Кучмій О.П.*

СТРАТЕГІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СТРУКТУРІ ВНУТРІШНЬОЇ Й ЗОВНІШНЬОЇ ПОЛІТИКИ КНР

В статье рассмотрены основные подходы китайского руководства к вопросам обеспечения национальной информационной безопасности, проанализированы особенности внутренней и внешней политики КНР касательно обеспечения безопасности национального информационного пространства, информационные угрозы и методы противодействия им; исследованы стратегии информационного противоборства КНР в международных отношениях.

Ключевые слова: КНР, национальное информационное пространство, телекоммуникации, Интернет, регулирование, национальная информационная безопасность, информационные угрозы, информационное противоборство, «мягкая сила».

У статті розглянуті основні підходи китайського керівництва до питань забезпечення національної інформаційної безпеки, проаналізовані особливості внутрішньої і зовнішньої політики КНР щодо забезпечення безпеки національного інформаційного простору, інформаційні загрози та методи протидії їм; досліджено стратегії інформаційного протиборства КНР у международних відносинах.

Ключові слова: КНР, національний інформаційний простір, телекомунікації, Інтернет, регулювання, національна інформаційна безпека, інформаційні загрози, інформаційне протиборство, «м'яка сила».

The article describes the main approaches of the Chinese leadership to issues of national security, analyzed features domestic and foreign policies of China regarding the security of national information space, information threats; investigated communication strategies ofChina's informatiom warfare in the international relations.

Key words: China, the national information space, telecommunications, Internet regulation, the national information security, information threats, informational confrontation, «soft power».

На сучасному етапі розвитку Китайська Народна Республіка завдяки ефективній державній інформаційній політиці досягла високих показників рівня інформаційного розвитку. Успіхи реалізації інформаційних стратегій продемонстрували значні можливості, що відкривають перед державою інформаційно–комунікаційні технології. Прагнення досягти до середини XXI століття статусу держави–лідера не тільки в АТР, а й у світі в ці-

* кандидат політичних наук, доцент кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

лому, керівництво КНР розпочало реалізацію стратегії посилення сукупної національної потуги, важливим стратегічним напрямком якої є ефективна політика забезпечення національної інформаційної безпеки. Тому розробка стратегії національної інформаційної безпеки здійснюється у двох основних напрямках: по–перше, створення оборонної стратегії на основі ефективного механізму протидії інформаційним загрозам для внутрішньополітичної стабільності китайського суспільства, для функціонування національної інформаційної інфраструктури, по–друге, створення наступальної стратегії, що ґрунтується на подоланні «асиметричності» інформаційного розвитку щодо потенційних супротивників, зокрема, США, для нейтралізації потенційної агресії ззовні.

Китайські політичні лідери продовжують розглядати внутрішньополітичну ситуацію в Китаї як стратегічний чинник, оскільки вважають, що внутрішньополітична нестабільність може стати приводом для втручання у внутрішні справи держави й навіть інтервенції, викликом національній єдності й економічному зростанню країни. Сьогодні китайське суспільство досягло значних успіхів в інформаційному й технологічному розвитку, уникаючи серйозних економічних й політичних проблем, пов'язаних зі специфікою розвитку та функціонування глобальної мережі Інтернет і телекомунікаційних систем. Водночас стрімке зростання кількості користувачів Інтернету й швидкий розвиток та поширення інформаційних технологій, що активно заохочувалися самою державою, створюють додаткові проблеми регулювання інформаційної безпеки. Суттєвий вплив на регулювання інформаційної діяльності в КНР став вступ до СОТ, оскільки держава зобов'язалася забезпечити більшу інформаційну відкритість, зокрема, дозволити 49–відсоткові іноземні інвестиції в сферу послуг з додатком вартості через рік вступу й 50–відсоткові – після двох років з метою ширшого доступу іноземних компаній до Інтернет–ринку країни.

Особливості політики регулювання інформаційної безпеки в Китаї оцінюється 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. У той же час захист національних інтересів і державної безпеки не повинен гальмувати загальний розвиток інформаційних технологій, які є одним з головних інструментів долучення китайців до досягнень світової культури, науки й техніки. За даними China Internet Network Information Center, сьогодні 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 важливим контроль за етичним контентом інформації в мережі. Державні заходи регулювання також дають можливість уряду нейтралізувати будь–які негативні потоки інформації, що шкодять репутації держави на міжнародній арені і підривають довіру громадян до уряду й китайської політичної системи в цілому [1].

Починаючи з 1994 р., коли Інтернет став доступним для суспільного користування, було ухвалено понад 60 різних нормативних актів, безпосередньо пов'язаних з регулюванням інформаційної діяльності, у тому числі, в мережі Інтернет. Одним з перших законодавчих актів у сфері регулювання інформаційної діяльності стали «Правила регулювання, що забезпечують безпеку комп'ютерних та інформаційних систем» (1994

р.), згідно з якими обов'язки громадян й організацій були розподілені в такий спосіб: 1) Організації, що надають послуги доступу до міжнародних інформаційних каналів, повинні створити центри управління мережею з метою посилення контролю за своїми клієнтами та забезпечення безпеки інформаційної діяльності; 2) Організації й громадяни, зайняті в сфері Інтернет–бізнесу, повинні впровадити системи контролю безпеки з метою запобігання діяльності, що загрожує державним інтересам і сприяє витоку державної таємниці, інформації про оригінальні винаходи промислового виробництва, копіювання або доступу до матеріалів, які загрожують громадському порядку або суперечать морально–етичним принципам; 3) Організації й приватні особи, зайняті в сфері Інтернет–бізнесу, повинні позитивно сприймати політику регулювання, перевірки і керівні директиви Міністерства безпеки, надавати міністерству необхідну інформацію, матеріали і документи, а також допомагати у розслідуванні інцидентів, пов'язаних з порушенням законів; 4) Організації й громадяни, що створюють віртуальні дошки оголошень, чати або ж групи новин, повинні пройти перевірку на відповідність вимогам щодо захисту державної таємниці. У випадках виявлення витоків інформації слід негайно повідомляти в місцеве поліцейське управління [2]. У документі також вказується, яка саме інформація є «небезпечною» і підлягає забороні. Так, забороняється використання мережі Інтернет для створення, поширення, копіювання або ж передачі такої інформації: заклики до невиконання або ж порушення державних законів, нормативних актів або Конституції; заклики до зміни соціалістичного ладу або державної системи у цілому; заклики до порушення цілісності країни; інформація націоналістичного характеру; поширення недостовірної інформації, чуток; поширення порнографічних матеріалів; пропаганда азартних ігор; пропаганда насильства; заклики до терористичної діяльності; інформація, що шкодить репутації державних органів влади тощо.

