МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ІНОЗЕМНОЇ ФІЛОЛОГІЇ
ТА СОЦІАЛЬНИХ КОМУНІКАЦІЙ

СОЦІАЛЬНО-ГУМАНІТАРНІ АСПЕКТИ РОЗВИТКУ СУЧАСНОГО СУСПІЛЬСТВА

МАТЕРІАЛИ VII ВСЕУКРАЇНСЬКОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ СТУДЕНТІВ, АСПІРАНТІВ, ВИКЛАДАЧІВ ТА СПІВРОБІТНИКІВ

(Суми, 18-19 квітня 2019 року)

Суми
2019

СЕКЦІЯ 8
СУЧАСНІ ЗАГРОЗИ БЕЗПЕЦІ У СХІДНОЄВРОПЕЙСЬКОМУ РЕГІОНІ

Андрій Лебідь,
д. філос.н., доцент кафедри політології,
психології та соціокультурних технологій
Сумського державного університету

ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА В УМОВАХ ГІБРИДНИХ ВОЄН: УКРАЇНСЬКИЙ КОНТЕКСТ

«Найкраща стратегія – це здолати ворога без бою»
(Сунь-Цзи)

Реалії новітньої історії України, зокрема, військова агресія Російської Федерації проти нашої країни, свідчать не тільки про зміну геополітичної мапи світу, а й інструментів її трансформації. Одним із таких, вочевидь, є феномен гібридної[1] війни як важелю РФ у її зовнішньополітичній діяльності. Гібридну війну можна помислити як скоординоване використання воєнних та невоєнних засобів впливу, що синхронізуються у фізичному, інформаційному, віртуальному та когнітивному вимірах конфлікту.

Поняття гібридної війни є доволі новим і у масовому ужитку воно широко застосовується із початком власне російської агресії проти України. До того часу мова здебільшого йшла про так звані «гібридні засоби ведення війни», якими РФ не цурається у її прагненні впливати на світову політику [7, 19]. До таких можна віднести:

[1] «Гібридний» ми концептуалізуємо як поєднання різнорідних елементів у цілісному об'єкті, явищі, дії. Доцільно відзначити, що і російська ідеологія і російська державність є гібридними за суттю та структурою, яка абсорбувала елементи попередніх епох, зокрема, елементи демократії та тоталітаризму, радянський і монархічний спадок, релігійні та націоналістичні наративи, поєднавши їх у системі путінської шовіністичної ідеології.

– інвестиції, фінансова підтримка політичних партій (як «лівих», так і «правих»);

– формування проросійського лобі в політичному середовищі інших країн (в тому числі і через корупційні механізми);

– проникнення у владні структури та інституції інших країн з метою розвідувальної діяльності;

– використання нерозв'язаних етнічних конфліктів (Балкани, Придністров'я, Південний Кавказ та ін.);

– пропаганда в інформаційному просторі інших країн, підтримка російських ЗМІ за кордоном (Sputnik, Russia Today);

– координовані кібератаки та ін.

Російська Федерація застосовує гібридні засоби ведення війни проти країн Європейського Союзу, головними цілями якої є послаблення, а в перспективі – й розпад ЄС, знищення об'єднуючих Європу цінностей і формування нового європейського устрою під егідою РФ, відродження «імперської величі» Росії і забезпечення домінуючих позицій в Європі.[2]

Дж. Ненет відзначає, що останнім часом Росія удосконалила стратегію та прийоми ведення гібридних воєн: у другій Чеченській війні, кібератаках в Естонії 2007 року, російсько-грузинській війні, а також використовуючи інші механізми так званої «м'якої сили» [5], коли обман, дезінформація, маніпулювання є більш дієвими за устави регулярних військ. Відтак, войовнича риторика, кібератаки, тролінг, масове виробництво фейків та дезінформація стають інноваційною базою російської пропагандистської машини та політтехнології, know how інформаційно-психологічної агресії РФ.

М. Галеотті зазначає, що гібридна (нелінійна) війна починається саме з інформаційної агресії і так само нею закінчується, коли інформаційний пресинг, інформаційно-психологічні впливи є її перманентними складниками [2].

