу роль, терористи, що здійснюють самостійно ініційовані атаки, також користувалися фізичними магазинами, особливо для придбання не вибухових елементів майбутнього пристрою. Так, Айдин Севігін, заарештований у Стокгольмі в лютому 2016 року, намагався виготовити СВП, використавши скороварку, куплену ним у меблевому магазині IKEA, а брати Абеді, за повідомленнями, здійснили кілька поїздок до господарських та будівельних магазинів протягом чотирьох місяців, коли готували атаку на Манчестерську арену.[47]

---

[43] Девід Кейтон, «Узбецький нападник у Стокгольмі на вантажівці присягнув на вірність ІД», *Associated Press*, 13 лютого 2018 р.

[44] Scheerhout, «Усі докази у справі про теракт у Манчестерській арені, день за днем».

[45] Бетані Міннел, «Обвинувачений у нападі на Парсонс-Грін Ахмед Хассан використав шкільний подарунковий сертифікат для купівлі матеріалів для бомби», *Sky News*, 7 березня 2018 р.

[46] *BBC News*, «Фантазер з Мідлсбро Анвар Дріуїш засуджений за вибухові речовини».

[47] Scheerhout, «Усі докази у справі про теракт у Манчестерській арені, день за днем».

Останнім важливим аспектом підготовки СВП є потреба у безпечному приміщенні для зберігання компонентів і складання пристрою. У кількох випадках – під час атаки в Ліоні, вибуху на станції Парсонс-Грін і підготовки теракту Мохаммедом Рехманом – терористи, які здійснювали самостійно ініційовані атаки, використовували власні помешкання для отримання та накопичення матеріалів.[48] Однак підготовка може бути настільки складною, що вимагає додаткового житла, і брати Абеді орендували ще два приміщення для проведення підготовчих робіт, які знайшли через платформу онлайн-оголошень Gumtree. Вони також скористалися Gumtree, щоб купити автомобіль для зберігання компонентів СВП під час своєї поїздки до Лівії у квітні 2017 року. Купуючи машину, брати запевняли продавця, що планують використовувати її для Uber-доставки.[49]

Вогнепальна Зброя

Безперечно, найскладнішим видом зброї для придбання є вогнепальна, головним чином через суворе національне законодавство щодо права на її володіння у багатьох європейських країнах, яке підкріплюється Європейською директивою про вогнепальну зброю, ухваленою ще у 1991 році. Це означає, що у випадках, коли нападники намагалися отримати вогнепальну зброю, їм часто було складно зробити це без певного попереднього легального доступу. Так, Тобіас Ратх'ен, нападник, який у лютому 2020 року атакував два кальян-бари в німецькому місті Ханау, мав ліцензію стрільця, який уже легально володів зброєю, придбаною ним в інтернеті.[50] В іншому випадку Штефан Балліт, який у жовтні 2019 року здійснив напад на синагогу в німецькому місті Галле, вже мав навички поводження з вогнепальною зброєю завдяки військовій підготовці, і, за повідомленнями, сам виготовив зброю, яку використав.[51]

Через такі обмеження на володіння зброєю багато терористів, що здійснюють самостійно ініційовані атаки, зверталися до кримінальних зв'язків, щоб дістати вогнепальну зброю. Для тих, хто мав уже наявних злочинних знайомих, як-от Омар Абдель Хамід Ель-Хусейн, який у лютому 2015 року атакував кафе Krudttønden і синагогу в Копенгагені, це виявилося відносно нескладним.[52] Для тих же, хто таких зв'язків не мав, здобути зброю було набагато важче. Так Алі Давид Зонболі, праворадикальний стрілець, який у липні 2016 року відкрив вогонь у Мюнхені, незаконно придбав зброю, попри відсутність будь-яких кримінальних контактів,[53] але цей випадок, схоже, є радше рідкісним винятком.

[48] Інтерв'ю авторів у форматі відеоконференції з французькими посадовцями, липень 2020 р.
[49] *Ibid.*
[50] Huggler, «Тобіас Ратх'ен».
[51] Moody, «Нападник на синагогу в Німеччині використав посібник зі зброї від британського ентузіаста Філіпа Люті».
[52] Oftedal, *Фінансування джихадистських терористичних осередків у Європі*, с. 37. Французька поліція також пов'язує його придбання зі зростанням кількості вогнепальної зброї у випадках насильницької злочинності у Франції приблизно в той самий час. Див. також: Andrew Osborn, «Арсенал французького стрільця підсвітив проблему незаконної торгівлі зброєю», *Reuters*, 23 березня 2012 р. Поліція оцінила вартість зброї Омара Абдель Хаміда Ель-Хусейна приблизно у 10 000 євро. Див. також: Nils Duquet та Kevin Goris, *Придбання вогнепальної зброї терористами в Європі* (Брюссель: Фламандський інститут миру, 2018), с. 137.
[53] Duquet та Goris, *Придбання вогнепальної зброї терористами в Європі*, с. 60.

Операційні Методи Фінансування

Готівка vs Цифрових Розрахунків

В той час як деякі терористи, які здійснюють самостійно ініційовані атаки, як-от нападниця з Ганновера Сафія S,[54] не мали жодних особистих фінансових інструментів, багато інших нападників, які вели більш усталений спосіб життя, користувалися звичайними фінансовими продуктами. Так, брати Абеді керували рахунком своєї матері в HSBC під час її відсутності, а Салман Абеді мав також рахунки щонайменше у двох різних банках Великої Британії.[55] Але навіть якщо рахунки у традиційних банках були відсутні, деякі нападники користувалися небанківськими фінансовими послугами. Наприклад, Мохамед М. використовував свої рахунки у Payoneer для отримання виплат від Udemy.[56] Шекатт також мав PayPal і платіжний рахунок Nickel, який можна відкрити у тютюнових крамницях або газетних кіосках.[57]

Попередні дослідження здебільшого свідчать, що терористи, які здійснюють самостійно ініційовані атаки, переважно використовували готівку для закупівель, аби уникнути створення цифрового сліду транзакцій. Наприклад, напередодні атаки в Ніцці Лахуайє-Бухлель протягом двох тижнів робив значні зняття готівки зі свого банківського рахунку, і ці кошти згодом були витрачені на придбання автомобіля та зброї для атаки.[58] Подібну картину можна простежити серед праворадикальних нападників. Так, Петтерссон під час двотижневої підготовки до нападу зняв решту своїх грошей у банку. Те, що не було витрачено в цей період, він залишив на кухонному столі свого брата перед тим, як здійснити атаку.[59]

Втім, випадки останніх п’яти років свідчать, що ті, хто планував більш масштабні атаки, не завжди могли обійтися без хоча б частково відстежуваних транзакцій. Наприклад, Мохамед М. придбав компоненти для свого СВП на Amazon, використовуючи кредитну картку,[60] а Салман Абеді, за повідомленнями, здійснив кілька оплат під час останніх закупівель перед атакою, використовуючи власну банківську дебетову картку.[61]

[54] Листування авторів з німецькими експертами, 8 жовтня 2020 р.
[55] BBC News, «Компоненти вибухівки для теракту в Манчестерській арені були придбані братами за допомогою картки матері».
[56] Payoneer — це платформа з фінансових послуг, що спеціалізується на забезпеченні платежів для осіб, які продають товари чи послуги через онлайн-майданчики, такі як eBay, AirBnb або Udemy.
[57] Інтерв’ю авторів у форматі відеоконференції із представником французьких правоохоронних органів, 9 липня 2020 р.
[58] *Ibid.*
[59] Erlandsson та Meloy, «Напад на школу у Тролльгеттані, Швеція».
[60] Інтерв’ю авторів у форматі відеоконференції із представником французьких правоохоронних органів, 9 липня 2020 р.
[61] Tom Parmenter, «Салман та Хашем Абеді: брати, які вчинили теракт у Манчестері», *Sky News*, 19 серпня 2020 р.; Scheerhout, «Усі докази у справі про теракт у Манчестерській арені, день за днем».

Віртуальні Активи

За останні п’ять років зафіксовано низку випадків, коли терористи, що здійснюють самостійно ініційовані атаки, демонстрували обізнаність у сфері віртуальних активів. Так, Мохамед М. придбав криптовалюту через криптобіржі, зокрема Coinmama.[62] Також було кілька прикладів використання віртуальних активів потенційними терористами для оперативного планування. Наприклад, Стівен Бішоп, заарештований у жовтні 2018 року під час підготовки вибуху у мечеті в Лондоні, за повідомленнями, використовував віртуальні активи у даркнеті для придбання детонатора для свого запланованого пристрою.[63] Втім, подібні випадки наразі залишаються радше поодинокими — таку думку підтвердили співрозмовники серед представників як приватного, так і державного сектору у Франції, Німеччині, Швеції та Великій Британії. Хоча віртуальні активи в окремих випадках і застосовуються для розрахунків за незаконні товари з терористичною метою, наразі це не становить усталеної тенденції.[64]

Інші Підготовчі Дії

Контрзаходи

Ряд терористів, які здійснюють самостійно ініційовані атаки, вдавалися до навмисних контрзаходів, щоб уникнути викриття під час закупівель. Так, виконавці теракту в Манчестерській арені застосували низку відволікаючих фінансових прийомів і намагалися розподіляти ризики, просячи кількох родичів і друзів купувати онлайн складові для СВП, пояснюючи, що вони потрібні для автомобіля чи генератора в Лівії, або що вони загубили банківські картки чи тимчасово не мають коштів.[65] Брати також користувалися дебетовою карткою своєї матері й купували товари в інтернеті під вигаданим ім’ям. 20 березня 2017 року вони створили електронну адресу *bedab7jeana@gmail.com* (що арабською означає «прийшли, щоб вбивати»), за допомогою якої відкрили новий акаунт на Amazon і придбали 30 літрів перекису водню на ім’я John O’Brian.[66] Інші контрзаходи включали спроби замаскувати значущість покупки шляхом додавання до неї додаткових предметів, щоб надати їй вигляду звичайної. Наприклад, Халід Алі, якого заарештували у центрі Лондона перед тим, як він мав здійснити напад із ножем у квітні 2017 року, разом із трьома ножами, призначеними для вбивства поліцейських у Вестмінстері, купив також інше кухонне приладдя.[67]

---

[62] Див. Coinmama, «About», https://www.coinmama.com/about-us

[63] John Simpson, «Расист-алкоголік планував стати першим британським ультраправим смертником», *The Times*, 9 квітня 2019 р.

