МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
ДЕРЖАВНА УСТАНОВА «ПІВДЕННОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ІМ. К.Д. УШИНСЬКОГО»

На правах рукопису

МАРУНЧЕНКО Олександр Петрович

УДК 323.2: 327

ІНФОРМАЦІЙНА ВІЙНА В СУЧАСНОМУ ПОЛІТИЧНОМУ ПРОСТОРІ

23.00.02 - політичні інститути та процеси

Д И С Е Р Т А Ц І Я

на здобуття наукового ступеня кандидата політичних наук

Науковий керівник –
доктор політичних наук,
професор
Сіленко Алла Олексіївна

Одеса – 2012

ЗМІСТ

ВСТУП

Актуальність дослідження. Однією з головних рис сучасності є широкомасштабне використання інформаційно-комунікаційних технологій (ІКТ), які стали уособленням нової стадії науково-технічного та соціально-економічного прогресу людства. Проте вони ж породили безліч проблем і загроз, про які раніше ніхто не відав. Однією з них є інформаційна війна, яка стає все більш важливою темою в дослідженні національної безпеки.

Інформаційна війна пронизує нині всі форми боротьби, починаючи від дипломатичної й економічної та закінчуючи збройною боротьбою, розвиваючись разом з тим, як самостійна сфера діяльності. Бурхливий розвиток інформаційних технологій призвів до переміщення конфліктів із традиційного фізичного простору в принципово інший - кіберпростір. На сьогодні повсякденні політичні практики дають безліч прикладів ведення найрізноманітніших інформаційних війн як у демократичних державах, так і в перехідних політичних системах.

Україна опиняється перед загрозою широкомасштабних акцій інформаційної війни, спрямованих на її інформаційні ресурси, систему прийняття рішень органами державної влади, а також на масову свідомість населення. І дійсно, останнім часом у світовому інформаційному просторі значно збільшилася кількість негативної інформації про Україну, яка зачіпає різноманітні аспекти політичного, економічного, соціально-гуманітарного життя українського суспільства. Ця інформація є невипадковою, а цілеспрямованою, створеною і поданою за певним сценарієм. Мета такої інформації - маніпулювання громадською думкою українців.

Характерною особливістю українського інформаційного простору стала наявність і внутрішньополітичних інформаційних війн:

інформаційні війни між олігархами, між владою й опозицією, а також інсценовані протистоянням різних сегментів влади.

Таким чином, дослідження сутності інформаційних війн як зовнішніх, так і внутрішніх, їхніх основних методів, засобів, закономірностей стає одним із найактуальніших напрямків наукових досліджень вітчизняної політичної науки, так як це необхідно для ефективної протидії загрозам інформаційно-психологічної безпеки особистості, суспільства й держави та забезпечення безпеки України в цілому.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження виконане в рамках наукової теми «Соціально-політичні та правові аспекти розвитку інформаційного суспільства в Україні» (2009-2014 рр..), яка здійснюється кафедрою політології Одеської національної академії зв'язку ім. О.С. Попова, одним із виконавців якої є дисертант.

Мета дисертаційного дослідження полягає в тому, щоб дослідити роль інформаційної війни в політичному житті сучасного суспільства.

Для досягнення поставленої мети визначені наступні **завдання**:

- дослідити ступінь розробленості проблем інформаційної війни вітчизняними та закордонними вченими;

- розглянути основні концепції та підходи до розуміння природи процесів інформаційної війни;

- проаналізувати поняття, сутність, структуру інформаційної війни;

- порівняти поняття «інформаційна війна» й «інформаційно-психологічна війна»;

- дослідити досвід закордонних країн у розвитку технологій політичної війни;

- розглянути застосування електронного шпигунства з політичною метою;

- показати роль ЗМІ в інформаційній війні;

- виявити причини та наслідки інформаційних війн у сучасній українській політиці;

- уточнити механізми формування позитивного іміджу України за кордоном як протидію інформаційній зброї, що застосовується ззовні.

Об'єктом дослідження є відкриті форми протистояння в сфері політичної комунікації як процесу інформаційного обміну між політичними акторами.

Предметом дослідження є інформаційна війна в сучасному політичному просторі.

Методи дослідження. Структурно-функціональний підхід був корисний при розгляді системи інформаційної війни як певної цілісності, системи, що характеризується складною структурою, кожен елемент якої має певне призначення і виконує специфічні функції (ролі), спрямовані на задоволення відповідних потреб системи.

Системний підхід дозволив розглянути інформаційну війну як динамічний процес, який відбувається в складній системі, здатній до самоорганізації. В ході війни ця система або змінюється, або зникає, і замість неї виникає нова. Застосування системного підходу зумовлене тим, що інформаційні війни відбуваються в складних соціально-політичних системах із великою кількістю елементів, зв'язки між якими мають не детермінований, а ймовірнісний характер.

Порівняльний підхід застосовувався для співставлення однотипних політичних явищ, які розвиваються в різних країнах і в різних культурних середовищах. Результати порівнянь дозволили визначити тенденції інформаційних процесів в розглянутих країнах.

Застосування нормативно-ціннісного підходу дозволило з'ясувати значення інформаційних війн для суспільства й особистості, їх оцінку з точки зору загального блага, справедливості, свободи та інших цінностей. Даний підхід вимагає відштовхуватися від належного і бажаного, від

етичних цінностей і норм та відповідно до них будувати поведінку в інформаційному просторі.

Психологічний підхід був орієнтований на вивчення суб'єктивних механізмів політичної поведінки, індивідуальних якостей, рис характеру, а також типових механізмів психологічних мотивацій в інформаційному суспільстві.

Наукова новизна полягає в тому, що вперше проблеми інформаційної війни розглядаються комплексно на рівні дисертаційної роботи. В ході проведеного дослідження були отримані результати, які мають наукову новизну.

Вперше:

обґрунтовано, що переміщення конфліктів із традиційного фізичного простору в кіберпростір, що спостерігається зараз, збільшує ризик виникнення локальних збройних конфліктів: технології інформаційної війни є привабливими саме через їхню відносну дешевизну, доступність та ефективність, а, отже, інтенсивність їх використання в політичній боротьбі буде тільки наростати;

з'ясовані політичні чинники розгортання інформаційної війни всередині країни: недосконаліть процесу державного управління, яка проявляється, перш за все, в кризі ідей щодо модернізації внутрішньої і зовнішньої політики; прагматизм політичних партій, який, прийшовши на зміну ідеології, став причиною розмивання відмінностей між ними. Результатом цього стає абсентеїзм, коли електорат виявляє до виборів байдужість і відсутність інтересу. А основним завданням державної політики стає не прогресивний розвиток, а підтримання існуючого порядку будь-якими засобами;

виявлено технічні фактори сучасного розвитку інформаційної війни: інформатизація основних сфер діяльності більшості держав; стрімке формування глобальної інформаційної інфраструктури; досягнення у

розвитку інформаційних технологій впливу на свідомість, волю і почуття людей; активний розвиток програмно-технічних засобів нанесення шкоди комп'ютерним і телекомунікаційним системам; недостатній рівень розвитку засобів і методів забезпечення захисту національних інформаційних просторів, свідомості населення;

доведено, що інформаційна війна як технологія політичної боротьби крім традиційного використання в геополітиці з метою ослаблення позицій країн-конкурентів, підриву їхніх національно-державних устоїв, порушення системи державного управління шляхом інформаційного впливу на політичну, дипломатичну, економічну і соціальну сфери життя суспільства, проведення психологічних операцій, підривних та інших деморалізуючих пропагандистських акцій, все частіше застосовується у внутрішній політиці держави, у відносинах між державою і суспільством, суб'єктами політичного простору;

вводиться у науковий обіг поняття «глобально-державна інформаційна війна», під яким пропонується розуміти ведення інформаційної війни одночасно на двох рівнях: глобальному (зовнішньому) та державному (внутрішньому). Прикладом такої війни може служити період «помаранчевої революції», коли на інформаційний простір України чинився потужний тиск як ззовні (з боку підтримуючих українську опозицію держав), так і зсередини (з боку самої опозиції).

вдосконалено:

визначення інформаційної війни. Вводиться в науковий обіг поняття «політична інформаційна війна», під яким пропонується розуміти сукупність взаємовідносин між суб'єктами політичного простору, в рамках яких дані суб'єкти з метою вирішення своїх політичних завдань (розв'язання суперечностей з приводу влади і здійснення політичного управління в інформаційно-психологічному просторі) активно впливають на інформаційну сферу один одного і протидіють аналогічній діяльності

протилежної сторони за допомогою програмно-технічних, радіоелектронних та інформаційно-психологічних засобів. Таким чином, на відміну від багатьох наявних визначень поняття інформаційної війни трактується не тільки через засоби і методи, а й через характер завдань і взаємин учасників - суб'єктів політичного простору.

отримало подальший розвиток:

визначення співвідношення понять «інформаційна кампанія» і «інформаційна війна». Встановлено, що інформаційна війна є найбільш поширеним типом інформаційної кампанії. Під інформаційною кампанією розуміється заздалегідь спланований комплекс взаємопов'язаних комунікаційних дій, спеціально розроблених для забезпечення конкретних цілей комунікатора шляхом цілеспрямованого впливу на громадську думку і позиції контрагента. Інформаційна війна - це найбільш гостра форма конфронтації в інформаційному просторі.

Апробація результатів дисертаційного дослідження. Дисертація виконана й обговорена на кафедрі політології Одеської національної академії зв'язку ім. О.С. Попова. Основні положення, висновки та пропозиції дисертаційного дослідження булі апробовані на Міжнародній науково-практичній інтердисциплінарній конференції «Етнос, мова та культура: минуле, сьогодення, майбутнє» (м. Рівне, 18-19 березня 2011 р.), VIII-ій Всеукраїнській науковій конференції студентів і молодих учених «Молодь: освіта, наука, духовність» (м. Київ, 13 квітня 2011 р.), III-ій Міжнародній науково-практичній конференції «Роль та місце ОВС у розбудові демократичної правової держави» (м. Одеса, 21 квітня 2011 р.), наукових семінарах кафедри політології Одеської національної академії зв'язку ім. О.С. Попова та кафедри політичних наук Державної установи «Південноукраїнський національний педагогічний університет ім. К.Д. Ушинського».

Публікації. За результатами дисертаційного дослідження опубліковано 5 наукових публікацій у спеціальних виданнях з політології.

Структура дисертації зумовлена характером проблематики, постановкою мети і завдань дослідження. Дисертація складається зі вступу, трьох розділів, перший і третій з яких містять по два підрозділи, другий - три підрозділи і висновків. Загальний обсяг дисертації становить 179 сторінок (без списку використаних джерел). Список використаних джерел містить 264 найменування (29 сторінок).

РОЗДІЛ 1
ІНФОРМАЦІЙНА ВІЙНА ЯК НАУКОВА КАТЕГОРІЯ

ПОЛІТИЧНОЇ НАУКИ

Даний розділ присвячений аналізу ступеня розробленості проблеми, основних теоретико-методологічних підходів до дослідження інформаційної війни як соціально-політичного феномена, уточненню понятійного апарату.

Сучасною тенденцією процесів військово-політичної конфронтації держав став перехід від відкритих силових методів до прихованих, не силових, інформаційних методів і засобів, одним із яких є інформаційна війна.

1.1. Основні концепції та підходи до розуміння природи процесів інформаційної війни

Як точно помітив відомий теоретик інформаційного суспільства Ф. Уебстер, попереднє покоління стало свідком занепаду індустріального способу ведення війн, на зміну якому поступово, але зі все зростаючим темпом, приходить той, який можна назвати інформаційним. При цьому способі ведення війни, інформаційна складова набуває набагато більшої ваги, її роль стає більш ясною, а масштаби використання - більш широкими, ніж в епоху індустріального способу ведення війн [212, с.291].

У працях С.М. Бухаріна, І. Панаріна. В. Циганова, А. Манойло, С. Расторгуєва пропонуються нові концепції та підходи до розуміння природи процесів, що відбуваються в ході інформаційної війни.

Вивченню й аналізу діяльності ЗМК і ЗМІ, їхньому місцю в соціокультурних і політичних процесах присвячені праці таких закордонних дослідників, як Т. Адорно, Н. Вінер, Г. Хербнер, Г. Лассуелл, Д. Макквейл, Ф. Уебстер, Ю. Хабермас, М. Хоркхаймер, В. Шрамм та ін.

Ролі Інтернету в політичних інформаційних війнах присвячені роботи Б. Докторова, Д.Г. Іванова, І.Л. Морозова, Д.М. Пєскова, С.Г. Туронка, О.О. Чеснакова, А.В. Чугунова, І.І. Скрипнюка, В. Юдаєва та ін.

Різні аспекти інформаційних війн розглядаються в роботах іноземних авторів - Т. Розана, Т. Стоуньєра, Ф. Вебстера, Б.І. Пружиніна, Н.В. Громико, І.В. Громико, А. Манойло, О. Петренко, С. Расторгуєва, С. Пюкке, Д. Фролова та ін. [Див.напр.: 135; 181]. У цих роботах відзначається, що виникаючі наприкінці XX - початку XXI ст. інформаційно-комунікативні технології є відображенням глобальної інформаційної революції, що наразі відбувається, в процесі якої інформація набуває статусу глобального ресурсу. Формуються інформаційно багаті та інформаційно бідні країни. Інформаційна війна як цілісна стратегія орієнтована на всі можливості й фактори уразливості, а також на використання інформації в різних конфліктах. Об'єктом уваги стають інформаційні системи, а також інформаційні технології. Дослідники виділяють характеристики інформаційної війни: стимуляція обговорення, багатоканальний вплив, орієнтація на однорідні групи, інформаційна агресія.

Неоціненним є внесок у дослідження проблематики інформаційної війни американських авторів - Д. Альбертса, Дж. Гарстку, Р. Моландера, П. Вілсона, Д. Ронфельдта, Дж. Арквіллу, Р. Кларка, Р. Нейко, Р. Шафранськи, М. Лібікі, О. Ієнсена та інших, які вважають, що в майбутньому конфлікті вирішальну роль буде грати сама інформація (точніше, знання), яка при цьому буде одночасно і зброєю, і метою, переслідуваною конфліктом. Такий тип конфлікту, за їхніми уявленнями, проходитиме у до невпізнанності змінених умовах. Передбачається, що в ході конфлікту, який принципово відрізняється від традиційного, не будуть задіяні не тільки традиційні системи озброєнь, а й такі високотехнологічні

системи як "цифрове поле бою" і т.п., що зазвичай асоціюються з веденням інформаційної війни.

Окремі аспекти проблем інформаційної війни відображені в працях українських дослідників О. Дубаса, В. Коляденка, В. Недбая, О. Маліса, Г. Почепцова та ін.

Особливо слід відзначити ряд наукових праць російського дослідника І. Панаріна з проблем інформаційної війни, зокрема, «Інформаційна війна і Росія» [162], «Інформаційна війна і дипломатія» [160], «Інформаційна війна і влада» [158], «Технологія інформаційної війни» [164], «Інформаційна війна і Третій Рим» [163], «Інформаційна війна і вибори» [159], «Інформаційна війна, PR і світова політика» [161].

Цінність книги С. Расторгуєва [185] полягає в тому, що інформаційна війна розглядається з різних сторін, аналізуються завдання, запропоновані алгоритми, стратегія й тактика інформаційної війни, в основу чого покладені досить суворі математичні обґрунтування і розвинена ним теорія структур, які самі зароджуються та руйнуються (СР-мереж).

Безперечну цінність для нашого дослідження становить монографія відомого фахівця в галузі інформаційного протиборства В. Пірумова «Інформаційне протиборство. Четвертий вимір протистояння» [172]. В. Пірумов на основі розгляду історичних аспектів зародження та розвитку інформаційного протиборства аналізує основні поняття і визначення, що дозволило автору сформулювати сучасне системне бачення термінологічної бази інформаційного протиборства. Особливу увагу В. Пірумов приділив основам, де сформульовані фактори, категорії, принципи, закони та закономірності підготовки і ведення інформаційного протиборства, а також розглянув концептуальні положення та навів короткі характеристики засобів ведення інформаційного протиборства і їхнього впливу на ефективність збройного конфлікту.

Цікавим є матеріал, присвячений розгляду історичних аспектів використання сил і засобів інформаційного протиборства в збройних конфліктах. Позитивним є те, що автор монографії розкриває зміст основних форм інформаційного протиборства: інформаційної війни, інформаційної боротьби і боротьби з інформаційною злочинністю.

Також автор розглядає правові та організаційно-технічні питання інформаційної безпеки, сутності та змісту її забезпечення, основні напрямки зміни ролі і місця інформаційного протиборства в конфліктних ситуаціях майбутнього.

Слід відмітити роботу В. Циганова і С. Бухаріна «Інформаційні війни в бізнесі та політиці. Теорія і методологія» [225], що нещодавно вийшла, і в якій розглядаються основи теорії та методології інформаційних війн і їхні практичні застосування. Автори представили систему адаптивних механізмів та їх спрощених моделей - архетипів інформаційних війн. Комбінації цих механізмів й архетипів можна використовувати для аналізу та проектування комплексних систем управління інформаційними війнами в соціально-економічних системах різної природи і масштабу - від підприємства й корпорації до держави та світового співтовариства. У роботі аналізуються архетипи та механізми інформаційних війн в умовах глобалізації. Безсумнівний науковий інтерес представляє запропонована авторами концепція інтелектуальних механізмів ведення інформаційних війн, заснованих на самоорганізації та адаптації.

З метою нашого дослідження була вивчена книга Л. Воронцової і Д. Фролова «Історія та сучасність інформаційного протиборства» [42]. Ця книга корисна тим, що автори аналізують історичні аспекти інформаційного протиборства, виявляють його основні методи та засоби, розкривають ряд закономірностей, викривають логіку становлення інформаційно-психологічних та дезінформаційних засобів і методів, що є

самостійним інструментом досягнення зовнішньополітичних завдань держави.

Безумовно, що, досліджуючи закордонний досвід ведення інформаційних війн, особливий інтерес для нас має досвід США як найбільш розвиненої інформаційної держави, що розробляє стратегію і тактику мережевих війн. Досвіду США присвячена книга В. Коровіна «Головна військова таємниця США: мережеві війни» [115]. Автор книги досліджує як США просуваються до здійснення плану зі встановлення контролю над усім світом без застосування збройних сил. В. Коровін відносить до арсеналу мережевої війни таємні змови та спецоперації, захоплення інформаційного простору і зміну суспільної свідомості, ідеологічні диверсії та "промивання мізків", підривну пропаганду й "кольорові" революції.

Розробники концепції інформаційної війни часто цитують відому тезу давньокитайського військового теоретика і полководця Сун Цзи: «Придушити супротивника, не вступаючи в сутичку з ним, є найбільша мудрість військового мистецтва». Якщо кінцева мета військового (і ширше - політичного) конфлікту - нав'язати супротивнику свою волю та встановити контроль над його економічними, технічними та іншими значущими ресурсами, навряд чи «мудро» досягати її шляхом фізичного знищення значної частини цих ресурсів. Придушення політичної волі та здатності супротивника до опору за допомогою впливу на його свідомість, інформацію про навколишній світ, безумовно, більше відповідає постулату китайського мудреця.

Як правомірно зазначає В. Разуваєв, інформаційні взаємодії, контакти, конфлікти та різні форми їх вирішення - основа розвитку суспільства. «У цьому сенсі ми завжди знаходимося в стані динамічного інформаційного середовища, яке змінюється та силу якого і фахівці не наважуються однозначно віднести до матерії або енергії. Віртуальність

знань і форм їх вираження, яка стала реальністю на основі нових технологій, не дозволяє зробити категоричний висновок. Здібність інформації впливати на сприймаючого її суб'єкта є настільки сильною, що може повністю змінити поведінку людини, суспільства або держави в необхідному напрямі» [184, с.6].

Поява концепції «мережевої» війни пов'язана з трансформацією загроз міжнародній безпеці на рубежі століть. Очевидно, що в майбутньому основну небезпеку слід чекати не від регулярних армій різних країн, а від усіляких терористичних, кримінальних та інших аналогічних організацій, учасники яких об'єднані в певні мережеві структури. Ці транснаціональні соціальні групи важко ідентифікувати, оскільки у них немає постійної адреси. Подібні групи та організації не мають чіткої ієрархічної підпорядкованості, нерідко у них немає і загального керівництва. Вони координують свою діяльність, використовуючи засоби глобальних комунікацій. Відмінна риса таких структур - наявність єдиної стратегічної мети і відсутність планування на тактичному рівні.

Деякі позиції даних концепцій були відображені в концепції побудови мережевих збройних сил, або мережевої війни, яка успішно реалізується Збройними Силами США. Таким чином, можна говорити про чіткий зв'язок між прикладними завданнями реформування ВС США і більш ранніми теоретичними побудовами, що стосуються ведення інформаційної війни.

Ще одна концепція, на яку слід звернути увагу, запропонована аналітиками Університету ВПС США. Дана концепція робить акцент не на психологічному, а на економічному і військовому (у традиційному розумінні) аспектах інформаційної війни.

