УДК 327.84

НАЦІОНАЛЬНА КОНКУРЕНТНА РОЗВІДКА У ГЛОБАЛІЗОВАНОМУ СВІТІ: НОВІ ВИКЛИКИ ТА ЗАГРОЗИ НА ТЛІ «КАЗУСУ СНОУДЕНА»

Ожеван Микола Андрійович,
доктор філософських наук, професор

Проаналізовано роль служб конкурентної розвідки та різноманітних спецслужб як постачальників та реалізаторів інформації конкурентного змісту, необхідної в торговельно-економічних війнах сучасності. Показано, що економічна розвідка національного рівня нетотожна бізнесовій або корпоративній розвідці.

Ключові слова: **економічна розвідка, конкурентна розвідка, спецслужби, національна конкурентна розвідка.**

Корпоративна конкурентна розвідка в епоху глобалізації

Глобальна економічно-торговельна конкуренція «за правилами» СОТ та інших подібних міжнародних організацій зовсім не знімає, а навпаки, ще більше загострює питання про економічно-торговельні війни, в яких з необхідністю далеко не останню роль відіграють різноманітні спецслужби як постачальники та реалізатори інформації. Відому тезу – «хто володіє інформацією, той володіє світом» – слід доповнити уточнюючою тезою про те, що «володарі світу» не просто володіють інформацією, а володіють інформацією розвідувально-конкурентного змісту [11].

Тісний взаємозв'язок і взаємодія національної економіки та національної безпеки ніколи не були настільки очевидними, як у нинішню епоху глобалізації, коли національна економіка, яка бажає бути конкурентоспроможною, має перебувати у стані перманентної «війни» (або ж іншою мовою – гострої конкуренції) за ринки збуту й сировини, за інновації, за доступ до фінансів, за «мізки» талановитих співробітників тощо.

Економічна або конкурентна розвідка (англ. *economic&competitive intelligence*) успішно поєднує зусилля вихідців із державних спецслужб («безпекарів» та «силовиків») та знавців сучасних ринків (маркетологів) і перетворилася впродовж останніх 30 років на Заході на важливий елемент прийняття рішень, стратегічного прогнозування та планування діяльності бізнесових компаній (корпорацій) в умовах гострої ринкової конкуренції. При визначенні конкурентної розвідки, які пропонують «Товариство професіоналів стратегічної й конкурентної розвідки» (*Strategic & Competitive Intelligence Professionals – SCIP*) та інші подібні професійні об'єднання, наголошується на етичній та легальній виправданості цієї інформаційної діяльності, що принципово вирізняє її від «промислового шпигунства» (*industrial espionage*).

Першою ґрунтовною працею з «конкурентної розвідки» вважається книга Майкла Портера «Конкурентна стратегія: технології аналізу галузей та конкурентів» (вперше вийшла друком у 1980 р.). Власне, питанням «методики аналізу конкурента» присвячений третій розділ цієї праці, де пропонуються чотири «діагностичних компоненти»: *майбутні цілі; наявна стратегія; уявлення; потенційні можливості*. Аналіз першого компоненту має, за задумом автора, дати відповідь на запитання «Що рухає конкурентом?» Аналіз другого компоненту присвячений пошуку відповіді на запитання «Що робить конкурент і на що він спроможний?» Компонент «уявлення» стосується «припущень конкурента» стосовно самого себе й галузі. І, нарешті, компонент «потенційні можливості» присвячений аналізу переваг і слабких сторін конкурента.

Синтетичне зведення усіх даних, які стосуються зазначених чотирьох компонентів, за

задумом Майкла Портера, має дати «на виході» характеристику наступальних або оборонних дій конкурента на певному «полі битви» [18, с. 109–111]. До честі Майкла Портера, у спеціальному додатку до своєї праці він деталізовано навів переліки всіх інформаційних джерел, які потрібно аналізувати, й принагідно дійшов слушного висновку щодо необхідності створення системної конкурентної розвідки: «Вочевидь, щоб отримати дані для всебічного аналізу, самої лише впертої праці недостатньо. Ефективний збір інформації потребує організованого механізму – своєрідної системи конкурентної розвідки [18, с. 114]. Згодом, у 1990 р., М. Портер видрукував іншу фундаментальну працю – «Конкурентні переваги країн», у якій, по суті, поняття «конкурентної розвідки» вивів на національно-державний рівень [19].

Водночас доводиться констатувати, що слабкі конкуренті позиції вітчизняного бізнесу чітко корелюють з відсутністю інтересу ділових людей у просторі СНД до питань конкурентної розвідки. Зокрема, про те, що більшість з них поки що не усвідомили необхідність подібної діяльності, можна судити за даними опитування, яке перманентно проводить інформаційно-аналітичний портал конкурентної, економічної розвідки, бізнес-розвідки й аналітики *SPY. KZ*. Станом на 15.03.2013 від загального числа респондентів 1515 на запитання «Чи користуєтеся Ви послугами конкурентної розвідки?» лише 212 (14 %) відповіли, що в їхніх бізнес-структурах є підрозділи конкурентної розвідки; 108 (7,13 %) заявили, що їхні бізнес-структури користуються послугами «сторонніх компаній». 326 (21,52 %) вважають, що в конкурентній розвідці немає потреби. Більше половини опитаних респондентів – 869 (57,36 %) взагалі не знайомі з поняттям «конкурентна розвідка» [9].