В іншому документі – «Про введення в дію правил регулювання, що забезпечують безпеку комп'ютерних та інформаційних систем» (1994 р.), – зокрема, вказується, що основні функції моніторингу китайського сегменту глобальної мережі Інтернет переходять до Міністерства державної безпеки КНР, якому надається право контролювати, інспектувати й спрямовувати діяльність щодо забезпечення безпеки комп'ютерних та інформаційних систем, розслідувати й запобігати злочинам в сфері безпеки передачі та зберігання даних, здійснювати іншу діяльність щодо контролю комп'ютерних та інформаційних систем [2]. Всі новини, що з'являються на сайтах, також підлягають обов'язковій цензурі з боку Департаменту інформації Держради. Право публікації оригінальних новин мають тільки державні засоби масової інформації, наділені спеціальними урядовими повноваженнями.

З огляду на складності централізованого регулювання, що виникла у зв'язку з динамічним зростанням кількості користувачів Інтернету, значну частку контрольних функцій було передано операторам зв'язку, що здійснюють контроль онлайнових операцій і нагляд за змістом інформаційних потоків. У виданому у 1996 р. Указі «Про порядок взаємодії локальних провайдерів Інтернет–послуг з відповідними міжнародними компаніями й системами зв'язку» підкреслювалося, що організації, що надають послуги доступу до міжнародних інформаційних каналів, повинні створити центри управління мережею з метою посилення контролю над своїми клієнтами відповідно до законів і нормативних актів, а також з метою забезпечення кращого захисту й безпеки сервісу, що надається клієнтам [3]. У період з 1997 р. до 2000 р. уряд КНР видав низку законодавчих актів, що регулюють інформаційний контент з метою забезпечення безпеки комп'ютерних інформаційних систем і телекомунікаційних мереж, зокрема, Розпорядження Міністерства громадської

безпеки КНР «Про порядок забезпечення безпеки комп'ютерних інформаційних систем у мережі Інтернет» (1997 р.) та Указ Держради КНР «Про державне регулювання телекомунікацій» (2000 р.), в яких містилися доповнення до переліку забороненого контенту щодо терористичної діяльності та державної таємниці [3].

У вересні 2000 р. Указом Держради КНР «Про порядок управління Інтернет–послугами» провайдери інформаційних послуг, що надаються через мережу Інтернет, зобов'язувалися протягом 60 днів зберігати протоколи доступу до мережі, у тому числі, списки відвідуваних користувачами сайтів і дані мережевого трафіку, а також телефонні номери користувачів. Якщо у процесі надання інформаційних послуг провайдери виявлять матеріали, що відносено до категорії законодавчо заборонених, вони повинні блокувати до нього доступ і повідомити про це місцеве управління поліції. А у 2002 р. провідні китайські Інтернет–підприємці підписали зобов'язання підвищувати самодисципліну під час користування мережею й сприяти «усуненню шкідливої інформації з Інтернету» [3; 4]. На думку китайських урядовців, державна політика контентної фільтрації Інтернету та надання гарантій захисту суспільству в цілому й кожному громадянину, зокрема, від шкідливого й незаконного контенту, є ефективним методом забезпечення морально–етичної цензури, захисту від різноманітних шкідливих програмних продуктів у національному сегменті інформаційної мережі.

З метою підвищення ефективності контролю інформаційної діяльності в Китаї було також запропоновано створити систему двоступеневого доступу громадян й організацій до Інтернет–ресурсів. Таким чином, всі користувачі одержували можливість виходу до глобальної мережі тільки через встановлені державою ключові вузли (backbone networks), кількість яких було жорстко регламентовано, і кожний з яких перебував під контролем певного міністерства, відомства або партійно–громадського об'єднання. У 2000 р. за ініціативи Держради КНР за сприяння Міністерства науки й технологій почалася реалізація «Проекту С219» – першого етапу зведення «електронної стіни» навколо національного сегменту Інтернету [5]. В рамках проекту, який отримав назву «Великий китайський файрволл», було створено спеціальну систему серверів, які встановлювалися на Інтернет–канали між користувачами і постачальниками Інтернет–з'єднання, і які фільтрували інформацію, що передавалася через інформаційні канали. Основним завданням проекту було проголошено забезпечення надійного інформаційного захисту мереж, що об'єднують урядові департаменти, регіональні адміністрації, засоби масової інформації, корпоративні комп'ютерні комплекси й системи масового Інтернет–доступу. Під інформаційним захистом розумілося запобігання таким явищам, як розголошення даних, що є державною таємницею, незаконний переказ грошей за кордон, хакерські атаки, поширення вірусів тощо. Якщо Інтернет–сайт містив некоректну інформацію, доступ до нього з Китаю ставав неможливим. До ресурсів, що підлягали фільтрації, увійшли також більшість західних ЗМІ, зокрема, сайти BBC, CNN, ABC й CBS News, журналу «Time», а також сайти більшості американських університетів, пошукова система Alta Vista. В реалізації проекту взяли участь понад трьох тисяч кваліфікованих китайських фахівців, а під час виконання роробіт, передбачених проектом, було запатентовано понад 45 технологічних інновацій міжнародного рівня. Західні фахівці неоднозначно оцінили таку систему безпеки: її назвали за аналогією з відомою Великою китайською стіною (Great Wall of China) «Великим китайським брандмауером» (Great FireWall of China), але відзначили, що подібні заходи безпеки вживають і більшість розвинених країн не тільки АТР, але й Заходу задля встановлення контролю за інформацією негативного змісту (порнографія, насильство), а також контролю за використанням службового Інтернету в особистих цілях (за допомогою

