УДК 327.8: 15

А. П. ДЕМАРТИНО

РЕСУРСИ ІНФОРМАЦІЙНОЇ ВІЙНИ У ВОЄННО-ПОЛІТИЧНІЙ СТРАТЕГІЇ США ТА КИТАЮ

Інформація охопила абсолютно усі сфери суспільства. Вона дедалі виходить на перший план у політиці сучасних держав, а інформаційна безпека є важливим питанням для кожної з них. Інформаційний розвиток стрімко йде вгору і на цьому тлі ми помічаємо чимало конфліктів, які згодом переростають в інформаційні війни. З огляду на це у статті розглянуто ресурси інформаційної війни на прикладі США та КНР. Ці держави потребують особливої уваги, оскільки є найбільш прогресивними в інформаційній складовій своїх воєнно-політичних стратегій. І від того, як буде продовжуватися їх протистояння, залежить доля світового інформаційного суспільства.

Ключові слова: *інформаційний простір, інформаційний вплив, холодна війна, «прохолодна війна», інформаційні війни, інформаційне протиборство, стратегія інформаційної безпеки, «група швидкого реагування», «м'який вплив».*

Demartyno Andrii. **Resources of the Information War in the military-political strategy of the United States and China**

Information covered absolutely all areas of society. It is becoming more and more important in the politics of modern states, and information security is an important issue for each of them. Information development is rapidly going up and against this background we notice a lot of conflicts, which later develop into o A. information wars. The article discusses the resources of the information war on the example of the United States and China. These states require special attention, since they are the most progressive in the information component of their military-political strategies. And the fate of the world information society depends on how their confrontation continues.

Key words: *information space, information impact, cold war, «cool war», information wars, information confrontation, information security strategy, «rapid response team», «mild impact».*

Відомо, що інформація в сучасному світі посідає важливе місце у його регіональному та глобальному вимірах. Від неї залежать і світові держави, і окремі суспільства, і об'єкти інф-

---

© *ДЕМАРТИНО Андрій Павлович* – кандидат історичних наук, докторант Інституту держави і права імені В. М. Корецького НАН України

раструктури. На даний момент інформатизація охопила усі сфери суспільного життя, включаючи військово-стратегічну. Вона змінила саме поняття «війни», дозволяючи без жертв і руйнувань планувати і здійснювати широкомасштабні операції зовнішньополітичного впливу. У цьому контексті інформаційна війна – найбільш актуальне явище, яке безперервно досліджується.

Американський генерал М. Маклюен відзначив, що у новітній час економічні відносини дедалі більше набувають форми обміну знаннями, а не обміну товарами. А засоби масової комунікації самі є новими «природними ресурсами», що примножують багатства. Тобто боротьба за капітал, простори збуту відходять на другий план, а головним стає доступ до інформаційних ресурсів, знань. І це призводить до того, що війни ведуться вже більше в інформаційному просторі та за допомогою інформаційних видів озброєнь[1].

З'явилися різноманітні інформаційні мережі, які мають власні засоби комунікації, економічне забезпечення та військово-стратегічну структуру. Особливо актуальними стали використання, пошук нової інформаційної зброї та ресурсів, які б дозволили провідним державам боротися за сфери впливу і контролювати інформаційні потоки опонентів. Відомий американський вчений М. К. Лібікі у своїй праці «Що таке інформаційна війна?» виділив сім форм останньої: боротьба з пунктами управління і зв'язку супротивника; боротьба за здобуття інформації про власні сили і сили противника в режимі реального часу; радіоелектронна боротьба; психологічна війна; хакерська війна проти комп'ютерних систем противника; блокування або спрямування економічної інформації в необхідне русло для досягнення економічного домінування, кібервійна[2].

Кожна країна має власну концепцію інформаційного протиборства і у стані війни, і під час мирного співіснування. Інформаційні ресурси використовуються в інформаційному середовищі не лише для безпосередніх бойових дій, а й для захисту власної інформаційної безпеки. Провідні держави включили цей аспект до своїх військово-політичних стратегій,

створили підрозділи спеціального призначення, які покликані запобігати інформаційним атакам та, з допомогою потужної інформаційної зброї, лобіювати інтереси своєї держави.

Цікавою та актуальною є тема ресурсів інформаційної війни. Адже, окрім визначеного набору, кожна держава має свої особливі інформаційні ресурси і намагається максимально користуватися ними у своїй воєнно-політичній стратегії. Відтак, спираючись на праці попередніх дослідників (І. Валюшко, О. Трофименко, О. Олійник, Я. Дубовой, О. Кучмій, Г. Пєвцов, М. Сенченко, М. Фесенко, А. Буравкова, Д. Дубов, А. Гордієнко, С. Залкін, С. Сідченко, К. Хударковський та ін.), пропонуємо розглянути їх особливості на прикладі двох наддержав – США та КНР.