Зазначені тенденції свідчать про те, що для вітчизняного бізнесу, який щойно виходить на міжнародні ринки й невпевнено почувається навіть на внутрішньому ринку, теза щодо невідворотності конкуренції ще не перетворилася на аксіому. Натомість вітчизняний бізнес успадкував чимало патерналістського плану уявлень про роль і значення держави у конкурентній боротьбі та все ще сподівається уникнути належної конкуренції на внутрішніх та зовнішніх ринках за рахунок або державного протекціонізму, або різноманітного «піратства», «товарного патріотизму». Однак із цими ілюзіями доводиться прощатися. Зокрема, після вступу України до СОТ та підписання в перспективі Угоди про асоціацію з ЄС поле протекціоністського маневру та «внутрішнього лобіювання», недоброчесної конкуренції тощо дедалі більше звужуватиметься. «Піратство», тобто грубі порушення прав інтелектуальної власності, випуск різноманітних «сірих» товарів, призводитиме й уже призводить до різноманітних міжнародних санкцій.

Зрештою, український споживач теж дедалі більше виявляється «антипатріотичним» і кволо реагує на заклики деяких політиків: «Будь українцем – купуй українське!» Упродовж останніх років українському бізнесу (як імпортерам, так і експортерам) довелося навіть розпрощатися з ілюзією виживання за рахунок запозиченого з арсеналу «рейганоміки» маніпулювання курсом національної валюти.

Усе зазначене має як у загальнонаціональному масштабі, так і в масштабі окремих виробництв, компаній, корпорацій тощо позитивний сенс, бо відмова держави від грубих методів втручання у функціонування різноманітних ринків на користь вітчизняних виробників чи учасників експортно-імпортних операцій підводить бізнес до усвідомлення необхідності модернізації та інноваційності як стабільних чинників конкурентних переваг, а також необхідності «грати» за світовими правилами конкурентної боротьби. Одним із цих жорстких імперативних правил є економічна або конкурентна розвідка.

Конкурентна розвідка корпоративного (бізнесового) типу стосується різноманітних операцій зі збору та аналізу інформації, необхідної для стратегічних оцінок реального стану та перспектив зовнішнього бізнесового довкілля, а також реальної й потенційної активності на різноманітних ринках компаній-конкурентів. Синонімічний ряд до терміна «конкурентна розвідка» включає такі терміни, як «менеджмент знань» (*knowledge management*); «ринкова розвідка» (*market intelligence*); «ринковий інсайт» (*market insight*); «розвідка конкурента» (*competitor intelligence*); «технічна розвідка» (*technical intelligence*); «бізнес-розвідка» (*business intelligence)* тощо.

Водночас деякі джерела не ототожнюють «конкурентну розвідку» з названими видами розвідувальної діяльності, а навпаки, наполягають на їх відмінностях. При цьому наголошується, що «бізнес-розвідка», на відміну від «конкурентної розвідки», фокусується виключно на внутрішніх процесах у компанії, спрямованих на підсилення її ринкової конкурентоспроможності за посередництвом кращого усвідомлення ринкової ситуації та по-

зиціонування конкурентів, вдаючись при цьому до методів, не завжди етично виправданих.

Тобто у подібній інтерпретації «бізнес-розвідка» є майже тотожною *контррозвідувальній діяльності* і є доменом «безпекарів» та «силовиків», вихідців із державних спецслужб, тоді як «конкуренту розвідку» у «чистому вигляді» вважають доменом діяльності «маркетологів».

«Конкурентну розвідку» органічно доповнюють «культурна розвідка» й «культурне вимірювання» (*cultural intelligence – CQ; CULTINT*), які пропонують *PR*-підрозділам компаній різноманітні методи мінімізації репутаційних ризиків компаній, знешкодження «чорного піару» тощо.

Прототипом «конкурентної розвідки» сучасного типу вважається «бенчмаркінг» (англ. *bench mark* – «початок відліку»), започаткований свого часу компанією *Xerox*, яка, зіткнувшись із конкуренцією з боку японських виробників, створила методику об'єктивного зіставлення власних прийомів і способів діяльності для завоювання ринків з прийомами, способами та методами діяльності конкурентів, порівнявши себе за низкою провідних показників із провідними «гравцями» даного сегмента ринку.

Від «бенчмаркінгу» згодом відбрунькувався «*HR* бенчмаркінг» як конкурентне управління людськими ресурсами (*HR – human resourses*), яке зводиться до порівняльних оцінок витрат компанії на оплату праці, підвищення кваліфікації співробітників тощо. Згодом до «бенчмаркінгу» також долучилися адаптовані та пристосовані у максимально можливому обсязі до світу бізнесу такі розвідувальні технології, як: «профілювання конкурентів» (*competitor profiling*); «стратегічна розвідка й раннє попередження»; (*strategic & early warning &-reconnaissance*); «розвідка даних щодо клієнтів компанії» (*customer intelligence*); «дейт-майнінг» (*data mining);* «моніторинг та аналіз соціальних мереж» (*social media monitoring & analysis*) тощо.

«Казус Сноудена» як момент істини: взаємодія політичного й економічного секторів конкурентної розвідки

Як показав «казус Сноудена», під знаком якого минуло все друге півріччя 2013 р., економічна розвідка національного рівня – це не лише бізнесова або корпоративна розвідка, а й добре відпрацьовані розвиненими країнами світу механізми взаємодії політичної й економічної розвідок, які дозволяють співробітникам державних розвідок («спецслужб») отримувати інформацію розвідувального змісту від співробітників служб конкурентної розвідки бізнесових (корпоративних) структур, і навпаки – у необхідних випадках ділитися з ними інформацію, яка дозволяє приватним транснаціональним структурам отримувати конкурентні переваги на світових ринках.