файрволлів забороняють, наприклад, службу ICQ, розважальні й блоггерські сайти). Представники ж уряду Китаю зазначають, що крім контентної фільтрації активно розробляються механізми боротьби з електронним шахрайством, хакерством і несанкціонованим використанням персональної інформації фінансового характеру, а також боротьби з вірусними атаками, задля чого був створений спеціальний підрозділ при Департаменті громадської безпеки Пекіна – Інтернет–поліція. Одним з перших об'єктів її пильної уваги став офіс компанії Sohu.com, що володіє найбільш популярним у країні порталом, який регулярно відвідують майже 100 мільйонів китайців. У зону уваги потрапили також компанії Beijing Telecom, Beijing Netcom і ще 11 найбільших провайдерських компаній Пекіна [6].

Внесеня змін до порядку реєстрації доменів другого рівня в китайській національній зоні Інтернету (зокрема, іноземні компанії одержали можливість зареєструвати домен у зоні «cn», що раніше дозволялося виключно урядовим структурам КНР та національним комерційним компаніям) у грудні 2002 р. викликало необхідність введення додаткових заходів контролю контенту в мережі Інтернет: відтепер перевірці підлягала й вся електронна пошта, «перлюстрація» якої була покладена безпосередньо на провайдерів поштових послуг. Вони самі повинні сканувати електронні листи громадян і доповідати при виявленні політичних, ідеологічних або морально–етичних порушень.

В ухваленому 2005 р. новому «Законі про телекомунікації» [3] було визначено обмеження щодо залучення іноземного капіталу в китайські Інтернет–компанії та встановлено жорсткі правила спостереження за інформацією, що розміщується на сайтах, зокрема, всі провайдери зобов'язувалися протягом 60 днів одержати в Міністерстві інформаційної промисловості ліцензію на свою діяльність, надавши усю інформацію про свій бізнес. За новими правилами Інтернет–компанії також повинні одержати дозвіл міністерства перед тим, як залучити іноземний капітал, створити спільне підприємство з іноземними партнерами або розмістити свої акції на фондовому ринку. Компанії також зобов'язувалися протягом 60 днів зберігати усі матеріали своїх сайтів та інформацію про їхні відвідування й надавати ці дані за першою вимогою урядовим структурам або поліції.

Особливості регулювання інформаційного простору з метою забезпечення національної інформаційної безпеки вплинули і на співробітництво з провідними світовими інформаційно–комунікаційними компаніями – Yahoo!, Google, Microsoft, Cisco, Sun, Nortel тощо, які також були зобов'язані співпрацювати з органами безпеки Китаю в рамках угод про «самодисципліну» та сприяти контролю за потоками інформації в національному мережевому просторі КНР. Механізми самоцензури, встановлені в нових комп'ютерних програмах, не дають доступу до інформації, коли користувач уводить ключові слова, пов'язані з неприйнятними для офіційного Пекіну темами. Це привело до того, що Yahoo! і низка інших відомих Інтернет–компаній, що прагнуть відповідати вимогам уряду КНР щодо самоцензури задля збереження позицій на китайському ринку інформаційних продуктів та послуг, стали об'єктом для критики правозахисних організацій. У липні 2005 р. у Конгресі США були висунуті для обговорення 14 законопроектів, метою яких є заборона американським компаніям співпрацювати з Китаєм в галузі цензури Інтернету. У відповідь на критику керівництво компаній зазначило, що компромісне рішення з цього питання відкриває перед китайськими користувачами доступ до світових джерел інформації.

Важливим напрямком державної політики в сфері інформаційної безпеки є розробка стратегій інформаційного протиборства. Відповідно до китайських оцінок, сучасна міжнародна ситуація в сфері безпеки характеризується розвитком складних суперечливих тенденцій, серед яких можна виділити рух до багатополярного світу, економічну глобалі-

зацію, посилення взаємодії й співробітництва в антитерористичній боротьбі після подій 11 вересня 2001 р. й, поряд з цим, загострення суперництва у формуванні сукупної національної потуги, де особливого значення набуває рівень інформаційно–технологічного розвитку країн і наявність сучасних озброєнь, створених з використанням новітніх досягнень науки й техніки.

Найбільш імовірним супротивником в інформаційному протиборстві Китай визначає Сполучені Штати Америки, які, з одного боку, кидають виклик у реалізації національної стратегії модернізації КНР, а з другого, виступають потенційним джерелом новітніх технологій. Тому Пекін шукає можливості зміцнення стабільності китайсько–американських відносин, одночасно розвиваючи відносини з іншими акторами міжнародних відносин, зокрема, Росією, Японією, ЄС, ООН задля створення стратегічної противаги США на регіональному та глобальному рівнях, а також впливу на ті напрями зовнішньої політики США, які можуть містити загрози для національних інтересів Китаю.

