У довгостроковій перспективі мінімізувати ризик використання енергетичних ресурсів як інструментів політичного та економічного тиску можливолише шляхом збільшення власного видобутку газу, зменшення обсягів його споживання та розвитку відновлюваної енергетики.

Список використаних джерел:

1. SVSPB (2021). Видобуток, споживання, імпорт та експорт природного газу. URL: http://surl.li/atgdi.
2. Reuters (2021). Ukraine's Naftogaz CEO still hopes NordStream 2 will be blocked. URL: http://surl.li/atgdn.
3. BBC NEWS (2021). Північний потік-2: Німеччина відклала сертифікацію. Що це означає? URL: http://surl.li/atgea.

КОНВЕРГЕНЦІЯ ГІБРИДНИХ ЗАГРОЗ В УМОВАХ НОВОЇ РЕАЛЬНОСТІ

Ляшенко О.М.
д.е.н, професор, директор Науково-навчального інституту менеджменту та освіти дорослих
ВНЗ Університет економіки та права «КРОК», м. Київ, Україна

Безпека об'єктивно відображає відсутність загрози основним цінностям суспільства в суб'єктивному сенсі відсутність страху, що ці цінності можуть бути знищені (Wolfers, 1962). Нова реальність суттєво завищила фокусування уваги усього людства на безпеці в усіх її виявах і проявах.

Поняття «гібридна війна» ("hybrid warfare") і «гібридна загроза» ("hybrid threats") наразі є усталеними не лише в офіційній термінології військової політики, але й у різних галузях знань освіти і науки. Відповідно відбувається генеза розуміння гібридних загроз.

Понад десятиліття тому науковці тлумачили поняття гібриднихзагроз як сукупність традиційних (класичних), так і новихзасобів, що слугують цілям завдання шкоди противнику. Зокрема мова йшла про війни в інформаційному просторі, використання і розробку сценаріїв конфліктів низької інтенсивності на території противника, міжнародний тероризм, міграцію, розпалювання етнічних і релігійних конфліктів, транснаціональну злочинність, демографічні ризики, глобалізаційні виклики та ін. (Горбулін, 2009).

Здебільшого динаміку гібридних загроз розглядали як предтечу гібридної війни, тобто тривалу комплексна підготовку, і тому головними тенденціями розвитку гібридних загроз вважалися:

- зростання кількості атак, багато з яких ведуть до великих втрат; – підвищення складності атак, які можуть включати кілька етапів і застосовувати спеціальні методи захисту від можливих методів протидії;

- вплив практично на всі електронні (цифрові) пристрої, серед яких останнім часом все більшої значущості набувають мобільні пристрої, а вони найбільше схильні до ризиків у сфері інформаційної безпеки;
- випадки нападу на інформаційну інфраструктуру великих корпорацій, найважливіших промислових об'єктів і навіть державних структур;
- застосування найбільш розвиненими у сфері комп'ютерних технологій країнами засобів і методів кібернападів на інші держави (Курбан, 2017).

Якщо апелювати до визначення HybridCoE (4), то можна віднайти такі характеристики гібридних загроз, як-от:

- скоординовані та синхронізовані дії, які свідомо спрямовані на системну вразливість демократичних держав та інституцій за допомогою широкого спектру засобів;
- діяльність, яка використовує атрибуції, різні інтерфейси та дихотомії (війна-мир, внутрішня-зовнішня безпека, місцева-державна та національна-міжнародна);
- вплив на різні форми прийняття рішень на місцевому (регіональному), державному чи інституційному рівні, скерований на подальше виконання стратегічних цілей противника, який одночасно підриває та/або завдає шкоди цілям його існування/функціонування.

Таким чином, наразі радше мова йде про гібридні дії, які характеризуються неоднозначністю як форм проявів, так і впливу, оскільки розмивають звичні межіуправління суб'єктами, бо діють у «коридорі» між зовнішнім і внутрішнім, законним і незаконним, миром і війною. Неоднозначність гібридних дій створюється поєднанням звичайних і нетрадиційних засобів – кібероперації; дезінформації, яка перетворюється маніпулятивним шляхом на дегуманізацію; атаки на критичну інфраструктуру; різні форми злочинної діяльності і, нарешті, асиметричне використання військових засобів для ведення війни.Гібридні дії є економічно виправданими з боку агресора, оскільки завдяки слабким («дешевим») сигналам уражають потужні цілі. Це робить гібридні дії складними для запобігання чи реагування на них.