Інша річ, якими є посередницькі (медіаторські) структури подібної взаємодії. Але, принаймні, сам факт активної взаємодії державних і корпоративних розвідувальних структур зазначали наближені до офіційної влади інформатори автора книги з конкурентної розвідки Ларі Каханера (*Kahaner*), які вказували на те, що представники владних спецструктур постійно постачають бізнесовим структурам інформацію конкурентного змісту й навчають бізнес-розвідників збирати й аналізувати інформацію конкурентного змісту та боротися з нелегальною розвідувальною активністю конкурентів – представників іноземних урядів та компаній [11].

Не роблять із цього приводу таємниці японці, які ще в 1951 р. створили посередницьку проурядову «рахункову» економічну організацію (*clearinghouse for economic information*) – *Japanese External Trade Organization* (*JETRO*). Хоча поза межами Японії *JETRO* має стійку репутацію «розвідувальної» структури, офіційний статус цієї організації є позаурядовим, а на офіційному сайті *JETRO* позиціонує себе як організація, яка має залучати іноземні інвестиції в японську економіку та сприяти японським інвестиціям в економіки зарубіжних країн [10]. Орієнтуючись на офіційний сайт *JETRO*, можна дійти висновку про позитивну динаміку розвитку цієї організації. Станом на 2008 р. *JETRO* мала 73 іноземні представництва у 53 країнах світу. Зокрема, в Німеччині її офіси були представлені у Берліні, Дюссельдорфі та Мюнхені. Станом на 2013 р. таких офісів побільшало до 79-ти у 59 країнах [10].

Левова частка розвідувальних зусиль американського розвідувального співтовариства (*US Intelligence Community*) за часів «холодної війни» припадала на цілі військового характеру, пов'язані з протиборством із СРСР. Скориставшись цим, як зазначалось у доповіді ЦРУ, датованій 1987 р., «Японія: Іноземна розвідка та спеціальні служби», Японія досягла помітних успіхів у національній конкурентній розвідці. За даними вказаної доповіді, до 80 % зусиль японських розвідників було сконцентровано не на політичних, а на економічних цілях. Причому йшлося переважно

про конкурентів із країн Західної Європи та США [11].

За даними *The New York Times*, уже в 1995 р. тодішній президент США Білл Клінтон поставив перед державними спецслужбами завдання якомога активніше включатися в конкурентну боротьбу на боці американських корпорацій, щоб «оборонити й захистити американську конкурентоспроможність, технології й фінансову безпеку у світі, де економічні кризи можуть впродовж хвилини поширюватися глобальними ринками» [21]. У листопаді 1992 р. тодішній керівник ЦРУ Роберт Гейтс заявив, що його відомство дуватиме рішучу відсіч спробам іноземних розвідок вивідувати секрети американського бізнесу.

Щоправда, наступники Білла Клінтона були менш відвертими у своїх настановленнях, а після 11 вересня 2001 р. виправдовували необхідність посилення розвідувальної діяльності виключно й переважно міркуваннями антитерору.

Отже, альянс «ТНК – національні спецслужби» є парадоксальним тільки з першого погляду. Мовляв, інтереси корпорацій виходять за межі національних держав, бо вони транснаціональні (транскордонні) за визначенням, тоді як державні спецслужби мислять категоріями національних кордонів. Насправді у глобалізованому світі неможливо забезпечити національні інтереси поза забезпеченням глобальних, транскордонних інтересів усіх приналежних до даної держави суб'єктів і передусім – ТНК. Особливо це стосується країн, які подібно до США претендують на світове лідерство.

Звичайно, така точка зору поки що не є загальновизнаною навіть у розвинених країнах, але число її прибічників дедалі зростає і «традиціоналістам» доводиться відступати, оскільки зростає число свідчень того, що «рицарям плаща й кинджала» та «акулам світового імперіалізму» дедалі частіше доводиться об'єднувати зусилля [2; 14]. Передача державою традиційних розвідувальних та безпекових функцій приватним структурам, щоправда, дедалі більше загострює проблему приватно-публічного партнерства у цій делікатній й неоднозначній сфері діяльності.

Щодо США, то процесам державно-приватного партнерства у сфері розвідки тут сприяють традиції переходу у бізнесові структури колишніх політиків та розвідників високого рівня, які, використовуючи попередні зв'язки та відому їм із надійних джерел інформацію розвідувального змісту, звичайно, ставлять на службу інтересам корпорацій з метою здобуття ними конкурентних переваг якщо не весь напрацьований ними арсенал знань, то принаймні методологічні й методичні підходи до розв'язання певних проблем.

Узагальнюючи подібний досвід державної розвідувально-інформаційної підтримки економічно-торговельної експансії національних фірм і корпорацій КНР та інших східно-азійських «тигрів», російські теоретики доходять логічного висновку, що між економічною та військовою думкою має відбутися зближення й одним із варіантів такого зближення є «конкурентна розвідка» [14].