Існують різні теоретичні підходи відносно соціально-психологічних аспектів інформаційної війни: «теорія залежності» Г. Лассуелла, за якою

людина абсолютно беззахисна перед маніпуляцією ЗМІ; або концепція П. Лазарсфельда, який говорить про більш складний вплив на споживача інформації через так званих «лідерів думок», «теорія засобу» М. Маклюена, згідно якій нові інформаційні технології призводять до змін парадигм сприйняття людиною навколишнього світу, а також ряд інших. Усі вони сходяться в одному: інформаційне середовище має величезний вплив як на індивідуальну, так і на масову свідомість, і зацікавлені групи людей, природно, цим активно користуються. Враховуючи те, що інформаційна війна включає в себе комунікативні дії щодо зміни масової свідомості, розглянемо зазначені теорії.

Як пише Г. Бакулєв, з метою досягнення перемоги під час Першої світової війни була потрібна мобілізація всіх виробничих потужностей, що було можливо за умови самовіддачі цивільного населення. Але виявилося, що різнорідність і індивідуалізм, що стали результатом поділу праці в суспільстві, вступають у протиріччя з виниклими потребами. Таким чином, з’явилася необхідність у кожній країні-учасниці війни зміцнити зв'язки між індивідами і суспільством. Мова йшла про те, щоб підвищити лояльність людей, прищепити їм ненависть до ворога та підтримувати в них високий моральний дух всупереч нужді й поневірянням і змусити їх думати, насамперед, про батьківщину.

Всі ці завдання могла вирішити пропаганда, з метою якої використовувалися всі засоби: новини, фотографії, кінофільми, грамплатівки, книги, проповіді, плакати, радіосигнали, щитова реклама і листівки. Від громадян чекали любові до своєї батьківщини, ненависті до ворога та жертв заради перемоги.

Через засоби масової інформації воюючі сторони активно поширювали дезінформацію про супротивника.

Всі ці пропагандистські зусилля базувалися на одній простій теорії масової комунікації, яка відповідала уявленням про масове суспільство.

Відповідно до даної теорії, мас-медіа здатні донести до кожного хитромудро складені стимули, їх однаково сприймуть усі люди, і реакція на них теж буде більш-менш однаковою. Вважалося, що медіа здатні формувати громадську думку і схиляти маси до будь-якої точки зору, бажаної комунікатору [17. с.51]. Гарольд Лассуелл, який спробував об'єктивно проаналізувати силу військової пропаганди та роль медіа в масовому суспільстві, прийшов до наступних висновків: «У Великому Товаристві більше немає можливості спаяти воєдино роз'єднаність індивідів у горні бойового танцю, потрібен більш новий і більш тонкий інструмент, щоб спаяти тисячі й навіть мільйони людей в єдину масу ненависті та волі і надії» [258].

Г. Лассуелл є одним із перших дослідників масової комунікації і фактично засновником наукового вивчення пропаганди. Ці явища вчений досліджував як найважливіші складові політичної проблематики. Теорію пропаганди Г. Лассуелл створив на основі об'єднання біхевіоризму з фрейдизмом. Дана теорія досить песимістично оцінює роль медіа. На думку Г. Лассуелла, успіх пропаганди залежить не від змісту конкретних повідомлень, а від того, наскільки піддається впливові свідомість середньої людини. На думку вченого, в умовах економічної кризи та політичної нестабільності люди стають більш уразливі перед обличчям пропаганди.

Так, наприклад, у Німеччині в період кризи вся країна стала психологічно неврівноваженою та податливою до маніпулювання.

Пізніше Г. Лассуелл переглянув свої погляди щодо «магічної» сили пропаганди. Він прийшов до висновку, що людей потрібно поступово готувати до прийняття абсолютно інших ідей і вчинків. Для цього слід мати детально розроблену стратегію тривалої кампанії, в результаті проведення якої можна було б обережно впроваджувати, а потім культивувати нові ідеї та образи. «Потрібно створювати символи і

поступово вчити людей пов'язувати з ними конкретні емоції. В разі успіху цих стратегій культивації вийде те, що Г. Лассуелл називав колективними або еталонними символами. Еталонні символи асоціюються з сильними емоціями, і якщо ними скористатися правильно, можна викликати масштабні масові дії позитивної властивості. На відміну від понять «магічної кулі», теорія Г. Лассуелла передбачала тривалий і вкрай складний процес підготовки. Один-два рази натрапивши на екстремістські ідеї, людина навряд чи відчувала їхній вплив [17].

Вже в 1927 р. вчений визначає пропаганду як «управління колективними аттитьюдами (установками) за допомогою маніпулювання значимими символами». Вона не може бути «поганою» або «доброю» і кваліфікуватися в термінах етики. Пропаганда - це спроба змінити погляди людей, вона є «масове переконання», її мета - насаджувати політичну міфологію. Пропаганда для нього «інструмент тотальної політики разом із дипломатією, економічними заходами та збройними силами. Її мета полягає в економії матеріальних витрат на світове панування.

Дійсно, під час Другої світової війни засоби масової інформації стали використовуватися як технології психологічної війни. У повчанні збройним силам США - «Вступі у психологічну війну» - з'явилися поняття «білої» пропаганди (розрахована на «своїх», поширюється та визнається джерелом або його офіційними представниками) і «сірої» пропаганди (спрямована на «ворога», видається за витікаючу з іншого джерела, ніж справжній).

Психологічний вплив може здійснюватися різними методами й основними інструментами, за допомогою яких виявляється вплив на свідомість і підсвідомість людей, є:

1) власне психологічні методи (переконання, навіювання, інформування, заохочення, примус, кара, метод прикладу);

2) використання військових засобів;

3) можливе використання системи торгових і фінансових санкцій, спрямованих на економічний підрив потенційного супротивника;

4) використання чисто політичних засобів [138, с.31].

«Головна відмінна особливість сучасних психологічних технологій - вони діють на психіку, минаючи свідомість. Через це ми позбавляємося можливості приймати зважені, логічно обґрунтовані рішення, а значить, втрачаємо свободу волі. В результаті все наше життя, включаючи поведінку, бажання, емоції та навіть здоров'я, опиняється під чужим контролем» [206, с.6].

Пропаганда як управління значущими символами передбачає поширення насамперед політичних міфів і стереотипів. Політичний міф Г. Лассуелл визначає як "сукупність соціальних переконань, що включають стійкі уявлення про ідеальний тип влади в рамках конкретного суспільного устрою». Політичний міф - це не тільки «ірраціональне». Прийняте на віру, аксіоматично, бездоказово. Г. Лассуелл вважає, що політичний міф реалізується в політичних доктринах та ідеологіях і відображається в структурі політичної свідомості через такі поняття як «креденда» і «міранда», у зв'язку з чим пропаганда завжди звернена як до розуму, так і до почуттів реципієнтів.

За допомогою пропаганди, «креденди» (довіра) і «міранди» (марево, надприродне) здійснюється політичне управління суспільством, політична комунікація, реалізується мова влади. При цьому функція мови влади має раціональні цілі (політична семантика, тобто зміст і стиль висловлювань) і емоційні ефекти (політична синтактика).

Як писав Г. Лассуелл, в XX ст. усі суспільні науки є в тій чи іншій мірі політичними. На його думку, політологія та комунікативні науки повинні використовувати не тільки методи емпіричної соціології, соціальної психології, але і психоаналізу та психіатрії у вивченні масових комунікацій, політичної комунікації, політичної поведінки та політичної

пропаганди. Г. Лассуелл вважав, що політичну науку «в широкому сенсі слід розглядати як орган самопізнання і самовдосконалення людства в процесі загальнокосмічної еволюції» [161. с.240].

Наймогутніше знаряддя політичного впливу на суспільство - засоби масової комунікації. Інтерес до вивчення пропаганди і впливу на масову свідомість стимулювався також історичними подіями, а саме, Першою світовою війною та революційними рухами першої половини XX століття. Г. Лассуелл писав, що в період Першої світової війни в 1918 р. скидалося на бік супротивника до 5 млн. листівок на місяць, досягаючи 150 миль за лінією фронту. Німці, в свою чергу, публікували газету по-французьки, де в числі іншого друкували імена захоплених ними в полон французьких солдат. Г. Лассуелл виявив при цьому ряд стратегій, які використовували обидві сторони: стратегія розділення ворога (наприклад, спроба відокремити Австро-Угорщину від Німеччини); стратегія деморалізації ворога (наприклад, підкреслення того, як багато мільйонів американських солдат висадилися у Франції); стратегія звинувачення ворога в звірствах (наприклад, у відношенні німецьких солдат до бельгійських дітей).

На рубежі 30-40 рр. минулого століття, будучи учасником організованого Фондом Рокфеллера семінару з масових комунікацій і автором ряду великих досліджень, Г. Лассуелл формулює свою модель масової комунікації, опубліковану в кінці 40-х років, яка і стала хрестоматійною: «ХТО говорить? - ЩО повідомляє? - КОМУ? – Яким КАНАЛОМ? - З яким ЕФЕКТОМ?». Ця модель, що одержала назву «лінійної» визначала основні напрями досліджень масової комунікації. ХТО? - дослідження джерела повідомлень. ЩО? - аналіз самих повідомлень (при цьому Г. Лассуелл фактично першим став застосовувати контент-аналіз для вивчення повідомлень масової комунікації). КОМУ - дослідження аудиторії масової комунікації. КАНАЛ - вивчення засобів комунікації. ЕФЕКТ – аналіз впливу повідомлень на масову свідомість.

Крім опису комунікативного процесу Г. Лассуелл проаналізував і соціальні функції масової комунікації в сучасному суспільстві.

Слід зазначити, що Г. Лассуелл переоцінював ефект впливу засобів масової комунікації на розум аудиторії. Він вважав, що аудиторія, яка складалася з атомізованих, відокремлених індивідів, реагує на дії пропаганди й інших повідомлень засобів масової комунікації практично однаково.

В основі єдності реакцій лежить єдність ірраціональних людських інстинктів, які Г. Лассуелл розглядав відповідно до постулатів психоаналітичної концепції З. Фрейда. Ефективна пропаганда повинна грамотно використовувати людські інстинкти. Головне завдання пропаганди - об'єднувати та мобілізувати суспільство.

Запропонована Г. Лассуеллом концепція пропаганди як «чарівної кулі», припускала, що масова комунікація, діючи на громадську думку, не «пролітає» повз цілі, доходячи до свідомості кожного. У масовому атомізованому суспільстві засоби масової комунікації замінюють і компенсують зруйновані соціальні зв'язки, діючи безпосередньо на кожного індивіда, і вплив одних і тих же сигналів-повідомлень викликає у всіх однакову реакцію. Г. Лассуелл використовував також метафору ін'єкції: засоби масової комунікації «впорскують» кожному індивіду «дозу» інформаційного впливу.

Цей підхід, що мав на увазі гомогенність і пасивність аудиторії, яка не в силах протистояти уніфікуючому впливові засобів масової комунікації та пропаганди, був згодом переглянутий і доопрацьований багатьма дослідниками, зокрема, П. Лазарсфельдом, який розробив концепцію «Лідерів думок». «Лідери думок» грають роль посередника між засобами масової комунікації та індивідом. «Лідери думок» - представники неформальних груп, найбільш авторитетні, поінформовані й активні їхні члени.

Саме точка зору лідерів думок найчастіше виявляється визначальною, будучи своєрідним «фільтром» на шляху масової комунікації. Мікрогрупова думка цілком здатна блокувати вплив пропаганди. Однак, як показали подальші дослідження, група може протистояти масованому впливу пропаганди, поки зберігає згуртованість і єдність думок. Ослаблення групової єдності робить людей більш податливими для інформаційної індоктринації.

Скептицизм Лассуелла з приводу здатності середньої людини розібратися у своєму суспільному світі та прийняти розумні рішення щодо своїх вчинків поділяв У. Липпман. У роботі «Громадська думка» він вказав на розбіжності, які обов'язково існують між «світом зовнішнім і картинами в наших головах». Оскільки ці розбіжності неминучі, У. Липпман висловлював сумнів у спроможності середньої людини самостійно орієнтуватися в навколишньому світі, як допускає класична теорія демократії. Світ у 1930-і роки був особливо складним, а політичні сили небезпечними. Люди просто не могли отримати достатньо інформації з медіа, щоб у всьому розібратися. Навіть якщо журналісти ставилися до своїх обов'язків із усією серйозністю, вони не могли подолати психологічні та соціальні бар'єри, які заважали середній людині намалювати потрібні «образи у своїй голові» [17. с.52].

Подібно Лассуеллу, Липпман вважав, що пропаганда несе таку серйозну загрозу американським медіа, що потрібні великі зміни в політичній системі. Оскільки народ уразливий до пропаганди, для його захисту потрібен якийсь механізм або орган. Медіа повинні функціонувати під контролем у якій-небудь прийнятній, але дуже суворій формі. Самоцензури, напевно, було б недостатньо. Як і Лассуелл, Липпман вважав, що контроль над збором і розповсюдженням інформації слід передати в руки технократії - інтелектуальної еліти, яка б за допомогою наукових методів відділяла факти від вимислу і приймала правильні

рішення про те, хто повинен отримувати ту чи іншу інформацію. Він запропонував створити квазіурядове бюро розслідувань, яке мало ретельно аналізувати інформацію та спрямовувати її іншим елітам для прийняття рішень. Це бюро також могло б визначати, яку інформацію варто поширювати через мас-медіа, а яку людям краще не знати [17. с.52].

На початку 1950-х років дослідження, проведені Лазарсфельдом, дозволили зібрати величезний обсяг даних (за докомп'ютерними мірками), які переконливо довели, що влада медіа не настільки велика, як уявлялося. Виявилося, що люди користуються різними способами, щоб вислизнути від впливу медіа. Останні ж не тільки не є руйнівною соціальною силою, а навпаки, посилюють існуючі громадські тенденції та зміцнюють статус-кво. На користь теорії масового суспільства знайшлося порівняно мало доказів. Хоча Лазарсфельд ніяк не називав свою теорію, надалі вона отримала назву теорії обмежених ефектів.

У даній теорії можна виділити три основні положення. По-перше, в кожній підгрупі свої лідери думки, так само як і в різних темах. По-друге, лідери думки походять з усіх прошарків суспільства, отже, медіаповідомлення в різних соціальних групах можуть бути інтерпретовані і використані по-різному. По-третє, ясно, що повідомлення на шляху до масової аудиторії проходять через різні фільтри і тому, щоб медіа досягли різних аудиторій, джерело повідомлень має модифікувати їх з урахуванням конкретних груп. Останньою проблемою зайнялися функціоналісти, перш за все Мелвін Дефлер [17, с.52].

Таким чином, модель П. Лазарсфельда (засіб масової комунікації - лідер думок - індивід) розглядає людину не як окремий «атом», а як члена неформальних об'єднань, які впливають на його мислення і поведінку. Надалі ця концепція (модель «багатоступінчастої комунікації») розроблялася й іншими дослідниками, у тому числі Е. Кацем і У. Шраммом.

Сучасні підходи до пропаганди виходять з того, що пропаганда повинна створюватися з урахуванням певних правил: 1) Мета пропаганди полягає в тому, щоб текст повідомлення і те, що ховається за ним, привернуло увагу читача, визвало в ньому внутрішній конфлікт або зміцнило упереджене ставлення; 2) У пропаганді зроблений акцент на тих змінах, які можуть стати можливими завдяки діям читача. При цьому негативні події з минулого в ній будуть порівнюватися з тим світлим майбутнім, яке стане можливим внаслідок скоєних читачем дій; 3) З допомогою пропаганди формується враження, що інформація, подана у ній - це об'єктивна правда, за якою ніхто не стоїть і яка виходить із суспільної сфери і не спрямована на те, щоб вплинути на аудиторію, 4) У пропаганді аудиторія розглядається як пасивний об'єкт, у ній немає і натяку на те, що аудиторія може використовувати диференціальне декодування, щоб «відсіяти» певні елементи повідомлення і тим самим позбавити себе мотиву до будь-яких дій; 5) У пропаганді неприкрито і явно використовуються візуальні, риторичні і символічні засоби, але вони повинні бути зрозумілими для суспільства, і повинен існувати простий і універсальний спосіб декодувати їх так, як це потрібно самому творцю пропаганди. [127, с.230-231].

Американський військовий аналітик Ричард Шафранськи розглядає інформаційну війну в контексті збройного зіткнення («warfare») як збройні дії, спрямовані проти будь-якої частини системи знань або припущень ворога. «Супротивник» - це будь-хто, чиї дії суперечать меті лідера. Поза державою це може бути «образ ворога» чи «не ми». Всередині ворогом може бути зрадник або мандрівник, будь-хто, хто протистоїть або недостатньо підтримує лідера, який керує засобами інформаційної війни. Якщо члени групи не підтримують цілі лідера в ході бойових дій, внутрішня інформаційна війна (включаючи такі речі як пропаганда,

брехня, терористичні акти та чутки) може бути використана в спробі змусити їх бути більш лояльними до цілей лідерів [124, с. 13].

У сучасній науковій літературі виділяють два основних підходи до аналізу інформаційної війни. Перший підхід досліджує явище інформаційної війни через її вплив на масову свідомість, маніпулятивний потенціал і психологічну дію інформаційних повідомлень. Другий підхід розглядає інформаційну війну як автономну систему в сучасному суспільстві за допомогою технічного, математичного понятійного апарату.

А. Манойло, відомий російський дослідник інформаційно-психологічної війни (ІПВ), пропонує розглядати ІПВ на різних рівнях пізнання: як соціальне явище; як поле політичних конфліктів; як особливу форму політичного конфлікту; як елемент системи інструментів політичного регулювання (інструмент інформаційної політики).

На кожному з даних рівнів розгляду ІПВ досліджується в рамках власної наукової гіпотези:

1. Соціологічна гіпотеза, відповідно до якої інформаційно-психологічна війна - це соціальне явище і нова форма суспільних відносин, що породжується інформаційним суспільством.

2. Статистична гіпотеза, за якою ІПВ - поле політичних конфліктів, що знаходяться в тісному взаємозв'язку і взаємодії.

3. Конфліктологічна гіпотеза. ІПВ - політичний конфлікт із метою розв'язання суперечностей по відношенню до влади і управління, в якому зіткнення сторін здійснюється у формі інформаційно-психологічних операцій із застосуванням інформаційної зброї. Відповідно до даної гіпотези мета інформаційно-психологічної війни - це розв'язання суперечностей по відношенню до влади і здійснення політичного управління в інформаційно-психологічному просторі. Досягнення цієї мети можливе при вирішенні таких політичних завдань інформаційно-психологічної війни:

- трансформація структури національних економічних, політичних, соціально-культурних, інформаційно-психологічних просторів учасників міжнародних відносин відповідно з власними принципами формування інформаційно-політичної картини світу;

- досягнення військово-політичної переваги і безумовного лідерства у сфері міжнародних відносин;

- досягнення цілей національної економічної, ідеологічної, культурної, інформаційно-психологічної експансії;

- забезпечення сприятливих умов для переходу власної національної системи соціально-політичних відносин на новий, більш високорозвинений і високотехнологічний етап еволюційного розвитку.

4. Системно-функціональна гіпотеза, за якою ІПВ - частина системи політичного регулювання, інструмент інформаційної політики [137. с.189-190].

Розглянемо наявні типології інформаційних кампаній, одним із типів яких є інформаційна війна. Різноманіття політичних відносин, систем і процесів надає інформаційним кампаніям дуже різноманітного вигляду і характеру. Тому їхня типологія достатньо складна. Наприклад, із точки зору цільового характеру інформаційних дій, вони можуть бути диференційовані на внутрішньополітичні і зовнішньополітичні. Зовнішньополітичні інформаційні дії поділяються на глобальні, міжрегіональні та національні. Прикладом може послужити відома інформаційна кампанія під умовною назвою «2000», в ході якої десятки зацікавлених виробників електронної техніки розгорнули масовану атаку на світове співтовариство, попереджаючи про потенційну загрозу глобального збою комп'ютерів при настанні третього тисячоліття.

Крім цього внутрішньополітичні кампанії можуть бути представлені як сукупність федеральних, регіональних, місцевих і локальних дій на інформаційному полі.

Інформаційні кампанії поділяються на ті, які орієнтовані на отримання прибутку, і ті, які проводять без розрахунку на прибуток. Кампанії першого типу здійснюються, коли політичні декларації служать інструментом перерозподілу власності. Кампанії другого типу орієнтовані на зниження популярності супротивника, руйнування його авторитету, «розкрутку» кандидата і т.д.

За темпами проведення кампанії поділяються на масовані, середньої (зниженої), наростаючої і низхідної інтенсивності. У цьому ряду знаходяться і кампанії, що характеризуються залповим характером і демонструють миттєвий викид інформаційної енергії за короткий час. Нерідко зустрічається і пульсуючий тип, що передбачає деяке повторення сюжетних тем, фаз та інших параметрів кампанії.

Ще одна типологія заснована на предметній сфері інформаційних кампаній. Тут прийнято виділяти іміджеву, мобілізуючу, стабілізуючу (дестабілізуючу) (політичні порядки в країні, регіоні, світі), провокуючу (форми поведінки, активності, реакції) та інші кампанії.

Відхід від застосування технології пропаганди в чистому вигляді і поворот до використання різних методик переконання з елементами пропаганди є одним із сучасних напрямків еволюції технологій впливу. М. Михайлов вказує на чотири тенденції розвитку пропаганди в XX ст.: активізація сфери пропагандистських демонстрацій; формування політичного інформування через ЗМІ; інтенсифікація способу пропагандистського інформування; глобалізація та універсалізація пропаганди [146, с.47].