[64] Інтерв’ю авторів у форматі відеоконференції зі Шведською службою безпеки, 2 липня 2020 р.; інтерв’ю авторів у форматі відеоконференції з банком HSBC, 26 квітня 2020 р.; інтерв’ю авторів у форматі відеоконференції з банком Lloyd’s, 27 квітня 2020 р.

[65] Daniel De Simone, «Шлях до теракту в Манчестерській арені», *BBC News*, 17 березня 2020 р.

[66] *Ibid.*

[67] *Chester Standard*, «Виробник бомби для “Аль-Каїди” постане перед судом за змову з метою вбивства депутатів у Вайтголлі», 26 червня 2018 р., https://www.chesterstandard.co.uk/news/national-news/16314954.al-qaida-bomb-maker-faces-jail-plot-murder-mps-whitehall/

Всплеск Активності

Останній аспект фінансової поведінки під час підготовки до атаки описують як «всплеск активності» (*burst activity*). Він не обов'язково безпосередньо пов'язаний з атакою, але свідчить про зміну звичного фінансового патерну. Магнус Нормарк і Магнус Ранстorп зазначають, що незвичні фінансові дії є типовими для самостійно ініційованого тероризму безпосередньо перед здійсненням атак,[68] і у вибірці цього дослідження також зафіксовано низку таких прикладів. Наприклад, нападники можуть знімати значні суми готівки, як це робили брати Абеді[69] чи Лахуайє-Бухлель, який протягом підготовки чотири рази зняв готівку приблизно по €2,000.[70] За кілька днів до нападу він мав перевищення ліміту на рахунку у розмірі €200 та кілька разів отримав відмову в обслуговуванні у банкоматах.

Іншим прикладом спалаху активності є непропорційно велика кількість кредитних заявок або спроб отримати великі позики. Кулібалі також подав кілька кредитних заявок за короткий час: більшість виявилися невдалими, але одну він отримав завдяки підробленим документам. Крім того, він вдався до нетипового кроку — відмовився від права на відкликання кредиту після його оформлення, щоб отримати кошти за вісім днів замість чотирнадцяти.[71]

Ще однією формою такої поведінки є перекази значних сум коштів за кордон незадовго до нападу, ймовірно з метою передати невикористані гроші екстремістським спільникам, а не допустити їх замороження владою після атаки. У березні 2017 року Салман Абеді попросив знайомого допомогти йому переказати £1,200 компанії в Китаї.[72] Абдулла Аль-Хамахмі, який у лютому 2017 року здійснив напад із мачете на поліцейських біля Лувру в Парижі, за повідомленнями, незадовго до атаки зробив два грошові перекази на суму в €3,000 та €2,000 іншому єгиптянину, який проживав у Польщі.[73]

[68] Magnus Normark та Magnus Ranstorp, *Зрозуміти Фінансування Тероризму: Modus Operandi та Національні Режими з ПФТ* (Стокгольм: Шведський університет оборони, 2015), сс. 23–24.
[69] *Ibid.*
[70] Інтерв'ю авторів у форматі відеоконференції з представниками правоохоронних органів Франції, 9 липня 2020
[71] *Le Point*, «Amedy Coulibaly avait contracté un crédit de 6 000 euros», 14 січня 2015 р., https://www.lepoint.fr/societe/amedy-coulibaly-avait-contracte-un-credit-de-6-000-euros-14-01-2015-1896379_23.php,
[72] Scheerhout, «Усі докази у справі про теракт у Манчестерській арені, день за днем».
[73] *Irish Times*, «Підозрюваний у нападі на Лувр заявив, що Ісламська держава не наказувала йому», 8 лютого 2017 р.

Оцінка

Наведений вище огляд підтверджує частину загальноприйнятих уявлень щодо фінансових, закупівельних та комерційних аспектів планування атак самостійно ініційованого тероризму. Загалом, терористи, які здійснюють самостійно ініційовані атаки і не мають достатніх коштів, здійснюють напади із застосуванням відповідно простішої зброї та меншої летальності, найчастіше використовуючи холодну зброю. Водночас це не означає, що атаки, вчинені такими терористами, є обов'язково менш смертельними чи менш масштабними, ніж ті, що організовуються угрупованнями. Як свідчать розглянуті випадки, за належної підготовки навіть відносно прості та «дешеві» напади можуть мати катастрофічні наслідки. Наприклад, серед французької вибірки цього дослідження, яка охоплює 35 атак, лише у двох випадках – стрілянина в редакції *Charlie Hebdo* у січні 2015 року та наїзд вантажівки у Ніцці в липні 2016 року – кількість загиблих сягнула двозначних чисел. Хоча двоє нападників на *Charlie Hebdo* теоретично мали більший «летальний потенціал», оскільки використовували вогнепальну зброю, ніж Лахуаєдж-Бухлель із вантажівкою, останній убив значно більше людей – 86 проти 17. Незважаючи на те, що вантажівка є «повсякденним» і відносно доступним предметом, вона завдала значно більшої шкоди, ніж вогнепальна зброя.

Летальність атак, які здійснюють такі терористи, визначається не лише їхньою оперативною автономією та обмеженими фінансами, а й рівнем підготовки, упевненістю, амбіціями та умовами середовища. Приклад Manchester Arena показує, що за несприятливого збігу обставин «дешеві» та «прості» напади можуть бути вкрай небезпечними, а багато з них могли б мати ще гірші наслідки за іншого контексту. У випадку з Ганновером Сафія S здійснила напад за допомогою ножа лише тому, що не змогла дістати вогнепальну зброю. Без банківського рахунку чи інших джерел коштів, а головне — без кримінальних зв'язків або посередників, здатних забезпечити доступ до вогнепальної зброї, її напад був приречений залишитися відносно малоефективним і призвів лише до одного поранення.

Для порівняння, у випадку в Ліоні фінансові ресурси Мохамеда М надали йому ширші можливості для більш летального нападу. Однак його кошти не відповідали масштабу фактично вчиненого, що свідчить про інший стримувальний чинник — імовірно, недостатній досвід у виготовленні СВП. Доступ до летальної зброї не завжди означає здатність ефективно її застосувати: приміром, коли норвежець Філіп Мансхаус у 2019 році напав на ісламський центр в Осло зі гвинтівкою та дробовиком, він не зміг поранити чи вбити жодного з вірян і був знешкоджений 65-річним чоловіком.[74]

Ще одне поширене припущення щодо самостійно ініційованого тероризму полягає в тому, що дешеві атаки фінансово й комерційно невидимі. Подекуди — так, особливо при використанні холодної зброї. Втім, аналіз показує: фінансова активність терористів, які здійснюють самостійно ініційовані атаки, складніша, ніж зазвичай вважають. Вони можуть привертати увагу саме через свою фінансову та закупівельну поведінку, і що складніші та амбітніші плани — то помітніші сліди.

[74] BBC News, «Напад на мечеть у Норвегії: побитий підозрюваний Мансхаус з'явився в суді», 12 серпня 2019 р.; BBC News, «Норвезький суд засудив стрільця у мечеті до 21 року ув'язнення», 11 червня 2020 р.

III. Протидія Фінансуванню Тероризму та Самостійно Ініційований Тероризм

ЯК ЗАЗНАЧАЛОСЯ у розділі II, нещодавні атаки терористів, які здійснюють самостійно ініційовані атаки, в ЄС зазвичай маловартісні й часто не потребують значної координації. Це має суттєві наслідки для ефективності режиму з ПФТ, який будувався на припущенні про великі, складні атаки, що фінансуються мережами через міжнародну фінансову систему. Спираючись на вже існуючий підхід з ПВК, режим ПФТ поклав на фінансові установи роль «гейткіперів» до цієї системи, шляхом виявлення фінансових даних та надання її компетентним органам у вигляді повідомлень про підозрілу операцію (STR).[75]

Водночас за останні два десятиліття конфігурація терористичної загрози змінилася, і результати режиму у протидії фінансуванню тероризму залишаються змішаними.[76] Тому заінтересовані сторони в екосистемі ПФТ намагаються реформувати підходи та впроваджувати інновації, аби поліпшити виявлення й зрив терористичної діяльності. На рівні ЄС та національних урядів вимоги ПВК/ФТ поширено на нові сектори та нові сегменти фінансової системи, які можуть бути вразливими до зловживань з боку терористів,[77] тоді як низка великих європейських фінансових установ запровадила просунуті аналітичні інструменти для ідентифікації потенційних терористів у своїй клієнтській базі.[78] У небагатьох європейських юрисдикціях фінансові установи також співпрацювали з правоохоронними органами та регуляторами над створенням партнерств з обміну фінансовою розвідінформацією (FISP) з метою посилення взаємодії у сфері ПФТ.[79]