Водночас загальновизнаним є той факт, що така чутлива сторона роботи американської розвідки, як її зв'язок з великим бізнесом, коли його інтереси перетинаються з інтересами держави, а іноді й суперечать цим інтересам, постійно перебувають «у тіні». Це та «зворотна сторона місяця» (*dark side of the moon*), про яку дозволяють собі говорити й писати лише журналісти, які спеціалізуються на викривально-розшуковій тематиці, відставні співробітники розвідки, опозиційні політики тощо. Принаймні жоден офіційний документ американських спецслужб, який стосується стратегії розвідки й контррозвідки, матеріалів і доповідей аналітичного та прогностичного характеру, які регулярно виходять із надр розвідувального співтовариства США, безпосередньо не стосується теми співпраці державних і приватно-корпоративних розвідок [14]. Зате у США вистачає друкованих матеріалів на тему подібної розвідувальної співпраці в країнах-конкурентах, що зазвичай відносять на рахунок «недоброчесної конкуренції».

Зокрема, відповідно до тез, викладених у викривально-розшуковій роботі Марка Леонарда «Про що думають в Китаї», на даному етапі її розвитку КНР не може (згідно з уявленнями китайських «експертів») кинути виклик військовій могутності головного конкурента – США, але зате може успішно конкурувати зі США, використовуючи трансмілітарні та немілітарні методи, зав'язані на торгівлю, інвестиції та експорт. Тому КНР надає, мовляв, такого значення розширенню виробництва «сірих» товарів, транскордонним злиттям і поглинанням, використанню наукового потенціалу китайської діаспори у США, активному промисловому шпигунству тощо [13].

В оприлюдненому на початку 2013 р. звіті американської фірми *Mandiant* із питань кібербезпеки безапеляційно вказується, що експерти даної фірми, проаналізувавши численні випадки спроб зламу електронних сис-

тем різних компаній і відомств США, дійшли висновку, що сліди цих зламів ведуть не просто до Китаю, а конкретно – до розташованої в одному з районів Шанхая 12-поверхової будівлі, в якій, за американськими даними, розміщено китайський військовий спецпідрозділ за номером 61398. Зрозуміло, що китайська сторона рішуче відкинула всі ці звинувачення та підозри [1].

До особливої категорії «викривальників-правдолюбців» розвідувально-підривної діяльності спецслужб, які іноді ставлять під великий знак запитання засади демократії та громадянського суспільства, належать громадянські активісти, яких за американською традицією прийнято називати «свистунами» (*a whistleblowers*) й щодо яких завжди існуватиме моральна «дилема Павлика Морозова», оскільки не завжди зрозуміло, наскільки ці люди є щиросердними та благородно мотивованими у своїх викриттях, – «герої» вони чи «зрадники» (*traitor or hero*). Термін *a whistleblower* пов'язаний із традиційним образом полісмена, який сюрчить у свисток, відлякуючи злочинців. Частина представників громадянського суспільства у США розглядає подібне «уайстлблауерство» як необхідний захід самооборони суспільства від держави, яка може зловживати секретною інформацією. У 1988 р. навіть було створено *National Whistleblowers Center*, який надає правову підтримку «свистунам». Типовим «свистуном» був Бредлі Меннінг (*Bradley Manning*), який з міркувань громадської пильності передав чимало секретних матеріалів главі «Вікіліксу» Джуліану Ассанжу. Приклад Б. Меннінга, вочевидь, надихнув Едварда Сноудена (*Edward Snowden*), екс-працівника Агенції національної безпеки (АНБ), а ще раніше ЦРУ (де він працював під дипломатичним прикриттям), який 5–6 червня 2013 р. *розкрив Washington Post* і *Guardian* деякі факти, пов'язані з існуванням шпигунської програми «ПРИЗМА» (*PRISM*), що дозволяє американським спецслужбам перехоплювати із серверів провідних інформаційних компаній світу листування, фото-, відео- й аудіофайли користувачів (включно з популярними сервісами *Microsoft, Google, Facebook, Skype* та ін.).

Характерно, що в листуванні з *Washington Post* Е. Сноуден називав себе *Verax*, що латиною означає «правдолюбець» («той, хто каже правду»). Перша інформація «від Сноудена» про діяльність спецслужб США в Мережі з'явилася 5 червня 2013 р., коли британська *Guardian* повідомила, що таємний суд США розпорядився щодо надання телефонною компанією *Verizon* АНБ даних (метаданих), які стосувалися мільйонів телефонних розмов. Згодом *Washington Post* повідомила, що американські спецслужби мають прямий доступ до серверів дев'яти найбільших інтернет-компаній, зокрема й *Facebook, Google, Microsoft* (якій належить популярний *Skype*) та *Yahoo*.

Прикметно, що всі згадані транснаціональні інтернет-компанії спочатку категорично заперечували передачу даних зі своїх серверів американському уряду, але згодом, рятуючи своє реноме, не заперечували, що в окремих випадках дійсно йдуть на легальну співпрацю з правоохоронними органами, надаючи їм персональні дані клієнтів. При цьому інформаційні ТНК заспокоїли громадськість, що йдеться про мізерну частку повідомлень, які надходили від мізерної частки користувачів. Компанія *Facebook*, зокрема, повідомляла 14 червня 2013 р., що впродовж другого півріччя 2012 р. отримала 9–10 тис. урядових запитів, які стосувалися 19 тис. користувачів (від загалу в 1,1 млрд). *Microsoft* за той самий період отримала нібито запити щодо 31 тис. користувачів (акаунтів). *Apple* оцінив число користувачів «дівайсів», якими цікавилися спецслужби уже в першій половині 2013 р., у 9–10 тис.