Неоднозначно сприймається Китаєм й факт військової присутності США в Азіатсько–Тихоокеанському регіоні. Визнаючи роль Сполучених Штатів як стабілізуючого фактору, Китай у той же час сприймає наявність американських військ у регіоні як прояв довгострокової стратегії, покликаної забезпечити домінуюче геостратегічне положення США за допомогою стримування зростання національної потужності Китаю. Нарешті, здійснюючи спроби налагодити співробітництво зі США в глобальній антитерористичній війні, китайські лідери усвідомлюють, що кінцевий результат цієї кампанії на чолі зі США, позначиться на стратегічному оточенні Китаю, особливо у зв'язку з розміщенням збройних сил США в Центральній Азії, зміцненням військових зв'язків Сполучених Штатів з Пакистаном, Індією і Японією й можливим поновленням американської військової присутності в Південно–Східній Азії. Так, на думку китайських фахівців, під приводом проведення акції проти Афганістану, американці створили цілу мережу нових військових баз поблизу кордонів Китаю, готуючись до майбутнього військового протиборства з КНР [7; 8].

У щорічній доповіді Міноборони США «Військова міць Китайської Народної Республіки», представленій американським законодавцям наприкінці травня 2007 р., представлено оцінки військового потенціалу КНР, розглянуто усі напрямки модернізації її збройних сил, і зазначено, що в Піднебесній створені спеціальні підрозділи з превентивного нанесенню ударів по об'єктах кіберпростору ймовірних супротивників. Керівництво Пентагона переконано, що в цей час протистояння між Вашингтоном і Пекіном у кіберпросторі загострюється, а Китай хоче зайняти провідні позиції у світовому інформаційному просторі, посунувши Америку з позицій лідера у віртуальному світі. Причому тільки КНР насмілюється відкрито заявляти про свої наміри атакувати комп'ютери заокеанських федеральних відомств. В аналітичному дослідженні також розглянуто можливість військового втручання США за умови розвитку негативних сценаріїв політичної ситуації у регіоні за участю Китаю (наприклад, поглиблення проблеми Тайваню, Тибету та територій Південно–Китайського моря) [7].

Заяви ж китайських офіційних осіб високого рангу свідчать, що дії Сполучених Штатів протягом останнього десятиліття призвели до зростання побоювань, що США під приводом захисту прав людини та інших загальнолюдських цінностей можуть приховано або відкрито втручатися в будь–який етнічний конфлікт на території Китаю, наприклад, пов'язаний з мешканцями Тибету або з уйгурами, що сповідають іслам. Китайські лідери усвідомлюють, що державі буде складно конкурувати зі США у темпах та масштабах нарощування військової потуги, тому вони прагнуть здійснювати програми модернізації

оборонного потенціалу з врахуванням пріоритету окремих напрямків, що дозволить насамперед запобігти інтервенції переважаючих сил США.

Як зазначає У. Белло, виконавчий директор науково–аналітичної та інформаційної програми «Focus on the Global South» Бангкокського університету, головну стурбованість Пентагону викликає Пекін як потенційний конкурент і наддержава. Серед п'ятьох головних сценаріїв в аналітичному дослідженні «Азія 2025» виділяються: 1) сценарій з нестабільним Китаєм, де авантюристична зовнішня політика стане спробою активізувати націоналістичні настрої для відродження ідей державності, підірваних економічним занепадом і викликаних зростаючим невдоволенням у містах і сільських районах; 2) сценарій, в якому з провалом китайського вторгнення в Південно–Східну Азію внаслідок військового втручання США починається новий виток китайської політики, додатковий поштовх якій може дати військовий переворот, що змусить Китай почати експансію, спрямовану на захоплення енергетичних об'єктів Сибіру, Далекого Сходу Росії й Казахстану, яка закінчиться ядерним протистоянням між Росією та Китаєм; 3) сценарій, в якому передбачається посилення домінуючої ролі Китаю в континентальній Азії, досягнення гегемонії в Південно–Східній Азії, фактично встановлення протекторату в Центральній Азії й масштабне економічне вторгнення в Росію на її Далекий Схід й у Сибір; 4) сценарій континентальної консолідації доповнюється стратегією, спрямованою на послаблення панування США і Японії на морі, що передбачає проникнення якнайдалі у води Південно–Китайського Моря й у Південно–Східній Азії, підпорядкування собі слабкої Індії, нейтралізація об'єднаної Кореї, ізоляція Японії й фактичний контроль над Тайванем; 5) сенарій, що передбачає використання комплексу різноманітних і складних заходів, що включають військову загрозу, спланованні воєнні дії й опортуністична дипломатія, за допомогою яких Китай зможе домогтися визнання Японією своєї стратегічної переваги й покласти кінець військовим альянсам США та їхній присутності в Азії (кінцевим підсумком стане Азія, де буде домінувати Китай – не шляхом завоювань, а в основному в традиціях доколоніальної системи сюзеренітету над підвладними державами – системи, названої в документі єдиною позитивною історичною моделлю Китаю).

Слід зазначити, що у кожному з п'яти можливих сценаріїв, розглянутих у дослідженні, одним з незмінних ключових чинників геополітичних змін є поява на міжнародній арені сильного Китаю, що несе в собі загрозу нестійкості й становить постійну небезпеку в якості суперник. Іншим чиннико є посилення Індії як регіонального лідера, що може стати потенційним партнером Сполучених Штатів на противагу Китаю. Можлива роль Індії як партнера могла б спонукати Сполучені Штати переглянути свою політику в сфері нерозповсюдження ядерної зброї, оскільки деякі з країн, які володіють такою зброєю, могли б зробити свій внесок в американську національну безпеку. Тому перед Департаментом Оборони США постають кілька ключових завдань: необхідність переміщення центру стратегічного планування й розвитку військових ресурсів з Європи до Азії, значне посилення військової присутності США в регіоні, де, на відміну від Європи, немає достатньої кількості баз, розвинутої інфраструктури, а територія значна за своїми розмірами.

Планувати війну з Китаєм у Пентагоні ще не почали, але одним зі сценаріїв, що реально розглядається військовим керівництвом США у рамках аналітичного документа Департаменту Оборони «Азія 2025» – воєнні дії, під час яких США завдадуть удар по «авантюрному курсу» Китаю, спрямованому на здобуття контролю над більшою частиною морської акваторії Філіппін і вторгнення в охоплену повстаннями Індонезію. На думку аналітиків Пентагону цей варіант міг би стати найбільш ймовірним сценарієм – і самим складним для Вашингтона, тому що він припускає, що Сполученим Штатам доведеться

протистояти супротивникові, який проводить непередбачувану політику, що не дозволяє військовим робити відповідні кроки і не дає Вашингтону явних переваг.

