Кіберзахист зосереджений на запобіганні, виявленні та своєчасному реагуванні на атаки або загрози, щоб не допустити втручання в інфраструктуру або інформацію. Технології та послуги для забезпечення безпеки захищають системи інформаційних технологій від атак шляхом виявлення загроз і вразливостей, що дає змогу ефективно реагувати та виправляти ситуацію [4]. Поряд із найновішими роботами в цій галузі, пов'язаними з технологіями та інноваціями в сфері безпеки, які мають на меті допомогти лідерам у сфері безпеки та управління ризиками вдосконалити свою стратегію [5]. Подальші дослідження полягають в розвитку платформ військового кіберсередовища, промислової моделі та рішення для виявлення загроз в рамках моделі гібридних загроз.

Джерела та література

1. Gawer, A. (2022). Digital platforms and ecosystems: remarks on the dominant organizational forms of the digital age. Innovation, 24(1), 110-124.

2. Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Computing and Applications, 34(18), 15241-15271.

3. Reda, H. T., Anwar, A., Mahmood, A. N., & Tari, Z. (2023). A Taxonomy of Cyber Defence Strategies Against False Data Attacks in Smart Grids. ACM Computing Surveys, 55(14s), 1-37.

4. Zheng, Y., Li, at all. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. Digital Communications and Networks, 8(4), 422-435.

5. Akram, J., & Ping, L. (2020). How to build a vulnerability benchmark to overcome cyber security attacks. IET Information Security, 14(1), 60-71.

УДК 355.02:004.738.5.053.6.

Станько А., доктор філософії; Тотосько О., канд. техн. наук, доц.; Голотенко О., канд. техн. наук, доц.; Королюк Р.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ВПЛИВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ЕВОЛЮЦІЮ ГІБРИДНИХ ВІЙН: ІСТОРИЧНИЙ АНАЛІЗ ТА СУЧАСНІ ТРЕНДИ

Анотація. *Технологічна революція та модернізація традиційної війни призвели до появи гібридної війни як засобу боротьби з ворогом. Гібридна війна поєднує традиційні та нетрадиційні методи ведення війни, такі як використання сил спеціального призначення, інформаційна війна, кібератаки та економічний тиск. Для боротьби з гібридною війною важливо впроваджувати процеси інформаційної безпеки та ідентифікувати інформаційні загрози. Глобалізація та інформаційно-технологічна революція поєднали класичні та нові форми війни, що призвело до широкого використання гібридної війни. Поєднання технологічних досягнень, глобалізації, історичних етапів у розвитку війни та інших факторів створили нові можливості та основи для гібридної війни.*

Ключові слова: *гібридна війна, кібератаки, стратегії війни, технології війни, комп'ютерні технології*

Stanko A., PhD; Totosko O., Ph.D., Assoc. Prof.; Golotenko O., Ph.D., Assoc. Prof.; Koroliuk R.
Ternopil Ivan Puluj National Technical University, Ukraine

THE IMPACT OF INFORMATION TECHNOLOGY ON THE EVOLUTION OF HYBRID WARFARE: HISTORICAL ANALYSIS AND CURRENT TRENDS

Abstract. *The technological revolution and the modernisation of traditional warfare have led to the emergence of hybrid warfare as a means of fighting the enemy. Hybrid warfare combines traditional and unconventional methods of warfare, such as the use of special forces, information warfare, cyber attacks and economic pressure. To combat hybrid warfare, it is important to implement*

information security processes and identify information threats. Globalisation and the information technology revolution have combined classical and new forms of warfare, leading to the widespread use of hybrid warfare. A combination of technological advances, globalisation, historical stages in the development of warfare and other factors have created new opportunities and frameworks for hybrid warfare.

***Keywords: hybrid warfare, cyberattacks, warfare strategies, warfare technologies, computer technologies**.*

З огляду на тенденції, що розвиваються, війна динамічна за своєю природою. Сучасне геополітичне середовище та технологічний прогрес призводить до нових стратегій і наслідків для ведення війни. Сучасні методи, що розвиваються, разом із традиційним розумінням війни визначають концепцію гібридної війни. Елементи гібридної війни, як загальну концепцію, можна спостерігати протягом всієї історії.

Термін гібридна війна є порівняно новим поняттям; таким чином, консенсус щодо загальноприйнятого визначення не переважає. Суб'єктивний характер терміну призвів до відмінних визначень у міжнародній системі. Термін вперше введений Вільямом Дж. Неметом у 2002 році, який висунув гіпотезу про те, що гібридна війна складається з поєднання синхронізованого невійськових та військово-стратегічних аспектів.

