УДК 316.259+355.01

Олександр Миколайович Гук[1]
Олексій Юрійович Чередниченко[1]
Роман Михайлович Штонда[1]
Ігор Олексійович Диба[2]

[1]***Військовий інститут телекомунікацій та інформатизації, Київ, Україна***
[2]***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

ДІЇ В КІБЕРПРОСТОРІ ПІД ЧАС ПІДГОТОВКИ ТА ВЕДЕННЯ МЕРЕЖЕЦЕНТРИЧНОЇ ВІЙНИ

У статті розглянуто зміни характеру ведення сучасних війн і ознаки переходу до мережецентричної моделі управління бойовими діями, спектр воєнних дій держави, основні напрямки та умови досягнення інформаційної переваги над противником. Визначено роль та місце дій в кіберпросторі під час підготовки та ведення мережецентричних війн та їх вплив на системи контролю та комунікацій життєво і стратегічно важливих об'єктів держави. Обґрунтовано необхідність захисту від кібератак об'єктів критичної інфраструктури держави та розвитку власних кіберозброєнь.

Ключові слова: *інформаційна війна, кіберпростір, мережецентризм, спектр воєнних дій держави, поріг оголошення війни, кібератака, кібербезпека, інформаційна перевага, мережецентрична війна, кібернетична зброя, кібернетичний вплив.*

Вступ

Аналіз останніх локальних війн і збройних конфліктів показав докорінні зміни у тактиці і стратегії ведення збройної боротьби. Супротивник, який має технологічну перевагу, замість зіткнення з противником по фронту, застосовує сили та засоби на всю глибину його території. Кількість військ, що розгорнуті на певному напрямі, вже не грає вирішальної ролі в досягненні мети операції. Для забезпечення переваги над противником вже недостатньо мати в своєму розпорядженні певний бойовий потенціал, а важливо застосувати його в потрібному місці та в потрібний час.

Постановка проблеми. Інформаційні війни в теперішній час є складовою частиною ведення сучасного військового протиборства. Головною метою ведення інформаційної війни є дезінформація, психологічне та інформаційне подавлення військ противника, а також порушення роботи систем управління військами, органів державного управління, систем цивільної оборони та життєзабезпечення країни.

Оборонний потенціал будь-якої держави може бути значно знижений противником через кіберпростір ще до початку бойових дій. Це необов'язково може бути вплив на бойові системи. В державі є банківські системи та структури державного управління, які використовують глобальну мережу. Порушення сталого функціонування цих систем або кіберсистем їх контрагентів може призвести до зниження обороноздатності та сприяти досягненню противником політичних цілей війни.

Аналіз остатніх досліджень і публікацій.

Питання, що стосуються сутності мережецентричних операцій та особливостей управління військами у ході їх ведення, досить широко висвітлюються у різних виданнях.

Основна модель ведення війн, діюча в арміях США і країн НАТО, заснована на концепції «мережецентричної війни». Модель «мережецентричної війни» представляється як система, що складається з трьох решіток-підсистем: інформаційної, сенсорно-розвідувальної та бойової. Основу системи складає інформаційна решітка, на яку накладаються сенсорна і бойова решітки, що взаємно перетинаються. Інформаційна решітка-підсистема пронизує собою всю систему в повному обсязі. Елементами сенсорної підсистеми є засоби розвідки, а елементами бойової решітки - засоби ураження. Ці дві групи елементів об'єднуються органами управління та командуванням. [1]

Значна увага приділяється нормативному регулюванню діяльності в кібернетичному просторі, порядок визначення шкоди, завданої кібератаками, визначення механізмів притягнення до відповідальності за її завдавання, а також співвідношення національних та міжнародних механізмів і засобів забезпечення безпеки кіберпростору.

Метою статті є визначення ролі та місця дій (операцій) в кіберпросторі під час підготовки та ведення мережоцентричної війни, а також основних завдань таких дій, та пріоритетних напрямів втілення такого досвіду в Україні.

Виклад основного матеріалу дослідження.