В інформаційному протиборстві Китай активно використовує методи «м'якої сили», що дозволяє їм ефективно протидіяти інформаційним атакам з боку США і вести наступальні дії [9]. До 1980–х рр. Китай широко не використав ці методи протиборства, дотримуючись переважно оборонної стратегії у забезпеченні національної інформаційної безпеки. Перші системні дослідження в сфері інформаційного протиборства в Китаї відносяться до середини 1980–х рр., коли науково–дослідницькі організації Народно–визвольної армії Китаю (НВАК) і Комітету з оборонної науки, техніки й оборонної промисловості (КОНТОП) почали проводити систематичні зустрічі, симпозіуми, конференції й публікувати матеріали з проблем інформаційно–психологічного протиборства [9; 10]. Китайські експерти, як і західні дослідники, вважають, що одним з основних принципів інформаційного протиборства є інформаційне домінування, яке розглядається як можливість захистити власні інформаційні системи і зруйнувати інформаційні структури супротивника [6].

Незважаючи на відсутність загальноприйнятого офіційного визначення поняття «інформаційна війна», китайські військові експерти вже давно оперують ним і тлумачать його у вузькому і широкому сенсах: у вузькому – як польову інформаційну війну, тобто бойові дії в сфері управління військами, які передбачають активне використання засобів розвідки, методи введення супротивника в оману й оперативного маскування, психологічні операції, нанесення ударів по всій інформаційній інфраструктурі супротивника, включаючи особовий склад, а також дії щодо захисту своїх систем від аналогічних дій супротивника; у широкому – як великомасштабні бойові дії з перевагою інформаційної складової, які передбачають застосування спеціально призначених для її ведення військових формувань, оснащених високоточними озброєннями (тобто застосування комп'ютерних вірусів, здатних руйнувати програмне забезпечення технічних засобів органів бойового управління і зв'язку, ініціювання збоїв у системах управління і наведення високоточної зброї з метою значного зменшення бойового потенціалу супротивника тощо). Війна із широким використанням високоточних озброєнь вимагає істотного збільшення швидкості отримання розвідданих, часу попередження про удари супротивника, поліпшення взаємодії командирів усіх щаблів, підвищення маневреності військ, а відтак, і ефективності усіх видів інформаційного забезпечення.

Сьогодні в Китаї точиться жвава наукова дискусія й про зміст інформаційно–психологічних операцій у сучасній війні. Перша група дослідників визначає психологічні операції як сукупність різних методів, що впливають на ідеологічну стійкість супротивника, його волю й поведінку. Ціль інформаційно–психологічних операцій в цьому випадку полягає в тому, щоб перемогти з мінімальними втратами. Досягнути цієї мети можливо тільки в умовах сприятливої військово–політичної ситуації, забезпечивши психологічну перевагу. Науковий колектив академії сухопутних військ НВАК трактує психологічну війну як пропаганду, засновану на реальній можливості використання матеріальної сили. При цьому для впливу на супротивника активно використовуються політичні, економічні, наукові, військові, дипломатичні, ідеологічні й культурні засоби тиску. На думку вчених, сучасна психологічна війна полягає насамперед у зіткненні цивілізацій, східної й західної культури. Іншими словами, наддержави, використовуючи свою військову потужність, прагнуть нав'язати іншим народам свою систему цінностей.

Друга група дослідників вважає теорію психологічної війни наукою на межі між психологією та військовою стратегією. На їхню думку, така війна має як психологічну ос-

нову, так й ідеологічну надбудову. Психологічна основа є постійним поняттям, у той час як ідеологічна надбудова здебільшого піддається змінам. Стратегія ведення психологічної війни – це втілення спрямованості національної й військової стратегій. При цьому фахівці з інформаційно–психологічних операцій НОАК визначають психологічну війну як багаторівневу діяльність на стратегічному, оперативному й тактичному рівнях. Головну мету психологічного впливу вони бачать у забезпеченні високого морально–психологічного потенціалу нації, трактуючи її через стан суспільної свідомості, культурні традиції, ритм економічного життя країни й бойовий дух армії. Китайські експерти при цьому наголошують на системі людських цінностей, що лежить в основі мотивації поведінки людини. На їхню думку, найбільш важливі стратегічні цілі психологічної війни можуть бути досягнуті шляхом руйнування державної ідеології через розмивання системи цінностей, прийнятої в культурі того чи іншого народу.

Отже більшість китайських наукових досліджень у сфері інформаційно–психологічних операцій присвячена проблемі забезпечення інформаційно–психологічної безпеки держави. У них стверджується, що КНР не тільки може, а й повинна перехопити ініціативу в сфері психологічної війни, тому що інформаційно–психологічна безпека є однієї з найважливіших складових державної безпеки. Психологічна війна не вимагає значних фінансових витрат, має відносно гуманний характер, але при цьому виступає надзвичайно ефективним засобом протиборства. Китайські вчені переконані, що Інтернет надає сьогодні нові, необмежені можливості й для ведення пропаганди. Уміло підготовлена й спрямована мережева атака може зруйнувати соціальне, політичне та економічне життя країни, перетворивши його на хаос, що негативно позначиться на морально–психологічному стані населення та армії. Саме це, з погляду китайських експертів, і доводить необхідність подальшого удосконалення способів ведення інформаційних операцій.