Китай характеризується розвиненою концепцією інформаційно-психологічної війни, яка вже потенційно може бути загрозою для ворога. Контроль за її виконанням здійснюють Дослідницьке бюро при Державній Раді КНР, а також Системно-аналітичний центр Міністерства державної безпеки. Китай також має державні й недержавні спецзагони, які не раз атакували американський та європейський кіберпростір. Не варто забувати і про роль релігії у цьому процесі, яка не забороняє здійснювати такі дії задля захисту інтересів держави.

Поряд із цим одним із найважливіших ресурсів інформаційної війни для Китаю є його власна історія, а саме т. зв. китайські стратегеми. Цікавим є той факт, що, за наявності інформаційної переваги у США, американські військові фахівці вважають, що китайські технології ведення психологічних операцій є унікальними й актуальними в інформаційну добу. В цілому вся доктрина ведення інформаційно–психологічних операцій у Китаї заснована на філософському вченні Лао Цзи (VI століття до н.е.), але значно більше поширення отримав відомий трактат давньокитайського філософа Сунь Цзи (VI–V століття до н.е.) «Мистецтво війни», в якому автор представляє сутність професійно організованої психологічної війни. Сунь Цзи, зокрема, зазначав: «У будь-якій війні, як правило, найкраща політика зводиться до захоплення держави цілісною; зруйну-

вати її значно легше. Взяти у полон армію противника краще, ніж її знищити... Одержати сотню перемог у боях – це не межа мистецтва. Скорити супротивника без бою – от вершина мистецтва». Автор доводить важливість володіння інформацією й прийомами дезінформації противника для маніпулювання його станом і діями[3].

Таким чином, підкреслюється, що найвигідніша з усіх військових стратегій – маніпулювання ворогом у такий спосіб, щоб домогтися легкої перемоги над ним без бою. Сунь Цзи першим узагальнив досвід, накопичений стародавнім Китаєм у сфері психологічних операцій. Він стверджував, що найгірше – напад на ворожі укріплені міста. У КНР цю концепцію перефразували так: «Краще атакувати розум супротивника, аніж його укріплені міста». Тому основними складовими сучасної китайської стратегії інформаційного протиборства є теоретичне залякування, протистояння інформаційного потенціалу; конкуренція інформаційних стратегій; прискорення інформатизації військ; економічно-інформаційна агресія; культурно-інформаційна агресія; інформаційна війна розумів[4].

Окрім власних розробок, китайські військові експерти значну увагу приділяють зарубіжному досвіду в сфері ведення інформаційної війни. Як і західні військові фахівці, вони вважають, що дослідження збройних конфліктів останнього часу дає можливість виділити кілька характерних рис, притаманних сучасним інформаційнім війнам: по-перше, «прозорість поля бою» (наприклад, оператор комп'ютерних систем може здійснювати безупинний контроль за ситуацією, спостерігати відображуване на дисплеї розташування своїх військ і військ противника, його об'єкти, концентрацію і переміщення його сил); по-друге, загальна координація дій військ за допомогою створення єдиного каналу управління для всіх бойових підрозділів і підрозділів тилового забезпечення (наприклад, оператор інформаційного центру, маючи дані про кількість, склад і координати виявлених цілей противника, робить розрахунки для їх розподілу за засобами ураження, визначає кількість необхідних боєприпасів тощо); по–третє, ведення бойових дій

у реальному масштабі часу, тобто негайне реагування на зміну бойової обстановки[5].

Базовим ресурсом ведення інформаційної війни для КНР є жорсткий контроль над суспільством і ЗМІ з боку держави. Знаковою подією стало прийняття «Правил регулювання, що забезпечують безпеку комп'ютерних та інформаційних систем», де чітко роз'яснено, яка саме інформація є забороненою і загрожує національній безпеці. Серед такої виділяються терористичні заклики, спроби повалення державного соціалістичного режиму, посягання на територіальну цілісність, наклеп на структури державного управління та інше. Надзвичайно великі повноваження в інформаційній сфері має Міністерство державної безпеки КНР та інші державні органи. Тільки за їх згоди та корекції новини, преса та інша інформація можуть доходити до суспільства.