Термін "мережецентризм" вперше з'явився в американській комп'ютерній індустрії і став результатом прориву в інформаційних технологіях, які дозволили організовувати взаємодію між комп'ютерами не дивлячись на використання в них різних операційних систем. Відповідно до "мережецентричної моделі обчислень" користувачу не потрібно володіти усім програмним забезпеченням

для вирішення прикладних задач, а достатньо мати лише спрощене обчислювальне обладнання (мережевий комп'ютер) для звернення до віддаленої центральної бази, яка здійснює всі необхідні обчислення і забезпечує користувача усією необхідною інформацією. Пізніше ідея "мережецентризму" була взята на озброєння спеціалістами армії США. [2]

У будь-якій військовій операції має місце такий цикл подій: розвідка противника – оцінка обстановки – прийняття рішення – дії відповідно до обраного плану. Такий цикл умовно можна розділити на дві фази: інформаційну та кінетичну. Остання, в основному, визначається можливостями засобів ураження. Раніше як вітчизняні, так і закордонні вчені займались пошуком технічних рішень, пов'язаних в першу чергу із другою фазою, а саме – підвищенням мобільності, точності та вогневої міці засобів збройної боротьби. Така модель управління отримала назву "платформоцентричної", відповідно до якої розвиток військової техніки відбувався у напрямку створення та удосконалення окремих "бойових платформ", а бойовий потенціал підрозділів визначався їх кількісним нарощуванням. Але, як показує практика, для підвищення ефективності кінетичної фази є певні обмеження, крім того суттєво підвищується і вартість розробок.

Рисунок 1. Спектр воєнних дій держави

На рисунку 1 показано поділ воєнних дій на дві фази: інформаційну і кінетичну. Зверніть увагу, що ці фази не виключають одна одну, а всі дії розподіляються по спектру між суто кінетичними або суто інформаційними. Чим вище дія по спектру, тим вона більш сильна; найвища тяжкість дій – це ядерний удар або кібератака, що руйнує національну енергосистему. Дії над червоною лінією, здебільшого, загальновизнано відповідають порогу оголошення війни; дії під червоною лінією або юридично неоднозначні, або явно нижче порогу оголошення війни. Зверніть увагу, що інформаційні дії, як правило, більш юридично неоднозначні через відсутність чіткого розуміння в результаті більш короткого історичного контексту використання інформаційної війни. Хоча кібератака, яка критично порушує фінансовий сектор, потенційно може бути настільки ж руйнівною або навіть більш руйнівною, ніж терористична атака, що спонсується державою або звичайне вторгнення, область інформаційної війни (особливо кібервійни) має тенденцію бути більш двозначною через проблеми із тлумаченням суверенітету, оскільки вона пов'язана з фізичними та логічними межами комп'ютерних мереж і серверів.

Вкрай важливо, що більшість дій війни потрапляють в сферу правової неоднозначності. Це не означає, що дії в сірій зоні є законними відповідно до міжнародного права, скоріше, відсутній консенсус щодо того, як країни вважають за краще інтерпретувати свою законність. Фактично, більшість цих дій під строгим тлумаченням міжнародно-правового кодексу вважаються незаконними. Розглянемо випадок використання Росією «Патріотичних хакерів» в 2007 році для проведення розподілених атак на відмову в

обслуговуванні на державних сайтах Естонії, тим самим завдаючи шкоду здатності Естонії здійснювати управління. За словами міністра оборони Естонії, ця кібератака стала «ситуацією в області національної безпеки», що спричинило прохання про надання підтримки НАТО та подальшому створенні Центру співпраці в області кібербезпеки НАТО в Таллінні, Естонія. Ясно, що естонці вважали, що цей напад є застосування сили. Очевидно, що росіяни, маючи намір використовувати силу, зуміли спотворити міжнародне сприйняття цього використання національної сили, щоб уникнути великого, невигідного конфлікту. [3]

За таких умов була створена нова – "мережецентрична" система поглядів на управління збройними силами і бойовими засобами, покликана збільшити їх бойовий потенціал за рахунок створення єдиної інформаційно-комунікаційної мережі. Принципи ведення "мережецентричних" війн (принаймні на даному етапі розвитку їх теорії і практики) перше за все спрямовані на досягнення інформаційної переваги над противником.

Інформаційна перевага – це не передача у великій кількості інформації "бойовим платформам", а досягнення більш глибокого, яке відповідає обстановці, усвідомлення і розуміння ситуації на полі бою, більш точного з'ясування своїх переваг та недоліків противника, здатність сформувати задум дій, в якому ці переваги будуть максимальною мірою реалізовані, а недоліки противника використані у своїх цілях, випереджене прийняття й негайне доведення до підлеглих та сусідів рішень, цілком адекватних обстановці, безперервний контроль їх виконання. Нові можливості для удосконалення мережевих організаційних форм відкриває значний розвиток засобів інформатизації, оскільки для ефективності дій подібних формувань необхідно, щоб швидкість і якість обміну інформацією між ланками мережі були набагато вищими, ніж у ієрархічних структурах.