Маніпулятивні технології доповнюють інші методи впливу та перетинаються з ними. Так. І. Дзялошинський згадує такі методи впливу на суспільство, використовувані сучасними маніпуляторами: управління інформаційними потоками (створення інформаційного шуму, підбір інформації, організація «випадкових витоків» інформації і використання

дезінформації); міфологічне маніпулювання: психологічні технології (використання страхітливих тем і матеріалів; спрощення проблеми і т.д.); ціннісно-емоційне маніпулювання; застосування механізмів соціального контролю (залучення груп впливу, мотивування людини чинити так, як усі); маніпулювання раціональними, переконуючими аргументами (соцопитуваннями, коментарями експертів, прогнозами) [65, с.34].

1.2. Інформаційна війна: еволюція, поняття, сутність, структура

Поняття «інформаційна війна» (в англомовній термінології Psychological Operations - PSYOP) є одним із найбільш вживаних при аналізі політичних комунікацій. І це не випадково. Адже саме цей формат організації інформаційної взаємодії найбільш ефективний при досягненні політичних цілей, реалізації навіть масштабних проектів у сфері влади. Як правило, поодинокі інформаційні повідомлення не можуть створити стійкої комунікації держави або партії з громадською думкою, служити підставою для їхньої довготривалої присутності в публічному просторі. Будь-які політичні цілі потребують постійного і, по можливості, інтенсивного інформаційного підкріплення, здатного до такого тиражування повідомлень, яке забезпечує вирішення завдання. Використання, наприклад, державою форм інформаційної політики часом занадто витратне, вимагає багато часу і тому не завжди ефективне.

Теоретики інформаційної війни зазвичай схильні до образного і художнього мислення, надаючи перевагу категоріям філософського порядку, ніж технічним термінам. Так, наприклад, співробітник коледжу Генерального штабу армії США Р. Шафранськи характеризує попередню

історію розвитку засобів і методів ведення війни як еволюцію фундаментальної здатності приматів використовувати штучні знаряддя для посилення і подовження даних їм від природи кінцівок; іншими словами, ми звертаємося до зброї тому, що знаходимо її більш ефективною, ніж наші кігті й ікла. Проте зараз, на його думку, прийшов час навчитися воювати головою: мозок людини стає основною зброєю й одночасно полем бою інформаційної війни [236].

З метою глибокого дослідження сучасних проблем інформаційної війни необхідно коротко розглянути історичні аспекти цього явища.

Термін «інформаційна війна» має сучасну історію. Виникнення цього терміну стало результатом роботи групи американських теоретиків, які займаються військовими проблемами, таких як Г.К. Екклз, Г.Г. Самерз й ін. Передбачається, що вперше термін «інформаційна війна» з'явився в 1976 р., коли американський інженер Томас Рона використав його в технічному звіті для компанії «Boeing», який називався «Системи зброї й інформаційна війна». Т. Рона підкреслив, що інформаційна інфраструктура, яка відтепер є ключовим компонентом американської економіки, стає вразливою ціллю як у воєнний, так і в мирний час.

Вперше про можливість війни в інформаційній сфері заговорили в середині 90-х р. XX ст. В кінці 1996 р. на одному з симпозіумів представник МО США Роберт Банкер представив доповідь, присвячену новій військовій доктрині збройних сил США XXI століття (концепції «Force XXI»). Ключовим моментом у ній є поділ усього театру військових дій на дві складові - традиційний простір і кіберпростір, причому останній має більш важливе значення. Банкер запропонував доктрину «кіберманевра», яка повинна стати природним доповненням існуючих військових концепцій, що мають на меті нейтралізацію або придушення збройних сил супротивника.

У число сфер ведення бойових дій крім землі, моря, повітря та космосу було запропоновано включити і інфосферу. Як підкреслюють військові експерти, основними об'єктами ураження в нових війнах будуть інформаційна інфраструктура та психологія супротивника (з'явився навіть термін «human network») [205].

Розробками теорії інформаційної війни займалися також представники теоретичної групи Університету ВПС США (Air University, Maxwell Airforce Base, Alabama) Джордж Стейн, Ричард Шафранськи і Оуен Дженсен. На їхню думку, в майбутньому конфлікті вирішальну роль буде відігравати сама інформація (точніше - знання), а не традиційні засоби ведення війни. Інформаційні технології, відповідно до цієї концепції, всього лише засіб, що забезпечує досягнення стратегічного інформаційного домінування. Під інформаційним домінуванням у даному випадку розуміється створення таких інформаційних умов, у яких дії супротивника в кінцевому підсумку неминуче виявляться вигідними протилежній стороні або будуть спрямовані на обслуговування її інтересів.

Можна сказати, що популярність до терміну «інформаційна війна» прийшла після закінчення так званої «холодної війни». Цей термін став використовуватися в документах Міністерства оборони США. Особливо часто він став згадуватися засобами масової інформації після проведення операції «Буря в пустелі» в 1991 році, де нові інформаційні технології вперше були використані як засіб ведення бойових дій. Офіційно ж цей термін вперше був ужитий в директиві міністра оборони США від 21 грудня 1992 р. Як вважає І. Шамін, на рубежі XX - XXI ст. в США фактично відбувся перегляд точки зору щодо місця і ролі фактора «інформаційної війни» в «організаційній системі» сучасного геополітичного протиборства на міждержавному рівні. Вирішальне значення в ініціюванні такого роду процесів зіграв ряд об'єктивних обставин і, в першу чергу, - це так звана «інформаційна революція», що

відбулася у світі в даний період, а також глобалізація, яка теж стала однією з найважливіших тенденцій сучасного світового розвитку [230, с.35].

В кінці 1996 р. Роберт Банкер, експерт Пентагону, на одному з симпозіумів представив доповідь, присвячену новій військовій доктрині збройних сил США XXI століття (концепції «Force XXI»). В її основу було покладено поділ усього театру військових дій на дві складові - традиційний простір і кіберпростір, причому останній має навіть більш важливе значення. Р. Банкер запропонував доктрину «кіберманевра», яка повинна з'явитися природним доповненням традиційних військових концепцій, що мають на меті нейтралізацію або придушення збройних сил супротивника [59].

У жовтні 1998 року, Міністерство оборони США вводить в дію «Об'єднану доктрину інформаційних операцій». Спочатку ця публікація називалася «Об'єднана доктрина інформаційної війни». Пізніше вона була перейменована в «Об'єднану доктрину інформаційних операцій». Причина зміни полягала в тому, щоб роз'яснити відносини понять інформаційних операцій та інформаційної війни. Вони були визначені, наступним чином:

- інформаційна операція: дії, що здійснюються з метою ускладнити збір, обробку, передачу та зберігання інформації інформаційними системами супротивника при захисті власної інформації й інформаційних систем;

- інформаційна війна: комплексна дія (сукупність інформаційних операцій) на систему державного та військового управління протилежної сторони, на її військово-політичне керівництво, яка вже в мирний час призводила б до прийняття сприятливих для сторони-ініціатора інформаційного впливу рішень, а в ході конфлікту повністю паралізувала б функціонування інфраструктури управління супротивника [59].

Поняття інформаційної зброї з'явилося лише у другій половині XX ст., і з 1970-х років інформаційно-психологічна війна стала самостійним

явищем. Хоча принципи ведення такого роду інформаційних кампаній були відомі давно. Воюючі сторони здавна знали, що боротися з ворогом можна не тільки збройними засобами, а й шляхом цілеспрямованого впливу на психіку воїнів. Основи ведення інформаційного протиборства в світовій політиці були сформульовані тисячі років тому за часів Трої.

Ще давньокитайський філософ Сунь-Цзи, який першим узагальнив досвід інформаційного впливу на супротивника, у своєму трактаті «Мистецтво війни» запропонував методи активного протистояння ворогу. Він писав: розкладайте все добре, що є в країні вашого супротивника; залучайте видних діячів супротивника у злочинні заходи: підривайте престиж керівництва супротивника та виставляйте його в потрібний момент на ганьбу громадськості; використовуйте з цією метою співробітництво з найпідлішими і наймерзеннішими людьми; розпалюйте сварки і зіткнення серед громадян ворожої вам країни; підбурюйте молодь проти старих; заважайте всіма засобами роботі уряду; заважайте всіма способами нормальному постачанню ворожих військ і дотриманню в них порядку; сковуйте волю воїнів супротивника піснями та музикою; робіть усе можливе, щоб знецінити традиції ваших ворогів і підірвати їхню віру у своїх богів; підсилає жінок легкої поведінки для того, щоб доповнити справу розкладання; будьте щедрі на пропозиції та подарунки, купуючи інформацію та спільників. Взагалі не економте ні на грошах, ні на обіцянках, тому що вони приносять прекрасні результати.

У II ст. н.е. в Китаї послідовники Сунь-Цзи вперше застосували новий прийом пропагандистського впливу - проголошення справедливого характеру війни.

У Стародавній Греції використовували глашатаїв, які під виглядом державних розпоряджень - едиктів проголошували політичні заклики та викриття. Найчастіше в цих «викриттях» повідомлялося про неприваблівi

деталі особистого життя політичних суперників, їхнє надмірне честолюбство, моральну неохайність і т.п.

Великий поштовх розвитку пропагандистського впливу на психіку воїнів і цивільного населення дала перша загальноєвропейська війна, що ввійшла в історію під назвою «Тридцятирічна війна (1618-1648 рр.). Досягнення граверного мистецтва дозволили широко застосовувати ілюстровані листівки, що випускалися значними для того часу тиражами. З друкованого верстата сходили перші «інформаційні листочки», які сповіщали аудиторію про будь-яку подію [161, с.138-139].

До недавнього часу інформаційно-психологічні операції носили допоміжний, випадковий і невпорядкований характер. Як відомо, американці програли війну у В'єтнамі саме через посилення всередині США опозиції уряду, падіння поваги до власної армії. Погано озброєні загони в'єтнамських партизан зломили опір Америки не танковими колонами та літаками, а пропагандою, хоча ЦРУ вже в ті роки мало підрозділ, що займався психологічними операціями, виявляючи забобони та звичаї місцевих племен і намагаючись використовувати їх у своїх цілях.

Саме в той час остаточно ствердилася думка, що ядерна рівновага робить неможливим відкрите військове зіткнення наддержав.

Таким чином, якісній зміні засобів і методів ведення війни в другій половині XX ст. сприяла віра у неможливість нової «великої війни». Вступ людства в ядерну еру призвів до перегляду традиційних уявлень про співвідношення військово-політичних цілей і засобів: термоядерна війна фатальна для обох сторін «не через політичні цілі воюючих, а в силу військових засобів, що знаходяться в їхньому розпорядженні... всупереч постулатам логіки, засоби сьогодні диктують цілі» [257, с.8]. Знадобились альтернативні способи протиборства. І вихід було знайдено. З 1980-х років економічні успіхи передових країн Заходу стали визначатися здатністю до якісної та кількісної обробки значимої інформації, до генерування нових

виробничих технологій. Саме усвідомлення неможливості використання ядерної зброї для досягнення політичних цілей і дало поштовх гонці високотехнологічних, інформаційно ємних неядерних озброєнь, наслідки застосування яких за рівнем шкоди цілком дозволяють зарахувати їх до категорії зброї масового ураження.

Інформаційна війна - це складна система, яка складається з декількох взаємопов'язаних елементів. У неї входять:

- контроль над ситуацією;
- захист інформації та поширення своїх ідей;
- інформаційний тероризм (хакерські атаки);
- інформаційна блокада;
- війна в засобах масової інформації;
- промисловий і економічний шпіонаж;
- інші методи та прийоми. [206, с.11].

У. Швартау, автор книги "Інформаційна війна: Хаос на електронному суперхайвеї" визначив інформаційну війну як "електронний конфлікт, в якому інформація є стратегічним активом, гідним завоювання або знищення [264, с.13].

С.П. Расторгуєв вважає, що інформаційна війна - це війна майбутнього, суть якої полягає в комплексі заходів з інформаційного впливу на масову свідомість в умовах інформаційної відкритості для зміни поведінки людей і нав'язування їм цілей, які не входять до числа їхніх інтересів [185, с. 230].

Л. Воронкова та Д. Фролов виділяють основні відмінності між інформаційною війною і війною традиційною.

По-перше, війна має відомий і чіткий арсенал впливу. Передбачуваність останнього створює можливість побудувати у відповідь оборонні системи і прийняти захисні заходи. В інформаційній війні арсенал впливу відрізняється гнучкістю та непередбачуваністю. Як

правило, відсутня можливість спрогнозувати напрямок і інструментарій можливої атаки.

По-друге, в традиційній війні територія захоплюється повністю, а в інформаційній - поступово. Проводиться робота з лідерами думок, із молоддю і т.д. Оскільки інформаційна війна може розвинутися на тлі всезагального миру та благополуччя, вона виглядає як «війна мирна».

По-третє, можливість багаторазового захоплення одних і тих же людей. У рамках традиційної війни діє логіка «так-ні», у разі війни інформаційної є варіант нечіткої логіки, коли оцінки можуть даватися з певною ймовірністю (на 40%, на 60% тощо). Більше того, одночасно на людину можуть діяти різні «супротивники», по суті, захоплюючи різні тематичні зони її свідомості.

По-четверте, у війні традиційній захоплюють і освоюють територію різні люди, які виконують різні соціальні ролі. В інформаційній війні ці позиції збігаються. В інформаційній війні присутня невизначеність щодо того, хто ж насправді є другом, а хто ворогом.

По-п'яте, людина не може протидіяти невидимому впливові. Вплив може приймати доброзичливу форму, на яку навіть чисто біологічно людина не готова відповідати агресивно.

По-шосте, у традиційній війні в межах зони ураження руйнується все, в інформаційній війні зброя діє вибірково, обираючи певні прошарки населення.

По-сьоме, підступність інформаційної війни полягає в тому, що видимі ознаки руйнівного впливу відсутні. Населення навіть не відчуває, що на нього чинився вплив, у результаті чого захисні механізми, зокрема відчуття небезпеки, не працюють [42, с.103-104].

Нові тенденції у сфері засобів і способів ведення війни, викликані розвитком інформаційних технологій, настільки фундаментальні та масштабні, що дозволяють військовим аналітикам говорити про нову

революцію у військовій справі (РВД). Така революція не зводиться до кількісного нарощування технічних характеристик озброєнь і появи нових технологічних рішень вже існуючих завдань у справі забезпечення національної безпеки. Вона передбачає також трансформацію способів і методів застосування окремих типів озброєнь і їх комбінацій, структури та форм організації військової справи і, в кінцевому рахунку, нове концептуальне розуміння цілей і завдань оборонної політики. Непрямими, але політично вкрай значимими наслідками цієї революції є зміни в пріоритетах бюджетних витрат на оборону та національну безпеку, у формах і методах взаємодії й координації в рамках "силового" блоку державних відомств, у відносинах між військово-політичними інститутами і суспільством, а також у ряді інших сфер [210, с .26].

Показовою є думка Вільяма Кроуела, колишнього заступника директора Управління національної безпеки США, який вважає, що «Протягом наступних 20-30 років кібератаки стануть невід'ємною частиною військової стратегії. Залишається тільки незрозумілим, чи будуть комп'ютерні мережі настільки всюдисущими і незахищеними, що військові дії повністю перемістяться у віртуальний простір» [132].

У сучасному розумінні «першою інформаційною війною» прийнято вважати війну в Перській затоці, яка тривала п'ять тижнів із січня по лютий 1991 р., так звану «Бурю в пустелі». Саме ця війна стала наочним доказом переваги інформаційного способу ведення війни і «технофілії у військовому мистецтві». У ході бойових дій використовувалися «стелси», що непомітно для радарів підкрадалися до супротивника, бомби з лазерним наведенням і ракети «Петріот», яким вдавалося перехоплювати іракські ракети середнього радіусу дії, запущені по Ізраїлю та Саудівській Аравії, і, звичайно ж, «наймасштабніша зі створених коли-небудь інформаційна система типу С31, яка пов'язувала між собою не тільки війська США в Перській затоці, але і ці війська з пунктами їх базування на

території самих Штатів, з національним командуванням у Вашингтоні та з іншими силами коаліції». Як написав кореспондент журналу «Економіст», описуючи події війни в Перській затоці, «Ключову роль (у перемозі союзників) зіграла перевага в системі зв'язку, що пов'язувала супутники, літаки радіолокаційного спостереження, штабістів, командирів на полі бою, танки, бомбардувальники, кораблі ВМС і багато іншого. Вона дозволяла союзникам весь час випереджати супротивника в тому, що стосувалося спостереження, орієнтації, прийняття рішень і бойових дій. Все це було пов'язане в єдине ціле і дозволяло союзникам діяти з вражаючою швидкістю і, так би мовити, постійно обходити супротивника з флангу. Був використаний абсолютно новий підхід до організації вильотів авіації: одночасно ставилися тисячі польотних завдань, які передбачають нанесення ударів по сотнях цілей, причому список цілей оновлювався кожні 72 години, і в нього могли бути внесені зміни навіть тоді, коли літак був уже в повітрі. Іракські радари були засліплені, а система радіозв'язку виведена з ладу» [212, с.295].

Слід зазначити, що в колах наукової громадськості не припиняється дискусія з приводу того, що ж насправді ховається під поняттям «інформаційна війна», в чому сутність явищ, які відносяться до інформаційних війн, а також суперечки з приводу коректності та принципової застосовності даного терміну до тієї сфери соціальних взаємин, яку прийнято називати інформаційним протиборством або конфліктом інтересів в інформаційній сфері соціальних систем. Як образно пояснив відомий теоретик інформаційної війни М. Лібіскі, "Спроби повною мірою усвідомити всі грані поняття інформаційної війни нагадують зусилля сліпих, які намагаються зрозуміти природу слона: той, хто обмацує його ногу, називає його деревом, той, хто обмацує хвіст, називає його канатом і так далі. Чи можливо так отримати вірне уявлення? Можливо, слона-то і немає, а є тільки дерева та канати. Одні готові

підвести під це поняття надто забагато, інші трактують якийсь один аспект інформаційної війни як поняття в цілому..." [259].

М. Лібіскі виділяє кілька відмінних ознак інформаційного способу ведення війни:

- особлива роль у командуванні та управлінні Збройними силами комп'ютерної системи зв'язку, здатної передавати інформаційні потоки, які потрібні сьогодні для ведення бойових дій та їх захисту;

- ймовірність того, що майбутні війни будуть миттєвими;

- відсутність потреби в мобілізації населення, а армія нечисленна, вона складатиметься з «інтелектуальних бійців». Це означає, що основна роль буде належати не озброєним силам і навіть не тим, хто сам натискає на курок, а тим, хто обслуговує складні обчислювальні комплекси: бойові літаки, системи збору даних і наведення;

- особлива увага «управлінню сприйняттям» війни населенням у власній країні й у всьому світі. Зразком першокласного «управління сприйняттям» стало висвітлення ЗМІ війни 1991 р. в Перській затоці: війна привернула увагу величезної кількості ЗМІ. Передана ними інформація з театру військових дій була, по суті, абсолютно «стерильною» настільки, що Жан Бодрійяр написав: ствердження «війни в затоці ніколи не було» - істинне. Це була його реакція на те, як майстерно союзники керували телебаченням і пресою;

- використання у військових цілях коштовних досконалих технологій у галузі електроніки, обчислювальної техніки, телекомунікацій та аерокосмосу;

- використання інформаційно-насичених технологій ведення кібервійни;

- ретельне планування інформаційного способу ведення війни. Невід'ємною частиною інформаційного способу ведення війни має стати використання теорії ігор, моделювання (часто супроводжується

створенням зорового образу за допомогою складних систем візуалізації та системного аналізу;

- автоматизація процесу прийняття рішень. Оцінка ситуації і прийняття рішення тепер покладені не на військових, а на технології [212, с.293-294].

Аналізуючи різні визначення інформаційної війни з технічної точки зору, слід відзначити одну її важливу властивість, іманентно їй властиву: ведення інформаційної війни ніколи не буває випадковим чи відокремленим, а має на увазі узгоджену діяльність із використання інформації як зброї для ведення бойових дій - чи то на реальному полі битви, або в економічній, політичній, соціальній сферах. Тому в якості першого найбільш загального визначення війни слід прийняти визначення І. Завадського, який вважає, що «Інформаційна війна - це всеохоплююча цілісна стратегія, зумовлена все зростаючою значимістю і цінністю інформації в питаннях командування, управління та політики» [182, с.15].

Виходячи з даного визначення, можна окреслити наступні сфери, що потрапляють у поле дії інформаційних війн: 1) інфраструктуру систем життєзабезпечення держави - телекомунікації, транспортні мережі, електростанції, банківські системи і т.д., 2) промисловий шпіонаж - розкрадання патентованої інформації, спотворення або знищення особливо важливих даних, послуг; збір інформації розвідувального характеру про конкурентів і т.п., 3) зламування та використання особистих паролів - VIP-персон, ідентифікаційних номерів, банківських рахунків, даних конфіденційного плану, виробництво дезінформації, 4) електронне втручання в процеси командування й управління військовими об'єктами та системами, «штабна війна», виведення з ладу мереж військових комунікацій; 5) всесвітня комп'ютерна мережа Інтернет, у якій, за деякими оцінками, діють 150 000 військових комп'ютерів, і 95% військових ліній зв'язку проходить по відкритим телефонним лініям [150, с.127].