Особливості політики регулювання інформаційної безпеки в Китаї оцінюються експертами по-різному. Так, представники західних кіл вважають, що система жорсткого контролю з боку уряду за інформацією та інформаційною діяльністю китайських громадян є не «регулюванням» з метою безпеки, а скоріше «цензурою» і виступає серйозним стримуючим чинником на шляху до демократизації країни й побудови відкритого інформаційного суспільства. Іншого погляду дотримуються представники уряду Китаю, які вважають, що такий контроль є необхідною передумовою формування національного інформаційного простору й гарантуванням безпеки політичної, економічної й професійної діяльності всіх учасників інформаційного обміну Водночас захист національних інтересів і державної безпеки не повинен гальмувати загальний розвиток інформаційних технологій, які є одним із головних інструментів долучення китайців до досягнень світової культури, науки й техніки. За даними China Internet Network Information Center, понад 80% мережевої аудиторії Китаю використовують Інтернет як джерело наукової і технічної інформації. При цьому 78% китайських користувачів Інтернету – це молоді люди віком від 21 до 35 років, що робить надзвичайно важли-

вим контроль за етичним контентом інформації у мережі. Державні заходи регулювання також дають можливість уряду нейтралізувати будь-які негативні потоки інформації, що шкодять репутації держави на міжнародній арені й підривають довіру громадян до уряду й китайської політичної системи в цілому[6].

Сполучені Штати Америки відзначаються вищим рівнем та якістю інформаційних ресурсів. Про це свідчить чітко сформована законодавча система у цій сфері. Серед найбільш значущих документів є «Стратегічна концепція суперництва», «Доктрина спільних дій з проведення інформаційних ситуацій», «Стратегія національної безпеки». У документі «Єдина перспектива – 2020» визначено, що «головною рисою збройної боротьби в XXI столітті буде її перенесення в сферу інформаційного протиборства, а досягнення інформаційного панування стане обов'язковою умовою перемоги над будь-яким противником»[7].

У США на державному рівні в рамках реалізації стратегії інформаційної безпеки функціонують близько 40 організацій. Загальна сума витрат на інформаційну безпеку в США в 2007 році становила майже 50 млрд доларів на рік. Координація їх діяльності здійснюється на найвищому державному рівні. В американському зовнішньополітичному відомстві створено спеціальну «групу швидкого реагування», завданням якої є: 1) здійснення моніторингу зарубіжних ЗМІ з широким використанням інформаційно-комп'ютерних мереж та сучасних інформаційних технологій для забезпечення домінування у зовнішньому інформаційному просторі; 2) заходи оперативної протидії антиамериканським публікаціям, що передбачають залучення до цієї роботи працівників дипломатичних представництв у різних країнах світу та створення регіональних «груп швидкого реагування». У разі потреби планується спрямовувати у кризові райони фахівців із PR-технологій. Представник держдепартаменту США назвала їх «інформаційним підрозділом спеціального призначення». Головною метою Держдепартаменту США є забезпечення «оперативної і рішу-

чої відповіді на інформацію, яку США вважають необ'єктивною або такою, що не відповідає дійсності», та формування позитивного іміджу США у світі.

Для ведення інформаційної війни у США створені та діють структури спеціальних психологічних операцій (ПсО) у межах ЦРУ та Міністерства оборони (підрозділи об'єднаного командування спеціальних операцій), налагоджено чітку систему підготовки кадрів для ведення інформаційної війни. У межах системи проходження військової служби офіцерським складом (Officer Personnel Management System, OPMS) передбачено існування функціональної структури «Психологічні операції та робота з цивільним населенням», де налічується близько 1000 офіцерів – від капітана до підполковника. Діють системи перепідготовки та підвищення кваліфікації, заохочується навчання офіцерів у магістратурі (докторантурі)[8].

Важливим підрозділом із запобігання інформаційно-електронним атакам у США є «U.S. Cyber Command», місія якого полягає у запобіганні стратегічним атакам і залученню сил, як зазначено, для забезпечення безпеки нації і союзників. Обов'язки командування включають стратегічне стримування; ядерні операції; космічні операції; спільні операції електронного спектру та ін.[9] Серед військових підрозділів у США є окремий батальйон, в якому служать близько трьохсот спеціалістів різних родів інформаційних військ: пропагандистів, інформаційних копірайтерів, агентів, психологів тощо. Цей батальйон покликаний миттєво реагувати на зміну інформаційних потоків і стратегічно адаптуватися до них. Цей підрозділ, як і інші інформаційні структури, діє згідно з директивою Пентагону «Інформаційні війни», в якій вказано, що їх діяльність має бути спрямована на контроль за інформаційним розвитком інших держав і, за потреби, використання усіх інформаційних ресурсів задля домінування США в інфопросторі.