Разом з тим, на особливу увагу заслуговують процеси міграції, мутації та конвергенції гібридних загроз зокрема в Україні, яка з 2014 року перебуває під тиском гібридних дій з боку РФ. На тлі збройної агресії РФ проти України відбувається поглиблення конфлікту цінностей, наслідки якого руйнуютьусталені норми поведінки і роблять суспільствокрихким. Конфлікт цінностей, що поширюється на внутрішню сферу українського суспільства, посилює його поляризацію та роз'єднаність, роблячи його більш уразливими до зовнішнього втручання. Цунамі нової реальності, спричинене пандемією COVID-19, зробило екзистенційнимиубезпеками усвідомлення загроз, здоров'ята реальні та потенційні збитки (формула «три З» - авт.).

У контексті вивчення конвергенції гібридних загроз слід звернути особливу увагу на їх екзистенційність. З одного боку, теорія слабких сигналів і «чорних лебедів» не втрачає своєї актуальності, а з іншого – постає теорія «сірих носорогів», тобто загроз, які ми мусимо бачити, але часто небачимо, або які ми бачимо, але свідомо ігноруємо (Wucker, 2016)

Одним з найпоширеніших векторів конвергенції гібридних загроз в Україні є антивакцинаторський рух. Кампанії, спрямовані проти вакцинації в інших країнах, були відносно очікуваним кроком зі сторони Кремля, однак масштаби подібної дезінформації виявились надзвичайно широкими. За оцінками Оксфордського інституту Інтернету, відповідальність за 92% дезінформації про коронавірусу 2020 році (сюди входять і питання вакцинації) несли Москва та Пекін (COVID-19 disinformation being spread). Зрив вакцинації у суспільствах, які Кремль прагне послабити, – в інтересах російського уряду. У довгострокові перспективі тривалий негативний вплив на систему охорони здоров'я суттєво підриває стійкість суспільства на базовому рівні. Вакцинація має значний потенціал до поляризації суспільств, і саме така поляризація не рідкоє одним з основних інтересів Кремля (Аналітичний звіт, 2021). Яка «ціна питання»?, тобто яким є/може бути вартісний вимір втрати від можливого локдауну через розповсюдження нових штамів коронавірусної інфекції? В Україні оцінюються в 0,6% річного ВВП у разі тривалості нокдауну протягом одного місяця (прогноз НБУ). Для порівняння: видатки бюджету у 2022 році бюджету на безпеку та оборону – понад 5% ВВП (на оборону близько 2,5%) на підтримку пріоритетних напрямів наукових досліджень і науково-технічних (експериментальних) розробок ву країнських університетах- 1,96%.

Отже, процес конвергенції гібридних загроз, наочно продемонстрований в Україні, є вкрай небезпечним. Його екзистенційна сутність торкається сплетіння політичних, воєнних, світоглядних, медичних, етичних процесів, маніпулятивні наслідки впливу котрих спираються на невігласство широких верств населення. Вправленню такої ситуації має слугувати посилення просвітницької діяльності як асиметричної відповіді гібридним загрозам та їхній конвергенції.

Список використаних джерел:

1. Wolfers A. (1962). *Discord and Collaboration: Essays on International Politics*. Johns Hopkins University Press.

2. Горбулін, В.П. та ін. (2009). *Інформаційні операції та безпека суспільства: загрози, протидія, моделювання*: монографія. Київ: Інтертехнологія.

3. Курбан, О.В. (2017). Основи сучасної національної інформаційної безпеки країни. *Вісн. ХДАК*. Вип. 50. 55-62.

4. Hybrid threats | Hybrid CoE. URL: https://www.hybridcoe.fi/hybrid-threats // (дата звернення 24.11.2021 р.)

5. Wucker, M. (2016). *The Gray Rhino. How to Recognize and Acton the Obvious Dangers We Ignore.* NewYork: St. Martin'sPressebook. P. 26, 34-35.

6. COVID-19 disinformation being spread by Russia, China, say experts | CBC News URL: https://www.cbc.ca/news/politics/covid-coronavirus-russia-china-1.5583961 // (дата звернення 25.11.2021 р.)

7. Аналітичний звіт Групи з аналізу гібридних загроз Українського кризового медіа-центру за І півріччя 2021 року URL: https://drive.google.com/file/d/1iGc0ltCf-Yp23vN_8WukS7pZp5dSRAYv/view// (дата звернення 23.11.2021 р.