Даний спосіб інформаційної взаємодії трактується як сукупність політико-правових, соціально-економічних або аналогічних дій, які спрямовані на захоплення інформаційного простору, витіснення супротивника з інформаційної сфери, руйнування його комунікацій, позбавлення засобів передачі повідомлень, а також інші подібні цілі. На думку деяких дослідників, зокрема відомого теоретика інформаційної війни С. Расторгуєва, інформаційні війни являють собою одночасно приховані та відкриті інформаційні взаємодії соціальних систем (акторів), які мають на меті отримання певних переваг, забезпечення свого виграшу в матеріальній сфері [185, с. 54]. Дослідники вважають, що в цій взаємодії сторонами постійно використовується інформаційна зброя, яка спрямована на запуск програм самознищення опонуючої інформаційної системи. Кампанії такого типу являють собою форму боротьби за інформаційні ресурси, спосіб забезпечення позиційних переваг у найважливішій сфері суспільного життя.

Як пише Ф. Уебстер, «В наші дні інформація виникає в результаті відстеження поведінки супротивника (або потенційних супротивників), обліку власних ресурсів та ресурсів супротивника, управління громадською думкою у себе в країні і за кордоном. Інформація пронизує всю структуру військової машини, чи йде мова про використання супутників для спостереження за супротивником, про комп'ютери, що зберігають дані й оцінюють будь-які потреби армії, про «розумну» зброю, яка запрограмована так, що стрілку залишається тільки «вистрілити і забути». Таким чином, інформація тепер - це не тільки турбота розвідки, яка збирає інформацію про супротивника і його ресурси, зараз вона закладена в саму зброю й у системи, що приймають рішення [212, с.291].

Як пише Р. Туронок, «Інформаційна війна передбачає порушення, пошкодження або модифікацію інформаційних ресурсів і "знань" людей про самих себе та навколишній світ і включає в себе вплив на громадську

думку та думку еліт, заходи дипломатичного характеру, пропагандистські та психологічні кампанії, підривні акції в галузі культури й політики, дезінформацію та проникнення в місцеві медіа-канали, комп'ютерні мережі та бази даних, технічне сприяння дисидентським й опозиційним рухам і надання їм інформаційної підтримки. Таким чином, проектування стратегії інформаційної війни нерідко полягає в комбінуванні у новому ракурсі низки заходів, що успішно застосовувалися в минулому, однак сприймалися самостійно й ізольовано. При цьому така війна може набути форми як більш-менш традиційного конфлікту між державами або групами держав у дусі холодної війни, так і протистояння між державою та недержавними акторами (боротьба з тероризмом, наркоторгівлею, розповсюдженням зброї масового ураження) або війни проти політики деяких держав у якихось конкретних питаннях (захист прав людини, охорона навколишнього середовища тощо), а задіяні в ній недержавні організації можуть бути позбавлені чіткої національно-державної приналежності та об'єднані в широкі транснаціональні мережі та коаліції» [210, с.24].

Інформаційна війна розуміється як і найбільш гостра форма конфронтації в інформаційному просторі. Тут робиться акцент на характері протистояння опонентів. При цьому першорядного значення набувають такі властивості інформаційної взаємодії як безкомпромісність, висока інтенсивність суперечки, а також короткостроковість гострого суперництва. Для позначення агресивності сторін у цьому дискурсі використовується поняття «інформаційна зброя».

Подібне трактування цього поняття істотно розширює коло акторів, які беруть участь в інформаційному протистоянні. Передбачається, що в інформаційних війнах одночасно задіяні не тільки дві протиборчі сторони, але й усі ті, хто так чи інакше присутні в цей час у політичному просторі, тобто всі учасники політичних комунікацій: громадськість, особи, які

приймають рішення, медіабюрократія і т.д. При такому трактуванні інформаційних війн до них нерідко відносять будь-які форми ідейного протистояння різних доктрин, релігій і навіть напрямів мистецтва. Ідейні протиріччя, розбіжності в позиціях, а часом і елементарні пристрасті прирівнюються до форм інформаційного протистояння.

У питаннях стратегії і тактики інформаційного протиборства виділяють три основні стратегічні цілі інформаційної війни: контроль за інформаційним простором; контроль за механізмом прийняття рішень у державі; контроль за державою в цілому. Тактика інформаційної війни - це практична форма реалізації методології інформаційного протиборства. Тактика випливає зі стратегії та є її практичною формою реалізації [237, с.17].

Слід відповісти, що в науковій літературі пропонується безліч підходів до визначення інформаційної війни.

Представники одного з них - в основному представники військових відомств, як зарубіжних, так і вітчизняних, - трактують інформаційну війну як форму забезпечення або ведення військово-силових дій.

Можна сказати, що інформаційна війна стала результатом нових підходів до застосування інформації, визначення її ролі та місця в суспільстві [157]. Нові тенденції у сфері засобів і способів ведення війни, викликані розвитком інформаційних технологій, настільки фундаментальні та масштабні, що дозволяють військовим аналітикам говорити про нову революцію у військовій справі [256]. Сенс цієї революції не тільки в кількісному нарощуванні технічних характеристик озброєнь і появі нових технологічних рішень вже існуючих завдань у справі забезпечення національної безпеки. Але й у трансформації способів і методів застосування окремих типів озброєнь і їх комбінацій, структури та форм організації військової справи і, в кінцевому підсумку, в новому концептуальному розумінні цілей і завдань оборонної політики.

Іноді інформаційна війна трактується як форма забезпечення або ведення військово-силових дій. Це поняття тісно пов'язане з концепцією розгортання «медіасил спеціального призначення», що формуються і діють за моделлю «спецназу». Однак ці сили озброєні медійною зброєю - цифровими камерами, супутниковими передавачами та іншими аналогічними засобами, які використовуються для вирішення суто військових завдань.

Відомий теоретик інформаційної війни М. Лібікі вважав, що в майбутньому інформація стане основним засобом стримування збройних конфліктів. На його думку, взаємопов'язана інформаційна система, що складається з мережі космічних супутників стеження, наземних, повітряних і морських датчиків, дасть можливість контролювати будь-яку військову активність на планеті, а значить, і застосовувати превентивні заходи проти агресора, оскільки глобалізація світових інформаційних систем дозволить паралізувати та відрізати його економічні й інформаційні системи від решти світу. Автор визначив 7 форм інформаційної війни: командно-управлінська; розвідувальна; психологічна; хакерська; економічна; електронна; кібервійна [259].

Як зазначає М. Павлютенкова, дві принципово різні сфери функціонування інформації - гуманітарна та технічна - задають два варіанти трактування терміна "інформаційна війна". У гуманітарному сенсі "інформаційна війна" розуміється як ті чи інші активні методи трансформації інформаційного простору. В інформаційних війнах цього типу мова йде про певну систему (концепції) нав'язування моделі світу, що покликана забезпечити бажані типи поведінки, про атаки на структури походження інформації - процеси міркувань.

Поняття інформаційної війни має досить багато визначень і з техніко-технологічної точки зору. Наприклад, у коридорах Пентагону

популярне таке жартівливе визначення «Інформаційна війна - це комп'ютерна безпека плюс гроші» [157].

У 1997 р. КНШ МО США додав до об'єктів нападу й оборони в інформаційній війні комп'ютерні мережі, мабуть через їхнє значне поширення у цей час і підвищену уразливість. У той же період МО США прийшло до висновку, що інформаційна війна може стати переважаючим і навіть вирішальним видом військового протиборства [79, с.2-9]. Збройні сили зможуть згодом здобувати перемогу над супротивником без окупації його території. Провідна роль належатиме діям із відстеження в реальному масштабі часу обстановки в будь-якому регіоні світу і точному наведенню засобів електронного ураження на будь-яку географічну точку земної кулі. Апробація таких способів ведення війни відбувається в сучасних локальних збройних конфліктах.

Можливості засобів радіоелектронної протидії достатньо відомі. В останні роки у їх розвитку відбуваються революційні зміни. Головний напрям прогресу в електроніці - комп'ютеризація. Тому особливо швидко і з вражаючими успіхами розробляються методи впливу на комп'ютерні системи. У кінці 1990 р. на замовлення ДАРПА (управління НДДКР Пентагону) була підготовлена доповідь "Комп'ютери в небезпеці" та зроблений висновок, що США стоять на порозі катастрофи в комп'ютерних мережах, а також було рекомендовано посилити заходи інформаційної безпеки. І ЦРУ, й АНБ досліджують можливості зараження інформаційно-технічних систем інших країн комп'ютерними вірусами, пастками, логічними бомбами і т.д. Для боротьби з подібними діями з боку інших держав у США створена служба "Комп'ютерно-вірусні контрзаходи" [167].

Цілком очевидно, що відповідні служби розвинених у галузі інформатики держав ведуть підготовку до "комп'ютерної війні", розробляють й апробують способи, прийоми впливу на комп'ютерні

системи. Відомості про це з'являються у пресі. У США існує Центр комп'ютерної безпеки (Пентагон), створений ще в 1981 р., є спеціально підібрані урядові групи експертів, які стежать за рівнем захищеності цілком таємних комп'ютерних систем. Немає сумніву, що ефективність комп'ютерного протиборства буде надзвичайно високою. Про це, наприклад, свідчить факт неможливості застосування Іраком проти багатонаціональних сил закуплених у Франції систем ППО. Їхнє програмне забезпечення містило логічні бомби, які були активізовані з початком бойових дій. Використанням такої бомби або вірусу, очевидно, можна буде досягати тих самих результатів, що й звичайним бомбардуванням органу державного управління, пункту (центру) бойового управління. Тому комп'ютерні системи державного управління та військового призначення (в першу чергу усі скільки-небудь важливі системи та мережі) будуть намагатися "замінувати" логічними бомбами, "заразити" вірусами, які чекатимуть своєї години.

На можливість того, що інформаційна складова військових дій у майбутньому стане переважаючою, вказують й англійські фахівці з інформаційної війни. Вони підкреслюють, що інформаційна перевага однієї армії над іншою, завдяки революції у військовій справі, дозволить з часом здобувати перемогу над ворогом, уникаючи фізичного зіткнення особового складу супротивників або роблячи це зіткнення дуже коротким й успішним. На їхню думку, війни майбутнього зможуть вигравати шляхом застосування виключно або майже виключно віддалених засобів ураження військових і цивільних електронних систем супротивника.

Такої ж позиції дотримуються й китайські військові фахівці. Китай вже давно включив термін «інформаційна війна» в лексикон своїх військових фахівців. Окрім цього, в документах КНР з'явився термін «інформаційний колоніалізм». Під цим китайськими фахівцями мається на увазі «експлуатація національного інформаційного простору іншими

країнами за рахунок повсюдного використання імпортних інформаційних технологій і високотехнологічної техніки й обладнання» [247]. Сьогодні Китай неухильно рухається до формування єдиної доктрини інформаційної війни.

Створення «мережевих сил» та розробка методів і способів ведення інформаційної війни (китайські військові теоретики вважають, вона «є прямим наслідком переходу від механізованої війни індустріального суспільства до війни рішень і стилю управління, війни знань та інтелекту») вже на офіційному рівні визначені Пекіном у якості одного з пріоритетних напрямків національного військового будівництва. Під «мережевими силами» маються на увазі компактні військові підрозділи чисельністю до батальйону, особовий склад яких буде досконало володіти передовими комп'ютерними технологіями. Фактично мова йде про формування в НВАК підрозділів «військових хакерів», які, як стверджують американські спецслужби, вперше з'явилися у 2000 році й у даний час можуть нараховувати до 1 млн. чоловік [247].

Фактично, якщо революція у військовій справі визначається як істотна зміна в технології, яка надає перевагу у військовому навчанні, організації, стратегії та тактиці бойових дій, то, можливо, Китай із усіх країн сьогодні зазнає справжньої революції в кіберпросторі.

За даними Контрольно-ревізійного управління Держдепартаменту Сполучених Штатів, за останні 15 років Китаю вдалося скоротити технологічне відставання від США в галузі мікроелектроніки та напівпровідникових технологій з 7-10 до 2 років і навіть менше. Мікроелектронна промисловість проголошена одним із пріоритетних напрямів забезпечення національної безпеки КНР, і в найближчі 5-10 років Пекін планує побудувати понад 20 сучасних заводів із виробництва напівпровідників (кожен вартістю більше 1 млрд. дол.), а з метою розвитку внутрішнього ринку мікроелектроніки в Китаї з'являться понад 50

високотехнологічних промислових зон за типом американської «Силіконової долини» [247].

Китайська концепція інформаційної війни включає в себе унікальні китайські уявлення про війну взагалі, засновані на сучасній концепції «народної війни», 36 стратегем великого Сун Цзи (згадані нами вище), а також на місцевих уявленнях про те, як воювати на стратегічному, оперативному й тактичному рівні. Багато що з його підходу має відношення до акценту на обмані, війні знань і пошуку асиметричних переваг над супротивником. Інформаційна війна визначена як «перехід від механізованої війни індустріального віку до... війни рішень і стилю управління, війни за знання та війни інтелекту» [59].

Точка зору британських фахівців у сфері інформаційної війни особливо не відрізняється від точки зору американських колег. Це визначення інформаційної війни як дій, що впливають на інформаційні системи супротивника, при одночасному захисті власних систем. Окрім того, Великобританія використовує юридичну структуру, засновану на існуючих законах, яка значною мірою може застосовуватися до дій у кіберпросторі - Regulation of Investigatory Powers Act (RIP), прийнятий в 2000 році. Він пропонує напади на інформаційні системи розглядати як звичайний кримінальний злочин із усіма послідуючими наслідками. Даний акт дозволяє британському уряду перехоплювати та читати електронну пошту, а також вимагати розшифровки особистих файлів на вимогу державних чиновників [50].

Аналіз понять інформаційної війни німецьких і канадських фахівців показує, що вони мало відрізняються від американських, англійських і китайських точок зору.

Проте, як вважають експерти французького Центру досліджень стратегічних технологій, діяльність європейських держав щодо збільшення власного потенціалу інформаційної зброї наштовхується на

серйозну протидію США. Прагнучи загальмувати власні розробки європейців, США навіть йдуть на продаж за демпінговими цінами космічних систем спостереження та контролю ліній зв'язку, надають доступ до накопичених баз даних. Таким чином США посилюють залежність союзників по НАТО від американських технологій.

Суть ще одного підходу до визначення інформаційної війни полягає в тому, що інформаційна війна трактується як сукупність політико-правових, соціально-економічних або аналогічних дій, які спрямовані на захоплення інформаційного простору, витіснення супротивника з інформаційної сфери, руйнування його комунікацій, позбавлення засобів передачі повідомлень, а також інші подібні цілі.

Ряд дослідників зводять інформаційну війну до окремих інформаційних заходів та операцій [27, с.9], інформаційних способів і засобів корпоративної конкуренції або ведення міждержавного протиборства або збройної боротьби [228, с.15; 210, с.252-253]. Термін «інформаційні операції» вперше з'явився в 1997 р. [48, с.79].

Г. Почепцов вважає, що «Інформаційна війна - це комунікативна технологія впливу на масову свідомість із короткочасними і довгостроковими цілями [177, с.20]. При цьому до комунікативних технологій Г. Почепцов відносить пропаганду, рекламу, виборчі технології, паблік рілейшнз [176, с.3].

Комунікативною технологією називає інформаційну війну і Д. Швець, який вважає, що «інформаційна війна - це комунікативна технологія впливу на інформацію та інформаційні системи супротивника з метою досягнення інформаційної переваги в інтересах національної стратегії, при одночасному захисті власної інформації та своїх інформаційних систем» [238. с.43].

На думку відомого фахівця в галузі дослідження інформаційних війн С. Расторгуєва, інформаційна війна не відрізняється від звичайної війни в

частині ознак поразки. Агресор домагається перемоги виключно підпорядкувавши собі структури управління супротивника, які є інформаційною мішенню [185, с.35-37]. Звідси, згідно С. Расторгуєву, випливають і основні напрямки організації захисту: зменшення розміру мішені, захист мішені; регулярне знищення «інформаційних бур'янів»; установка власного жорсткого контролю за власною системою управління. Як вважає С. Расторгуєв, стратегія застосування інформаційної зброї носить виключно наступальний характер. Цей дуже важливий результат, який ще не до кінця усвідомлений науковою громадськістю, дозволяє вийти на твердження про те, що наступальний характер інформаційної зброї багато в чому визначає обличчя інформаційної війни та дозволяє визначити потенційного агресора. Таким чином, можна припустити, що обсяг інформації, який цілеспрямовано передається з однієї країни в іншу, і є мірою інформаційної агресивності.

В. Пірумов, ще один відомий фахівець у цій галузі, визначає інформаційну війну як нову форму боротьби двох і більше сторін, яка полягає в цілеспрямованому використанні спеціальних засобів і методів впливу на інформаційні ресурси супротивника, а також захисті власного інформаційного ресурсу для досягнення намічених цілей. На його думку, в мирний час інформаційна війна носить переважно прихований характер. Її основним змістом є ведення розвідувальних і політико-психологічних дій по відношенню до супротивника, а також здійснення заходів щодо власної інформаційної безпеки. У загрозливий період, як вважає В. Пірумов, з'являються додаткові завдання, які вирішуються в інтересах забезпечення необхідної ефективності планованих бойових дій. До особливостей ведення інформаційної війни в цей період можна віднести граничну обмеженість у використанні сил і засобів інформаційної війни; дотримання існуючих норм міжнародного права (наприклад, заборона, радіоелектронного придушення певних частот і систем, передбачених

Статутом Міжнародного союзу електрозв'язку та Регламентом радіозв'язку) і т.д. З початком військових дій сили та засоби інформаційної війни вирішують такі завдання, як масований вплив на інформаційний ресурс супротивника та запобігання зниженню бойових можливостей своїх сил, проведення заходів щодо зниження рівня морально-психологічної стійкості військ супротивника і забезпечення нейтралізації інформації, що впливає на морально-психологічний стан свого особистого складу; ведення розвідувальної діяльності, забезпечення скритності найважливіших заходів своїх військ і т.д. [173, с.44-47].

З розвитком психології виявлялися все нові механізми маніпуляції людьми. З'явився цілий напрям військових і політичних технологій, заснованих на спотворенні інформації. Проте лише масове поширення Інтернету дозволило отримати універсальний спосіб впливу на психіку індивіда. Інтернет став центральною ланкою ланцюга, який з’єднав інформаційну та психологічну війни. Наприклад, комп'ютер комітету Республіканської партії США не тільки збирав і обробляв інформацію, а й безпосередньо впливав на виборців. Через автоматизовану телефонну систему цей комп'ютер зв'язався з 25 млн. абонентів у різних штатах, закликаючи їх голосувати за певні кандидатури. Питання впливу інформації на політичну владу та її розподіл є, мабуть, центральним у західному політичному житті. Можна стверджувати, що за рахунок концентрації інформації, більш широких можливостей її використання відбувається посилення виконавчої влади, влади державного апарату в порівнянні з владою виборних представників. Використання комп'ютерних мереж розширює можливості апарату в маніпулюванні масами [167].

Поширення свідомо використовуваних засобів переконання людей стало яскравою особливістю XX століття, особливо його післявоєнного періоду. Як зазначає Ф. Уебстер, методи управління за допомогою інформації формувалися в період між двома світовими війнами. Методи ці

ставали все більш і більш популярними. «Всі три основні риси управління за допомогою інформації - надання інформації штучного глянцю, залякування та цензура, - не кажучи вже про режим секретності, який представляє іншу сторону тієї ж медалі, особливо чітко проявляються під час кризових ситуацій» [212, с.268].

Інформаційна війна - це техніка, використовувана для впливу на цільову аудиторію з метою зміни поведінки людей у потрібну для ініціаторів сторону. Для досягнення цієї мети об'єктами впливу та трансформації стають емоції, системи цінностей і вірувань, умовиводи й аргументи, аж до підміни у свідомості об'єкта впливу одних фактів (безперечних суджень) на інші. Ініціаторами подібних операцій можуть бути як різні відомства держав, так і приватні установи, неурядові організації, впливові політичні групи, у тому числі ті, які спонсорують тероризм і екстремізм. У свою чергу об'єктами впливу можуть ставати як широкі верстви простих громадян, так і більш вузькі групи національних еліт, які володіють ключовими позиціями і впливом [64].

Інформаційна зброя здатна ефективно впливати й на психіку, свідомість людей, і на інформаційно-технічну інфраструктуру суспільства й армії. В даний час створено багато нових засобів впливу на психіку людей, управління їхньою поведінкою. Правда, за даними зарубіжних джерел, стійких і прогнозованих способів управління колективною поведінкою людей поки не знайдено, але такі дослідження ведуться. У пресі періодично з'являється інформація про американську програму "МК-Ультра", а також про аналогічні програми у Франції, Японії й інших країнах. Досягнення в цій галузі такі, що вже зараз можна говорити про ефективність зомбування (програмування поведінки, діяльності) окремих людей. З цією метою створені та використовуються не тільки фармакологічні засоби, а й психотропні генератори [167].

Ще один підхід виходить із того, що інформаційна війна - це явище зовні мирного періоду міждержавного протиборства, що дозволяє вирішувати зовнішньополітичні завдання несиловим у традиційному розумінні шляхом. Як приклад можна навести промову Президента США Б. Клінтона, який, виступаючи на нараді начальників штабів, сказав: «Використовуючи помилки радянської дипломатії, надзвичайну самовпевненість Горбачова та його оточення, в тому числі тих, хто відверто зайняв проамериканську позицію, за допомогою вміло застосованого електронно-інформаційного впливу ми домоглися того, що збирався зробити президент Трумен із Радянським Союзом за допомогою атомної бомби. Правда, з однією істотною відмінністю - ми отримали сировинний придаток, а не зруйновану атомом державу...» [219, с.14].