Характерною рисою китайської стратегії інформаційного протиборства є поєднання давньокитайських стратегій (Сунь–Цзи, Лао–Цзи), досвіду радянських розробок в цій сфері (інформаційну концепцію начальника Генерального штабу Збройних Сил СРСР маршала Н.В. Огаркова) і американських (з досвіду участі США в збройних конфліктах кінця XX – початку XXI століття) технологій ведення інформаційної війни. 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 [7]. У цілому вся доктрина ведення інформаційно–психологічних операцій у Китаї заснована на філософському навчанні Лао–Цзи (VI століття до н.е.), але значно більшого 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; зруйнувати її значно легше. Взяти у полон армію супротивника краще, ніж її знищити... Одержати сотню перемог у боях – це не межа мистецтва. Скорити супротивника без бою – от вершина мистецтва». Автор пояснює важливість володіння інформацією й прийомами дезінформації супротивника для маніпулювання його станом і діями [11].

Сунь–Цзи виділив основні стратегеми інформаційного протиборства, а саме: руйнуйте все добре, що є у країні вашого супротивника; втягуйте видатних діячів супротивника в злочинні заходи; підривайте репутацію керівництва супротивника й виставляйте його в найгіршому вигляді на осуд громадськості; використовуйте з цією метою співпрацю із самими підлими й мерзенними людьми; розпалюйте сварки й зіткнення серед громадян ворожої вам країни; заважайте всіма способами роботі уряду; перешкоджайте всіма спо-

собами нормальному оснащенню ворожих військ і підтримці в них порядку; знищуйте волю воїнів супротивника піснями й музикою; робіть все можливе, щоб знецінити традиції ваших ворогів і підірвати їхню віру у своїх богів; будьте щедрими на пропозиції й подарунки для покупки інформації й спільників; домагайтеся довіри супротивника й навіюйте йому спокій; завжди зберігайте упевнений вид, не допускай прорахунків у своїй позиції; зберігайте свої сили, уникаючи відкритого протистояння тощо [11].

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.

Подальший розвиток воєнного мистецтва незмінно супроводжувався удосконаленням форм морального впливу на супротивника. До II ст. н.е. відносять появу самостійної теми пропаганди – проголошення справедливого чи несправедливого характеру війни. Прагненням підірвати бойовий дух воїнів ворога можна пояснити й звичай, коли одна з воюючих сторін виступає зі звинуваченням на адресу свого суперника і закликає своїх союзників приєднатись до «боротьби за справедливість». Здавна в Китаї вважали обман (дезінформацію) та пряме маніпулювання поглядами супротивника на реальність одним із найбільш надійних засобів примусу вживати заходів у бажаному напрямі. Як зазначав у своєму трактаті Сунь Цзи, «війна – це гра обману. Тому прикидайся немічним, коли сильний; прикидайся млявим, коли готовий завдати удару; здавайся далеким, коли насправді знаходишся поруч, і навпаки. Коли ворог жадає наживи, підмани його наживкою; коли він у безладді, нападі і здобудь перемогу над ним; коли він хвалиться значними силами, будь подвійно готовий діяти проти нього; коли він страшний, обходь його; якщо він податливий до гніву, провокуй його; якщо він боязкий і обережний, заохочуй його марнославство; якщо сили його свіжі, виснажуй їх; якщо він єдиний, розділи його; атакуй його, коли він найменше готовий; дій, коли він найменше тебе очікує. У цьому полягають тонкощі командування стратега, що неможливо заздалегідь передати чітко визначеними правилами, готовими для негайного застосування».

Стратегеми, запропоновані Сунь Цзи, активно використовувалися, наприклад, під час громадянської війни між Гоміданом і Комуністичною партією (1927–1950 рр.). Обидві сторони успішно здійснювали психологічні операції, демонструючи глибокі знання особливостей своїх супротивників, їхні сильні і слабкі сторони, використовуючи наявні можливості для контролю за потоками інформації. КПК і НВАК, зокрема, намагалися переконати воюючих проти них гоміньданівців, що їхні вороги дурні, боягузи, слабкі, відступатимуть при першому ж натиску. Крім того, особливий наголос робився на складному поєднанні пропаганди і чуток, щоб спонукати лідерів націоналістів розділити армійські підрозділи і направити їх для з'єднання в небажаному (і навить помилковому, з погляду військової тактики) для них напрямі.

Після утворення КНР (1949 р.) у всіх конфліктах, у яких брала участь НВАК, психологічні операції перетворилися на постійну складову її стратегії. Так, під час Корейської війни (1950–1953 рр.) політичні органи НВАК постійно прагнули за допомогою агіта-

ційно–пропагандистських матеріалів подати її як агресію американського імперіалізму, дискредитувати військово–політичне керівництво США і Південної Кореї, вихваляти бойову потугу і військові успіхи північнокорейських і китайських військ, демонструвати випадки расової дискримінації в армії США.

Особливу увагу китайські підрозділи спецпропаганди приділяли закликам здаватися у полон. Аргументи, що наводилися в розповсюджуваних ними листівках, мали посіяти страх у солдатів супротивника перед невизначеністю того, що їх чекає «на тому боці», підводили до думки про те, що доцільно перебігти до ворога в ім'я кінцевої мети – повернутися додому живим. Причому багато матеріалів копіювали композиційні і стилістичні особливості американських газет, нерідко повідомлення підтверджувалися посиланнями на назви друкованих ЗМІ США з указівкою дати їхнього випуску. Листівки, так би мовити, «сентиментального характеру» мали на меті викликати тугу за батьківщиною, занепокоєння за власне життя. Серед них виділялася серія різдвяних листівок–поздоровлень, виконаних у стилі традиційних американських листівок з написаним на звороті побажанням щастя в новому році. Китай також продемонстрував, що він здатний успішно вести «чорну пропаганду». Яскравим прикладом цього є зчинений під час Корейської війни галас про застосування США біологічної зброї, щоб створити позитивне сприяняття дій КНР і КНДР міжнародною громадськістю. Водночас відносна ізольованість Китаю від Заходу до початку 1970–х рр. не давала можливості широко використовувати дезінформацію в повсякденних міждержавних відносинах. Під час психологічної війни проти Москви і Вашингтона в 1960–1970–х рр. пропаганда стала одним з головних елементів національної стратегії, результатом якої було прийняття в 1972 р. КНР до складу ООН і встановлення дипломатичних відносин між Пекіном і Вашингтоном.