У подальшому з'ясувалося, що британські колеги американських розвідників з кіберрозвідки (*The Government Communications Headquarters – GCHQ*) теж вели електронне стеження за іноземними лідерами включно з тодішнім російським президентом Д. Медведєвим під час лондонського саміту *G20* у 2009 р. Дещо згодом з'ясувалося, що *GCHQ* в рамках операції *Tempora* підключається до трансатлантичних оптиковолоконних мереж, отримуючи доступ до даних про інтернет-трафік, історії переглядів інтернет-сторінок, відправлених *email*-повідомлень, телефонних дзвінків тощо. Британські спецслужби стежили навіть за німецькими політиками.

Принагідно, варто нагадати про існування спеціальної угоди від 1946 р. *UKUSA* (*UK-USA Security Agreement*) про співпрацю електронних розвідувальних служб США та Великої Британії й трьох її домініонів – Канади, Австралії та Нової Зеландії. Це є типовим прикладом розвідувальної мережі, дані якої використовують водночас і державні, й бізнесові структури США та їх союзників. Йдеться, зокрема, про спільне використання комп'ютерної мережі «Ешелон» (*Echelon*).

Реакція американських високопосадовців на викриття Е. Сноудена була однозначно негативною щодо персоналії «свистуна-викривальника». Екс-віце-президент США Дік Чейні 15 червня 2013 р. характеризував

Е. Сноудена як «зрадника», вказавши на те, що він може бути китайським шпигуном (свої перші викриття Е. Сноуден зробив в одному з готелів Гонконга), на що китайський МЗС відреагував рішучим запереченням.

Коментуючи даний скандал, президент США Барак Обама вибрав контрнаступальну тактику, розкривши «деталі» діючих програм перехоплення інформації АНБ (інтерв'ю громадському каналу *PBS*). Об'єктами збору розвідувальної інформації американських спецслужб, за словами Президента, є не громадяни США, а передусім іноземці, підозрювані в тероризмі, хакерстві, зв'язках з міжнародною організованою злочинністю тощо. За даними Президента, існує внутрішня програма перехоплення інформації «2015», але йдеться лише про фіксацію самого факту з'єднання абонентів провайдером (зокрема компанією *Verizon*, яка потрапила під вогонь медіа). При цьому спецслужби нібито зовсім не цікавляться контентом телефонних та інших переговорів. Об'єктами іншої програми з кодовою назвою «702» (це і є, напевно, *PRISM* Е. Сноудена), відповідно до тверджень Барака Обами, є іноземці, а американські громадяни можуть стати об'єктом подібного електронного стеження лише за рішенням суду.

Справді, 30 грудня 2012 р. президент Б. Обама підписав законодавчі доповнення, які продовжили до 31 грудня 2017 р. чинність 7-ої секції надзвичайних поправок до контрозвідувального закону *FISA*, вперше запровадженої у 2007 р. Це надало американським спецслужбам легальні підстави для моніторингу діяльності іноземних громадян та американців, які перебувають за межами США, підозрюваних у зв'язках із ворожими спецслужбами, терористичними та злочинними угрупуваннями тощо.

Той факт, що викриття Е. Сноудена не були для американського суспільства сенсаційними, засвідчує хоча б те, що після «самовикривальних» заяв американського президента його рейтинг практично не змінився. А згідно *Pew Research Center* більше половини респондентів із числа громадян США (56 %) підтримує моніторингову діяльність спецслужб в інтернеті. Щоправда, інший зондаж громадської думки – *Rasmussen*, під час проведення якого респондентам задавалися уточнюючі запитання, дав показники набагато скромнішої підтримки громадянами спецмоніторингу електронних комунікацій (26 %).

Характерно також, що «Сноуден-скандал» не перетворився на привід для внутрішньопартійної боротьби у США. Принаймні станом на середину листопада 2013 р. Е. Сноуден не уподібнився до того інформатора із ЦРУ, який започаткував у 1972 р. скандал Уотергейт, що коштував президентської посади Р. Ніксону.

«Казус Сноудена» у вимірах геополітики й геоекономіки

Питання кібербезпеки були однією з провідних тем обговорення каліфорнійської зустрічі президента США Б. Обами та новообраного голови КНР Сі Цзіньпіна, яка розпочалася 7 червня 2013 р., тобто наступного дня після того, як Е. Сноуден поділився з журналістами своїми сенсаційними матеріалами. З точки зору подібної кон'юнктури, китайський слід у «Сноуден-скандалі» справді на той момент видавався реальним. Тим більше, що автор публікації «На захист Едварда Сноудена» у китайській *China daily* закидав США, що зазвичай вони звинувачують інших у злочинах, які чинять самі (у даному разі – у кібершпигунстві) [7]. Окрім того, справа Сноудена пожвавила дискусії в КНР щодо можливостей та обмежень китайського суверенітету в Інтернеті.

За даними китайських джерел, у святая святих АНБ у Форт-Міді є надсекретний Відділ з операцій спеціалізованого доступу (*Office of Tailored Access Operations – TAO*), який буцімто уже впродовж 15 років шпигує за мережами КНР. У складі *TAO* є надсучасний операційний центр – Центр дистанційних операцій (ЦДО), у якому працюють близько 600 військових і цивільних хакерів.