Інформаційна війна розглядається як комплексна стратегія досягнення інформаційної переваги при протиборстві в конфлікті шляхом впливу на інформаційне середовище супротивника при одночасному забезпеченні безпеки власного інформаційного середовища. Дослідники вказують на деякі характерні риси інформаційної війни: універсальність (може застосовуватися на різних рівнях - від особистісного до міжнародного, і при використанні різних засобів); завуальованість (суб'єктові інформаційної війни не завжди очевидний деструктивний вплив, таку війну необов'язково оголошувати); масштабність (чим більше розвинені інформаційні технології, тим масштабніша шкода від подібної війни, тим більше об'єктів у неї залучені); перманентність (ведеться і в мирний час, і, власне, у воєнний); превентивний, попереджувальний характер (по суті, будь-який конфлікт починається з інформаційної війни, а далі вже може йти безпосередньо «фізичний» вплив, знищення) [68, с.261].

Ряд американських аналітиків, які спеціалізуються в галузі так званих «оборонних досліджень», у 1990-ті - на початку 2000-х рр.

сформулювали принципово новий підхід щодо оцінки ролі «інформаційної війни» у сфері сучасної міждержавної геополітичної боротьби. Ці фахівці, як можна зрозуміти, констатували ідею про те, що в реаліях постбіполярного світу значимість фактора «інформаційного протиборства» посилилася настільки, що власне «інформаційна війна», яка виступала в роки «холодної війни» лише як просто метод впливу на супротивника, на межі XX - XXI ст. фактично перетворилася на повноцінну та «функціонально оригінальну» концепцію ведення геополітичної боротьби на міждержавному рівні. Наприклад, подібну тезу особливо активно стали відстоювати співробітники провідного американського аналітичного центру корпорації РЕНД Дж. Аркуілла та Д. Ронфельдт, які вважаються одними з найбільш авторитетних американських експертів-теоретиків у галузі інформаційних технологій. Ці дослідники для позначення даної «бойової» технології використовували поняття «мережева війна» [230, с.35].

Авторами терміну «мережна війна» є співробітники RAND Corporation Дж. Аркуілла і Д. Ронфельдт, які хотіли показати специфіку нетрадиційного, менш воєнізованого та інтенсивного, більш соціального полюсу конфліктного спектру. Вперше цей термін був згаданий ними в журнальній статті «Гряде кібервійна!». Концепція мережевої війни була детально розроблена в доповіді корпорації РЕНД «Напередодні мережевої війни». Вона була проілюстрована дослідженням повстання сапатистів у Мексиці і, нарешті, переформульована на основі аналізу досвіду недержавних організацій, які застосовують мережні стратегії у своїй політичній діяльності [254, p. 275-279].

На відміну від інформаційної війни мережевій війні притаманні нелінійність, множинність і різноманітність. Завдяки зниженню витрат, таких, наприклад, як вартість мережевих комп'ютерних технологій, значно розширюється коло її потенційних учасників. У підсумку, на одній стороні

барикад можуть опинитися держави, не здатні вступити у відкриту боротьбу з лідируючими в технологічному й військовому відношенні країнами світу, недержавні організації, наркокартелі та злочинні транснаціональні синдикати, приватні корпорації, екстремістські та терористичні мережі, глобальні ЗМІ і навіть міжнародні фінансові спекулянти й харизматичні авантюристи. Кожен із компонентів подібної багатовимірної коаліції буде переслідувати власні політичні чи економічні інтереси, діючи асинхронно, можливо, без єдиного стратегічного плану, десь множачи спільні зусилля, десь роздроблюючи їх. Це приклад нелінійної, нерівновагової, «складно дезорганізованої» системи, в якій нестабільність на одному рівні може поєднуватися з тимчасовою стабільністю на іншому. Запорука успіху такої коаліції не в традиційному («Вестфальському») «балансі сил», а в умінні забезпечити правильну комбінацію гравців у потрібний час і в потрібному місці [263].

Академічне співтовариство визнало концепцію мережевої війни не так давно, приблизно у 1997-1998 роках, коли її дослідженням зайнялися такі відомі вчені, як М. Кастелс, Г. Клівер і Д. Брин. Поняття мережевої війни вони розглядали при аналізі переважно невійськових, соціальних конфліктів. Дане поняття використовується і практиками мережевих рухів, такими як голова мексиканських сапатистів субкомандante Маркос, лідер Міжнародної кампанії за заборону протипіхотних мін, лауреат Нобелівської премії миру Дж. Вільямс.

У науковій літературі останнім часом використовується поняття «кібервійна». Поняття це поки що перебуває в процесі розробки, який розділений на два напрямки. Суть першого напрямку в тому, що кібервійни розглядаються як розвиток і поширення інформаційних технологій у військовій галузі, являючи собою високоточну зброю, технології "стелс", бойові та розвідувальні радіоелектронні засоби і навіть футуристичні розробки у сфері роботизації й автоматизації. Інший напрям

досліджень розуміє кібервійни як елемент інформаційних війн, здійснюваний за допомогою всесвітньої павутини. Г. Акопов визначає кібервійну як інформаційне протиборство з використанням інформаційно-комунікаційних комп'ютерних мереж загального користування для досягнення поставлених цілей і завдань [5].

Поняття кібервійни розвиває й уточнює здійснювані раніше спроби концептуалізації природи військового конфлікту в епоху інформаційної революції (комп'ютеризована, автоматизована, роботизована або електронна війна) і використовується для опису відносно традиційного полюсу конфліктного спектру, представленого такими категоріями, як "великий регіональний конфлікт", "збройний конфлікт високої інтенсивності", "військово-політичний конфлікт". При цьому понятійна специфіка визначається переважно за рахунок акцентування інструментальних аспектів ведення конфлікту при збереженні багато в чому традиційних суб'єкт-об'єктних і цільових характеристик [210. с.24].

Кібервійни можуть мати різні цілі та завдання. Найпоширеніші з них: розміщення в мережі "Інтернет" завідомо неправдивої або провокаційної інформації для її подальшого поширення в ЗМІ та мережевому співтоваристві; маніпулювання суспільною свідомістю, нав'язування необхідної ідеології (вплив на громадську думку); вербування прихильників і рекрутування однодумців; несанкціонований доступ до інформаційних ресурсів із подальшим їх спотворенням або розкраданням; підрив міжнародного авторитету держави; вплив на прийняття політично значущих рішень; створення атмосфери бездуховності й аморальності, негативного ставлення до культурної спадщини; дестабілізація політичних відносин у суспільстві; поширення компромату й інших відомостей, що ганьблять честь і гідність політичної еліти країни, створення атмосфери напруженості між партіями, громадськими об'єднаннями та рухами; політичний або інший шантаж; розпалювання міжнаціональної ворожнечі

та расової нетерпимості; вплив на економічну інфраструктуру державної освіти; ініціювання масових заворушень та інших акцій протесту [5].

Відповідно до концепцій кібернетичної та мережевої війни досягнення інформаційної переваги можливе за рахунок широкого впровадження нових технологій у системи бойового управління та зв'язку і, що особливо важливо, за рахунок удосконалення військової організації.

Ряд авторів, серед яких Г. Ємельянов та А. Стрельцов, вважають, що інформаційна війна - це особливий вид відносин між державами, при якому для вирішення існуючих міждержавних протиріч використовуються методи, засоби та технології силового впливу на інформаційну сферу цих держав [77, с.34]. Проте думається, що сучасна політична практика вказує на те, що технології інформаційної війни використовуються не тільки в зовнішній, але вже й у внутрішній політиці держави. Так, наприклад, Е. Тоффлер у своїй книзі «Метаморфози влади» пише про інформаційні війни, починаючи від рівня супермаркету до міждержавних відносин [208, с.17-21].

Отже, незважаючи на різні тлумачення поняття «інформаційна війна», очевидно, що основна ознака цього типу кампаній - гостра, агресивна взаємодія протиборчих сторін в інформаційній сфері, яка негативно відбивається на стані політичних комунікацій суспільства в цілому. Застосування таких кампаній політичними акторами пов'язане з наростанням ризиків, результатом яких може стати швидка зміна статусів і позицій у відносинах влади. Через високу інтенсивність суперечки інформаційні війни погано піддаються управлінню та свідомому регулюванню і тому виступають як двосічна зброя для протиборчих сторін. Досягнення цілей подібними способами посилює політичну конфронтацію, знижує можливості поширення консенсусної культури, підриває стабільність у суспільстві.

Таким чином, під інформаційною війною розуміється інформаційне протиборство з метою нанесення збитку критично важливим структурам супротивника, дестабілізації його політичної та соціальної системи. Психологічна війна - це прихований вплив на свідомість усього населення або його окремих категорій, здійснюваний спеціальними методами спотворення інформації або іншими технологіями, які впливають на процеси сприйняття світу та відключають раціонально-критичний рівень осмислення зовнішніх подразників.

Наявність такого розмаїття визначень кіберпростору, у свою чергу, відображає всю складність визначення "кібервійни" (Cyber Warfare). Визнаючи, що військові операції в кіберпросторі могли б розглядатися у якості "акта війни", ряд експертів США та Великобританії пропонує при аналізі широкого спектру військових операцій у кіберпросторі замість терміну "кібервійна" використовувати термін "бойові операції в кіберпросторі" (Cyber Warfare Operations). А для кібервійни між державами поза станом офіційно оголошеної війни вони запропонували наступне визначення: «використання мережевих можливостей однієї держави для викривлення, порушення цілісності, деградації, маніпулювання або знищення інформації, що постійно знаходиться в комп'ютерах або циркулює в комп'ютерних мережах, або власне комп'ютерів і мереж іншої держави» [165].

Аналіз наукової літератури, присвяченої проблемам інформаційної війни, показує, що одні дослідники надають перевагу терміну «інформаційна війна», інші - «інформаційне протиборство». Чи є суттєва різниця між цими поняттями? Наприклад, Г. Перепелиця вважає, що різниця полягає в тому, що поняття «інформаційне протиборство» доречне для мирного часу, а «інформаційна війна» - для військового часу [168].

Як випливає з вищевикладеного, поняття «інформаційна війна» поширюється не тільки на політичну, а й на економічну, та соціальну

сфери життя. А значить, є актуальним уточнення поняття «інформаційна війна» в політичному аспекті.

«Інформаційним війнам у XXI столітті властивий високий ступінь публічності: їх відгомони чутні в різних куточках світу. Ступінь публічності може бути різний залежно від обсягу розповсюджуваних відомостей, можливостей мас-медіа впливати на політику. Звичайно, взаємні претензії, навіть образи, виражені публічно, ускладнюють пошук компромісів, шляхів до примирення, і політичні лідери ясно усвідомлюють це. Однак якщо суб'єкт політики не розраховує на швидке примирення в конфлікті, так на що ж він сподівається? Ініціюючи протистояння у сфері інформації, актор робить спробу використати канали політичної комунікації з найбільшою ефективністю, з тим щоб він був почутий громадянами країни, регіону чи міста і щоб вони розділили його думку як діючого суб'єкта, який у гострій боротьбі нібито відстоює виключно їхні інтереси.

Суб'єкти політики отримують безсумнівну вигоду в інформаційній війні, в якій проявляється висока прихильність учасників до групових цілей» [74].

Незважаючи на наявне розмаїття визначень, визначень інформаційної війни в політичній сфері не так уже й багато. Одне з них: «інформаційне протиборство в політиці представляється як конкурентна взаємодія суб'єктів політики, при якій вони прагнуть нанести шкоду один одному за допомогою інформаційних й інших засобів і способів впливу при одночасному прагненні захистити об'єкти власної інформаційної інфраструктури та інформаційного простору», автором якого є російський дослідник О. Горбенко. Він сформулював основні цілі інформаційного протиборства в політиці: а) досягнення інформаційної переваги над протиборчою стороною; б) недопущення інформаційної переваги з боку ймовірних супротивників або основних конкурентів; в) захист

інформаційних ресурсів і суспільної свідомості від негативного інформаційного впливу [51, с.8].

В. Євдокимов пропонує таке визначення інформаційної війни, яка ведеться в політичному процесі. На його думку, це сукупність засобів впливу, спрямованих на поширення правдивих і неправдивих відомостей із метою дестабілізації системи управління супротивника, придушення його в сфері комунікацій, витіснення суперника з інформаційного простору та нанесення найбільшої шкоди його соціально-політичним інтересам [74, с.110] .

Російський дослідник К. Будилін виділяє фактори, які впливають на зміст інформаційної війни. У першу чергу, це політичний фактор, який «визначає: причини її виникнення та шляхи запобігання; засоби, способи й особливості ведення; розмах і тривалість; забезпечення матеріальними та фінансовими ресурсами. Економічний фактор має великий вплив на вибір засобів інформаційного протиборства. Від економічного розвитку залежить рівень інформатизації суспільства й держави, а значить, і ефективність ведення інформаційного протиборства як у мирний, так і у воєнний час.

Духовний фактор чинить вирішальний вплив на реалізацію положень теорії інформаційного протиборства. Загальна та професійна підготовка обслуговуючого персоналу інформаційних систем, його морально-політичний і психологічний стан, готовність до самовідданого захисту інтересів своєї країни мають першорядне значення при реалізації завдань інформаційного протиборства.

Військовий фактор формує зміст інформаційного протиборства, виходячи з вимог військової доктрини держави, концепцій війни та можливостей протиборчої сторони, а також стан і перспективи розвитку засобів інформаційного протиборства» [28, с.11-12].

Висновки до розділу 1

Високо оцінюючи внесок вітчизняних і зарубіжних учених, які здійснили значну дослідницьку роботу в галузі теоретичного вивчення й осмислення процесів інформаційного впливу та взаємодії у сфері політики взагалі та інформаційної війни зокрема, слід зазначити, що політична інформаційна війна поки ще не стала об'єктом комплексних теоретико-методологічних досліджень. Науковий пошук в основному ведеться за декількома суміжними, але недостатньо пов'язаними між собою

напрямками; при цьому вивчаються лише окремі сторони процесів інформаційної війни, їхні поодинокі аспекти.

Дослідження еволюції інформаційної війни показало, що даний феномен веде свою історію з моменту виникнення людства. Ще в давні часи мали місце спроби дезінформувати супротивника, залякати його та підірвати тим самим бойовий дух. Мистецтво керувати думками та вчинками людей розвивалося і використовувалося як секретна зброя правителями Шумеру, Вавилону, Стародавнього Єгипту, Китаю, Стародавньої Греції та Риму. У працях Геродота, Плутарха, Юлія Цезаря можна зустріти опис деяких прийомів, які дозволяють підірвати волю до опору, викликати зраду або спровокувати паніку.

Розглянувши основні наявні визначення поняття «інформаційна війна», автор приходить до висновку, що в даний час це поняття все ще носить публіцистичний характер і ще не отримало повсюдного визнання в українських і зарубіжних наукових колах. Незважаючи на те, що в науковій літературі використовується досить багато різних формулювань інформаційної війни, їхні явні переваги та настільки ж явні недоліки не дозволяють віддати однозначну перевагу будь-якій з них. Однак усі разом ці визначення достатньо повно виділяють із усілякого різноманіття існуючих у сучасному суспільстві взаємин ті соціальні явища, взаємовідносини та процеси, які можна виділити в окрему групу з умовною назвою «інформаційна війна».

Дослідивши безліч наявних визначень інформаційної війни, можна зробити висновок, що дане поняття використовується не тільки для характеристики діяльності військово-політичного керівництва держав, а й для характеристики діяльності засобів масової інформації та комунікації, конкуренції в економіці, групових і міжособистісних відносин. Тому виникла необхідність уточнити поняття «інформаційна війна» в контексті політики. У зв'язку з цим доцільно використовувати поняття «політична

інформаційна війна», під яким слід розуміти сукупність взаємовідносин між суб'єктами політичного простору, в рамках яких дані суб'єкти з метою вирішення своїх політичних завдань (розв'язання суперечностей з приводу влади та здійснення політичного управління в інформаційно-психологічному просторі) активно впливають на інформаційну сферу один одного та протидіють аналогічній діяльності протиборчої сторони за допомогою програмно-технічних, радіоелектронних й інформаційно-психологічних засобів. Таким чином, поняття інформаційної війни трактується не тільки через засоби та методи, а й через характер завдань і взаємин учасників - суб'єктів політичного простору.

Визначене співвідношення понять «інформаційна кампанія» й «інформаційна війна». Встановлено, що інформаційна війна є найбільш поширеним типом інформаційної кампанії. Під інформаційною кампанією розуміється заздалегідь спланований комплекс взаємопов'язаних комунікаційних дій, спеціально розроблених для забезпечення конкретних цілей комунікатора шляхом цілеспрямованого впливу на громадську думку та позиції контрагента. Інформаційна війна - це найбільш гостра форма конфронтації в інформаційному просторі.

Зроблено висновок про те, що поняття «інформаційна війна», «інформаційне протиборство» є синонімами, оскільки в перекладі з англійської мови (information and psychological) означають, по суті, одне й те ж саме.

Уточнено структуру інформаційної війни: це технологічна складова, спрямована на руйнування технічних систем зв'язку та комунікацій, і гуманітарна складова, мета якої - вплив на свідомість людей.

У науковій літературі виділяється два напрями в інформаційній війні: інформаційно-технічний та інформаційно-психологічний. В інформаційно-технічній війні головними об'єктами впливу та захисту є

інформаційно-технічні системи (системи зв'язку, телекомунікаційні та комп'ютерні системи, радіоелектронні засоби й т.д.).

В інформаційно-психологічній війні головними об'єктами впливу, а, отже, й захисту є психіка військово-політичного керівництва, особового складу збройних сил, спецслужб і населення, а також системи формування громадської думки та прийняття рішень.

РОЗДІЛ 2
ІНФОРМАЦІЙНА ВІЙНА В СУЧАСНІЙ ПОЛІТИЧНІЙ ПРАКТИЦІ

Як стверджує один із авторів доповіді «Віртуальна криміналістика», дослідник Оксфордського інституту інтернету Айан Браун, вже сьогодні більше 120 країн тим чи іншим чином активно залучені в комп'ютерне протистояння або зайняті кібершпіонажем через всесвітню павутину. Тому в даному розділі досліджуємо досвід найбільш розвинених з точки зору

технологій інформаційної війни зарубіжних країн. Враховуючи, що будь-яка війна має політичну мотивацію, розглянемо її зміст. Також розглянемо роль засобів масової комунікації в інформаційній війні, оскільки вони служать провідниками найбільш стійких уявлень, що вкорінюються як усередині країни, так і за її межами. Таким чином, особливо важливо, щоб ЗМІ слідували поведінковим стандартам, починаючи з елементарних понять і форм мовленнєвої культури.

2.1. Досвід зарубіжних країн у розвитку технологій політичної інформаційної війни

У другій половині XX ст. розвинені демократичні країни пережили дві революції у сфері доступу громадян до інформації, результатом яких стали масова освіта і масове телебачення. Визначну роль у перетворенні політичного простору зіграли поява на інформаційному політичному ринку електронних ЗМІ, виникнення діалогових способів політичної комунікації, різке збільшення швидкості передачі повідомлень, формування «електронних спільнот» (наприклад, користувачів Інтернет) та ін. Ці та пов'язані з ними явища й факти якісно змінили умови і можливості конкуренції за державну владу. Звичайно, як вважає Липпман, інформаційні засоби були не здатні «транслювати весь обсяг суспільного життя людства, так щоб кожен індивід міг винести компетентну думку з кожного питання» [261, p.362]. Більше того, інформаційні технології зробили свій внесок у занепад суспільного капіталу, оскільки теле-відео-аудіо-мультимедіа розваги дозволяли людям задовольняти свої потреби в

емоціях і адреналіні не виходячи з дому, сприяючи пасивному сприйняттю людьми інформації, скороченню ресурсів зворотного зв'язку й т. д.

Тим не менш, активно проникаючи в сферу політики, нові інформаційні та комунікативні технології не тільки якісно видозмінили, але й зламали багато старих уявлень, установок, стереотипів, форм поведінки, моделей взаємовідносин між індивідами та групами, політичними інститутами і структурами. «При цьому ствердження, що сучасні комунікаційні технології допомагають встановити нові дружні зв'язки між людьми, яких розділяють культурні бар'єри, державні кордони та фізичні відстані, маскує безперервну боротьбу між провідними державами світу за встановлення власного домінування в інформаційному просторі і право розповсюдження необхідних соціально-політичних концепцій серед населення як своєї країни, так і інших держав» (використання за кордоном мережі Інтернет в інтересах ведення інформаційних війн) [92].

Як висловився віце-президент американського Інституту вивчення тероризму і політичного насильства, в минулому - аналітик Міністерства оборони США П. Пробст: «Розвиваючись, держави все більшою мірою стають залежними від високих технологій. Комплексні національні системи являють собою потенційну небезпеку, тому що мають життєво важливі вузли, удар по яких може призвести до руйнівних наслідків. Така атака може бути здійснена комп'ютерним шляхом або з використанням вибухівки, або шляхом виведення з ладу кабелів із метою викликати ланцюг аварій із підсумковим колапсом усіх контрольних систем трубопроводу або аеропорту» [111, с.10].