Мережецентрична війна – війна, орієнтована на досягнення інформаційної переваги. Це концепція ведення бойових дій, що передбачає збільшення бойової потужності угруповання об'єднаних сил за рахунок утворення інформаційно-комутаційної мережі, що поєднує джерела інформації (розвідки), органи управління та засоби ураження (придушення), що забезпечує доведення до учасників операцій достовірної та повної інформації про обстановку практично в реальному масштабі часу. За рахунок цього досягається прискорення процесу управління силами та засобами, підвищення темпу операцій, ефективності ураження сил супротивника, живучості своїх військ та рівня самосинхронізації бойових дій.[4]

Враховуючи особливість "мережевої" війни стосовно будь якого театру військових дій передбачається чотири основні фази ведення бойових дій:

досягнення інформаційної переваги за допомогою випереджуючого знищення (виводу з ладу, придушення) системи розвідувально-інформаційного забезпечення супротивника (засобів та систем розвідки, мережеутворюючих вузлів, центрів обробки інформації та управління);

завоювання переваги (панування) в повітрі за рахунок придушення (знищення) системи ППО супротивника;

поступове знищення залишених без управління та інформації засобів ураження супротивника, в першу чергу ракетних комплексів, авіації артилерії, бронетехніки;

остаточне придушення або знищення осередків спротиву ворога.

Успішне здійснення кожної з фаз ґрунтується на значно меншій тривалості бойового циклу "виявлення-впізнання-цілевказання-ураження" порівняно з супротивником, на більш точних та повних відомостях про угруповання супротивника, що протистоїть. [2]

Проведення операцій в кібернетичному просторі дозволяє дистанційно вивести з ладу системи життєзабезпечення, державного та військового управління, саме тому обґрунтування ефективності, стратегії та тактики даних операцій привертає значну увагу військових спеціалістів з інформаційної безпеки, збройні сили яких планують ведення "мережецентричних війн".

З військової точки зору кіберпростір являє собою специфічну складову частину більш широкого – інформаційного або інформаційно-комунікаційного простору. В структурному відношенні кіберпростір включає в себе апаратно-програмні комплекси та комп'ютерні мережі, в яких накопичується, зберігається та циркулює інформація. [4]

Необхідність порушення функціонування інфраструктури та системи життєзабезпечення населення, дозволяє зробити висновок про те, що цілями кібернетичних атак стануть системи контролю та комунікацій життєво і стратегічно важливих об'єктів:

інформаційні та комунікаційні ресурси країни;

ядерна та хімічна промисловість;

автоматизовані системи управління

технологічні процеси на стратегічно важливих підприємствах;

фінансова і банківська сфери;

енергетична система життєзабезпечення;

дорожній рух і транспортні мережі;

системи управління та зв'язку держави, поліції і армії.

Характерними рисами дій в кіберпросторі у військових цілях є:

високий темп проведення кібервпливу;

не завжди явний характер деструктивного впливу;

не завжди явне джерело деструктивного впливу;

необмежені масштаби впливу;

непередбачуваність місця і часу кібервпливу противника;

загроза незворотних катастрофічних наслідків деструктивного впливу.[1]

Збройні сили будуть вести реальні дії в кіберпросторі у військових цілях тільки з початком війни, а в мирний час вони повинні займатися всебічною підготовкою до їх ведення, маючи, у своєму кіберарсеналі такі засоби і способи дій, які в мирний час можуть навіть кваліфікуватися як негуманні, незаконні, катастрофічні за наслідками.

Слід чітко розуміти, що кіберпростір як поле

ведення протиборства двох або більше сторін буде набувати все більшого значення. Вже сьогодні бюджети відомств безпеки розвинених країн, задіяних в системі кібербезпеки держави (а кількість структур, які в цих процесах задіяні, постійно збільшується), складають мільярди доларів, і жодна з країн ще не зменшувала витрат за цими статтями (Рис.2). Не варто думати, що ці кошти вкладаються виключно в системи "оборони" і "захисту", – неформально майже всі держави займаються розробкою кіберозброєння.

Ще з моменту анексії Криму Російська Федерація використовувала кібератаки як складову своєї гібридної війни проти нашої держави. Різноманітні спеціальні підрозділи структур безпеки нашого супротивника здійснювали атаки на державні інформаційні ресурси і на персональні дані окремих політиків і громадських діячів. Найбільш відомі випадки таких дій – DDoS-атаки на урядові ресурси (МЗС , сайт Президента України , сайти органів сектору безпеки та оборони), цільові атаки на державні органи за допомогою шахрайських електронних листів, спроби порушити роботу системи ЦВК під час виборів Президента і на парламентських виборах 2014р а також функціонування вірусу Uroboros, який, з високою долею ймовірності, ідентифікований як російський.