Еволюція війни безпосередньо пов'язана з технологічним прогресом. Результатом технології є вдосконалена зброя та стратегії ведення війни. Таким чином можна відстежити деякі етапи еволюції. Війна першого покоління з'явилася після Вестфальського договору 1648 року. Було введено поняття територіального суверенітету. Ця концепція перетворилася на державну монополію на ведення війни між групами осіб. Війна другого покоління була запроваджена французькою армією та закінчилася після Першої світової війни [1]. Культура порядку була продовжена, тоді як жива сила була замінена масовою вогневою силою з точки зору панування над полем бою. Війна третього покоління була розроблена Німеччиною під час Другої світової війни. Під час Першої світової війни Німеччина практикувала тактику проникнення, що призвело до розвитку танків у Другій світовій війні. Війна четвертого покоління розвивалась за останні шість десятиліть. Це покоління представило недержавних акторів як учасників війни, як наслідок, державна монополія на ведення війни закінчилася. Війна п'ятого покоління чітко змінила філософію війни, оскільки була введений інструмент для сприйняття та інформації. Згідно з цією ідеєю, конкуруючі держав отримали маніпульований погляд на світ і політику, що призвело до нестабільності держави. З такими технологічними досягненнями, як комп'ютери та електроніка, інформація, зв'язок, зброя, більша швидкість, ефективні давачі, швидке розгортання, більш прихована технологія, економія палива, смертоносність, космічні системи, біохімія та штучний інтелект різко змінили ведення війни. У цій системі суперники маніпулюють за допомогою інформації, що зрештою породжує нестабільний стан.

Розвиток бойових дій у зв'язку з технологічною еволюцією призвів до феномену гібридної війни. Гібридна війна часто розглядається як певна невизначеність між війною та мирним часом [2]. Поряд із цим держави прагнуть досягти своїх цілей, якомога довше не переступаючи поріг відкритої війни. Як наслідок, поєднується використання як звичайних, так і нерегулярних інструментів, які застосовуються державними і недержавними акторами. Головною метою гібридної війни є розсіювання насильства, за якого жертва не підозрює про заплановану війну. Поглядами громадян маніпулюють і змінюють через психологічну та соціальну боротьбу. Бажаного результату досягають через використання соціально-політичної вразливості, використання релігійних почуттів і культурних символів. Такі дії здійснюються за допомогою фейкових новин, дипломатії та втручання у вибори.

Основні інструменти гібридної війни зображено на рис. 1.

Рис. 1. Інструменти гібридної війни

З розвитком технологій кіберпростору, медіа та соціальних медіа у війнах п'ятого покоління гібридна війна включила інформацію як інструмент. За допомогою інформації культурами маніпулюють на несвідомому рівні за допомогою дипломатії та пропаганди. Як наслідок, масова несвідомість нездатна виявити маніпуляції політичною інформацією, а суперницькі держави можуть генерувати бажані результати. Дезінформація поширюється через газети, листівки, комп'ютери, спам та інші пов'язані технології [3].

Війна поступово переходить до шостого покоління. Цей розвиток відкидає нав'язування балансу через ядерне стримування між державами, а нові методології гібридної війни вважаються ключовими та потужними. Війна розширюється до націлювання на мережеві критичні активи держав, такі як банківська система, електроенергія та інші об'єкти критичної інфраструктури. У цьому контексті надмірна залежність держави від звичайної військової техніки та технологій матиме прямі наслідки [4].

У результаті гібридна війна вважається інформаційною, де дезінформація поширюється через газети, листівки, комп'ютери, спам та інші пов'язані технології. Як наслідок, звичайні люди стають бунтівниками проти своїх урядів, і виникає нестабільність держави. Таким чином, гібридна війна поступово розсіює насильство, тоді як жертви не знають про заплановану війну.

Джерела та література

1. Qureshi, W. A. (2019). Fourth-and fifth-generation warfare: Technology and perceptions. San Diego Int'l LJ, 21, 187.

2. Hayat, R. A. B. B. I. A. (2021). Hybrid Warfare: A Challenge to National Security. PCL Student Journal of Law, 5(1), 102-127.

3. Solmaz, T. (2022). Hybrid warfare': one term, many meanings. Small Wars Journal, 25.

4. Steingartner, W., & Galinec, D. (2021). Cyber threats and cyber deception in hybrid warfare. Acta Polytechnica Hungarica, 18(3), 25-45.

УДК: 2:316.74(=161.2)]:355.48(470+571):477):159.9

Стоцький Я., д-р істор. наук, проф.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

КОНФЕСІЙНІ ТРАНСФОРМАЦІЇ ПІД ЧАС РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ ТА ЇХНІЙ ПСИХОЛОГІЧНИЙ ВПЛИВ НА РЕЛІГІЙНІСТЬ УКРАЇНСЬКОГО СУСПІЛЬСТВА У ПОРІВНЯННІ З ДОВОЄННИМ ПЕРІОДОМ

Анотація. *У дослідженні проаналізовано компаративістику переходу релігійних громад із Української Православної Церкви Московського патріархату (у травні 2022 року внесла у свій Статут зміну назви на УПЦ, щоб відмежуватися, ілюзорно, від Російської Православної Церкви, але в релігієзнавчій науці й надалі використовується попередня назва – УПЦ МП) у канонічну приналежність до Православної Церкви України (ПЦУ). Висвітлено, як внаслідок російської агресії у громадах вірян УПЦ МП поступово зростає національна самосвідомість,*