Однак попри загалом позитивний характер цих змін, їхній вплив поки що обмежений щодо загрози терористів, які здійснюють самостійно ініційовані атаки. Небагато підзвітних установ у

[75] «Повідомлення про підозрілу операцію (STR)» у різних юрисдикціях називаються по-різному; у Великій Британії та США їх позначають як «повідомлення про підозрілу діяльність (SAR)».
[76] Інтерв'ю авторів у форматі відеоконференції з Peter Neumann, 4 травня 2020 р.; інтерв'ю авторів у форматі відеоконференції з Nicholas Ryder, 24 квітня 2020 р.; Neumann, «Don't Follow the Money».
[77] Європейська Комісія, «Боротьба з Відмиванням Коштів тв Фінансуванням Тероризму: Комісія Оцінює Ризики та Закликає до Кращого Впровадження Правил», пресреліз, 24 липня 2019 р., https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4452
[78] Інтерв'ю автора у форматі відеоконференції зі старшим фахівцем із комплаєнсу Deutsche Bank, 20 березня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшими фахівцями з комплаєнсу HSBC, 23 квітня 2020 р.; інтерв'ю автора у форматі відеоконференції зі старшими фахівцями з комплаєнсу Lloyds Bank, 22 та 27 квітня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшим фахівцем з регуляторних технологій (A), 23 березня 2020 р. та 30 квітня 2020 р.
[79] Nicholas M. Maxwell, «Survey Report: Five Years of Growth in Public–Private Financial Information-Sharing Partnerships to Tackle Crime», RUSI, Future of Financial Intelligence Sharing (FFIS), серпень 2020 р.

сфері ПВК/ФТ нині здійснюють моніторинг транзакцій із рівнем деталізації, достатнім для виявлення слідів такої діяльності, і їм бракує належних настанов з боку державного сектора, щоб точно налаштовувати пошукові критерії відповідно до актуальних типологій фінансування таких терористів. Більше того, чинна модель не інтегрує фінансові розвіддані в нові слідчі та превентивні ініціативи, що впроваджуються для протидії проблемі самостійно ініційованого тероризму. Тож, аби повністю реалізувати цінність фінансових розвідданих, режиму слід знайти кращі механізми керування процесами її ідентифікації та передачі.

Режим Протидії Фінансуванню Тероризму

Чинний глобальний режим з ПФТ значною мірою сформувався після атак 11 вересня 2001 року.[80] У жовтні 2001 року держави-члени FATF доручили організації розширити свій мандат, включивши ФТ.[81] Згодом FATF опублікувала дев'ять «Спеціальних рекомендацій» щодо ПФТ, які у 2012 році було інтегровано до 40 Рекомендацій з ПВК.[82] ЄС додав вимоги з ПФТ до третьої редакції своєї Директиви з протидії відмиванню коштів у 2005 році,[83] а пізніші версії Директиви оновлював відповідно до переглядів FATF своїх Рекомендацій.[84]

Підхід FATF до фінансування тероризму значною мірою ґрунтувався на припущенні, що тероризм є «корпоративним» явищем, у межах якого групи збирають кошти з різних джерел — пожертв, легального бізнесу, злочинної діяльності та державного спонсорства — для підтримки своєї діяльності. У цій моделі фінансування тероризму кошти переказуються через міжнародну фінансову систему, а також через інші механізми переказу вартості, такі як хавала (hawala), для забезпечення підготовки та здійснення атак.[85]

Виходячи з цих припущень, роль ПФТ полягала у виявленні та перериванні потоків підозрілих коштів. Подібно до режиму ПВК, на якому вона базується, система з ПФТ покладається на фінансові установи та інші підзвітні установи для здійснення пильного нагляду за клієнтами та їхньою діяльністю, відомого як належна перевірка клієнта (CDD). Вимоги CDD еволюціонували, але по суті й надалі складаються з двох ключових елементів:[86]

---

[80] Nicholas Ridley, *Фінансування Тероризму: Невдача Контрзаходів* (Челтнем: Edward Elgar Publishing, 2012), с. 3; Juan Zarate, *Treasury's War: Розв'язання Нової Ери Фінансової Війни*(Лондон: Hachette UK, 2013), с. xiii.

[81] FATF була створена країнами G7 у 1989 р.; FATF, «International Standards on Combating and the Financing of Terrorism and Proliferation», с. 7.

[82] *Ibid.* сс. 13-30

[83] ЄС, «Directive 2005/60/ЕС», 25 листопада 2005 р., https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:EN:PDF

[84] ЄС, «Directive (EU) 2015/849», 5 червня 2015 р., https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849; ЄС, «Directive (EU) 2018/843», 19 червня 2018 р., https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843

[85] Інтерв'ю авторів у форматі відеоконференції з двома аналітиками FATF, 16 березня 2020 р.; FATF, «Нові Ризики Фінансування Тероризму», жовтень 2015 р., сс. 9–10; Freeman, «Джерела Фінансування Тероризму», с. 461; James Windle, «Фандрейзінг, Організована Злочинність та Фінансування Тероризму», Andrew Silke (ред.), *Routledge Handbook of Terrorism and Counterterrorism* (Лондон: Routledge, 2018), с. 195.

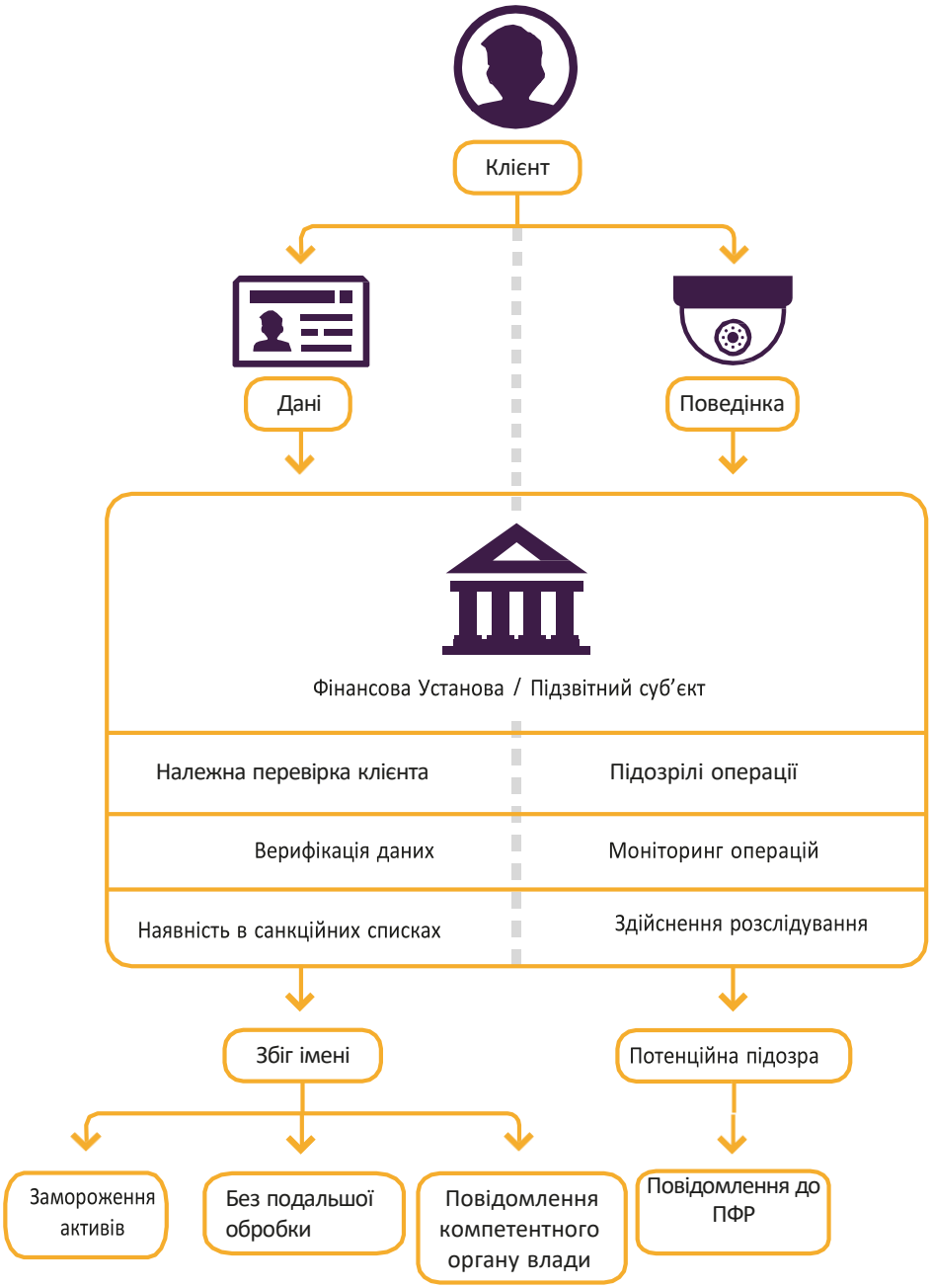
[86] Peter Reuter та Edwin M. Truman, *Переслідуючі Брудні Кошти: Боротьба з Відмиванням Коштів* (Вашингтон, округ Колумбія: International Institute of Economics, 2004), сс. 46–48.