Окрім власних розробок, китайські військові експерти пильну увагу приділяють зарубіжнмому досвіду у сфері ведення інформаційної війни. Як і західні військові фахівці, вони вважають, що дослідження збройних конфліктів останнього часу надає можливість виділити кілька характерних рис, притаманних сучасним інформаційнім війнам: по–перше, «прозорістъ поля бою» (наприклад, оператор комп'ютерних систем може здійснювати безупинний контроль за ситуацією, спостерігати відображуване на дисплеї розташування своїх військ і військ супротивника, 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 супротивника, робить розрахунки для їх розподілу за засобами враження, визначає кількість необхідних боєприпасів тощо); по–третє, ведення бойових дій у реальному масштабі часу, тобто негайне реагування на зміну бойової обстановки.

За аналогією з американськими аналітичними розробками в сфері інформаційної безпеки, представлених у документі «Спільне бачення 2020» [12], китайські дослідники виділяють шість основних структурних елементи інформаційних операцій: фізичне знищення – використання всіх засобів збройної боротьби для знищення системи керування супротивника; радіоелектронна війна – застосування електронних засобів придушення або електромагнітної зброї для нанесення ударів по системах збору інформації й розвідувальних даних; мережева війна – використання комп'ютерних технологій та телекомунікаційного обладнання для завдання шкоди комп'ютерним системам і мережам супротивника; дезінформація, маніпулювання – заходи, спрямовані на введення в оману командування супротивника з метою впливу на систему прийняття тактичних і стратегічних рішень; оперативне маскування – використання всіх засобів для збереження таєм-

ності й недопущення збору супротивником розвідувальних даних про свої дії; психологічна війна – використання засобів масової інформації і комунікації задля здійснення пропаганди з метою впливу на моральний стан військ супротивника, їх емоційний стан, систему психологічного сприйняття реальності тощо.

Використання американських досліджень в сфері інформаційного протиборства обумовлене необхідністю здійснювати порівняльний аналіз стратегій ведення інформаційних війн між двома потенційними супротивниками майбутнього глобального протистояння та вироблення більш ефективної і досконалої стратегії протиборства у міжнародних відносинах. Китай також пришвидчує скорочення інформаційно–технологічного відриву від Заходу (в першу чергу, США) і намагається протиставити американській військово–інформаційній міцці не меньш ефективну тактику ведення сучасних війн з широким застосуванням новітніх інформаційних озброєнь. Китайський військовий експерт Фу Яньсун в інтрев'ю агентству Сіньхуа зазначає, що політичне і військове керівництво особливу увагу приділяється проблемі інформатизації НВАК, оскільки основною специфікою війн XXI ст. стане масштабне використання досягнень інформаційно–технологічного розвитку, тому необхідно інтенсифікувати процеси інформатизація китайської армії. НВАК ставить за мету у XXI ст. повністю інформатизувати армію, зокрема, військові системи й озброєння, а також інформатизувати інфраструктурну базу.

Сьогодні в Китаї вже сформована державна система ведення інформаційного протиборства, що дозволяє застосовувати інформаційні та психологічні технології впливу на супротивника. Основними державними структурами, що відповідають за реалізацію стратегій інформаційного протиборства є Дослідницьке бюро при Держраді КНР і Системно–аналітичний центр Міністерства державної безпеки. Важливим чинником здійснення інформаційних операцій з боку Китаю є також широке використання спецслужбами цієї країни, а також (що показово) кримінальними організаціями мережевих принципів організації, про що свідчать часті офіційні заяви європейських та американських урядовців про постійні хакерські атаки на комп'ютерні системи і мережі з боку КНР. З іншого боку, відсутність християнського підґрунтя у китайській культурі значно спрощує здійснення інформаційних операцій, фактично знімаючи проблеми моральності.

Найбільш яскравими прикладами успішного інформаційного протиборства зі США є: інформаційна кампанія спецслужб Китаю після студентських заворушень на площі Тяньаньмєнь 1989 р., інформаційного протиборства у фінансовій сфері під час азіатської кризи 1997–1998 р., успіх китайських спецслужб у встановленні контролю над найбільшими банками азіатського регіону, вихід з гострого геополітичного конфлікту на початку квітня 2001 р., спровокованого вимушеною посадкою американського літака на китайському острові Хайнань, атаки на сервери Google тощо. Значних успіхів китайські спецслужби досягли й на території самих США, використовуючи численність китайської діаспори в Америці, особливо на Тихоокеанському узбережжі, де китайська розвідка має настільки міцні позиції, що американські спецслужби не в змозі повністю контролювати китайську активність у таких містах як Сіетл, Лос–Анджелес, Сан–Франциско, Х'юстон. Своєрідним попередженням США стало обрання етнічного китайця Ло Цзяхуея губернатором штату Вашингтон (столиця штату Сіетл є основними воротами китайської еміграції в Америку) [12].