Коли наприкінці травня 2013 р. *Washington Post* в опублікованій на першій шпальті статті звинуватила Китай в кібершпигунстві, припустивши, що на китайську армію працюють хакери, які вкрали у американців креслення понад трьох десятків американських систем озброєнь [15], Хуан Ченцін (*Huang Chengqing*), один із високопоставлених китайських чиновників, що відповідають за Інтернет, заявив у відповідь, що у Пекіна є «гори інформації», яка показує, що Сполучені Штати активно використовують хакерів, аби викрадати китайські урядові секрети. Наводились навіть відповідні цифрові показники. Зокрема, за даними зазначеного посадовця, впродовж 1 січня – 31 травня 2013 р. з 4062 американських серверів було здійснено 2, 91 млн атак на китайські комп 'ютери [3].

Згодом до китайського «сліду» в історії з Е. Сноуденом додався ще й «слід» російський, оскільки цьому викривальнику діяльності американських спецслужб було дозволе-

но транзитом через російський аеропорт попрямувати до Гавани. Станом на 23.06.2013, коли Сноуден відправився з Гонконга до Москви, російська медіа-увага до персоналії Сноудена досягла апогею. В російськомовних ЗМІ, за даними бази *Integrum*, цього дня йому було присвячено 571 публікацію (для порівняння: В. Путіну – вдвічі менше (269). Згодом такий шалений інтерес медіа до персоналії та викриттів Е. Сноудена дещо вщух, хоча й підтримувався на досить стабільному рівні завдяки черговим вкиданням цим розвінчувачем спецслужб чергових доз компрометуючої інформації. Зокрема, за даними тієї ж бази *Integrum*, у День незалежності США 4 липня 2013 р. у російськомовних ЗМІ Е. Сноуден був третьою за популярністю персоналією після В. Путіна та щойно призначеного в Єгипті військовими тимчасового президента А. Мансура.

Станом на 04.07.2013, за офіційними російськими даними, Е. Сноуден усе ще перебував у транзитній зоні російського аеропорту Шереметьєво у пошуках країни, яка б гарантовано надала йому політичний притулок. Список країн, які йому в цьому категорично відмовили, побоюючись зіпсувати стосунки зі США, за даними сайту *Wikileaks*, досягав на той час 10-ти (із 19-ти, до яких Е. Сноуден звернувся за політичним притулком). Деякі країни типу Болівії або Венесуели готові були піти йому назустріч, але теж вагалися. А висловлювання болівійського президента Е. Моралеса щодо потенційної згоди на надання подібного притулку навіть спричинило крупний міжнародний скандал. Офіційні владні структури Франції й Португалії 3 липня 2013 р. не пустили, зокрема, літак Е. Моралеса у свій повітряний простір, тому він зробив вимушене приземлення на летовищі Відня, де до президентського літака з обшуком увірвалися представники спецслужб. Це було, безумовно, грубим порушенням норм міжнародного права.

Зрозуміло, що така «нахабна» поведінка країн Заходу відновила у лідерів Латинської Америки «антиімперіалістичні» настрої. Відповідно, вони вимагали від країн Заходу офіційного вибачення перед президентом Е. Моралесом. Зокрема, йшлося про узгоджену акцію президентів Венесуели, Аргентини, Еквадору та Уругваю. Проте станом на 5.07.2013 р. з-поміж західних країн лише Франція звернулася до Е. Моралеса з подібним вибаченням. Понад те, «сенсації» від Е. Сноудена настільки обурили французьких політиків, що вони пригальмували початок переговорів ЄС-США щодо підписання Угоди про зону вільної торгівлі.

Згодом, коли Е. Сноуден вкинув у медіа інформацію щодо прослуховування американськими спецслужбами бразильського президента Д. Русеф і перехоплення її листування, ця жінка-лідер найбільшої країни Латинської Америки навіть відмінила з цього приводу запланований на 23 жовтня 2013 р. візит до США. Згідно з інформацією Е. Сноудена у бразильському випадку дійсно йшлося не лише про політичну, а й про конкурентну розвідку, оскільки американці нібито мали доступ до конфіденційних матеріалів державної нафтовидобувної компанії «Петробраз», яку використовували для отримання конкурентних переваг під час проведення тендерів на видобуток нафти на бразильському шельфі [12].

Згодом хвиля обурення, спричиненого викривальними матеріалами Е. Сноудена, накрила не лише латиноамериканців та французів, а й німців, оскільки нові «подарунки» від Е. Сноудена, якими він ділився зі світовою громадськістю уже з Москви (яка, зрештою, надала йому тимчасовий притулок), стосувалися також німецьких політиків, й передусім А. Меркель, за якою спецслужби США стежили нібито більше 10-ти років.

З різким осудом дій спецслужб у Мережі виступила Американська спілка громадянських прав (*The American Civil Liberties Union – ACLU*), яка навіть вимагає скасування тих законів та підзаконних актів, на засадах яких діють спецслужби, які моніторять Мережу (йдеться передусім про загадані антитерористичний закон *USA PATRIOT* і Федеральний закон *FISA*).