А співробітник вашингтонського Центру міжнародних і стратегічних досліджень У. Лакер вважає, що «...втручання комп'ютерних хакерів може зробити всю країну нездатною до нормального функціонування. Звідси зростаюча тривога з приводу можливостей інформаційного тероризму і

кібервійни... достатньо 20 кваліфікованих хакерів і одного мільярда доларів, щоб знищити Америку» [260, p.35].

Як зазначається в науковій літературі, поняття хакерської боротьби зводиться головним чином до здійснення «атак» на різні компоненти комп'ютерних мереж і інформаційні ресурси, що зберігаються в них. Основною особливістю хакерських «атак» є те, що вони носять не апаратний, а програмний характер. Це означає, що використовувана хакером програма проникнення здатна виявляти вразливе місце в структурі захисту комп'ютерної системи супротивника та проникати через неї, що в результаті дає можливість керувати працездатністю системи або маніпулювати (стирати, змінювати) інформацією, що міститься в ній [91, с.45]. Так, зовсім нещодавно, в липні 2011 р. стало відомо, що хакери з групи Anonymous зламали сервер підрядника Пентагону - компанії Booz Allen Hamilton - і вкрали адреси електронної пошти більше 90 тисяч американських військових. При цьому хакерам, можливо, дісталися й паролі від пошти. Небезпека, яка відтепер загрожує Пентагону, полягає в тому, що хакери можуть спробувати, використовуючи електронну пошту, заразити вірусами комп'ютери військових. У 2010 році хакери з групи Anonymous атакували сайти Visa, Mastercard і Paypal, що блокували перекази для сайту WikiLeaks, який опублікував тисячі секретних документів американського уряду. В останні місяці ймовірні члени групи були арештовані в Іспанії, Туреччині й Італії.

Деякі західні аналітики, наприклад, В. Швартау і Р. Хаєні, схильні навіть вважати, що інформаційне протистояння в цілому може бути зведене виключно до хакерської боротьби [20, с.16].

Експерти Пентагону поділяють прийдешню арену військових дій на традиційний простір і кіберпростір, який у нових війнах буде відігравати вирішальну роль [60, с.5].

Р. Багіров правомірно зауважує, що під впливом сучасних політичних комунікацій відбуваються фундаментальні зрушення в соціокультурних характеристиках війн і збройних конфліктів. «Образ війни як запеклого збройного протиборства тьмяніє на тлі образів нанотехнологічної, психологічної, інформаційної, консцієнтальної (війна свідомостей) і преємптивної («перероблення націй») війн. Світ вступає в новий етап боротьби як конкуренції форм організації свідомостей, де предметом поразки та знищення є певні типи свідомостей.

Найважливішим об'єктом сучасних і особливо майбутніх війн стають менталітет націй, духовні основи армій, віра, ідеологія, історія, патріотизм, культура. Звідси зрозуміла та увага, яку розвинені країни приділяють питанням інформаційної складової військової безпеки, захисту свого способу життя» [16, с.10]. Результати останніх досліджень у сфері міжнародного Інтернет-спілкування свідчать про те, що уряди деяких країн, активно використовуючи потенціал інформаційних технологій для розпалювання ненависті між представниками різних рас і релігійних конфесій на інформаційному просторі країн, що входять у сферу їхніх інтересів, остаточно втратили контроль над власною програмою і спровокували вибух націоналістичних ініціатив окремих людей і груп по всьому світу. Так, у 2005 році словацькі націоналісти тлом своєї сторінки в Інтернеті обрали карту Європи, на якій була відсутня Угорщина. У 2007 році в одній із угорських Інтернет-спільнот провели конкурс на кращий антициганський плакат. Іншим прикладом є створення неповнолітнім китайцем у 2006 році сайту, на якому були зібрані матеріали, що підтверджують антикитайську спрямованість західних засобів масової інформації [92].

Слід погодитися з В. Цигановим, що основна мета інформаційних війн полягає в оволодінні капіталом і владою. У свою чергу, системи та механізми оволодіння капіталом і владою складають предмет теорії

управління еволюцією організації, яка й утворює фундамент теорії інформаційних війн. [226].

Військові фахівці вважають, що сьогодні загроза початку «комп'ютерних війн» («кібервійни») досить реальна і вимагає постійного і дуже серйозного ставлення до неї. Це підтверджується відомими фактами регулярних вірусних і хакерських атак на комп'ютерні мережі США та інших країн. Як вважають експерти, останній напад на комп'ютерні мережі Пентагону, найімовірніше був спланований і проведений спеціально з метою їхнього масштабного ураження. Ці та інші факти лише підтверджують розмови про початок «комп'ютерних війн». За оцінками фахівців, у такій війні переможеною може виявитися навіть та держава, яка володіє військовою міццю, що перевершує міць супротивника [34].

Інформація перетворюється на стратегічний ресурс, значимість і вплив якого можна порівняти з роллю капіталу і праці в індустріальну епоху. Питання володіння, розподілу та контролю над інформацією з неминучістю зміщуються в зону владних відносин і, як наслідок, у площину політичного конфлікту. Сьогодні вже цілком очевидно, що інформаційна революція здатна принципово змінити як цілі, в ім'я яких те чи інше співтовариство вступає в конфлікт, так і форми та засоби їх досягнення [210, с.26].

Кожна нова епоха передбачає висунення провідної парадигми світопорядку. Для періоду інформаційної революції однією з парадигм став постмодернізм, який розглядає в якості ознаки виникнення глобального інформаційного простору масову появу симулякрів. Постмодернізм і його прояви в мас-медіа підтверджуються багатьма фактами виборчих технологій, висвітлення військових, національних й інших конфліктів, створення іміджу влади та іншими PR-стратегіями.

К. Олехнович вважає, що в просторі «постмодерну» захиститися можна, тільки використовуючи адекватні методи - методи «мережевих

війн». Цей автор зазначає, «що ні наявність багатомільйонної армії, ні ядерна зброя, ні спецслужби «старого зразка» не гарантують надійного захисту. Повернути ефективність і дієвість зброї минулої історичної епохи - індустріальної - можна тільки одним єдиним способом. Для цього необхідно в масштабах планети знищити технологічну інфраструктуру глобальних комунікацій. Навряд чи це реальна перспектива, за винятком, звичайно, есхатологічного сценарію глобальної «ядерної зими». Таким чином, єдиний варіант захисту при неможливості, як повної самоізоляції від глобального інформаційного співтовариства, так і фізичного знищення його технологічної інфраструктури, - це підключення до вже існуючої мережі, але не в якості пасивного об'єкта, а активно діючого суб'єкта. Органи влади, політичні партії та рухи, що виступають із позицій державного патріотизму, повинні вивчити парадигмальні закони постмодерну не гірше його творців і архітекторів та використовувати їх для захисту власного права на культурну і цивілізаційну ідентичність, геополітичну суверенність у рамках певного сегменту багатополярного світу. Необхідне підвищення PR-компетентності органів управління, що являє собою єдність діагностичної, прогностичної та програмуючої комунікативно-технологічної діяльності» [155, с.9].

Як вважає П. Шариков, «Інформаційний простір глобальний, у ньому практично не існує ніяких кордонів національного інформаційного простору. Тим не менше, в інформаційному протиборстві перевага буде у тієї сторони, яка доб'ється інформаційної переваги - панування в інформаційному просторі космічних систем і засобів розвідки, попередження, навігації, метеорології, в управлінні зв'язком» [233, с.4].

У багатьох країнах розробляються стратегії ведення віртуальної війни, між ними йдуть перегони кіберозброєнь, які створюються з метою виведення з ладу державних комп'ютерних мереж і об'єктів життєзабезпечення. Такі кібератаки можуть призвести до істотних

руйнувань і загибелі багатьох людей - це не просто війна комп'ютерів, віртуальна боротьба може обернутися реальними жертвами [132]. «Кібервійна вже почалася. В очікуванні ворожих дій багато держав заздалегідь готують поле бою... засилають хакерів один до одного, готують чорні ходи та закладають логічні міни... у мирний час. Кібервійна, що ведеться зараз, змішує звичні поняття війни і миру, додає новий небезпечний вимір до світової нестабільності», стверджує у своїй новій книзі Ричард Кларк, колишній радник президента США Б. Клінтона з кібербезпеки [165].

Як відзначає О. Горбенко, інформаційне протиборство, будучи невід'ємною складовою політичних відносин, виступає одним із основних інструментів політичного примусу в сучасних умовах. Тому не випадково воно пронизує всі форми політичної боротьби. Іншими словами, інформаційне протиборство вже не обмежується широкомасштабним впливом на населення і війська, а активно націлюється на вищі ешелони влади та суспільну свідомість держав-супротивників і партнерів, на системи прийняття державних рішень у різних сферах життєдіяльності. Політичні актори, перебуваючи в стані жорсткої конкуренції (або конфлікту), безперервно обмінюються інформаційними впливами, які стають все більш витонченими та небезпечними [52, с.25].

Збільшення кількості політично вмотивованих атак протягом останнього року все більше турбує світову громадськість. Так, наприклад, відомо, що цифровий світ жорстко протистоїть США у відповідь на політику, яка проводиться по відношенню до Іраку і підтримки Ізраїлю. В результаті, кібератаки були спрямовані проти таких значущих об'єктів як Білий Дім, Міністерство національної безпеки, Секретна Служба та Міністерство оборони. Ще одне підтвердження цьому - поява нового хробака VBS/Nedal (Laden навпаки). Для свого поширення хробак використовує текст, пов'язаний із сумними подіями 11 вересня 2001 р. у

Нью-Йорку. VBS/Nedal - руйнівний шкідливий код, що знищує вміст виконуваних файлів. Він поширюється через електронну пошту, розсилаючи себе кожному адресату, знайденому в адресній книзі Microsoft Outlook на зараженому комп'ютері. Тема інфікованого листа: "Osama Bin Laden Comes Back!" (Осама Бен Ладен повертається). У тілі листа знаходиться текст, який закликає стерти з лиця землі Ізраїль і США [50].

Не приховують своїх намірів використовувати Інтернет у якості засобу для здійснення своїх терористичних акцій проти Заходу й ісламські фундаменталісти. Вони вивчають усі види високих технологій, щоб із метою електронного джихаду використовувати найсучасніші досягнення. У планах терористів центральне місце займає руйнівний вплив на національні інфраструктури. Як заявив один із лідерів злочинних угруповань Близького Сходу: "...Дуже скоро світ стане свідком атак на фондові біржі Нью-Йорка, Лондона і Токіо". Це є підтвердженням того, що проблема кібертероризму є глобальною. Групи джихаду розкидані по всьому світу, й у своїй діяльності активно використовують Інтернет. Неодноразовими стають заяви, про те, що Аль-Кайєда має висококваліфікованих фахівців із комп'ютерних технологій. Ряд мусульманських хакерських угруповань загрожує кібератаками урядовим сайтам США й Ізраїлю [50].

Те, що новоявлені терористи вчаться технології ведення агресивних дій за допомогою Інтернету, підтвердив терористичний акт у Мадриді, який стався навесні 2004 р. Як з'ясувалося в результаті ретельного розслідування, вся підготовка до нього велася не де-небудь, а безпосередньо в самій столиці Іспанії. Інформація про технологію застосування пристрою надходила безпосередньо з Інтернету, з одного із ісламістських веб-сайтів. Аналогічна ситуація розкрилася після скрупульозного вивчення британською поліцією і спецслужбами схожого теракту, що відбувся в Лондоні влітку 2005 р. З'ясувалося, що терористи-

смертники не були членами якої-небудь закордонної організації, але розробили свій «простий і недорогий» план дій на основі інформації, також отриманої з Інтернету [110].

Як стверджує один із авторів доповіді «Віртуальна криміналістика», дослідник Оксфордського інституту інтернету Айан Браун, уже сьогодні понад 120 країн тим чи іншим чином активно залучені в комп'ютерне протистояння або зайняті кібершпіонажем через всесвітню павутину. Кіберзлочинність стала значно мобільнішою в міжнародному масштабі.

Політика та кіберзлочинність стали з'являтися разом у заголовках новин. За даними Міністерства національної безпеки США, тільки в США з 2006 по 2008 рік кількість відомих атак на державні комп'ютери зросла більш ніж удвічі. За словами Пола Фергюсона, старшого фахівця з дослідження загроз Trend Micro, не виключено, що кібертерористи вже впровадили шкідливі програми в систему електропостачання США, щоб у якийсь момент віддалено порушити її роботу.

Після повномасштабної кібератаки, що відбулася після зустрічі президента Ніколя Саркозі з тибетським духовним лідером Далай-Ламою, сайт французького посольства в Пекіні не працював кілька днів. Багато експертів вважають, що ця атака була організована групою хакерів для досягнення націоналістичних цілей. «Теоретично, будь-яка людина з комп'ютером і доступом в Інтернет може завдати руйнівного удару. У США спостерігалися атаки хакерів, спрямовані на сайти регіональних і федеральних державних органів, - каже Фергюсон. - Невеликі організації не завжди мають у своєму розпорядженні достатньо коштів та персоналу, і тому нерідко доручають створення сайтів стороннім компаніям. Згодом сайтові потрібне обслуговування або оновлення, і у ці моменти він стає уразливий для хакерів, які потім із його допомогою намагаються виразити свої політичні погляди» [191].

Одним із прикладів кібервійни експерти називають атаку на Естонію, яка сталася у травні 2007 року, після того як влада вирішила перенести пам'ятник «Бронзовий солдат». Атаки DDoS на цивільні й урядові сайти Естонії призвели до порушення працездатності комп'ютерних мереж. За кілька днів естонський сегмент інтернету був практично відрізаний від зовнішнього світу, а ряд урядових сайтів виведений із ладу хакерськими атаками. Більшість атак здійснювалося з території Росії, хоча Кремль категорично відкинув наявність будь-якого злого наміру зі свого боку і причетність до цієї історії.

На думку фахівців НАТО, ситуація в Естонії була лише «верхівкою айсберга» в порівнянні з тим, із чим може зіткнутися світ [143].

На початку липня 2009 р. хвиля кібератак, імовірно з території КНДР, тимчасово придушила роботу веб-сайтів деяких державних установ Південної Кореї та США. Сталося це в період проведення КНДР послідовної серії пусків балістичних ракет, посилення загальної дипломатичної напруженості, пов'язаної з її ядерною програмою, і загрози введення санкцій із боку США й ООН.

До інших прикладів можна віднести кібератаку Ізраїлю проти Сирії в 2007 р. при підготовці авіаційного удару по її ядерному об'єкту, застосування США кіберзброї в Іраку і постійно освітлювані в ЗМІ та приписувані Китаю проникнення в державні та приватні комп'ютерні мережі США.

Мабуть, найбільш гучною подією останнього часу, що сталася 23 вересня 2010 р., стала вірусна атака на комп'ютери співробітників атомної електростанції в іранському Бушері, причому, напевно, через заражені вірусом Stuxnet флеш-носії постраждала комп'ютерна система управління електростанцією. Правда, за заявою іранських офіційних осіб у газеті Iran Daily, ця атака не завдала серйозних збитків основному контуру управління, що швидше за все, на думку фахівців, можна поставити під

сумнів. Дана подія, безумовно, вплине на терміни введення станції в повномасштабну експлуатацію, через необхідність не тільки ретельного розслідування події, а й проведення ряду додаткових заходів щодо забезпечення безпеки станції. Всього на багатьох промислових об'єктах в Ірані, за даними британської газети The Daily Mail, даним вірусом були заражені понад 30 тис. комп'ютерів.

Всі ці факти зайвий раз підтверджують те, що проблематика наростання протиборства в кіберпросторі стала вельми актуальною.

19 листопада 2009 року компанія McAfee, Inc. (NYSE: MFE) опублікувала свій п'ятий щорічний «Звіт про віртуальну злочинність», згідно якого міжнародні перегони кіберозброєнь стали реальністю. В ході підготовки звіту компанія виявила, що кількість політично мотивованих кібератак зросла, а п'ять країн - США, Росія, Франція, Ізраїль і Китай - тепер володіють кіберзброєю.

Деякі автори схиляються до того, що повстання народних мас у країнах Близького Сходу стали можливими в результаті застосування технологій інформаційно-мережевого впливу. І якщо у випадку Тунісу та Єгипту ці технології були ще недостатньо виявлені, то в Лівії відбувся «генеральний прогін» сценарію інформаційно-мережевої війни. Лівійська «революція» з'явилася на екранах світових ЗМІ як певний симулякр, сфабрикована «копія революційного дійства без оригіналу», хід якої був поданий глобальними мас-медіа без адекватного співвіднесення з дійсністю, зате в точній відповідності зі сценарієм, написаним авторами цього політичного спектаклю [97].

«Цікаве зізнання одного з лідерів єгипетської опозиції, співробітника інтернет-компанії «Гугл» (Google) В. Гонима про те, що він був одним із організаторів у січні акцій протесту в Єгипті, які координувалися через соціальні мережі в Інтернеті шляхом пропаганди та агітації, а також сповіщення молоді про місце і час їх проведення. Безумовно, на настрої

єгипетського населення вплинули публікації сайту «Вікілікс» (Wikileaks) про підготовлюваний Вашингтоном у 2011 році державний переворот у Єгипті, активна діяльність електронних ресурсів «Твіттер» (Twiner, створено в 2006 році, має майже 200 млн. користувачів, які кожен день залишають 50 млн. коротких повідомлень), «Фейсбук» і «Блекберрі мессенжер» (Blackberry Messenger). У цій країні при організації акцій протестів соціальні мережі мали найбільший успіх, тому що всесвітньою мережею користується майже кожен третій єгиптянин.

Відомо, що під час вуличних заворушень, які розпочалися, єгипетська та лівійська влада пішла на безпрецедентний крок - відключила в країні Інтернет. Однак соціальні мережі все одно залишалися джерелом інформації, повідомляючи про ситуацію в Єгипті всьому світові. Не без участі компанії «Гугл» був створений сервіс Speak-2Tweet, що дозволяв єгиптянам дзвонити і залишати голосові повідомлення, які потім транслювалися в «Твіттер» [92].

Спровоковані на «революційні» виступи інформаційними атаками з соціальних мереж Facebook і Twitter, арабські суспільства на Близькому Сході привели в рух революційне цунамі небувалої сили. Вибух на арабській вулиці показав, що соціальні мережі стали свого роду «запалом» для неспокійної атмосфери Близького Сходу. Практично у всіх країнах, залучених у цей вир подій, революційний флешмоб був організований за допомогою розсилки повідомлень про намічені мітинги й акції протесту через соціальні мережі, електронну пошту та мобільні телефони. При цьому слід враховувати той факт, що керуючі сервери глобальних електронних мереж Facebook, Twitter, Hotmail, Yahoo і Gmail знаходяться в США і контролюються американськими спецслужбами, які мають доступ до всієї циркулюючої в них інформації. Це дозволяє організувати розсилку повідомлень заздалегідь підібраній «клієнтурі» - своїм агентам впливу в країнах арабського Сходу, які за сигналом ззовні збирають у потрібний час

і в потрібному місці критичну масу людей, використовуючи для цього так зване «сарафанне радіо». А служби безпеки держав, що зазнали інформаційного вторгнення, не зуміли протистояти новій для них формі організації руху протесту, який відразу ж набув лавиноподібного, некерованого характеру. Виявилося, що неможливо було передбачити початок вуличних заворушень, як і джерела розсилки підбурювальних повідомлень, а після початку заворушень відключення доступу до Інтернету та мобільного зв'язку вже нічого не дало, так як процес набув характеру лісової пожежі [97].

Як заявив президент і генеральний директор McAfee Дейв Деволт, «Компанія McAfee попереджає про небезпеку глобальних перегонів кіберозброєнь уже більше двох років, але тепер наші побоювання починають виправдовуватися. Зараз декілька країн активно готуються до кібервійни та проводять кібератаки. В наші дні небезпека походить не від ядерної зброї, а від віртуального світу, і ми повинні бути до цього готові» [132].

Небезпеку кібервійн особливо підкреслюють фахівці в сфері захисту кіберпростору. Наприклад, помічник начальника управління з кіберзлочинів Федерального бюро розслідувань (ФБР) США в своєму інтерв'ю відобразив точку зору, що комп'ютерні атаки являють собою навіть більший ризик «для забезпечення національної безпеки, ніж застосування зброї масового ураження або підрив ядерного пристрою в одному з наших найбільших міст». Керівник підрозділу зі співпраці в галузі оборони кіберпростору НАТО Кевін Колеман заявив, що «кібертероризм та кібератаки представляють собою таку ж за ступенем загрозу національній безпеці, як і ракетна атака» [165].

Більше того, ряд американських експертів із інформаційної безпеки закликав усі зацікавлені державні та приватні організації об'єднати зусилля та приступити до реалізації «Проекту кібер-Манхеттен» (проект

«Манхеттен» - створення атомної бомби в США. - В.Щ.). «Це дозволить забезпечити країні захист від ударів із мережевого простору та дозволить зміцнити інформаційну безпеку США, загроза руйнування якої останнім часом постійно і стрімко зростає», - підкреслюється в поширеній ініціативною групою заяві [247].

Провідні країни світу мають у своєму розпорядженні широкі та різноманітні інформаційні можливості для досягнення своїх політичних цілей, захисту державних інтересів як всередині країни, так і за кордоном. Інформаційне протиборство в політиці сучасних держав передбачає використання різноманітних інформаційно-технічних і інформаційно-психологічних технологій впливу на індивідуальну, групову та суспільну свідомість протилежної сторони [51, с.11].

