УДК 355.02:004.056.5:004.738.5.053.6.

Станько А., доктор філософії; Микитишин А., канд. техн. наук, доц.; Блавіцький А.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ІНТЕГРАЦІЯ СУЧАСНИХ ТЕХНОЛОГІЙ У ВІЙСЬКОВІ ДОКТРИНИ: КІБЕРЗАГРОЗИ ТА АДАПТАЦІЯ ДО ЦИФРОВОГО ВИМІРУ КОНФЛІКТІВ

Анотація. *Майбутнє війни буде в цифровому багатодоменному середовищі, яке потребує нових доктрин. Очікується, що нові технології різко збільшать швидкість та кількість конфліктів. Військова стратегія стикається з повсюдним підключенням давачів і різних джерел інформації. Інтернет речей та штучний інтелект вносять радикальні зміни в оцифрування поля бою. Швидка трансформація також вплине на рішення командування збройними силами і на спосіб обробки та аналізу інформації. Військове кіберсередовище потребує розробки власних засобів та методів захисту від атак для оборони військової та національної в цивільної кіберінфраструктури. Цей спектр відповідальностей часто недооцінюється. Головний результат оцінки кіберзагроз показує, що існуючі стратегії кіберзахисту потребують вдосконалення для протидії існуючим кіберзагрозам.*

Ключові слова: *кібератаки, інформаційний захист, цифровізація, інтернет технології, військова стратегія*

Stanko A., Ph.D; Mykytyshyn A., Ph.D., Assoc. Prof.; Blavitskyi A.
Ternopil Ivan Puluj National Technical University, Ukraine

INTEGRATION MODERN TECHNOLOGIES INTO MILITARY DOCTRINES: CYBER THREATS AND ADAPTATION TO THE DIGITAL DIMENSION OF CONFLICTS

Abstract. *The future of warfare will be in a digital, multi-domain environment that requires new doctrines. New technologies are expected to dramatically increase the speed and number of conflicts. Military strategy is faced with the ubiquitous connectivity of sensors and various sources of information. The Internet of Things and artificial intelligence are bringing about radical changes in the digitisation of the battlefield. The rapid transformation will also affect the decisions of the armed forces commanders and the way they process and analyse information. The military cyber environment requires the development of its own means and methods of defence against attacks to protect military and national and civilian cyber infrastructure. This range of responsibilities is often underestimated. Main result of the cyber threat assessment shows that existing cyber defence strategies need to be improved to counter existing cyber threats.*

Keywords: *cyberattacks, information defence, digitalisation, internet technologies, military strategy*

Національні мережі стикаються з широким спектром кіберзагроз. Вони включають в себе сучасні та стійкі небезпеки, які можуть обійти комерційно доступні інструменти виявлення. Кібератаки стають все більш інтенсивними і складними. Це середовище загрози має глобальний характер, коли виходить за межі географічних кордонів і характеризується розвитком наступальних кібератак, які є невід'ємною частиною конфліктів.

Залежність від Інтернету сильно впливатиме на безпеку суспільства. Зважаючи на запроваджені тенденції - цілісність даних, конфіденційність, безпека даних, індивідуальна безпека і громадська безпека можуть опинитися під загрозою [1]. Поширення підключених пристроїв та вплив кіберпростору на життя громадян призведе до необхідності покращення захисту безпеки та захищеності [2]. Кібератака - це акт або дія, ініційована в кіберпросторі з метою порушення, відмови, деградації або знищення шляхом компрометації комунікаційних, інформаційних та інших електронних систем або інформації, яка зберігається, обробляється або передається в цих системах. Кіберзахист - це засоби досягнення та виконання оборонних заходів для протидії кіберзагрозам та пом'якшення їх наслідків, і таким чином збереження та

відновлення безпеки комунікаційних, інформаційних чи інших електронних систем або інформації, яка зберігається, обробляється чи передається в цих системах [3]. Глобальна безпека залежить від міжнародної стабільності та глобального процвітання. Стрімкий розвиток і поширення технологій та комунікацій уможливили нові засоби впливу.

Ворожа сторона постійно діє за межею збройного конфлікту. Поширення впливу державами, не вдаючись до фізичних дій, є одним із ключових аспектів гібридних воєн. Можна провокувати і залякувати громадян, організації, без правових або військових наслідків. Це розуміння ворожої активності може бути використане для використання залежностей і вразливостей у кіберпросторі: систем, процесів і цінностей. Метою таких дій є послаблення демократичних інститутів і отримання економічних, дипломатичних і військових переваг. Тому забезпечення спільної оборони та безпеки є кінцевою метою, на яку має бути спрямована діяльність усього демократичного світу, адже широкомасштабний, нерегулярний збройний конфлікт чи гібридна війна є небажаним аспектом міжнародних відносин. Світ зараз це конкуренція та конфлікти, світ в якому супротивники позиціонують інші елементи своєї влади (політичні, соціальні, дипломатичні та економічні) таким чином, щоб мати явну перевагу.

Нові інформаційні технології значно скоротили фізичну, часову та інформаційну відстань між військами та їхнім командуванням. Дистанційне ураження противника перетворюється на основну тактику досягнення цілей бойової дії або операції. Об'єкти противника атакуються в будь-якій точці ворожої території. Зникають відмінності між стратегічними, оперативними і тактичними діями, між нападом і обороною. Високоточна зброя використовується у все більших масштабах. На озброєння у великих кількостях надходить зброя, заснована на нових фізичних принципах, а також роботизовані системи. Стрімкий розвиток інформаційних технологій, широке використання інформації в суспільстві та збройних силах провідних країн світу суттєво змінили характер, методи і способи діяльності державних і урядових політичних та економічних структур, вплинули на суспільні відносини, характер, методи і способи ведення воєнних дій, породили нові інформаційні загрози і виклики [10]. Кібератака може бути невидимою, асиметричною, багаторольовою, глобальною, миттєвою, що робить її ідеальним інструментарієм як для великих, так і для малих суб'єктів. У кіберпросторі діють найрізноманітніші сторони (актори), в тому числі власні війська, війська союзників, нейтральні сторони і противники. Ряд акторів можна класифікувати як реальні або потенційні загрози:

– Держави - це добре забезпечені ресурсами актори, які характеризуються геополітичними, економічними або військовими мотивами. Вони здатні здійснювати тривалі атаки, часто з розвідувальною і диверсійною метою.

– Посередники - це приватні організації або установи, які спонсоруються і підтримуються урядом, щоб допомогти цьому уряду досягти своїх геополітичних, економічних або військових цілей.

– Кібертерористи: групи людей або окремі особи, які атакують або впливають на мережі, системи та інформацію, особливо проти цивільного населення, з метою поширення терору або переслідування політичних цілей.

– Кіберзлочинці: злочинні угруповання, що діють заради наживи. Зазвичай вони шукають інформацію, що дозволяє ідентифікувати особу, критичні цифрові ресурси для викрадення з метою отримання викупу або прибутку.

– Хактивісти: особи, які дотримуються певної мети і атакуючи з метою поширення пропаганди або нанесення шкоди організаціям.

– Інсайдерські загрози: особи з власної організації, які випадково або навмисно зловживають привілеями та ресурсами (незадоволені працівники).

Між різними категоріями суб'єктів загрози можуть існувати взаємозвязки, оскільки суб'єкти можуть використовувати інші категорії як довірених осіб.

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*