Китайська стратегія інформаційного протиборства найбільш ефективною виявилася у фінансовій сфері. КНР одержує інформацію від діаспор країн тихоокеанського регіону й розвідки. Здійснюється тотальний контроль за ЗМІ країн тихоокеанського регіону. Значна кількість газет, теле– і радіоканалів придбані агентами й офіцерами китайської

розвідки. За допомогою контрольованих ЗМІ здійснюються активні комплексні інформаційно–психологічні операції. Феноменальним успіхом китайських спецслужб є встановлення контролю над найбільшими банками азіатського регіону. Китайцям вдалося повністю «переграти» американців під час інформаційного протиборства у фінансовій сфері у період азіатської кризи 1997–1998 рр. Китайська перемога показала, що в 1998 році склалася нова світова фінансова ситуація, ситуація «двовладдя». На початку квітня 2001 р. почався другий етап інформаційної війни за владу у фінансовому світі між США й Китаєм. Натиск юаню, як власної в рамках АТЕС (незалежної від долара США) міри вартості й розрахункової одиниці в торгівлі країн АТР стане потужним викликом для США. Китай, ніколи не декларувавши свій контрнаступ проти американської політики глобалізації, вже тривалий час «наступає» на інтереси США. Методами «інформаційної народної війни» в економіці й через діаспору Китай тіснить Америку в тихоокеанській зоні, здійснює світову товарну експансію, не втрачаючи при цьому внутрішню національно–культурну самобутність.

Запровадження Китаєм вільної торгівлі і поширення ідеї про те, що це стане джерелом для прямих іноземних інвестицій, підписання договору про вільну торгівлю з Південно–Східною Азією, налагодження тісного економічного партнерства з окремими державами Південно–Східної Азії, збільшення у 2006–2007 рр. загального торговельного обігу між Південно–Східною Азією та Китаєм, який врешті може перевищити торговий обіг між Південно–Східною Азією та США, чи Японією суттєво зміцнили позиції КНР на міжнародній арені. Незважаючи на те, що Китай поки не є великим іноземним інвестором, прямі іноземні інвестиції Китаю зростають набагато швидше, ніж прогнозували експерти; Китай став найбільшим джерелом прямих іноземних інвестицій, що надійшли до Камбоджі у 2004 р. Відтік населення з Китаю трансформує демографічну картину Південно–Східної Азії, від Бірми до В'єтнаму, де вчорашні Китайські емігранти сьогодні керують бізнесом, а відтак, й суспільством.

Несподівана для американців подія на узбережжі Китаю перетворилася на гострий інформаційно–геополітичний конфлікт. Вимушена посадка американського літака–розвідника на китайський острів Хайнань стала своєрідним індикатором для системних політичних аналітиків. Китайці змусили американців вибачитися. Показовими стали також дії КНР після студентських хвилювань на площі Тяньаньмень в 1989 р., коли через ЗМІ до широкої громадськості була доведена інформація, що в Пекіні, Шанхаї й деяких інших великих містах діяли невеликі групи екстремістів і кримінальних угруповань. Лідери Китаю переконали народ у тому, що безладдя інспірувалися США. Китайці тоді здобули першу перемогу в інформаційній війні проти США. Найбільшу роль у перемозі відіграв ефективний інформаційний вплив на китайську діаспору в США та Західній Європі. Водночас, як зазначають есперти, китайський «м'який вплив» може мати негативні наслідки для демократизації, для антикорупційної діяльності та для ефективного управління у Південно–Східній Азії, про що свідчить участь китайських компаній в екологічно шкідливих проектах у на території країн Південно–Східної Азії, підтримка авторитарного режиму в Камбоджі та Бірмі на противагу американським спробам демократизувати ці країни, участь у сумнівних комерційних проектах тощо.

Таким чином, політика інформаційної безпеки визначає пріоритетними напрямами діяльності держави розробку національних стратегій, які поєднують оборонні і наступальні доктрини для забезпечення національних інтересів і захисту внутрішнього інформаційного середовища та інформаційної інфраструктури, подолання асиметричності

інформаційного розвитку щодо інформаційно розвинених країн як потенційних супротивників в інформаційному протистоянні.

Література

1. Internet Statistics 2010 [Електронний ресурс] / China Internet Network Information Center. – Режим доступу: http://www.cnnic.net.cn/en/index/0O/index.htm
2. Госрегулирование Интернет в Китае [Електронний ресурс]. – Режим доступу: http://www.agentura.ru/equipment/psih/info/china.
3. Базаров Р. Все под контролем (часть 1) [Електронний ресурс]/ Р. Базаров // Журнал «CIO». – 2006. – №9. – Режим доступу: http://www.cio–world.ru/offline/2006/52/286660.
4. Китай: угрозы, риски, вызовы развитию / Под ред. В. Михеева. – М.: Московский центр Карнеги, 2005. – 647 с.
5. Китай приступил к реализации проекта по созданию «Великой стены» для защиты информационных сетей [Електронний ресурс]. – Режим доступу: http://www.rian.ru/world/20011213/34314.html.
6. Ткачева Н.В. Информационные стратегии стран Восточной Азии в условиях рыночных реформ / Н.В.Ткачева. – М.: РИП–холдинг, 2003. – 152 с.
7. Хуан Цинь. Безпековий стан інформаційного простору Китаю// Актуальні проблеми міжнародних відносин: Збірник наукових праць. – 2006. – Випуск 64. – Частина І. – С. 159–162.
8. Kurlantzick J. China's Charm: Implications of Chinese Soft Power [Електронний ресурс]/ J. Kurlantzick. – Режим доступу: http://www.CarnegieEndowment.org/pubs for these and other publications.
9. Toshi Yoshihara. Chinese Information Warfare: A Phantom Menace or Emerging Threat? [Електронний ресурс] / Toshi Yoshihara. – Режим доступу: http://www.pirp.harvard.edu.
10. Димлевич Н. Информационные войны в киберпространстве – Китай и Индия [Електронний ресурс] / Н. Димлевич. – Режим доступу: http://www.truenet.info/analitika/informatsionnye–voyny–v–kiberprostranstve–kitay–i–indiya.html.
11. Сунь–Цзы. Искусство войны. Стратегия и тактика победителя / Сунь–Цзы. – М.: Эксмо, 2003 – 800 с.
12. Joint Vision 2020. [Електронний ресурс] – Режим доступу: http://www.ndu.edu/ndu/nwc/AY00/5602SYL/Topic10.html.
13. Панарин И. Технология информационной войны / И.Панарин. – М.: КСП+, 2003. – 320 с.