Розвідслужби регулярно випробовують мережі інших країн, шукаючи в них слабкі місця, причому методи перевірки з кожним роком стають все більш витонченими. В даний час спецслужби різних країн або окремі користувачі мережі отримали можливість без обмежень задіяти блоги, соціальні мережі, електронні карти та сайти відеохостингу для публікації різного роду інформації - від альтернативного погляду на політику й історію до відверто расистських і націоналістичних матеріалів, тим самим впливаючи на аудиторію в потрібному напрямку. Ефективність подібної діяльності істотно зростає в міру розширення аудиторії, а, враховуючи постійне зростання користувачів Інтернету (зараз їх у світі більше 1 млрд.), будь-який матеріал агресивного характеру, який сприяє ескалації соціально-психологічних, етнічних і релігійних протиріч, миттєво отримує підтримку однодумців із різних країн світу [92].

Країни створюють не тільки засоби захисту від віртуальних загроз, а й розробляють атакуючі озброєння для ураження таких інфраструктурних об'єктів як електроенергетичні мережі, транспорт, телекомунікації, фінансові системи та водопостачання, оскільки невеликими зусиллями

можна нанести істотних збитків супротивникові. У більшості розвинених країн об'єкти життєзабезпечення під’єднані до Інтернету та недостатньо захищені, що робить їх уразливими. Якщо не забезпечити ключові інфраструктурні об'єкти сучасними системами безпеки, атака на них обернеться величезною шкодою і виявиться більш руйнівною, ніж усі попередні напади [132].

За оцінками багатьох експертів, світовим лідером у веденні інформаційної війни є Китай. Директор розвідувального та дослідницького центру в Вашингтоні Джеймс Малвенон стверджує, що китайці першими почали використовувати кібератаки в політичних і військових цілях [143].

У Китаї термін «інформаційна війна» був введений у науковий та громадський дискурс у 1985 р. провідним китайським теоретиком інформаційної війни Шень Войгуаном.

В основі теоретичних підходів китайських фахівців у галузі інформаційного протиборства лежать згадані нами вище (підрозділ 1.3.) погляди давньокитайського філософа Сунь-Цзи.

Очевидно, що позиції Китаю щодо ведення інформаційної війни сформувалися під впливом американських концепцій інформаційних операцій. На думку китайських фахівців, перемога у війнах майбутнього неможлива без інформаційної переваги на полі бою. Це означає, що військові повинні володіти найсучаснішими технологіями отримання, аналізу та використання інформації. Це дозволить їм впливати на супротивника. В той же час китайський підхід до інформаційної війни відрізняється від американського тим, що в ньому закладено оборонний принцип. А головним завданням є протидія потенційній військовій загрозі з боку США [66].

Сучасна концепція ведення інформаційної війни стала активно розроблятися в Китаї в кінці 1980-х років XX ст. Під інформаційною війною розумілися дії (політичні, економічні, культурні, технологічні й

інші) з захоплення глобального інформаційного простору та створення захисного інформаційного кордону Китаю, Великої Китайської стіни у 5-му вимірі. Дослідники виділяють декілька основних елементів китайського підходу: теоретичне залякування; протистояння інформаційних потенціалів; конкуренція інформаційних стратегій; підвищення інформатизації військ (штучний інтелект); економічна інформаційна агресія; культурна інформаційна агресія; інформаційна війна розумів. Головним об'єктом є психологія. Головним методом - мирне залякування.

Свідченням того, що китайське керівництво розуміє роль інформаційного протиборства в сучасному світі є та увага, яка приділяється розвитку ЗМІ. Так, щорічно в Китаї видається понад 2,5 млрд. журналів, а загальний тираж випущених газет становить близько 200 млрд. Усім цим займається 538 видавництв. У Китаї близько 1,5 тис. радіопередавальних станцій [161, с, 212]. Такі цифри, звичайно ж, вражають.

Як зазначають Р. Кларк і Р. Нейко, китайці впродовж уже декількох років відкрито визнають, що вони багато чому навчилися завдяки «Бурі в пустелі». Якщо раніше, в разі війни, вони сподівалися отримати перемогу над США завдяки чисельній перевазі, то тепер вони визнають помилковість своїх розрахунків. Результатом цього стало скорочення китайських військ і збільшення обсягу інвестицій у нові технології, зокрема «мережевізацію» - освоєння нового комп'ютерного поля бою. «Їхні публічні заяви разюче нагадували вислови генералів ВПС США. Один китайський експерт пояснював у військовій газеті, що «ворожа країна може отримати паралізуючий удар через Інтернет». Інший полковник, можливо розмірковуючи про США та Китай, писав, що «переважаючі сили, які втратять інформаційну перевагу, будуть повалені, а

менші, захопивши інформаційну перевагу, зможуть здобути перемогу»» [104, с.69].

На думку китайських фахівців, Китай домігся в останні роки великих успіхів у ході інформаційної війни з США [161, с.212]. Так, наприклад, у доповіді Міністерства оборони США Конгресу зазначалося, що в період із 20 по 25 червня 2007 року після масованої комп'ютерної атаки Китай отримав доступ до ряду інформаційних мереж Міністерства оборони США. Так, відзначалися спроби проникнення в комп'ютери апарату Міністра оборони, отримання інформації про новітній винищувач F-35, а також проникнення в комп'ютерну систему управління американськими мережами електропостачання [66].

Незважаючи на помітні успіхи, китайське керівництво, проте, вважає, що КНР поки відстає від найбільш розвинених у військовому й економічному відношенні країн, що говорить про її неготовність у даний час до ведення інформаційної війни та досягнення інформаційної переваги. У зв'язку з цим передбачається прискорити комплексний розвиток усіх компонентів інформаційного протиборства, перш за все у військовій галузі. Це стосується, зокрема, розвитку інформаційної інфраструктури та технологій військового призначення, а також спеціальної підготовки особового складу.

Визнаючи своє суттєве відставання від провідних країн Заходу у сфері створення командно-керуючих систем на базі дочасових інформаційно-телекомунікаційних технологій, КНР робить у даний час ставку на формування можливостей для проведення нестандартних інформаційних атак й інших асиметричних дій.

Найбільш перспективними видами інформаційної зброї в Китаї вважають: електронно-вірусну зброю (ЕВЗ); засоби, що дозволяють вклинюватися в трансляції радіо- та телепрограм; пристрої створення радіоперешкод; одноразові та багаторазові генератори різних видів

електромагнітної енергії (вибухомагнітні, вибухові магнітогідродинамічні, пучково-плазмові й інші) [66].

У Китаї проводиться реалізація концепції Мережевих сил, яка передбачає створення військових підрозділів, що складатимуться з висококваліфікованих комп'ютерних експертів, які отримали освіту в кращих державних університетах, академіях і спеціальних навчальних центрах. Залучається освічена молодь, для якої використання інформаційно-комунікаційних технологій є звичною справою.

У практичному і науковому обігу китайських фахівців використовується вираз «асиметрична війна». Про її суть можна дізнатися з невеликої книжки під назвою «Необмежена війна», яка вийшла в світ у 1999 року й авторами якої є високі військові чини. Автори книги запропонували план, реалізувавши який більш слабкі країни зможуть змінити існуючу розстановку сил і домогтися переваги, використовуючи зброю та прийоми, що виходять за межі традиційного військового арсеналу. Примітно, що англійські видавці назвали цю книгу «генеральним планом знищення Америки». Однак цінність цієї книги очевидна, вона показує ставлення китайський збройних сил до кібервійни [104, с.72].

Важливою умовою успішності будь-яких акцій інформаційних війн є інституалізація даного роду комунікацій. Причому кожен політичний актор використовує для цього власні можливості. Найкраще становище в цьому сенсі в держави, у розпорядженні якої знаходиться розгалужена система інститутів, здатних організувати та підтримати кампанії в форматі інформаційних війн. Злагоджена та скоординована робота такого типу інститутів забезпечує високу ефективність досягнення політичних цілей держави, їхнє інформаційне забезпечення.

Тому досвід Китаю цікавий і корисний для нас тим, що тут створена потужна державна система ведення інформаційної війни, завдяки якій

Китайська держава має можливість масованого застосування сил і засобів у потрібний час. Основою системи є Дослідницьке бюро при Держраді КНР і Системно-аналітичний центр Міністерства державної безпеки. Китайська система ведення інформаційної війни найбільш ефективно діє у фінансовій сфері. Вона отримує інформацію від діаспор країн Тихоокеанського регіону та 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. Міністерство державної безпеки Китаю забезпечує виїзд із країни «потрібних» людей з гарною освітою, дає кошти на облаштування на новому місці проживання. Результатом цієї діяльності є те, що через величезні китайські діаспори розвідка КНР проникає в державний апарат, засоби масової інформації та органи влади багатьох країн.

Агресивна інформаційна політика Китаю відображена в багаторазових фактах несанкціонованого доступу до конфіденційної інформації та спроб порушення працездатності комп'ютерних мереж ряду розвинених у промисловому й у військовому відношенні країн (у тому числі США, Німеччини, Великобританії, Індії та Японії), що було неодноразово зафіксовано спецслужбами цих країн .

Основна частина легальної китайської діаспори в Америці зосереджена на Тихоокеанському узбережжі, де китайська розвідка має настільки сильні позиції, що американські служби стають безсилими перед китайською активністю в таких містах як Сіетл, Лос-Анджелес, Сан-Франциско, Х'юстон. Тривожним сигналом для США став той факт, що етнічний китаєць Ло Цзяхуея став губернатором штату Вашингтон [161, с.215].

За заявою представників Міністерства оборони Великобританії в липні 2007 р. була здійснена невдала спроба проникнути в інформаційні мережі цього Міністерства з боку КНР.

Аналогічні заяви надходили з боку спецслужб Японії та Індії. Зокрема, в 2008-2009 рр. були зафіксовані спроби злому з китайського боку мереж військового відомства Індії, офіційних сайтів Далай-лами і тибетських лідерів у вигнанні, які знаходяться на індійській території. Повідомлялося про викрадення конфіденційної інформації з військово-технічного співробітництва Делі з іншими державами світу [66].

Крім того, за даними відповідних служб Тайваню, в ході підготовки до президентських виборів на острові 2000 року Китай задіяв 168 комп'ютерних центрів для здійснення атак на тайванські комп'ютерні мережі. Особливе зацікавлення китайці виявляли до можливості отримання доступу до даних Центральної виборчої комісії [66].

За задумом американських розробників, інформаційне протиборство, що реалізовується через інформаційні операції, має на увазі використання сил і засобів інформаційної боротьби для підготовки та застосування збройних сил США і включає в себе діяльність вищого військово-політичного керівництва, органів державного та військового управління, засобів масової інформації, відповідних компонентів інформаційного протиборства, спрямовану на підготовку та застосування збройних сил США, формування сприятливого інформаційного середовища та створення умов для виконання поставлених перед ними завдань [63, с.11].

Формування нормативно-правової бази для ведення інформаційних війн у США почалося з виходу директиви Міністерства оборони США Т 3600.1 від 21 грудня 1992 р. під назвою «Інформаційна війна». В 1993 р. у директиві Комітету начальників штабів № 30 вже були викладені основні принципи ведення інформаційної війни. Визначення інформаційної війни було дано в 1997 р.: «Дії, зроблені для досягнення інформаційної переваги

в інтересах національної стратегії і здійснювані шляхом впливу на інформацію та інформаційні системи супротивника при одночасному захисті власної інформації у своїх інформаційних системах» [161, с.217].

Ряд офіційних документів, таких як доповідь Міністерства оборони США "Report of the quadrennial Defense Review", концептуальний документ Комітету начальників штабів "Joint Vision 2010", доповідь комісії з національної оборони "Transforming Defense National Security in the 21st Century, Report of the National Defense Panel ", констатує відповідно:

"...Ми визнали, що світ продовжує швидко змінюватися. Ми не в змозі повністю зрозуміти або передбачити проблеми, які можуть виникнути в світі за часовими межами, що визначаються традиційним плануванням. Наша стратегія приймає такі невизначеності та готує збройні сили таким чином, щоб впоратися з ними".

"Прискорення темпу змін робить майбутні умови більш непередбачуваними та менш стабільними, висуваючи широкий діапазон вимог до наших сил".

"Проблеми XXI століття будуть кількісно та якісно відмінні від тих, які були характерні для періоду холодної війни, у зв'язку з чим будуть потрібні докорінні зміни інститутів національної безпеки, військової стратегії і підходів до питань оборони до 2020 року" [58].

Інформаційна війна стає темою офіційних наукових конференцій, у яких беруть участь визначні представники військово-політичного керівництва країни.

Політика інформаційних війн вважається американським керівництвом настільки важливою, що в американських армії, флоті та військово-повітряних силах США введені посади офіцерів, які займаються технологіями інформаційної війни. Ці технології були апробовані у всіх збройних конфліктах за участю США («Буря в пустелі», операція на Гаїті, агресія проти Югославії й ін.).

У червні 1995 р. Національний університет оборони у Вашингтоні здійснив випуск першої групи фахівців у галузі інформаційної війни. Через місяць у Військово-морському коледжі в Ньюпорті було завершено ігрове відпрацювання планів ведення інформаційних війн. У січні-червні 1995 р. в США була проведена командно-штабна воєнна гра (КШВГ) за участю представників усіх силових структур, метою якої була розробка концепції стратегічної інформаційної війни.

У серпні 1995 р. національний Інститут Оборони США публікує роботу Мартіна Лібікі «Що таке інформаційна війна», в якій було визначено 7 форм інформаційної війни: командно-управлінську; розвідувальну; психологічну; хакерську; економічну; електронну; кібервійну.

Придушення та знищення систем управління протиборчої сторони (Command-and-Control Warfare) скероване на фізичне знищення командних пунктів супротивника, порушення управління його силами та засобами.

Інформаційне забезпечення бойових дій (Intelligence-Base Warfare), або стратегічна розвідка, яка має на меті надання та використання в системах управління військами і зброєю інформації, що збирається інформаційними системами в ході бойових дій.

Електронне придушення (Electronic Warfare) орієнтоване на порушення функціонування каналів розповсюдження інформації протиборчої сторони та розкриття її криптографічного захисту.

Метою хакерської війни (Hacker Warfare) є проникнення в телекомунікаційні та інформаційні системи протиборчої сторони, нанесення шкоди їм і ресурсам, що знаходяться в них.

Метою війни в галузі економічної інформації (Economic Information Warfare) є дестабілізація економіки шляхом встановлення економічної блокади або інформаційної агресії.

Метою кібервійни (Cyber Warfare) є руйнування інформаційних систем супротивника, тому кібервійна розглядається як інформаційний тероризм.

Метою психологічної або інформаційно-психологічної війни (Psychological Warfare) є вплив на психіку індивіда. Дана форма інформаційної війни спрямована на інформаційно-психологічну обробку населення, керівного складу військ, політичних лідерів протиборчої сторони, операції з модифікації культури.

Не секрет, що США, ведучи інформаційні війни, переслідує цілком конкретні цілі: послабити позиції країн-конкурентів, підірвати їх національно-державні підвалини, дестабілізувати систему державного управління шляхом інформаційного впливу на політичну, дипломатичну, економічну та соціальну сфери життя суспільства, провести психологічні операції, підривні й інші деморалізуючі пропагандистські акції. Так американським керівництвом бачиться вирішення завдань із захисту національних інтересів США, попередження міжнародних конфліктів, припинення провокаційних і терористичних акцій, а також забезпечення безпеки національних інформаційних ресурсів.

Інформаційні операції США спрямовані на досягнення інформаційної переваги над супротивником (у першу чергу в управлінні військами) і захист власних систем управління, для чого застосовуються будь-які військові та технічні сили і засоби, наявні в розпорядженні, при формальному дотриманні правових, моральних, дипломатичних, політичних і військових норм. Як зазначає, О. Деньщиков, «Під інформаційною перевагою стали розуміти здатність до збору, обробки та розповсюдження безперервного потоку вичерпної та достовірної інформації, одночасно ускладнюючи або попереджуючи аналогічні дії супротивника. Для досягнення інформаційної переваги було сформульовано дві умови: по-перше, комерційні технології, що стрімко

розвиваються, необхідно використовувати й адаптувати для потреб оборони швидше, ніж це роблять військові конкуренти США, по-друге, державі необхідно мати ефективні наступальні й оборонні інформаційні можливості, які повинні захищати інформаційні ресурси та системи від нападу та забезпечувати співмірні відповідні дії» [63, с.23].

Перед Збройними Силами США вперше поставлено задачу впливати на супротивника ще до початку активних бойових дій для того, щоб забезпечити вигідну для Сполучених Штатів спрямованість процесів управління та прийняття рішень протиборчої сторони. Завдання з досягнення інформаційної переваги над супротивником шляхом проведення інформаційних операцій відображені в документах КНШ МО США "Єдині перспективи 2010" та "Єдині перспективи 2020", а також у документах МО США "Чотирирічний огляд стану збройних сил" від 2001 та 2006 років. У них визначено мету, завдання та основні принципи інформаційної боротьби, обов'язки керівних органів та посадових осіб щодо її організації та планування в мирний час і у кризовій обстановці.

Як зазначає О. Бедрицький, «У військовому відомстві США під інформаційними операціями (ІО) розуміється використання основних можливостей радіоелектронної боротьби, операцій у комп'ютерних мережах, психологічних операцій, військового обману та заходів щодо забезпечення інформаційної безпеки з метою впливу або захисту інформації й інформаційних систем і впливу на процеси прийняття рішення. Основні ІО супроводжуються специфічними допоміжними та забезпечуючими заходами. Дане визначення повністю відповідає раннім теоретичним побудовам, що стосуються інформаційної війни, та положенням військово-політичних документів, подібних "Єдиним перспективам", а також "Чотирирічному огляду стану збройних сил" від 2001 і 2006 років» [20, с.23].

Політика США в інформаційній сфері при адміністраціях Б. Клінтона і Дж. Буша була спрямована на досягнення, а потім - на закріплення домінування США в глобальному інформаційному просторі. Оцінюючи політику США в інформаційній сфері, можна зробити висновок, що вона поєднує як ринкові інструменти лібералізації та дерегуляції, так і прагнення встановити прямий державний контроль над інформаційними ресурсами, причому не тільки в національних, але й у міжнародних масштабах [233, с.33].

Тим не менше, як повідомляє газета The Washington Post, Держсекретар США Хілларі Клінтон вважає, що США програють війну за громадську думку арабським, китайським і російським ЗМІ. "Ми знаходимося в стані інформаційної війни, і ми програємо її", - заявила Клінтон під час виступу перед комітетом Сенату з міжнародних справ. На її думку, образ США спотворений популярною культурою, тому багато людей у всьому світі вважають США країною жінок у бікіні та професійних рестлерів.

Держсекретар повідомила, що після закінчення холодної війни міжнародне мовлення США стало скорочуватися, у той час як арабомовні ЗМІ заповнили цю нішу на Близькому Сході та створили популярний образ США, який поділяють мільйони жителів регіону. Крім арабомовних ЗМІ ефір захоплюють китайські та російські англомовні канали. Хоча Держдепартамент робить ставку на соціальні мережі, запустивши Twitter арабською мовою і мовою фарсі, слід приділяти увагу традиційним ЗМІ, радіо і телебаченню, вважає Клінтон.

Держсекретар закликала збільшити бюджет держдепартаменту США для того, щоб розширити іномовлення. Проте раніше партія республіканців зажадала, щоб бюджет Держдепартаменту США був значно скорочений [105].

В кінці травня 2009 р. президент США Б. Обама заявив про свій намір розглядати безпеку кіберпростору як одну з пріоритетних проблем його адміністрації. Тоді рішенням президента від 29 травня 2009 р. в апараті Білого дому був сформований штаб із питань національної безпеки (National Security Staff) і призначений координатор із питань кібербезпеки (Cyberspace Coordinator), який одночасно є членом як Ради з національної безпеки, так і Ради з національної економіки. Відповідно до концепції «інформаційної переваги», відображеної в документі про стратегію розвитку ВС США «Єдина перспектива - 2020», перевага в інформаційній сфері є одним із ключових факторів успішного ведення бойових дій.

Контури майбутньої стратегії були окреслені в «Огляді політики кібербезпеки» (Cyberspace Policy Review), підготовленому у травні 2009 р. апаратом Білого дому в кооперації з комісією із питань кібербезпеки Центру стратегічних і міжнародних досліджень (Center for Strategic and International Studies (CSIS) bipartisan Commission on Cybersecurity) [90].

За повідомленням британської газети The Guardian, в США на сьогодні реалізується програма інформаційного впливу на проблемні регіони з використанням соціальних мереж Twitter і Facebook, центр управління якої розташовується на базі ВПС США «Макділл» у штаті Флорида. У ньому працюють 50 операторів, кожен із яких курирує до 10 «агентів впливу», які знаходяться в різних країнах світу і проводять інформаційну війну за всіма правилами політичних технологій руйнування своїх держав. Вартість даної програми, за оцінкою британської газети, оцінюється в 2,76 млн. доларів. Вона передбачає для кожного з таких «бійців інформаційної війни» наявність переконливої легенди та заходів щодо їхнього захисту від викриття. За словами прес-секретаря Центрального командування збройних сил США Білла Спікса, будь-який вплив на американську аудиторію заборонений правилами. Англійська мова в роботі не використовується. Спілкування ведеться тільки

арабською, урду, пушту та фарсі, тобто мовами тих країн, які представляють інтерес для Вашингтона з точки зору впливу на їхню суспільну стабільність.