- **Запобігання через ідентифікацію:** Фінансові установи зобов'язані «знати свого клієнта», щоб запобігати зловживанню фінансовою системою. У разі виявлення відомих терористів установи мають заморожувати їхні активи та повідомляти про це компетентні органи.
- **Виявлення через моніторинг і звітування:** Фінансові установи повинні здійснювати безперервний моніторинг поведінки клієнтів на предмет можливих невідповідностей відомим даним CDD/KYC та підозрілих патернів діяльності, що можуть свідчити про фінансові злочини, включно з потенційним фінансуванням тероризму, і звітувати про це до національних підрозділів фінансової розвідки (ПФР) через подання STR. Далі ПФР уповноважені, якщо вважатимуть це доцільним, передавати ці матеріали правоохоронним органам.

Те, як саме приватний сектор має виконувати ці зобов'язання, значною мірою лишається не конкретизованим. Водночас протягом останніх двох десятиліть стало звичним, що фінансові установи використовують схожі підходи: платформи скринінгу для виявлення потенційних збігів імен із санкційними переліками або списками терористів у режимі реального часу, а також системи моніторингу транзакцій для ретроспективного виявлення потенційно підозрілої діяльності за рахунками.[87] Те, як ці два різні потоки діяльності (ідентифікація та моніторинг) поєднуються й підживлюють ширшу систему ПВК/ФТ, показано на Рисунку 2.

[87] Matthew Redhead, «Сильний ефект? Перефокусування моделі протидії відмиванню коштів на доказах і результатах», *RUSI Occasional Papers* (жовтень 2019 р.), с. 16.

Рисунок 2: ПФТ на Практиці



Джерело: Підготовлено автором на основі: «Європейська Комісія, 'Протижія Відмиванню Коштів та Фінансуванню Тероризму в ЄС: Як Це Працює на Практиці?', 2018, <https://ec.europa.eu/info/sites/info/files/ diagram_aml_2018.07_ok.pdf>; Yanan Liu та Jayant Ramen, 'Комплаєнс у Сфері Фінансових Злочинів: Поточний Стан Справ у Світі, Brink, *15 жовтня 2017, <https://www.brinknews.com/financial- crime-compliance-current-global-state-of-play/>.*

Основні Виклики ПФТ

Дослідники тероризму, зокрема Пітер Нойман і Ніколас Райдер, стверджують, що чинний режим ПФТ має змішані результати, оскільки терористичні групи знаходять способи обійти створені ним бар'єри.[88] Водночас існують, імовірно, більш фундаментальні проблеми ефективності цього режиму, що випливають із труднощів приватного сектору щодо генерування корисних фінансових розвідданих.

Відносна грубість наявних методів ідентифікації терористів і моніторингу фінансування тероризму є базовою перешкодою. Методи комп'ютеризованого «перекладу» (часто позначувані як «fuzzy matching» — нечітке зіставлення), які застосовуються під час скринінгу імен, породжують велику кількість хибних спрацювань і зазвичай дозволяють виявляти лише «відомих» терористів — тих, кого вже внесено до санкційних переліків або хто раніше вчиняв злочини. Особи, що становлять підвищений інтерес для органів влади, але не відомі приватному сектору, зазвичай не включені до списків для скринінгу.

Крім того, платформи моніторингу транзакцій використовують підходи на основі правил для пошуку комбінацій червоних прапорців у поведінці на рахунку, що здебільшого генерує хибнопозитивні спрацювання. Формування та опрацювання сповіщень відбувається переважно ретроспективно, а будь-які подальші дії займають тижні чи місяці, через що цінність STR як індикаторів планування атак може бути обмеженою.[89] Хоча сповіщення, що трансформуються в STR, часто створюють корисну базу розвідданих на основі атаки, на момент подання вони зазвичай мають обмежену негайну корисність для органів влади: лише 1–2% STR, як правило, стають підставою для розслідувань правоохоронців щодо будь-якого виду злочину.[90] Серед опитаних для цього дослідження посадовців існував відчутний скептицизм щодо цінності STR для ПФТ: один колишній високопосадовець британської поліції із великим стажем зауважив, що він «ніколи» не бачив STR, «яке призвело до розслідування щодо фінансування тероризму», і подібні погляди висловлювали також шведські та нідерландські посадовці.[91]

Існує низка проблем із системами моніторингу транзакцій, які впливають на їхню здатність виявляти кримінальні патерни. Командам з комплаєнсу фінансових установ часто бракує точності у моніторингу і вони користуються доволі базовими наборами червоних прапорців або типологій, такі як надходження коштів із юрисдикцій підвищеного ризику або міжнародне

[88] Інтерв'ю авторів у форматі відеоконференції з Peter Neumann, 4 травня 2020 р.; інтерв'ю авторів у форматі відеоконференції з Nicholas Ryder, 24 квітня 2020 р.; Neumann, «Не слідуй за грошима», с. 101; Ridley, *Фінансування Тероризму*, с. 208.

[89] Інтерв'ю автора у форматі відеоконференції зі старшим фахівцем із комплаєнсу Deutsche Bank, 20 березня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшими фахівцями з комплаєнсу HSBC, 23 квітня 2020 р.; інтерв'ю автора у форматі відеоконференції зі старшими фахівцями з комплаєнсу Lloyds Bank, 22 та 27 квітня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшим фахівцем із регуляторних технологій (B), 29 квітня 2020 р.

[90] Redhead, «Глибокий Вплив?», с. 16

[91] Інтерв'ю авторів у форматі відеоконференції з колишнім високопосадовцем правоохоронних органів Великої Британії, 14 травня 2020 р. та 4 червня 2020 р.; інтерв'ю авторів у форматі відеоконференції з аналітиком Шведського ПФР, 3 липня 2020 р.; інтерв'ю автора у форматі відеоконференції з колишнім посадовцем правоохоронних органів Нідерландів, 3 червня 2020 р.

переміщення великих чи структурованих сум.[92] Платформи також зазвичай мають недостатню здатність до виявлення дрібних деталей, що є проблемою з огляду на порівняно невеликі обсяги багатьох операцій з фінансування тероризму.[93] Команди з комплаєнсу також застосовують порогові значення, аби система не була перевантажена великою кількістю сповіщень про невеликі операції.[94]

Доступ до контекстної інформації є додатковою проблемою для фінансових установ, які гарантовано мають доступ лише до власних фінансових та клієнтських даних. Оцінка того, чи є транзакція підозрілою, може залежати від інформації, що зберігається в інших фінансових установах або в альтернативних джерелах.[95] Це особливо помітно у ПФТ щодо засекречених матеріалів, які, якби були доступні, могли б змінити оцінку фінансової установи з «нешкідливої» операції на більш тривожну.[96]

Попри те, що наведені труднощі можуть наштовхувати на думку, що саме низька якість звітності є причиною обмеженого використання STR органами влади, так буває не завжди — навіть повідомлення вищої якості можуть мати незначний вплив, якщо правоохоронці їх визнають нерелевантними для поточних розслідувань. Більшість STR не розповсюджуються ПФР проактивно і залишаються в їхніх базах даних, очікуючи подальших пошуків із боку правоохоронців.[97]

Розповсюдження інформації є проблемою не лише в правоохоронних органах, оскільки інші відомства, відповідальні за боротьбу з тероризмом - особливо розвідувальні служби - не отримують ці звіти за замовчуванням. Такі відомства, безумовно, використовують фінансові розвіддані у контртерористичних розслідуваннях, але збирають її лише в окремих випадках, на підставі юридично санкціонованих запитів до фінансових установ щодо конкретних осіб, які вже перебувають під слідством. Загалом розвідка значною мірою залишається ізольованою від процесів формування фінансових розвідданих для ПФТ у приватному секторі.[98]

---

[92] Інтерв'ю автора у форматі відеоконференції зі старшим фахівцем із комплаєнсу Deutsche Bank, 20 березня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшими фахівцями з комплаєнсу HSBC, 23 квітня 2020 р.; інтерв'ю автора у форматі відеоконференції зі старшими фахівцями з комплаєнсу Lloyds Bank, 22 та 27 квітня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшим фахівцем із регуляторних технологій (B), 29 квітня 2020 р.

[93] Інтерв'ю авторів у форматі відеоконференції зі старшим фахівцем із регуляторних технологій (B), 29 квітня 2020 р.

[94] Matthew Redhead, «Майбутнє моніторингу транзакцій: кращі способи виявлення фінансових злочинів», *SWIFT Institute Working Paper*, березень 2021 р., с. 18.

[95] *Ibid.* с.25

[96] Інтерв'ю авторів у форматі відеоконференції з колишнім високопосадовцем правоохоронних органів Великої Британії, 4 червня 2020 р.; інтерв'ю автора у форматі відеоконференції з колишнім офіцером розвідки Великої Британії, 20 травня 2020 р.

[97] Інтерв'ю авторів у форматі відеоконференції з колишнім високопосадовцем правоохоронних органів Великої Британії, 4 червня 2020 р.; інтерв'ю авторів у форматі відеоконференції з аналітиком Шведського ПФР, 3 липня 2020 р.; інтерв'ю автора у форматі відеоконференції з колишнім посадовцем правоохоронних органів Нідерландів, 3 червня 2020 р.

[98] Інтерв'ю авторів у форматі відеоконференції з колишнім високопосадовцем правоохоронних органів Великої Британії, 4 червня 2020 р.; інтерв'ю автора у форматі відеоконференції з колишнім офіцером розвідки Великої Британії, 20 травня 2020 р.; інтерв'ю автора у форматі відеоконференції з колишнім посадовцем правоохоронних органів Нідерландів, 3 червня 2020 р.; інтерв'ю авторів у форматі відеоконференції із представниками Служби Безпеки Швеції, 2 липня 2020 р.