12 червня 2013 р. Фундація *Mozilla* (популярний інтернет-броузер та ін.) спільно з низкою інтернет-компаній і правозахисних організацій запустили кампанію «Досить за нами стежити!» (*Stop Watching Us*), учасники якої вимагали від американського Конгресу повного звіту про те, яким чином АНБ та ФБР моніторять інформацію інтернет-користувачів. У зверненні до законодавців йдеться про необхідність заборонити стеження за інтернет-користувачами, а також провести розслідування та покарати відповідальних за нього [22]. А правоохоронна організація *The Electronic Frontier Foundation* навіть закликала за аналогією з Уотергейтом сформувати в Конгресі комісію з розслідування, аналогічну тій, яку було організовано в Конгресі США у 1975 р. після відставки Р. Ніксона на чолі із сенатором Ф. Черчем (*Frank Church*).

У європейських країнах «Сноуден-скандал» знайшов продовження на трьох рівнях: персональному, державному, громадському.

«Пересічні громадяни» звернулися з багатьма судовими позовами на популярні інформаційні ТНК зі звинуваченнями в незаконному знятті з їхніх серверів персональних даних (більше всього грошових відшкодувань виплатила компанія *Google*).

Державні спецслужби Великої Британії та Німеччини посилили тиск на національні парламенти й загальноєвропейські структури з вимогою забезпечити для них законодавчі передумови стеження в Інтернеті та комунікаційних мережах на тому ж рівні, яким користуються американці. Федеральна розвідувальна служба Німеччини (*Bundesnachrichtendienst – BND*) заявила, що планує за прикладом американських колег розширити спостереження за інтернет-простором і в найближчі п'ять років витратить на такі цілі до 100 млн євро. Глава *BND* Г. Шіндлер (*Gerhard Schindler*) на зустрічі з комітетом довірених осіб бундестагу, перед яким розвідслужба звітує щодо виконання бюджету, повідомив про існування секретної програми з розширення інтернет-спостереження, яка передбачає збільшення штату підрозділу технічної розвідки на 100 осіб, а також його суттєву технічну модернізацію (на що вже виділено перші 5 млн євро на 2014 р.).

Німецький закон «Про обмеження таємниці листування, а також поштового, телеграфного та іншого електрозв'язку» (закон *G10*) дозволяє *BND* перевіряти до 20 % повідомлень і з'єднань між Німеччиною та іншими країнами, а сучасні комп'ютерні й серверні потужності дають змогу *BND* обробляти тільки 5 % телефонних дзвінків, повідомлень електронною поштою, обговорень у *Facebook* і бесід через *Skype*. У 2011 р. *BND* перевірила майже 2,9 млн *sms* і *email*-листів, які або були передані за кордон, або ж надійшли з-за кордону у ФРН. Серед країн і регіонів, повідомлення з яких і до яких цікавлять німецьку розвідслужбу передусім, – Росія, Східна Європа з Україною включно, африканські конфліктні регіони, Близький Схід, а також Пакистан та Афганістан [20].

На жаль, Україна поки що не належить до того кола країн, які навчилися «планувати власне майбутнє», опановувати на національному рівні стратегії конкурентної боротьби у глобалізованому світі та ефективно опонувати цим стратегіям, якщо вони виходять від країн-конкурентів. Щоправда, усе це не заважає Україні посідати гідні позиції в найрізноманітніших рейтингах міжнародних організацій, які за різними критеріями визначають конкурентоспроможність країни. Хоча подібними рейтингами не слід втішатися, бо вони дуже рідко відображають об'єктивну ситуацію, а мають радше пропагандистське, маніпулятивне значення, оскільки акцент робиться на окремих суто формальних аспектах, без їх поглибленого аналізу.

Зокрема, Швейцарська бізнес-школа *IMD–Lausanne* проголосила у травні 2013 р. поліпшення рівня міжнародної конкурентоспроможності України, виходячи з таких чотирьох критеріїв, як ефективність економіки, якість роботи органів влади, ефективність бізнесу та рівень інфраструктури. В новому глобальному рейтингу цієї структури Україна піднялася відразу на сім пунктів – до 49-го місця (роком раніше додавши собі лише одну позицію) у загальному спискові із 60-ти країн [23].

Зростання конкурентоспроможності України фіксує й аналогічний рейтинг Всесвітнього економічного форуму (ВЕФ), у якому враховується більш широкий спектр критеріїв. У звіті ВЕФ, оприлюдненому у вересні 2012 р., Україна піднялася з 82-го на 73-е місце (із 144 країн). У рейтингу *Doing Business* Україна піднялася аж на 15 позицій. Щоправда, вся ця позитивна динаміка є докризовою, тобто відображає з певним запізненням стан, який передував спадові української економіки, що розпочався у другому півріччі 2012 р. [23].

Стосовно України, то найпершим висновком для неї із скандалу з перехопленням інформації у вітчизняного сегменту Мережі має бути подальше вдосконалення законодавства, що санкціонує стеження та зняття інформації у Мережі, яке є оперативно-розшуковим заходом нормальним і потрібним у будь-якій державі.

«Сноуден-скандал» ще раз настійливо вказує на те, що проблема моніторингу телекомунікацій та моніторингу за діяльністю тих, хто моніторить телекомунікаційний простір, виходить далеко за межі України й потребує негайного вирішення в інтересах національно-державного «цифрового суверенітету». Не дивно, що така «війна» часто-густо перестає бути умовною метафорою і переростає у справжні торговельно-економічні війни, які не обходяться без участі держав та їхніх блоків і коаліцій, загрожуючи трансформацією у великі та малі (локальні) політичні війни, які, своєю чергою, також неможливі без потужної «економіки війни». Коло замикається.