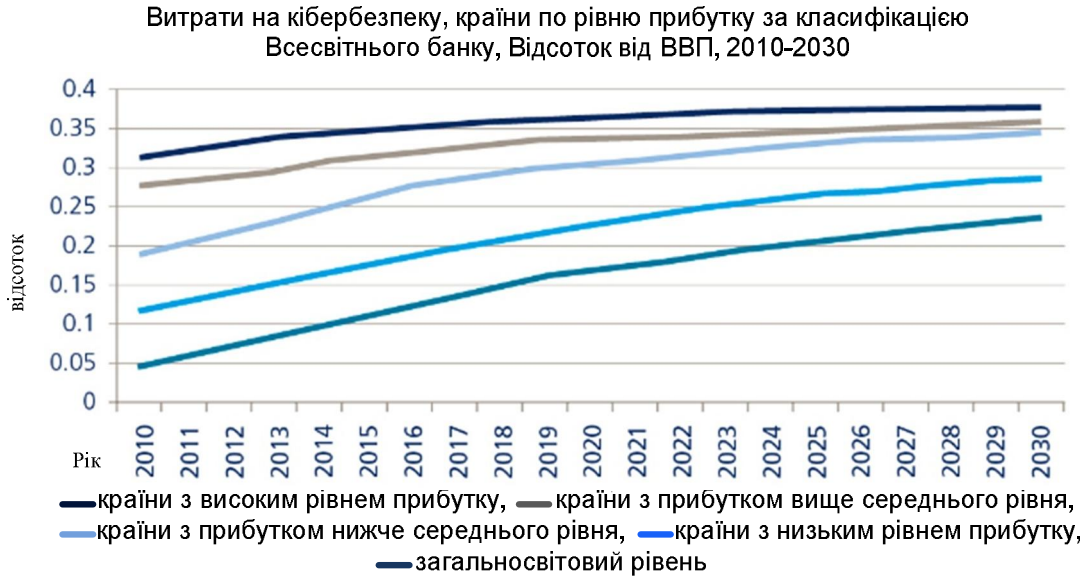

Рисунок 2. Витрати на кібербезпеку країн світу. [6]

Противник повинен знати, що намагаючись використовувати кіберпростір на шкоду національним інтересам України, він може зіткнутися з діями у відповідь. Це, у свою чергу, призведе до зростання його витрат на оборону, що і може бути однією з цілей асиметричної відповіді.[7] Саме тому потрібно приділяти більше уваги розвитку кіберозброєнь та кіберзахисту.

Висновки й перспективи подальших досліджень

Таким чином дії (операції) в кіберпросторі є невід'ємною складовою підготовки та ведення "мережецентричних війн". Зазвичай проводяться в рамках інформаційної операції (хоча не виключено проведення окремої операції в кіберпросторі), на першій фазі бойових дій, під час здобуття інформаційної переваги над противником. Відмінними ознаками дій в кіберпросторі у військових цілях є: наявність чітко сформульованої мети кібервпливу (узгодженої за цілями і завданнями операції, бою, битви); ретельне планування дій з досягнення поставленої мети і наявність відповідного комплекту сил і специфічних засобів кібервпливу. Кібернетична зброя вже зараз володіє потенціалом поразки, порівнянним зі зброєю масового ураження, а зі збільшенням комп'ютеризації державних, інфраструктурних та життєзабезпечуючих об'єктів потенціал даного виду зброї буде тільки зростати.

Література

1. Макаренко С. И. Проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне/Спецтехника и связь №3, 2011. **2. Тітов І. В.** Мережоцентрична концепція ведення війни XXI сторіччя / І. В. Тітов // Системи озброєння і військова техніка. – 2008. – № 3. **3. Jason Rivera.** Understanding and Countering Nation-State Use of Protracted Unconventional Warfare./ Jason Rivera//Режим доступу:http://smallwarsjournal.com/jrnl/art/understanding-and-countering-nation-state-use-of-protracted-unconventional-warfare **4. Alberts, David S. (David Stephen)**, Network centric warfare : developing and leveraging information superiority, 2nd Edition (Revised) / David S. Alberts, John J. Garstka, Frederick P. Stein. Second printing February 2000. **5. Дубов Д. В.** Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.**6. Overcome by cyber risks? Economic benefits and costs of alternate cyber futures**./ Zurich Insurance Group's and the Atlantic Council's Brent Scowcroft Center's on International