Проблеми Самостійно Ініційованого Тероризму

Проблеми з наданням розвідданих, які можна оперативно використати, особливо загострюються у випадку терористів, які здійснюють самостійно ініційовані атаки. Системи скринінгу, що намагаються зіставляти імена клієнтів і контрагентів із санкційними переліками та списками терористів, ідентифікують тільки помітних осіб, пов'язаних із забороненими або визначеними організаціями; натомість більшість терористів, які здійснюють самостійно ініційовані атаки, не внесені до цих списків, навіть якщо вже відомі органам влади. Типові червоні прапорці ФТ, які зосереджені на великих сумах і закордонних операціях, також здебільшого нерелевантні для цієї категорії терористів. Дані, наведені у попередньому розділі, свідчать, що такі терористи зазвичай є периферійними фігурами зі скромними фінансовими ресурсами, які фінансуються всередині країни з легальних джерел, таких як заробітна плата та соціальні виплати, а також за рахунок дрібної злочинності. Хоча їхня діяльність і має викликати занепокоєння, вона зазвичай виходить за рамки параметрів поточного моніторингу.[99] Насправді планування атак такими терористами особливо важко виявити, коли моніторингові платформи не налаштовані розрізняти, де саме витрачаються кошти (наприклад, на Amazon або eBay), і що саме купується. У випадку з терористами, які здійснюють самостійно ініційовані атаки, зазвичай важливішим є те, що купують, а не хто продає.

Еволюція Режиму з Протидії Фінансуванню Тероризму

Від часу свого становлення засадові елементи режиму з ПФТ залишалися незмінними, хоча рамка з часом розширювалася й розвивалася. Основний підхід FATF і її членів полягав у поширенні вже наявних вимог з ПВК/ФТ на дедалі ширше коло секторів, які вони вважають потенційно вразливими до злочинних і терористичних цілей. Останнім часом було охоплено постачальників послуг у сфері віртуальних активів (VASP), зокрема криптовалютні біржі.[100]

Ще одним урядовим підходом є виявлення та закриття прогалин після терористичних подій. Наприклад, унаслідок атак у Парижі в листопаді 2015 року французька влада запровадила суворіші обмеження на використання передплачених карток — продуктів, якими користувалися нападники; подібні обмеження були відображені в п'ятій версії Директиви ЄС з протидії відмиванню коштів (AMLD5), що набула чинності в липні 2018 року.[101]

---

[99] Інтерв'ю автора у форматі відеоконференції зі старшим фахівцем із комплаєнсу Deutsche Bank, 20 березня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшими фахівцями з комплаєнсу HSBC, 23 квітня 2020 р.; інтерв'ю автора у форматі відеоконференції зі старшими фахівцями з комплаєнсу Lloyds Bank, 22 та 27 квітня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшим фахівцем із регуляторних технологій (A), 23 березня 2020 р., 30 квітня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшим фахівцем із регуляторних технологій (B), 29 квітня 2020 р.

[100] FATF, «Керівництво з Ризик-Орієнтованого Підходу для Віртуальних Активів та Постачальників Послуг з Віртуальних Активів», червень 2019 р. Франція нещодавно запровадила суворі вимоги «знай свого клієнта» (KYC) для всіх постачальників послуг у сфері віртуальних активів, посилаючись на дані про те, що осередки в країні раніше фінансували себе за допомогою криптовалют. Див.: Danny Nelson, «Франція Оголосила Війну Криптоанонімності, Вказавши "Тероризм" у Мандаті з KYC», *CoinDesk*, 9 грудня 2020 р., https://www.coindesk.com/france-kyc-crypto

[101] Консультативна рада з питань ПВК/ФТ, «Національний аналіз ризиків ВК/ФТ у Франції», вересень 2019 р., сс. 58–59, https://www.economie.gouv.fr/files/files/directions_services/tracfin/analyse-nationale-des-risques-lcb-ft-en-France-septembre-2019.pdf,; ЄС, «Directive (EU) 2018/843».

Інновації у Сфері Фінансових Послуг

Alongside governments, leading European financial institutions have also sought new ways to approach CTF. In the last decade, financial institutions have recruited many former law enforcement, military and intelligence staff, often with backgrounds in counterterrorism, into financial crime compliance and risk-management functions.102 Although this recruitment surge has not been specifically CTF focused, it has had an impact on the devotion of resources within financial institutions, with erstwhile government professionals taking a greater interest in the investigation of networked or national security-related threats.103 This has encouraged several European banks to undertake proactive analytic and investigative work in recent years on headline CTF issues, especially on travel to and from the Middle East by Europe-based foreign terrorist fighters.104 Much of this work has involved the use of new tools, such as machine learning algorithms and social network analysis, to find patterns and relationships in bulk client data. Machine learning is also being used to improve the performance of existing AML/CTF controls such as screening and transaction monitoring, making it easier to categorise known patterns of suspicious behaviour with greater accuracy and speed than before.105

Паралельно з урядами провідні європейські фінансові установи також шукали нові підходи до ПФТ. Упродовж останнього десятиліття вони активно залучали до підрозділів з комплаєнсу та управління ризиками колишніх співробітників правоохоронних органів, військових та розвідників, часто з досвідом у контртероризмі.[102] Хоча ця хвиля найму не була націлена виключно на ПФТ, вона вплинула на пріоритезацію ресурсів усередині установ: колишні держслужбовці приділяють більше уваги розслідуванню мережевих загроз і ризиків, пов'язаних із національною безпекою.[103] Це спонукало низку європейських банків упродовж останніх років здійснювати проактивну аналітичну та розслідувальну роботу щодо ключових питань з ПФТ, зокрема стосовно поїздок до й з Близького Сходу іноземних бойовиків, які проживають в Європі.[104] Значна частина цієї роботи ґрунтувалася на використанні нових інструментів, таких як алгоритми машинного навчання та аналізу соціальних мереж, для виявлення закономірностей і зв'язків у великих масивах клієнтських даних. Машинне навчання також застосовується для підвищення ефективності наявних заходів з ПВК/ФТ, таких як скринінг і моніторинг транзакцій, що полегшує класифікацію відомих патернів підозрілої поведінки з більшою точністю та швидкістю, ніж раніше.[105]

[102] Redhead, «Глибокий Вплив?», с. 27
[103] Інтерв'ю авторів у форматі відеоконференції зі старшими фахівцями з комплаєнсу Lloyds Bank, 27 квітня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшими фахівцями з комплаєнсу HSBC, 23 квітня 2020 р.
[104] Інтерв'ю автора у форматі відеоконференції зі старшим фахівцем із комплаєнсу Deutsche Bank, 20 березня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшими фахівцями з комплаєнсу HSBC, 23 квітня 2020 р.; інтерв'ю автора у форматі відеоконференції зі старшими фахівцями з комплаєнсу Lloyds Bank, 22 та 27 квітня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшим фахівцем із регуляторних технологій (A), 23 березня 2020 р., 30 квітня 2020 р.
[105] Інтерв'ю авторів у форматі відеоконференції зі старшим фахівцем із регуляторних технологій (B), 29 квітня 2020 р.

Партнерство з Обміну Фінансовими Розвідданими (FISP)

Зростання інтересу до підвищення ефективності ПФТ як у державному, так і в приватному секторах зумовило спроби розв'язати цю проблему через FISP. На практиці такі домовленості означають передання правоохоронними органами стратегічних та типологічних розвідданих сектору фінансових послуг, щоб допомогти йому тонше налаштовувати контролі з ПВК/ФТ і забезпечувати рамки для швидкого обміну розвідданими щодо підозрюваних у відповідь на атаки. У дев'яти європейських країнах є функціонуюче FISP, і з них сім наразі визначили фінансування тероризму пріоритетною сферою співпраці.[106]

Водночас більшість держав-членів ЄС не пішли цим шляхом, а у випадку Франції уряд обрав альтернативний підхід до обміну фінансовими розвідданими. Починаючи з 2015 року Франція надала мандат Tracfin, місцевому ПФР, здійснювати прямий моніторинг фінансової активності осіб, включених до бази даних Міністерства внутрішніх справ Франції щодо відомих терористів, злочинців і підозрюваних.[107] Хоча це не скасовує зобов'язань з ПВК/ФТ для фінансових установ та інших суб'єктів, такий підхід забезпечує французькій владі безпосереднє бачення фінансової активності осіб, які вже викликають занепокоєння.

Вплив Реформ у Сфері Протидії Фінансуванню Тероризму

Оцінити внесок цих змін у загальну результативність ПФТ складно. Хоча поширення чинних правил на нові сфери діяльності у відповідь на появу загроз є необхідним кроком, це фактично безкінечний процес, адже всі терористи, зокрема ті, хто здійснює самостійно ініційовані атаки, виявляють мінливість і гнучкість у своїй фінансовій поведінці. Як зазначив у інтерв'ю французький посадовець, споживчі кредити, які використовував Кулібалі, були привабливою типологією фінансування тероризму у Франції, але після запровадження суворіших контролів після його нападу терористи звернулися до нерегульованого онлайн-простору або до кримінальної діяльності.[108] Зміни правил призвели до переміщення активності, а не до її усунення.

Водночас оцінки практиків щодо впливу інновацій приватного сектору переважно позитивні. Хоча використання фінансовими установами передових технологій для виявлення зрушень у поведінці або нетипових патернів перебуває на відносно ранній стадії, багато представників приватного сектору вважають, що це має потенціал генерувати нові корисні для ПФТ фінансові розвіддані, особливо якщо її формування спирається на поради правоохоронних органів і

[106] Юрисдикції, де діють партнерства з обміну фінансовою розвідінформацією, — Австрія, Велика Британія, Ірландія, Латвія, Литва, Нідерланди, Німеччина, Фінляндія та Швеція. Із них лише Австрія та Німеччина не визначають ПФТ пріоритетом. Див.: Maxwell, «Survey Report», сс. 28–50.