[2] На думку генерала В. Гєрасімова, якому приписують авторство воєнної доктрини сучасної Росії (відомої як «доктрина Гєрасімова»), завдання «гібридної війни» мають бути досягнуті, першочергово, за рахунок підриву військового та економічного потенціалу противника, інформаційно-психологічного тиску на нього, активної підтримки внутрішньої опозиції, застосунку диверсійних методів.

Д. Кілкуллен конкретизує меседж М. Галеотті у тому сенсі, що інформаційні кампанії якнайкраще одночасно вести на глобальному, регіональному та локальному рівнях [3].

В цьому контексті варто зазначити, що не лише Росія використовує гібридні інструменти впливу. Китай, як могутній геополітичний гравець, також зацікавлений у швидкому переході до сучасних видів управління і методів гібридної війни[3] та для якого доктрина «народної війни» вже вкрай неактуальна. Їй на зміну прийшла «доктрина активної оборони», яка уможливлює нанесення превентивних локальних ударів за будь-якої загрози безпеці Піднебесній. Паралельно з цим доктрина передбачає використання дипломатичних, юридичних, інформаційних та інших засобів для усунення загрози [1].

Воєнна доктрина Китаю передбачає ведення війн майбутнього у тривимірному просторі, що зактуалізовує координацію космічних сил, систем розвідки та управління операціями. За цих умов неочевидною вже є межа між фронтом та тилом, ба, більше – реальність як така стає аморфною, спотворюваною, дифузною. Відтак, новою доктриною Китаю передбачено посилення своєї присутності в інтернеті та війни у віртуальностях. Особливої уваги приділено веденню інформаційних воєн, створенню спеціальних родів військ, на які буде покладено завдання ведення пропаганди.

Таким чином, реалії сьогодення зактуалізовують перед Україною віднаходити відповіді на глобальні виклики, враховуючи геополітичні мегатренди та глобальні тренди. Надважливим видається завдання забезпечення інформаційної, кібербезпеки, безпеки інформаційних ресурсів.

Пріоритетами забезпечення інформаційної безпеки є:

– забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії;

[3] Гібридні війни за китайською моделлю є необмеженими війнами [4], для якої характерними є багатовекторність та асиметрія дій, обмежені цілі, необмежені ресурси для досягнення цих цілей, динамічний контроль.

– створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

– протидія інформаційним операціям, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації;

– розробка і реалізація скоординованої інформаційної політики тощо.

Пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів є:

– розвиток інформаційної інфраструктури;

– створення системи забезпечення кібербезпеки, розвиток CERT;[4]

– моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації;

– розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів;

– забезпечення захищеності об’єктів критичної інфраструктури, інформаційних ресурсів від кібератак;

– захист інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації та ін.

Особливої ваги ці пріоритети набувають в умовах гібридних воєн та використання гібридних інструментів впливу, загроз і злочинів майбутнього. Злочинні угрупування, терористичні організації, хактівісти, біохакери усе активніше освоюють такі сфери як робототехніка, синтетична біологія,[5] штучний інтелект. Кримінальний світ, тероризм мігрує з фізичного простору у віртуальний, використовуючи особисті дані із злочинною метою.[6] З клієнта

[4] Спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам (Computer Emergency Response Team).

[5] Синтетична біологія – новий напрям в генній інженерії. Її основною метою є створення принципово нових, більш досконалих живих систем. Зокрема, виробництво програмованих організмів, чия поведінка, особливості та функції можна задати на момент їх створення. Це одна з найпотужніших технологій в світі. Клітини - це міні-комп'ютери, а ДНК – мова програмування. Зловмисники зможуть створити мікроорганізми, які будуть «зламувати» людський мозок і керувати розумом (за аналогією із хакерською атакою). Серед можливостей застосування синтетичної біології вчені називають, наприклад, фармакологію – можна буде створювати «потрібні» бактерії для виробництва «потрібних» препаратів. Або вирощувати організми для використання в якості біопалива. Синтетична біологія стане основою для появи нових форм біотероризму. Головне, аби синтетична біологія не вийшла з-під контролю.