Security report//Available at: http://publications.atlantic-council.org/cyberrisks//**7. Горбулін В.П.** У пошуках асиметричних відповідей: кіберпростір у гібридній війні. – 2015. Режим доступу: https://gazeta.dt.ua /internal /u-poshukah-asimetrichnih-vidpovidey-kiberprostir-u-gibridniy-viyni-_.html

ДЕЙСТВИЯ В КИБЕРПРОСТРАНСТВЕ ВО ВРЕМЯ ПОДГОТОВКИ И ВЕДЕНИЯ СЕТЕЦЕНТРИЧЕСКОЙ ВОЙНЫ

***Александр Николаевич Гук*[1]**
***Алексей Юрьевич Чередниченко*[1]**
***Роман Михайлович Штонда*[1]**
***Игорь Алексеевич Дыба*[2]**

[1] *Военный институт телекоммуникаций и информатизации, Киев, Украина*
[2]*Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина*

В статье рассмотрены изменения характера ведения современных войн и признаки перехода к сетецентрической модели управления боевыми действиями, спектр военных действий государства, основные направления и условия достижения информационного превосходства над противником. Определена роль и место действий в киберпространстве во время подготовки и ведения сетецентрических войн и их влияние на системы контроля и коммуникаций жизненно и стратегически важных объектов государства. Обоснована необходимость защиты от кибератак объектов критической инфраструктуры государства и развития собственных кибервооружений.

Ключевые слова: *информационная война, киберпространство, сетецентризм, спектр воен действий государства, порог объявления войны, кибератака, кибербезопасность, информацио преимущество, сетецентрическая война, кибернетическое оружие, кибернетическое влияние*

ACTIONS IN CYBERSPACE DURING THE PREPARATION AND CONDUCT OF NETWORK CENTRIC WARS

***Oleksandr M. Guk*[1]**
***Oleksiy Y. Cherednychenko*[1]**
***Roman M. Shtonda*[1]**
***Ihor O. Dyba*[2]**

[1]*Military Institute of Telecommunications and Informatization, Kyiv, Ukraine*
[2]*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

The article considers changes in the nature of conducting modern wars and signs of transition to a network-centric model of combat management, the spectrum of military actions of the state, the main directions and conditions for achieving information superiority over the enemy. The role and place of actions in cyberspace during the preparation and conduct of network centric wars and their influence on the control and communication systems of vital and strategically important objects of the state were determined. The necessity of protection of the state's critical infrastructure objects and development of own cyber weapons is grounded.

Keywords: *information warfare, cyberspace, net-centric, the spectrum of state military operations, the threshold of war, cyberattack, cybersecurity, information superiority, network centric warfare, cybernetic weapons, cybernetic influence.*

References

1. Makarenko S. I. Perspectives and problems of employment of the cybernetic weapon by in the modern net-centric war [Problemyi i perspektivyi primeneniya kiberneticheskogo oruzhiya v sovremennoy setetsentricheskoy voyne] /Special equipment and communication №3, 2011. **2. Titov I.V.** Network centric warfare concept of conducting war of XXI century [Merezhotsentrychna kontseptsiia vedennia viiny XXI storichchia]/I.V. Titov // Weapons systems and military equipment. – 2008. – № 3. **3. Jason Rivera.** Understanding and Countering Nation-State Use of Protracted Unconventional Warfare./ Jason Rivera// Access mode: http://smallwarsjournal.com/jrnl/art/understanding-and-countering-nation-state-use-of-protracted-unconventional-warfare **4. Alberts, David S. (David Stephen)**, Network centric warfare : developing and leveraging information superiority, 2nd Edition (Revised) / David S. Alberts, John J. Garstka, Frederick P. Stein. Second printing February 2000. **5.** Dubov D. V. Cyberspace as a new dimension of geopolitical rivalry: monograph [Kiberprostir yak novyi vymir heopolitychnoho supernytstva : monohrafiia]/ D. V. Dubov. – K. : NISS, 2014. – 328 pg. **6. Overcome by cyber risks? Economic benefits and costs of alternate cyber futures**./ Zurich Insurance Group's and the Atlantic Council's Brent Scowcroft Center's on International Security report// Access mode: http://publications.atlantic-council.org/cyberrisks// **7. Gorbulin V.P.** Finding asymmetric responses: cyberspace in hybrid warfare. [U poshukakh asymetrychnykh vidpovidei: kiberprostir u hibrydnii viini.] – 2015. Access mode: https://gazeta.dt.ua /internal/u-poshukah-asimetrichnih-vidpovidey-kiberprostir-u-gibridniy-viyni-_.html