[107] Michael Stothard, «Франція прагне нових повноважень для моніторингу банківських рахунків підозрюваних у тероризмі», *Financial Times*, 23 листопада 2015 р.; інтерв'ю авторів у форматі відеоконференції з аналітиками французького підрозділу фінансової розвідки (ПФР), 10 вересня 2020 р.

[108] Інтерв'ю автора у форматі відеоконференції з колишнім аналітиком французького ПФР, 30 червня 2020 р.

розвідувальних служб щодо актуальних типологій.[109] Наявні дані про користь від FISP є обнадійливими. Наприклад, у Нідерландах спеціалізоване на фінансуванні тероризму FISP — Робоча група з питань фінансування тероризму Нідерландів — у період із липня 2017 р. по червень 2019 р. підготувала 300 тематичних звітів, які містили у 6,4 раза більше придатної до розкриття розвідінформації, ніж середньостатистичне STR, пов'язане з фінансуванням тероризму.[110] Втім, через обмежений масштаб FISP дотепер можуть зосереджуватися лише на відносно невеликій кількості резонансних розслідувань. У Нідерландах ПФР отримав майже 2,5 млн STR лише у 2019 році,[111] тож згадані 300 справ становлять мізерну частку від загального масиву.

Реформи у Сфері Протидії Фінансуванню Тероризму та Самостійно Ініційований Тероризм

Ще складніше визначити, який вплив ці зміни справили на протидію загрозі від терористів, які здійснюють самостійно ініційовані атаки, і практики скептично оцінювали спроможність режиму з ПФТ розв'язати цю проблему без радикальних реформ. Як зауважив в інтерв'ю один зі шведських посадовців, обмежена здатність режиму з ПФТ надавати корисні розвіддані до атаки — це «a feature, not a bug».[112]

У Великій Британії обмін типологічною інформацією саме щодо атак терористів, які здійснюють самостійно ініційовані атаки, через Об'єднану цільову групу з розвідки у сфері протидії відмиванню коштів (Joint Money Laundering Intelligence Taskforce, JMLIT) допоміг низці великих фінансових установ провести пошуково-аналітичну роботу довкола цієї проблематики.[113] Провідні фінансові установи у Франції та Німеччині також виконували подібні аналітичні дослідження щодо таких терористів.[114] Втім, публічно доступної інформації, щоб оцінити, чи мав отриманий матеріал позитивний ефект, немає, і є свідчення, що через те, що ці приватні аналізи ґрунтуються на оцінках «ризику», а не на юридичному критерії «підозри», вони часто

[109] Інтерв'ю автора у форматі відеоконференції зі старшим фахівцем із комплаєнсу Deutsche Bank, 20 березня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшими фахівцями з комплаєнсу HSBC, 23 квітня 2020 р.; інтерв'ю автора у форматі відеоконференції зі старшими фахівцями з комплаєнсу Lloyds Bank, 22 та 27 квітня 2020 р.; інтерв'ю авторів у форматі відеоконференції з колишнім високопосадовцем правоохоронних органів Великої Британії, 4 червня 2020 р.; інтерв'ю автора у форматі відеоконференції з колишнім офіцером розвідки Великої Британії, 20 травня 2020 р.; інтерв'ю автора у форматі відеоконференції з колишнім посадовцем правоохоронних органів Нідерландів, 3 червня 2020 р.

[110] Maxwell, «Survey Report», с. 20.

[111] ПФР Нідерландів, «Щорічний Огляд: 2019», с. 31, https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/fiu-nederland_jaaroverzicht_2019_en_0.pdf

[112] Інтерв'ю авторів у форматі відеоконференції з аналітиком Шведського ПФР, 3 липня 2020 р.

[113] Інтерв'ю авторів у форматі відеоконференції з британською компанією у сфері регуляторних технологій (RegTech), 29 квітня 2020 р.; інтерв'ю авторів у форматі відеоконференції з ізраїльською компанією у сфері регуляторних технологій (RegTech), 30 квітня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшим фахівцем із комплаєнсу Lloyds Bank, 27 квітня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшими фахівцями з комплаєнсу HSBC, 23 квітня 2020 р.

[114] Інтерв'ю автора у форматі відеоконференції зі старшим фахівцем із комплаєнсу Deutsche Bank, 20 березня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшим фахівцем із регуляторних технологій, 23 березня 2020 р. та 30 квітня 2020 р.

залишаються невикористаними органами влади — навіть там, де існують FISP.[115] Хоч це і проблема, зумовлена чинним законодавством у сфері ПВК/ФТ, її посилює стаття 7 Загального регламенту ЄС із захисту даних (GDPR), яка забороняє обмін інформацією про фізичних осіб без згоди, якщо тільки, відповідно до статті 29, це не відповідає «суспільному інтересу».[116]

Набагато кращі свідчення стосуються ролі FISP в обміні розвідданими в режимі реального часу щодо терористів, які здійснюють самостійно ініційовані атаки, вже після здійснення атаки, коли фінансові установи підтримували розслідування.[117] Кілька великих фінансових установ відзначали свою участь у таких зусиллях, а державні слідчі підтверджували цінність їхнього внеску — оперативної інформації щодо закупівель, матеріалів CDD та ідентифікації додаткових підозрюваних за даними транзакцій. Під час інтерв'ю високопосадовець із Нідерландів наголосив, наскільки корисними були фінансові розвіддані, передані через механізми FISP, для встановлення місцеперебування підозрюваного у стрілянині в трамваї в місті Утрехт у березні 2019 року.[118]

Попри це, такий обмін має обмежений вплив на проактивну діяльність спецслужб і поліції з недопущення подібних атак, за винятком ідентифікації через фінансові зв'язки екстремістських спільників, які самі в подальшому можуть здійснити самостійно ініційовані атаки. Оскільки FISP переважно зосереджені на пріоритетних і стратегічних питаннях, у більшості юрисдикцій не існує повсякденної операційної інфраструктури, потрібної для масштабного обміну такою інформацією щодо відомих, але менш пріоритетних цілей, за винятком, можливо, Франції, де Tracfin уже безпосередньо відстежує фінансову діяльність широкого кола осіб, підозрюваних у тероризмі.

Угоди в рамках FISP також не мають очевидного зв'язку з превентивними контртерористичними діями, спеціально спрямованими на подолання загрози самостійно ініційованого тероризму у самому зародку. У Швеції Служба безпеки SÄPO тісно взаємодіє з багатьма елементами державного сектору — соціальними службами, охороною здоров'я, освітою — для виявлення осіб групи ризику, особливо з проблемами психічного здоров'я.[119] Останніми роками Велика Британія також розширила рамку свого контртерористичного підходу, створивши локальні багатовідомчі центри, де поліція та спецслужби працюють спільно з відомствами охорони здоров'я, освіти й соціального забезпечення, здійснюючи взаємний обмін інформацією про осіб, що викликають занепокоєння, у безпечному та перевіреному середовищі.[120] Однак ці програми передусім залучають державні органи та громадські інституції, а не приватних постачальників розвідінформації, як-от фінансові установи чи соціальні медіа. З огляду на минулі випадки, є достатні підстави припускати, що додавання матеріалів від таких постачальників могло б надати потенційно корисну інформацію про діяльність уразливої особи.

---

[115] Інтерв'ю авторів у форматі відеоконференції зі старшими фахівцями з комплаєнсу Lloyds Bank, 22 та 27 квітня 2020 р.; інтерв'ю авторів у форматі відеоконференції зі старшими фахівцями з комплаєнсу HSBC, 23 квітня 2020 р.

[116] GDPR.EU, «General Data Protection Regulation», https://gdpr.eu/tag/gdpr/

[117] Інтерв'ю авторів у форматі відеоконференції зі старшими фахівцями з комплаєнсу **HSBC**, 23 квітня 2020 р.

[118] Інтерв'ю автора у форматі відеоконференції з колишнім посадовцем ПФР **Нідерландів**, 3 червня 2020 р.

[119] Інтерв'ю авторів у форматі відеоконференції з посадовцями Служби безпеки Швеції (SÄPO), 2 липня 2020 р.

[120] Home Office, *CONTEST: Стратегія Сполученого Королівства щодо Боротьби з Тероризмом* (Лондон: The Stationery Office, червень 2018), с. 42.

Шлях Уперед

Попри спроби вдосконалити режим з ПФТ, методи збирання та розповсюдження фінансових розвідданих у ФТ залишаються грубими й некерованими, що створює особливі труднощі для протидії загрозі самостійно ініційованого тероризму. Це прикра ситуація, адже очевидно, що терористи, які здійснюють самостійно ініційовані атаки, залишають фінансові сліди, але їх не трансформують у розвіддані, придатні для використання органами влади. Розвиток FISP свідчить, що режим з ПФТ рухається у правильному напрямку, однак ці механізми все ще за кілька кроків від того, щоб відчутно впливати на самостійно ініційований тероризм. З огляду на ширші контртерористичні зусилля, більш масштабна взаємодія в режимі реального часу між розвідувальними службами, правоохоронними органами та «нетрадиційними» партнерами, такими як фінансові установи, може виявитися ефективнішим шляхом до подолання цієї прогалини.