Пріоритетами національної інформаційної політики США визначені: підтримка досліджень і розробок у галузі інформації і комунікації; вплив на їхнє спрямування та заохочення до поширення технічних знань і можливостей в економіці; спри-

яння обміну технологіями між лабораторіями та фірмами, запровадження нововведень на ринках; побудова та вдосконалення інформаційної інфраструктури, контроль за її діяльністю, побудова глобальних систем комунікації і дослідження впливу систем на міжнародні, національні та приватні пріоритети; збереження порушеної новими технологіями рівноваги між чотирма основними інформаційними цінностями: конфіденційність інформації, інформація як суспільне благо, інформація як товар, інформація як невід'ємний компонент існування держави (необхідне відновлення цієї рівноваги і встановлення нових засобів контролю для нових інформаційних відносин); недоторканність приватного життя, конфіденційність інформації приватного характеру на різних рівнях і в різних сферах державного управління та в приватному секторі; вироблення урядової політики в галузі інформації і комунікації[10].

Отже, США має надзвичайно потужні ресурси ведення інформаційної війни, і жодна держава поки що не має таких можливостей. Однак Китай готовий із цим посперечатися і становить чи не найбільшу загрозу для Сполучених Штатів у інформаційній сфері. Про це свідчать останні тактичні його перемоги. Однією з них є вибачення США перед Китаєм (безпрецедентна подія) за посадку свого літака на острові Хайнань. Також заслугою китайських спецслужб стало спростування обвинувачення в екстремізмі у 1989 році під час студентських протестів на площі Тяньаньмен, і навіть підозра, що вони не обійшлися без втручання США. Варто згадати знакову подію, коли китаєць Гері Лок став губернатором штату Вашингтон. Таким «м'яким впливом», через залучення своїх численних діаспор, Китаю вдається бути важливим актором у міжнародних відносинах.

Англійський дослідник Х. Макрей передрікає перетворення Китаю у повноправного конкурента Сполученх Штатів приблизно у 2020 році («Якщо США не покращать свою систему освіти й не продемонструють більше самодисципліни»). Можна припустити виникнення біполярного світу з полюсами

у вигляді США і Китаю. Як зазначає колишній держсекретар США й досі впливова у республіканській партії К. Райс, «Китай не є державою, схильною зберігати «status quo», навпаки, він хотів би змінити існуюче становище, змінити баланс сил в Азії на свою користь. Вже одне це робить його стратегічним суперником Америки»[11]. Але, якщо виходити з реалій сьогодення, слід визнати, що нині є лише одна наддержава – США, які збережуть цей статус щонайменше до середини XXI століття, коли КНР досягне з ними паритету не лише за економічним потенціалом, а й наблизиться до бажаного балансу у військовій сфері[12].

Д. Роткопф, головний редактор видання «The Foreign Policy», називає новий тип протистояння між США та КНР не «холодною війною» (cold war), а «прохолодною війною» (cool war), і передусім саме через технології, що застосовуються: «Технології «холодної війни» зробили її неможливою. Технології «прохолодної війни» роблять її непереборною (irresistible)»; «Метою «холодної війни» було отримання переваги, яка стане в пригоді при переході на рівень «гарячої» війни або повністю її попередить. Мета «прохолодної війни» – мати можливість завдавати удару, не розв'язуючи «гарячої» війни»[13].

«В інформаційній війні завжди програє той, хто говорить правду. Тому що він обмежений правдою, тоді як брехун може говорити все що завгодно», – вважає Роберт Шеклі[14]. Але, звичайно, жодна держава в інформаційній війні ніколи не керується лише правдивими засобами. Не є винятком і США, КНР, які повністю занурилися в пошуки нових ресурсів та новітньої інформаційної зброї, яка не вміє вбивати, не має пороху, однак має надзвичайний вплив на свідомість та психологію людей та суспільств, наслідки якого часто навіть перевищують наслідки збройних війн.

1. Валюшко І. О. Еволюція інформаційних війн: минуле і сучасність. *Історико-політичні студії.* Збірник наукових праць. 2015. № 2 (4). С. 131. **2.** Трофименко О. Г., Дубовой Я. В. Еволюція поглядів на інформаційні війни в епоху інформаційного суспільства. *Порівняльно-аналітичне право: електронне наукове фахове видання.* Ужгород, 2017. № 1. С. 190.