[6] В цьому контексті доцільно говорити про таке усталене поняття як «крадіжка особистості».

користувач перетворюється на продукт, навіть не підозрюючи про це. Присутність злочинності і тероризму в інтернеті усе зростає і завадити цьому поки не вдається.

Ми живемо в добу мереж, добу влади мереж, добу переплетінь.[7] І як зауважують Е. Шмідт та Дж. Коен: «Нинішня мережева технологія насправді працює для громадян» [6, 7], засвідчуючи позитивні зміни людського досвіду. Як видається, це надто оптимістичний висновок, поскільки мережі приховують у собі чималі загрози для її творця – людини. І якщо таки брати до уваги геополітичний вимір, то насправді загрозою національній безпеці країн є еволюція мереж. Кібероборона на десятиліття відстає від кібератак, а тому зведення «віртуальної завіси» на заміну «залізній» чи вирішить питання інтелектуальної гонитви озброєнь, метою якої є створення життєздатної та дієвої доктрини кібербезпеки? Зрозуміло, доктрини, що ґрунтуються на принципах традиційного мислення в рамках національної безпеки приречені. Тоді, мабуть, доцільно регулювати різноманіття мереж, а не стримувати її атаки. Питання риторичне.

Список використаних джерел:

1. China's Military Strategy, 2015 – China's Military Strategy in 2015 [Electronic resource]. URL: https://china.usc.edu/prc-state-council-chinas-military-strategy-2015-may-26-2015

2. Galeotti, 2015 – Galeotti M. (2015). Hybrid War and Little Green Men : How It Works, and How It Doesn’t [Electronic resource]. URL: https://www.e-ir.info/2015/04/16/hybrid-war-and-little-green-men-how-it-works-and-how-it-doesnt/

3. Kilcullen, 2006 – Kilcullen D. (2006). Three Pillars of Counterinsurgency. [Electronic resource]. URL: http://www.au.af.mil/AU/awc/awcgate/uscoin/3pillars_of_counterinsurgency.pdf

4. Morris, 2015 – Morris V. (2015). Grading Gerasimov: Evaluating Russian Nonlinear War Through Modern Chinese Doctrine [Electronic resource]. URL :

[7] Світ природи складається з оптимізованих, розгалужених мереж, що заповнюють собою простір (кровоток людини, колонія мурах, харчові ланцюги-мережі тощо), соціальні мережі, віртуальні мережі та ін.

https://smallwarsjournal.com/jrnl/art/grading-gerasimov-evaluating-russian-nonlinear-war-through-modern-chinese-doctrine

5. Neneth, 2015 – Neneth J. (2015). Russia's State-centric Hybrid Warfare [Electronic resource]. URL: https://icds.ee/russias-state-centric-hybrid-warfare/

6. Schmidt, Cohen, 2013 – Schmidt E, Cohen J. (2013). The New Digital Age : Reshaping the Future of People, Nations and Business. New York: Alfred A Knopf Publishers. 336 p.

7. Schnaufer, 2017 – Schnaufer Tad A. II (2017). Redefining Hybrid Warfare : Russia's Non-linear War against the West. Journal of Strategic Security. Vol. 10, №1. P. 17–31.

Сергій Король,
к. політ. н., ст. викладач кафедри політології,
психології та соціокультурних технологій
Сумського державного університету
Олена Черкасова,
студентка Сумського державного університету

ІНФОРМУВАННЯ ГРОМАДСЬКОСТІ ЩОДО ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ УКРАЇНИ: ПРАВОВИЙ АСПЕКТ

Виходячи з довгострокової цілі приєднання до загальноєвропейської системи колективної безпеки, основою якої є НАТО, Україна вибудовує нові підходи до забезпечення національної безпеки. З цим Україна здійснюватиме інтеграцію до європейського політичного, економічного, правового простору з метою набуття членства в Європейському Союзі, а також поглиблюватиме співробітництво з НАТО щоб досягти критеріїв, необхідних для набуття членства у цій організації. Питання євроатлантичної інтеграції України повинні знати і розуміти громадяни України. З цією метою Президент України підписав