Висновки та Рекомендації

САМОСТІЙНО ІНІЦІЙОВАНІ ТЕРОРИСТИЧНІ АТАКИ залишаються сталою загрозою в Європі, хоча зазвичай їх не розглядають крізь призму фінансування тероризму. У цьому документі зроблено спробу започаткувати будівництво кращої доказової бази щодо фінансової поведінки терористів, які здійснюють самостійно ініційовані атаки, під час планування нападів, а також оцінити, наскільки ефективними були чинні контролі з ПФТ у їх виявленні. Дослідження дало низку висновків — і потенційних варіантів подальших дій — викладених у цьому розділі.

Фінансова Поведінка Терористів, Які Здійснюють Самостійно Ініційовані Атаки

Наявна академічна література щодо вимірів фінансування самостійно ініційованого тероризму обмежена, а інтерв'ю з правоохоронцями та іншими посадовцями у сфері протидії тероризму виявили поширене припущення, ніби у відповідних справах майже немає суттєвих фінансових аспектів для аналізу.

Більшість атак, розглянутих у цьому дослідженні, справді були відносно маломасштабними та проявляли низький рівень складності. Найпоширенішими залишаються напади із застосуванням гострих предметів, як-от ножа, який легко дістати у побуті. Втім, те, що таку зброю можна придбати без помітної фінансової активності, не означає, що це завжди так і відбувається. Дослідження знайшло приклади, коли терористи спеціально купували холодну зброю з метою вчинення нападу, інколи в мережевих роздрібних магазинах, інколи у спеціалізованих продавців. Такі дії залишають слід.

Інші форми підготовки також можуть залишати фінансові «сліди». Якщо транспортні засоби чи вогнепальну зброю не викрадено, за них доводиться платити, навіть коли їх отримують через злочинні канали. Підготовка до атак із використанням СВП, що передбачає закупівлю різних компонентів, так само пов'язана зі значною фінансовою та комерційною активністю, як показують випадки ліонського нападника 2019 року Мохамеда Хічема Меджуба та братів Абеді в Манчестері.

Ключовий висновок 1: Планування атак терористами, які здійснюють самостійно ініційовані атаки, може мати фінансовий і комерційний вимір, який практики поки що недооцінюють.

- **Рекомендація 1**: Важливо, щоб Європол, Євроюст та інші дотичні інституції на рівні ЄС спільно з правоохоронними та розвідувальними органами держав-членів збирали й аналізували чутливу та непублічну фінансову й комерційну інформацію у справах самостійно ініційованого тероризму, аби сформувати доказове розуміння поведінки під час планування атак і бібліотеку типологій, що допоможе фінансовим установам краще розуміти логістику таких подій.

Ще одне поширене припущення полягає в тому, що будь-яка фінансова активність терористів, які здійснюють самостійно ініційовані атаки, переважно «невидима», здійснюється готівкою або поза межами традиційних фінансів, у нових фінансових технологіях (наприклад, у криптовалютах). Це дослідження свідчить, що готівка справді відіграє значну роль, але поєднується з цифровими транзакціями, які залишають більш стійкий слід. Деякі з терористів користувалися продуктами поза «традиційною» банківською системою, такими як спеціалізовані платіжні послуги і у невеликій кількості випадків, криптовалютами, але це поєднувалося з послугами традиційних постачальників послуг, включно з банками.

Ключовий висновок 2: Фінансова активність таких терористів не обов'язково незначна чи «невидима»; для реалізації своїх намірів вони використовують різні канали та продукти, включно з готівкою, цифровими платежами та, у невеликій кількості випадків, фінансовими технологіями.

- **Рекомендація 2a:** Приватний сектор і органи ЄС мають кращі шанси відстежити підозрілу діяльність там, де не використовується готівка. Тому Європейська Комісія має розглянути потенційні переваги обмеження готівкових розрахунків (або запровадження вимог ідентифікації та верифікації клієнта) під час купівлі обмеженого переліку предметів підвищеного ризику, таких як декоративні чи ритуальні види холодної зброї, а також хімікати, що застосовуються у СВП.
- **Рекомендація 2b:** У межах ширших повноважень з ПВК/ФТ Європейська Комісія має щорічно разом із відповідними агенціями ЄС переглядати, чи охоплюють Директиви з ПВК усі відповідні нові фінансові технології та платформи, які можуть використовувати злочинці та терористи.

Ще один помітний вимір розглянутих випадків — значна взаємодія терористів, які здійснюють самостійно ініційовані атаки, з «універсальними» інтернет-ритейлерами на кшталт Amazon та eBay, особливо під час закупівлі компонентів для СВП. Хоч це й не є суто фінансуванням тероризму, очевидно, що такі майданчики відіграють важливу роль як потенційні постачальники та акумулюють значні обсяги даних про фінансову активність своїх клієнтів, а відтак і про можливу логістику підготовки атак окремими терористами.

Ключовий висновок 3: Економічна екосистема, у якій нині діють терористи, є широкою, а їхня фінансова активність також залишає комерційні відбитки, пов'язані з купівлею предметів підвищеного ризику. Наразі немає вимог до комерційних установ здійснювати моніторинг, ідентифікацію чи звітування щодо потенційно підозрілих закупівель, пов'язаних із фінансуванням тероризму.

- **Рекомендація 3a:** Європейська Комісія має розглянути можливість створення переліку «предметів підвищеного ризику», які можуть бути використані в атаках самостійно ініційованого тероризму, щоб допомогати продавцям приймати рішення про здійснення продажу.
- **Рекомендація 3b:** Європейська Комісія має розглянути питання, чи слід заохочувати окремі типи роздрібних торговельних точок, що продають високоризикові предмети, до запровадження добровільних механізмів повідомлення про підозрілі предмети або ж охопити їх обов'язковими вимогами з ПВК/ФТ щодо моніторингу та звітування.

Ефективність Протидії Фінансуванню Тероризму та Самостійно Ініційований Тероризм

Як зазначалося у попередньому розділі, чинний режим з ПФТ передусім зосереджений на виявленні фінансування тероризму, пов'язаного з відомими терористичними угрупованнями. На фінансові установи та інші підзвітні суб'єкти покладено обов'язок ідентифікувати потенційних терористів серед клієнтів або контрагентів, заморожувати рахунки та передавати фінансові розвіддані до ПФР для подальшого використання правоохоронними органами.

Загалом вплив такого підходу є змішаним, частково через його відносну негнучкість перед обличчям мінливої терористичної загрози. Більше того, він покладається на те, що фінансові установи матимуть знання та технологічні спроможності для виявлення відповідних фінансових розвідданих, а бюрократичні процеси ефективно доставлятимуть і поширюватимуть її в межах державного сектору. Ці базові виклики ПФТ особливо загострюються стосовно терористів, які здійснюють самостійно ініційовані атаки, адже інструменти скринінгу виявляють лише «відомих» терористів, а системи моніторингу транзакцій зазвичай не калібровані на виявлення поведінкових патернів, що можуть свідчити про їхню діяльність.

Ключовий висновок 4: ПФТ стикається з базовими проблемами у виявленні фінансових розвідданих через фокус на застарілих моделях фінансування тероризму; ці проблеми посилюються у випадках невеликого масштабу, але складної природи — як із терористами, що здійснюють самостійно ініційовані атаки.

- **Рекомендація 4:** Європейська Комісія та відповідні агенції ЄС мають провести консультації щодо шляхів забезпечення того, щоб фінансові установи та інші підзвітні суб'єкти генерували більш якісні та своєчасні фінансові розвіддані про терористів, які здійснюють самостійно ініційовані атаки. Це може включати:
    - розроблення доказово обґрунтованих типологій, кейсів та супровідних матеріалів щодо терористів, які здійснюють самостійно ініційовані атаки (спираючись на роботу з Рекомендації 1), для поширення серед урядів і агенцій держав-членів та приватного сектору - суб'єктів ПВК/ФТ;
    - дослідження доцільності того, як платформи моніторингу транзакцій можуть найкраще використовувати сучасні платіжні дані для більш деталізованого бачення клієнтської активності, а також того як нові технології можуть наблизити установи до моніторингу ризиків життю в режимі реального часу.

Ще одне проблемне питання ПФТ — донесення фінансових розвідданих до відповідних ланок державного сектору. Це часто пояснюють проблемами якості STR — інакше кажучи, сприйняттям, що STR не є достатньо корисними, аби їх варто було розповсюджувати. Але так трапляється не завжди, якісні матеріали залишаються невикористаними або через те, що їх вважають нерелевантними для поточних розслідувань, або через те, що їх не розповсюджують іншим зацікавленим сторонам у контртерористичній спільноті.

Ключовий висновок 5: Навіть коли приватний сектор надає добре підготовлені фінансові розвіддані у сфері ПФТ, вони часто слабко узгоджені з пріоритетами розслідувань або неналежно розповсюджуються — і, як наслідок, лишається невикористаною.

- **Рекомендація 5:** Європейська Комісія та відповідні агенції ЄС мають провести консультації щодо шляхів кращого узгодження фінансових розвідданих щодо ПФТ з актуальними пріоритетами ризику та їх доведення до всіх релевантних учасників. Це може включати:
    - розробку механізмів пріоритезації та зворотного зв'язку щодо STR між державним і приватним секторами. Відповідальні державні органи можуть встановлювати конкретні вимоги до видів фінансових розвідданих, яку вони хочуть отримувати (наприклад, потенційна активність терористів, які здійснюють самостійно ініційовані атаки), і надавати оцінки того, чи ці вимоги виконуються;
    - вимогу, щоб усі розвідувальні служби з контртерористичними повноваженнями стали стандартними та інтегрованими учасниками каналів розповсюдження й зворотного зв'язку щодо STR, пов'язаних із ПФТ.