3. Кучмій О. П. Стратегія інформаційної безпеки в структурі внутрішньої й зовнішньої політики КНР. *Актуальні проблеми міжнародних відносин*. 2011. Вип. 102 (1). С. 166. **4.** Там само. С. 167. **5.** Там само. С. 168. **6.** Там само. С. 159. **7.** Досвід і концепції ведення інформаційної боротьби у провідних країнах світу / Г. В. Пєвцов, А. М. Гордієнко, С. В. Залкін, С. О. Сідченко, К. І. Хударковський. *Наука і техніка Повітряних Сил Збройних Сил України*. 2015. № 1. С. 14. **8.** Сенченко М. І. Запорука національної безпеки в умовах інформаційної війни. *Вісник Книжкової палати*. 2014. № 6. С. 5. **9.** U. S. Strategic Command. About. URL: https://www.stratcom.mil/About/ **10.** Олійник О. В. Інформаційна безпека США. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. Вип. 1. С. 283. **11.** Фесенко М. В. Боротьба США та Китаю за глобальне лідерство у XXI столітті. *Міжнародні відносини*. Серія «Політичні науки». 2015. № 6. С. 8. **12.** Буравкова А. Г. Американсько-китайські відносини в постбіполярну епоху: глобальний і регіональний вимір. *Політичний менеджмент*. 2013. № 59. С. 155. **13.** Дубов Д. В. Геополітичне суперництво у кіберпросторі як чинник впливу на національну безпеку України: дис. ... д-ра політ. наук : спец. 21.01.01 «Основи нац. безпеки держави (політ. науки)»; Нац. ін-т стратег. дослідж. Київ, 2016. С. 132–133. **14.** Шеклі Р. Цитати та афоризми. URL: www.inpearls.ru/author/7182

Demartyno Andrii. **Resources of the Information War in the military-political strategy of the United States and China**

Information covered absolutely all areas of society. It is becoming more and more important in the politics of modern states, and information security is an important issue for each of them. Information development is rapidly going up and against this background we notice a lot of conflicts, which later develop into o A.information wars. The article discusses the resources of the information war on the example of the United States and China. These states require special attention, since they are the most progressive in the information component of their military-political strategies. And the fate of the world information society depends on how their confrontation continues.

It is known that information in the modern world occupies an important place in its regional and global dimensions. It depends on world states, individual societies, and infrastructure objects. At the moment, informatization has covered all spheres of public life, including military-strategic. She changed the very concept of «war» and captures the goals of civilization and people without sacrifices. In this context, information warfare is the most urgent phenomenon that is constantly being explored. There were various types of information networks that have their own communication tools, economic security and military-strategic structure. Particularly relevant were the use, as well as the search for all new information weapons and resources that would allow the leading powers to fight for the sphere of influence and control the

information flows of opponents. Each country has its own concept of information confrontation both in a state of war and during peaceful coexistence. An interesting and relevant topic is the information warfare resources, which the author suggests to consider on the example of two superpowers – the United States and China.

The peculiarities of the information security regulation policy in China are assessed by experts in different ways. So, Westerners believe that the system of strict government control over the information and information activities of Chinese citizens is not «regulation» for the sake of security, but rather «censorship» and acts as a serious constraint on the road to democratization of the country and the construction of an open information society . Other views are shared by representatives of the Chinese government who believe that such monitoring is a prerequisite for the formation of a national information space and the security of the political, economic and professional activities of all participants in the information exchange. At the same time, the protection of national interests and state security should not hinder the overall development of information technology, which is one of the main tools for the Chinese to contribute to the achievements of world culture, science and technology.

The priorities of the national information policy of the USA are defined: support of researches and developments in the field of information and communication; influence on their direction and encouraging the spread of technical knowledge and opportunities in the economy; promoting the exchange of technologies between laboratories and firms, introducing innovations in markets; construction and improvement of information infrastructure, control over its activities, construction of global communication systems and studying the impact of systems on international, national and private priorities; the preservation of the balance between the four main information values: the confidentiality of information, information as a public good, information as a commodity, information as an integral component of the state's existence (the restoration of this equilibrium and the establishment of new controls for new information relations); privacy, privacy of private-sector information at various levels and in various areas of public administration and the private sector; creation of government policy in the field of information and communication.

The experience of the two superpowers testifies that no state in the information war is guided only by true means. This is evidenced, in particular, by the active search for new resources and latest information weapons that do not know how to kill, has no gunpowder, but it has a tremendous impact on the consciousness and psychology of people and societies, the consequences of which are often even greater than the consequences of armed warfare.

Key words: information space, information impact, cold war, «cool war», information wars, information confrontation, information security strategy, «rapid response team», «mild impact».