За нинішніх глобалізаційних умов жодна країна світу, задіяна у світовій ринковій конкуренції, не може дозволити собі такої «розкоші», як переведення економіки, за взірцем сталінського СРСР, на суто «воєнні рейки».

У стратегічному вимірі це означає потребу підпорядкування політичної конкуренції країн потребам їхньої економічної конкуренції, адаптації до вітчизняних умов кращого світового досвіду пристосування, а в потрібних випадках – швидкісної переорієнтації ринково-орієнтованої економіки на економіку мобілізаційного типу.

Список використаних джерел

1. *Америка* обвиняет Китай в кибернападениях // ВПК. Военно-промышленный курьер. 2013. – № 8. – 27 февраля. – С. 3.
2. *Бобылов Ю. А.* «Третьи отделы» в условиях глобальной конкуренции // Атомная стратегия. – 2012. – № 69.
3. *China* is victim of hacking attacks // China Daily. – 2013. – June 5 [Електронний ресурс]. – Режим доступу: http://www.chinadaily.com.cn/china/2013–06/05/content_16567174.htm
4. *D'Aveni Richard.* Waking up to the New Era of Hypercompetition // The Washington Quarterly. – 1997. – P. 183–195.
5. *Hancock Garth.* U. S. Economic Intelligence Policy & Global Competition Monterey Institute of International Studies 12/30/96 [Електронний ресурс]. – Режим доступу: http://www.freerepublic.com/focus/f-news/968794/posts#comment
6. *Hansen James H.* Japanese Intelligence : The Competitive Edge. Washington, DC : National Intelligence Book Centre Press, 1996 [Електронний ресурс]. – Режим доступу: http://journals.hil.unb.ca/index.php/jcs/article/view/11757/12534
7. *In defense* of Edward Snowden // China daily. – 2013. – June 20 [Електронний ресурс]. – Режим доступу: http://usa.chinadaily.com.cn/epaper/2013–06/20/content_16641177.htm
8. *Inkster Nigel.* Chinese Intelligence in the Cyber Age // Survival : Global Politics and Strategy. Vol. 55. – 2013. – № 1. – P. 45–66.
9. *Информационно-аналитический* портал SPY. Kz. [Електронний ресурс]. –Режим доступу: http://spy.kz/modules
10. *JETRO* – Japan External Trade Organization [Електронний ресурс]. – Режим доступу: www.jetro.go.jp
11. *Kahaner Larry.* Competitive Intelligence : From Black Ops to Boardrooms – How Businesses Gather, Analyze, and Use Information to Succeed in the Global Marketplace. N. Y. : Simon & Schuster. – 1996. – 300 p.
12. *Карташов Иван.* Президент Бразилии отменила визит в США // Российская газета. – 2013. – 18 сентября [Електронний ресурс]. – Режим доступу: http://www.rg.ru/2013/09/18/russeff-site.html
13. *Леонард Марк.* О чем думают в Китае / Леонард Марк ; пер. с англ. – М. : АСТ, 2010. – 222 с.
14. *Минакова Н. В.* Американские спецслужбы и крупный бизнес / Н. В. Минакова, Н. Л. Семин // США – Канада. Экономика, политика, культура. –2010. – № 2. – С. 45–63.
15. *Nakashima Ellen.* Chinese hackers who breached Google gained access to sensitive data, U. S. officials say // The Washington Post. – 2013. – May 20 [Електронний ресурс]. – Режим доступу: http://articles.washingtonpost.com/2013–05–20/world/39385755_1_chinese-hackers-court-orders-fbi
16. *NSA Busted* Conducting Industrial Espionage In France, Mexico, Brazil, China and All Around the World // Global Research / Washington's Blog., – 2013. – October 21 [Електронний ресурс]. – Режим доступу: http://www.globalresearch.ca/nsa-busted-conducting-industrial-espionage-in-france-mexico-brazil-china-and-all-around-the-world/5355026
17. *People's Daily* : How to Understand and Maintain Internet Sovereignty // Chinascope. Mar/Apr. 2012, Issue 56, P. 50, 1/4 p.
18. *Портер Е. Майкл.* Конкурентная стратегия : Методика анализа отраслей и конкурентов / Майкл Е. Портер ; пер. с англ. – М. : Альпина Бизнес Букс, 2005. – 454 с.
19. *Портер Е. Майкл.* Конкурентные преимущества стран [Електронний ресурс]. – Режим доступу: http://www.seinstitute.ru/Files/Veh6-35_Porter.pdf
20. *Разведка* в ФРГ хочет расширить наблюдение за интернет-пользователями // Тема. Ру. – 2013. – 16 июня [Електронний ресурс]. – Режим доступу: 1001tema.ru.
21. *Sanger David E.* Emerging Role For the C. I. A. : Economic Spy / Sanger David E., Weiner Tim // The New York Times. 1995. – October 15 [Електронний ресурс]. – Режим доступу: http://www.nytimes.com/1995/10/15/world/emerging-role-for-the-cia-economic-spy.html?pagewanted=all&src= pmSean; *Gregory S.* Economic Intelligence in the Post-Cold War Era : Issues for Reform. – February 10, 1997 [Електронний ресурс]. – Режим доступу: http://www.fas.org/irp/eprint/snyder/economic.htm
22. *Stop* watching us [Електронний ресурс]. – Режим доступу: https ://optin.stopwatching.us/
23. *Украина* по конкурентноспособности обогнала Колумбию, – рейтинг // Экономические известия. – 2013. – 31 мая.