На тлі різних проблем режим ПФТ останніми роками розвивався як через політичні настанови, так і завдяки органічним інноваціям. Уряди розширили охоплення режиму ПВК/ФТ, а фінансові установи залучили талановитих слідчіх та аналітичні технології для проактивних, ризик-орієнтованих проєктів. Також у низці юрисдикцій державний і приватний сектори почали працювати разом у рамках спеціальних FISP, а у Франції — у форматі прямого державного моніторингу транзакцій.

Однак проактивні напрацювання приватного сектору, які можуть генерувати індивідуальні «сліди» для розслідувань, не передаються між державним і приватним секторами через обмеження на обмін персональними даними. Хоча це й не зупинило роботу приватного сектору над проблемою самостійно ініційованого тероризму, це обмежило можливості ширшого використання результатів їх роботи.

Ключовий висновок 6: Чинні ініціативи з формування початкових оперативних сигналів, які здатні виявляти потенційну фінансову розвідінформацію щодо терористів, які здійснюють самостійно ініційовані атаки, не були повною мірою заохочені або використані державним сектором.

- **Рекомендація 6a:** Європейська Комісія та відповідні агенції ЄС, зокрема Європол і новий регуляторний орган ЄС з ПВК/ФТ, мають заохочувати національні правоохоронні органи й регуляторів, а відтак і приватний сектор, до ширшого використання нових технологій і аналітики даних, зокрема щодо проблеми терористів, які здійснюють самостійно ініційовані атаки. Оптимально, це має відбуватися в межах кооперативних середовищ на кшталт FISP.
- **Рекомендація 6b:** Європейській Комісії варто розглянути питання підтримки такої форми співпраці шляхом перегляду та, за потреби, розширення правових підстав і порогових критеріїв для обміну даними з ПФТ у законодавстві з ПВК/ФТ та у сфері захисту даних.

Поточну роботу з ПФТ також ускладнює бюрократичний характер наявних партнерств. Періодичний, заснований на зустрічах формат більшості FISP не дозволяє здійснювати обмін розвідданими в режимі реального часу, окрім як після атаки. До того ж FISP зосереджені на відомих, високоризикових цілях, а не на менш пріоритетних або невідомих особах, які часто й стають терористами, що здійснюють самостійно ініційовані атаки. У кількох юрисдикціях, крім того, такі потенційні терористи нині є фокусом локальних превентивних інтервенцій, де агрегуються розвіддані з усього державного сектору, проте, схоже, не охоплюють фінансові розвіддані або інші види розвідданих від приватного сектору.

Ключовий висновок 7: Нинішні форми співпраці у сфері ПФТ не мають достатньої структурної гнучкості та широти, щоб проактивно протидіяти проблемі самостійно ініційованого тероризму.

- **Рекомендація 7:** Європейська Комісія та відповідні агенції рівня ЄС мають розглянути варіанти більш гнучкого та швидкого обміну розвідінформацією з ПФТ для проактивної ідентифікації терористів, які здійснюють самостійно ініційовані атаки. Це може включати оцінку ймовірних витрат та операційних вигод:
    - прямого обміну даними/моніторингу транзакцій щодо ризиків ФТ державним органом (за зразком Франції) або потенційно у співпраці з приватним сектором;
    - розбудови приватно-публічних осередків з розвідданих для створення обміну даними в режимі реального часу з питань ПФТ, зокрема щодо потенційних терористів, які здійснюють самостійно ініційовані атаки.

Оцінювання Витрат

Ймовірно, що таке оцінювання вкаже на потребу в додаткових інвестиціях з державного та/або приватного секторів для підтримки запропонованих опцій, що порушує базове практичне питання: «хто платить?». Потрібно враховувати реальні обмеження державних видатків. Якщо ці варіанти розглядатимуться — особливо у межах Рекомендації 7 — слід також оцінити потенційні моделі фінансового навантаження між секторами, наприклад запропонований у Великій Британії збір із банків для підтримки розширеної урядової відповіді на економічну злочинність.[121]

Заклики до реформ, що потребують більших інвестицій, порушують також питання фінансової пропорційності, з огляду на відносно обмежений людський та економічний вплив більшості самостійно ініційованих терористичних атак порівняно з масштабними атаками, скоординованими терористичними угрупованнями. Питання, чи вважатимуть уряди такі інвестиції виправданими з точки зору зменшення кількості подібних атак, містить політичні та етичні припущення, і в рамках подібного документу складно рекомендувати, де саме провести баланс. Хоча в цьому документі не пропонується конкретних рекомендацій в цьому контексті, автори вважають життєво необхідним розглянути ці питання. Той факт, що щось можна зробити, не означає, що це потрібно робити, особливо якщо це тягне небажані наслідки.

[121] HM Treasury, *Збір за Економічні Злочини: Фінансування Нових Урядових Заходів для Боротьби з Відмиванням Коштів* (Лондон: The Stationery Office, 2020).

Крім того, деякі потенційні шляхи руху вперед можуть бути більш інвазивними: йдеться про тісніший нагляд за фінансовою активністю окремих осіб, як із боку приватного, так і з боку державного сектору, та, імовірно, ширший обмін такою інформацією. Знову ж таки, це породжуватиме як практичні, так і етичні питання, враховуючи важливість громадянських свобод у європейських суспільствах. Якщо фінансові установи тісніше співпрацюватимуть із правоохоронними органами та розвідувальними службами щодо моніторингу окремих осіб, які потенційно становлять терористичний ризик, мають бути запроваджені належні гарантії; щонайменше, використання захищених систем і перевірка благонадійності відповідних працівників приватного сектору, підтверджена державними органами, з якими співпрацюють фінансові установи. Технологічні рішення, як-от зашифровані технології підвищення конфіденційності (privacy-enhancing technologies), можуть дозволити державному сектору віддалено моніторити фінансову активність таких осіб, не розкриваючи фінансовим установам або їхньому персоналу коло осіб, що становлять інтерес.[122]

[122] Nick Maxwell, *Майбутнє Розповсюдження Фінансових Розвідданих (FFIS): Інноваційний та Дискусійний Документ: Типології Використання Аналізу, що Зберігає Конфіденційність, для Боротьби з Фінансовими Злочинами*, **RUSI/FFIS**, червень 2020 р., сс. 9–12.

Про Авторів

Stephen Reimer - науковий співробітник Центру досліджень з питань фінансових злочинів і безпеки (Centre for Financial Crime and Security Studies, RUSI).

Matthew Redhead - автор, який пише на теми національної безпеки, розвідки та фінансової злочинності. У 2018 році став асоційованим науковим співробітником RUSI у межах програми Financial Crime 2.0. Працював сім років фахівцем із ризиків фінансових злочинів у великому міжнародному банку, а також консультантом із питань фінансових злочинів для секторів FinTech і RegTech. Крім того, обіймав посади державного службовця в Home Office (Міністерстві внутрішніх справ Великої Британії) та Міністерстві оборони Великої Британії.

Додаток

Наведена нижче таблиця подає відомості про 106 випадків самостійно ініційованого тероризму, ідентифікованих за результатами огляду англомовних матеріалів провідних національних друкованих і онлайн ЗМІ з усіх країн, що увійшли до сфери дослідження, за період від січня 2015 до листопада 2020 року. Розподілена за країнами, таблиця показує кількість нападів, учинених однією («Solo»), двома («Dyad») або трьома («Triad») особами, а також ідеологічну мотивацію атак — ісламістський екстремізм («Isl/Ex») або праворадикальний екстремізм («Xrw»). Таблиця також надає розподіл за видами застосованої зброї, включно з тупими предметами («Blunt weapon»), холодною зброєю — зокрема ножами чи мечами («Edged weapon»), вогнепальною зброєю («Firearm»), саморобними вибуховими пристроями/бомбами («IED»), транспортними засобами («Vehicle»), та біохімічною зброєю («Biochem»). Випадки, що включають будь-яку комбінацію інших типів зброї, віднесено до останньої колонки («Combo»).

Рисунок 3: Загальна кількість випадків, розглянутих у відповідних юрисдикціях у період з січня 2015 року по листопад 2020 року

Юрисдикція	Кейси	Розмір Осередку				Ідеологія			Тип Зброї						
		Solo	Dyad	Triad		Isl/Ex	Xrw		Blunt weapon	Edged weapon	Firearm	IED	Vehicle	Biochem	Combo
Франція	35	33	1	1		35	0		1	17	5	2	6	0	4
Велика Британія	25	20	4	1		18	7		0	9	0	8	2	0	6
Німеччина	21	17	1	3		13	8		0	7	4	5	2	1	2
Швеція	4	4	0	0		3	1		0	1	0	1	2	0	0
Австрія	1	1	0	0		1	0		0	0	0	0	0	0	1
Хорватія	1	1	0	0		0	1		0	0	1	0	0	0	0
Італія	3	3	0	0		2	1		0	1	1	0	1	0	0
Данія	3	2	1	1		3	0		0	0	1	2	0	0	0
Норвегія	1	1	0	0		0	1		0	0	1	0	0	0	0
Польща	2	1	0	0		1	1		0	1	0	1	0	0	0
Фінляндія	1	1	0	0		1	0		0	1	0	0	0	0	0
Латвія	1	1	0	0		0	1		0	0	0	0	0	0	1
Нідерланди	4	3	1	0		4	0		0	2	1	1	0	0	0
Бельгія	4	4	0	0		4	0		0	2	0	1	0	0	1
Загалом	**106**	**92**	**8**	**6**		**85**	**21**		**1**	**41**	**14**	**21**	**13**	**1**	**15**