Іран намагається захиститися від зовнішнього інформаційного впливу за допомогою нової агресивної форми цензури - так званого національного Інтернету. Планується, що в майбутньому іранський кіберпростір буде відключений від решти світу.

У лютому 2011 р., коли продемократичні акції протесту швидко поширилися Близьким Сходом і Північною Африкою, Реза Багері Асл, директор науково-дослідного інституту при Міністерстві телекомунікацій, повідомив іранському інформаційному агентству, що незабаром 60% будинків і підприємств країни будуть підключені до нової внутрішньої мережі. А через декілька років це поширіться на всю країну. Ці кроки робляться з метою боротьби із тим, що режим вважає серйозною загрозою: віртуальним вторгненням західних ідей, культури і впливу, в першу чергу, з США.

Як зазначив Алі Агамохаммаді, відповідальний за економічну сферу в уряді Ірану, Іранська національна мережа буде "істинно халяльною мережею, яка відповідатиме етичному та моральному рівню мусульман". За словами Агамохаммаді, спочатку нова мережа буде працювати паралельно зі звичайним інтернетом - у банків, урядових відомств і великих компаній збережеться до нього доступ. У підсумку, за його словами, національна мережа прийде на зміну всесвітньому Інтернету як в Ірані, так і в більшості мусульманських держав.

Однак окрім видимих, для іранського керівництва, позитивних моментів, є й негативні. Як відомо, навіть для країни, ізольованої від Заходу економічними санкціями, Інтернет є важливим інструментом бізнесу. Обмеження доступу може перешкодити інвестиціям із Росії та Китаю, від інших торговельних партнерів. Це також питання досвіду та

ресурсів, необхідних для створення іранського еквіваленту популярних пошукових систем та веб-сайтів, таких як Google [35].

Корисний для нас і досвід Індії. Забезпечення інформаційної безпеки в цій країні покладене на Міністерства зв'язку й інформаційних технологій, внутрішніх справ, оборони.

Успіхи індійських фахівців у розробці нових інформаційно-комунікаційних технологій дозволяє їм розраховувати на ефективне застосування цих технологій із метою дестабілізації функціонування об'єктів інформаційної та телекомунікаційної інфраструктури закордонних держав.

Відповідно до інструкції об'єднаного штабу оборони ЗС Індії про порядок проведення незалежної оцінки вразливості комп'ютерних мереж, що використовуються і впроваджуються в національних Військово-морських Силах у штабах, з'єднаннях і частинах із залученням цивільних фахівців будуть проводитися щоквартальні перевірки. Їх мета - вирішувати наступні завдання: дистанційний (прихований і неруйнівний) аналіз наявності недоліків апаратного, програмного та адміністративного забезпечення комп'ютерних мереж ВМС; злом парольного захисту систем розмежування доступу до інформації та здійснення кібератак типів DDOS (Distributed Denial of Service), DOS (Denial of Service) та інших; пошук інших "вікон уразливості" у браузерах, поштових агентах, програмному забезпеченні серверів і шлюзів.

Регламентування діяльності індійських міністерств і відомств у сфері інформаційних і телекомунікаційних технологій, включаючи можливе їх використання для порушення функціонування об'єктів інформаційної та телекомунікаційної інфраструктури зарубіжних держав, здійснюється відповідно до положень прийнятого парламентом Індії в 2000 році закону про інформаційні технології (Information Technology Act 2000) з доповненнями, затвердженими в 2008 році.

З метою контролю за Інтернетом та протидії кібертероризму, Кабінет Міністрів Індії в липні 2003 року поставив до відома органи виконавчої влади про те, що уряд має право закрити веб-сайти з міркувань збереження цілісності та захисту суверенітету країни, в інтересах підтримки дружніх відносин із іноземними державами та громадського порядку.

Координація діяльності структур, що відповідають за вирішення задач порушення функціонування об'єктів інформаційної та комунікаційної інфраструктури зарубіжних держав, до числа яких входять уповноважені органи виконавчої влади, наукові організації та промислові компанії, покладена на нещодавно створений міжвідомчий комітет (National Cyber Cop Committee). Члени комітету - представники уряду, промисловості, Міністерства внутрішніх справ, а також експерти з комп'ютерної безпеки.

Дана структура займається розробкою стандартів безпечного використання мереж, інформуванням користувачів про можливі кіберзагрози, а також підготовкою рекомендацій із розробки та виробництва спеціалізованого програмного забезпечення для захисту інформаційних потоків.

У збройних силах Індії з метою координації діяльності видів ЗС та взаємодії з іншими силовими структурами в сфері інформаційного протиборства в складі об'єднаного штабу оборони створено Агентство з інформаційної війни (Defence Information Warfare Agency). Основними функціями цієї структури є: розробка форм і методів ведення інформаційної війни; контроль за забезпеченням інформаційної безпеки військ; координація діяльності органів інформаційної війни видів ЗС Індії, організація проведення ними спільних операцій, проведення спільно з МВС психологічних операцій на території країни [66].

Безсумнівно, що не менш цікавим для нашого дослідження є досвід Росії у веденні інформаційної війни. Те значення, яке надається Росією

методам інформаційної війни, підтверджується наявністю спеціальної концепції. Уточнимо її основні положення:

- придушення елементів інфраструктури державного та військового управління (ураження центрів командування й управління);

- електромагнітний вплив на елементи інформаційних і телекомунікаційних систем (радіоелектронна боротьба);

- отримання розвідувальної інформації шляхом перехоплення та дешифрування інформпотоків, переданих каналами зв'язку, а також через побічні випромінювання;

- несанкціонований доступ до інформресурсів (шляхом використання програмно-апаратних способів прориву систем захисту інформаційних і телекомунікаційних систем супротивника) з подальшою їх деформацією, знищенням, розкраданням або порушенням нормального функціонування цих систем («хакерна» війна);

- формування та масове поширення інформканалами супротивника або глобальними мережами інформвзаємодії дезінформації або тенденційної інформації для впливу на оцінки, наміри й орієнтацію населення та осіб, які приймають рішення (психологічна війна);

- отримання потрібної інформації шляхом перехоплення й обробки відкритої інформації, переданої незахищеними каналами зв'язку і циркулюючої в інформсистемах, а також опублікованої у ЗМІ. При цьому реалізація концепції (за винятком першої її складової) може активно здійснюватися й у мирний час [168].

Як відомо, під час російсько-грузинського конфлікту 2008 р. битва розгорнулася не лише на землі, а й віртуальному просторі Інтернету. Так, російським хакерам вдалося помістити на головній сторінці сайту МЗС Грузії колаж із фотографій Адольфа Гітлера та Михайла Саакашвілі. Представники МЗС Грузії звинуватили російських хакерів в організації кібератак і оголосили, що у зв'язку з тим, що відбувається, офіційні заяви

влади країни будуть поширюватися через інформаційні агентства та інші канали.

Влада Росії, в свою чергу, звинуватила хакерів із Грузії в атаках на російські інформаційні сайти, такі як портал агентства РІА "Новини". Крім того, за деякими даними, нападу зазнав і інтернет-сайт російського державного англомовного телеканалу Russia Today.

Експерти в галузі інформаційної безпеки вважають цілком передбачуваним те, що війна на Кавказі вилилася на простір Інтернету. За словами експерта MessageLabs Алекса Шиппа, колишні республіки Радянського Союзу, разом із Китаєм і Бразилією, є найбільшими зонами беззаконня в кіберпросторі. Експерт MessageLabs каже, що хакери з Китаю спеціалізуються на промисловому шпіонажі, їхні бразильські колеги - на фінансових махінаціях, а російський кіберпростір рясніє різними програмами, які дозволяють ламати сайти.

Як зауважують експерти, те, що Росію облюбували хакери, не випадково. Розпад СРСР збігся зі світанком ери Інтернету на Заході, і тисячі підлітків із колишніх республік побачили в комп'ютерних технологіях можливість для себе досягти успіху. Тим більше, що в Радянському союзі була відмінна математична школа: програмісти, які працюють в країні, були змушені розробляти прості та ефективні алгоритми, щоб економити невисокі технічні можливості вітчизняних комп'ютерів.

Мрії багатьох колишніх радянських підлітків збулися, і вони стали програмістами в Силіконовій долині. Однак багато хто вирішив реалізувати свій талант інакше. Країни колишнього СРСР, де після розпаду країни часто не виконувалися закони, були дуже зручними для хакерів. Білл Томсон, експерт у галузі інформаційних технологій, називає цей ринок «темним боком Силіконової долини» [40].

2.2. Електронний шпіонаж у політичних цілях

Вперше про комп'ютерні злочини, одним із яких є електронний шпіонаж, заговорили в 1960-х рр. Саме тоді були виявлені злочини, скоєні за допомогою комп'ютера.

Дослідники навіть класифікували комп'ютерних злочинців у відповідності зі скоєними ними злочинами:

а) порушники правил користування ЕОМ - скоюють злочини через недостатнє знання техніки, бажання ознайомитися з інформацією, яка їх цікавить, викрасти будь-яку програму або безкоштовно користуватися послугами ЕОМ;

б) "білі комірці" - так звані респектабельні злочинці: бухгалтери, скарбники, керівники фінансів різних фірм. Для них характерні: використання ЕОМ із метою моделювання планованих злочинів, комп'ютерний шантаж конкурентів, фальсифікація інформації і т.д. Мета їхніх дій - отримання матеріального зиску або приховування інших злочинів;

в) "комп'ютерні шпигуни" - добре підготовлені в технічному відношенні фахівці, метою діяльності яких є отримання стратегічно важливої інформації з різних галузей;

г) "хакери" ("одержимі програмісти") - найбільш технічно та професійно підготовлені особи, які відмінно розбираються в обчислювальній техніці та програмуванні. Їхня діяльність спрямована на несанкціоноване проникнення в комп'ютерні системи, крадіжку, модифікацію або знищення наявної в них інформації. Найчастіше вони

скоюють злочини, не переслідуючи при цьому прямого матеріального зиску [112, с.168].

Інформація в принципі є надбанням суспільства, всіх організацій і людей. Без неї в суспільстві нічого не відбувається, це невід'ємний компонент будь-якого людського колективного або індивідуального вчинку, доцільної матеріальної чи духовної діяльності. Спроби з тих чи інших причин її сховати, приховати, затаїти, засекретити призводять до протилежних дій, тобто стеження, виявлення, розкриття. Секретність автоматично викликає протилежну дію – шпіонаж [76, с.63].

Новини про електронний шпіонаж займають перші шпальти друкованих засобів масової інформації. Щорічно компанії втрачають мільярди доларів на втратах інтелектуальної власності та розкраданні комерційних таємниць із подальшим перепродажем конкурентам з метою вимагання та незаконного отримання прибутку. Корпоративні мережі по всьому світу є прекрасною мішенню для злочинців, здатних дістатися до інформації, минаючи всі системи захисту.

«Кіберзлочинці користуються шкідливими програмами для отримання прибутку та досягнення геополітичних цілей, - зазначає П. Фергюсон. - Ми навіть стикалися зі спробою розкрадання комерційних таємниць у підрядників Міністерства оборони США. Ймовірно, ці атаки походили від китайської сторони. Однак через анонімність Інтернету дуже важко знайти людей, які стоять за всім цим» [191].

Електронний шпіонаж, Інтернет-шпіонаж, кібершпіонаж - новітні види збору інформації, в основі яких лежать інформаційно-комунікаційні технології, що забезпечують процесам спостереження та стеження всюдисущість і повсюдність. Ступінь насиченості суспільства електронними пристроями та їх ефективність такі, що під контролем опиняються навіть стаціонарні предмети та предмети, які пересуваються у просторі, більшість подій, що відбуваються. Вони дозволяють точно

фіксувати об'єкти та процеси, в реальному режимі часу передавати про них дані, класифікувати, обробляти інформацію та надавати її в потрібний час і в будь-яке місце для прийняття рішень, накопичувати, аналізувати та синтезувати величезні масиви даних, виділяти все цінне, що в них міститься, і зберігати стільки часу, скільки необхідно. За масштабами цей вид шпіонажу вже набагато перевершив особистісний канал отримання інформації, що домінував до недавнього часу [76, с. 64].

Шпіонаж завжди супроводжував державну діяльність. Ясно, що знання особливостей іншої держави дозволяє вибудовувати по відношенню до неї будь-яку політику та здійснювати відповідні дії. Крадіжка та витік конфіденційної інформації через мережу існують у всіх країнах світу, оскільки їх технології в принципі добре відомі. У 2005 р. офіційні служби США викрили діяльність хакерів, які створили особливу програму-вірус, що дозволила передати «на сторону» практично всю інформацію приблизно з 14 млн. карток Visa і Master Card (за іншими даними - з 40 млн. або 10% всіх платіжних електронних карток американських громадян). Це сталося в результаті порушення правил безпеки фірмою Cardsystem Solutions, яка обслуговувала спільні платежі. Найбільший витік інформації стався в 2006 р. У травні того ж року міністр у справах ветеранів США Дж. Ніколсон заявив про крадіжку персональних відомостей із бази даних відомства. Зловмисники вкрали інформацію про номери соціального страхування, особисті та фінансові дані про 26,5 млн. ветеранів країни.

Кілька років тому в США стався інцидент, який розбурхав усю країну. До друку потрапила інформація про комп'ютерну крадіжку секретних даних Пентагону, яку нібито здійснили російські спецслужби. Неординарна ситуація отримала назву «Лабіринт місячного світла». Заяви про те, що могли бути вкрадені відомості про системи наведення стратегічних ракет, викликало паніку у населення. Виходить, що життєво

важливі для країни та світу документи доступні стороннім. В інтересах національної безпеки керівництво Пентагону розпорядилося відключити від Інтернету 2 млн. комп'ютерів [75, с.95].

Злочини з використанням Інтернету стають усе більш витонченими. Дешевий спосіб добування інформації, який не потребує жодних фізичних зусиль, грошей, незаконних зисків стимулює кримінальні структури до його технологічного вдосконалення.

Сотні мільйонів людей користуються Інтернетом. При цьому вони не підозрюють, що залишають сліди, за якими, з допомогою пошукової техніки й «організованого віртуального погляду», можна отримати відомості про них, часом абсолютно несподівані. Ключем до отримання інформації про конкретну особистість є GD, тобто ідентифікатор користувача, який має й інші назви - екранне ім'я, ім'я входу, псевдонім тощо. Кожен власник намагається зберігати свій пароль. Проте можливості сучасної техніки такі, що його можна отримати й минаючи власника. Не секрет, що в Інтернеті можна знайти багато інформації про конкретну людину. Цікаво, що більшість цих відомостей зібрана в основному офіційними організаціями та особами: страховою компанією, яка застрахувала життя, житло та автомашину; роботодавцем, банком й іншими установами, що надають кредит; лікарем або лікарнею, де проходило лікування; автоінспекцією та ін.

Для збору приватної і навіть компрометуючої людину інформації в Мережі створені комерційні служби розслідувань, які виконують функції детективів і слідчих.

Давно вже не є секретом той факт, що американська система електронної розвідки «Ешелон» цілодобово сканує інформацію з усієї поверхні Землі, перехоплюючи телефонні та факсові повідомлення, листування в Інтернеті, дані ЗМІ і т.д. Майже кожен комп'ютер, виготовлений американськими виробниками та проданий за межі США,

забезпечений програмою, яка дозволяє Агентству національної безпеки (АНБ) читати зашифровані повідомлення [204, с.34-37].

Система «Ешелон» була створена з ініціативи Агентства національної безпеки США, яке згодом підключило до неї союзників із Англії, Нової Зеландії, Австралії та Канади. Ця глобальна мережа, сформована з кількох супутників і шістьох станцій прослуховування, здатна перехоплювати 3 млрд. повідомлень у день. Майже 80% одержуваної інформації використовувалося союзниками з метою економічного шпіонажу, і перш за все проти компаній країн-партнерів по Європейському союзові. Це не раз було приводом для багаторазових протестів Франції, Німеччини й інших країн, чиї компанії не отримували вигідних пропозицій через те, що конфіденційна інформація ставала відомою конкурентам [174, с.262]. Так, технічний консультант Європарламенту А. Помпіду вважав, що саме завдяки «Ешелону» французька фірма «Томсон-СіЕсЕф» втратила великий контракт із Бразилією на створення радарних комплексів через те, що американській стороні стали відомі деталі підготовлюваної угоди. В результаті контракт отримала американська фірма «Рейтеон» [91, с.140].

Лондонська газета Sunday Times опублікувала витяги зі спеціальної доповіді МІ-5, в якій йдеться про те, що контррозвідка Британії звинувачує Китай в електронному шпіонажі. Діяльність китайських розвідувальних органів у цій сфері «є однією з найсерйозніших загроз для безпеки Сполученого Королівства», цитує газета висновки експертів МІ-5. За даними британської контррозвідки, китайські комп'ютерні хакери, які працюють на спецслужби, здійснюють кібератаки на інформаційні системи британських компаній у галузі оборонного комплексу, енергетики, зв'язку й обробної промисловості. Як зазначається у виданні, нещодавно влада США також вимагала від Пекіна розслідувати проведену з

китайської території хакерську атаку проти служби електронної пошти Інтернет-компанії Google.

Автори доповіді попереджають британських бізнесменів: «Під час конференцій або візитів на запрошення китайських компаній ви можете отримати в подарунок фотоапарати або інші пристрої, що з'єднуються з комп'ютером через вхід USB. Були випадки, коли такі «подарунки» містили в собі пристрої - «трояни» або інші види шкідливих програм», - йдеться в документі.

Китайці успішно комбінують високотехнологічні методи збору інформації з найдавнішими прийомами шпіонажу, відзначають у МІ-5.

Два роки тому у помічника прем'єр-міністра Британії Гордона Брауна під час поїздки до Китаю був вкрадений смартфон - мобільний телефон із функціями персонального комп'ютера. Електронний пристрій зник після того, як держслужбовець познайомився з китаянкою на дискотеці в шанхайському готелі.

В іншій доповіді, підготовленій минулого року Об'єднаним комітетом британського уряду у справах спецслужб, стверджувалося, що китайські хакери нібито здатні в потрібний для Пекіна момент порушити роботу електронних систем життєво важливих галузей британської економіки, таких як енергетика, водопостачання та постачання продуктів харчування [115].

Як стверджує HGlobe and Mail, посилаючись на неназване джерело в державних структурах, Китай знає про рішення Канади більше, ніж міститься в публічних заявах Оттави. "На цьому тижні (в березні 2009 р.) проблема кібершпіонажу привернула загальну увагу: канадські фахівці розкрили велику шпигунську мережу в інтернеті, вже прозвану GhostNet", - нагадують журналісти Омар ель Аккад і Колін Фриз. Шпигунські програми потрапили майже на 1300 комп'ютерів на планеті, у тому числі в міністерства та посольства. Кістяк мережі, очевидно, знаходився на

серверах у Китаї, але канадські політики остерігаються публічно звинувачувати Пекін у кібершпіонажі, відзначають автори. І лише фахівець із комп'ютерної безпеки, який побажав залишитися анонімним, заявив газеті: "Причетність Китаю до деяких атак - це секрет Полішинеля" [211].

Південна Корея також обвинуватила Китай в електронному шпіонажі, заявивши, що, "неназвані китайські хакери" провели шпигунські кампанії через Інтернет на ряд урядових і великих промислових об'єктів країни.

Як повідомляється, атаки велися традиційними способами - розсилкою спаму з вірусами, цільовими атаками та створенням шахрайських сайтів. З такою заявою в кінці минулого тижня виступили МЗС Південної Кореї, ряд високопосадових чиновників у Сеулі й офіційні представники розвідки країни.

Національна служба розвідки Кореї виявила факти хакінгу з боку КНР ще на початку цього року, попередивши всі урядові органи та великі компанії про небезпеку з боку сусідньої держави. Повідомляється, що хакери відправляли іменні e-mail на ящики корейських дипломатів, здійснювали спроби впровадження вірусів в урядові мережі країни та інші негласні операції.

Юрист із південнокорейської правлячої Національної партії Південної Кореї Лі Джун Хун заявив у корейському парламенті, що в результаті атак Китаю в руки Пекіна міг потрапити якийсь "значимий клас засекречених документів", які, ймовірно, стосуються Північної Кореї [250].

Усього якихось десять років тому, близько 70% світового Інтернет-трафіку припадало на США. Американці використовували цю унікальну ситуацію у власних соціально-політичних цілях, а також у діяльності розвідслужб. Циркулююча Інтернетом інформація про різні країни, фірми,

організації, людей ретельно відстежується та використовується спеціальними службами США, щоб забезпечити максимальні переваги американському урядові та корпораціям на світовій арені. Не дивно, що багато країн, у тому числі друзів і союзників США, в останні роки насторожував підвищений їхній інтерес до фінансової й економічної інформації компаній, що проходить через американські маршрутизатори.

Для отримання ще більших обсягів електронної інформації американський уряд під приводом боротьби з тероризмом задіяв і прикордонний контроль. За останній час Міністерство національної безпеки значно посилило правила огляду ноутбуків й інших цифрових пристроїв при проходженні паспортно-митного контролю на в'їзді в країну. Перевірка цифрових пристроїв проходить спільно з особистим оглядом пасажирів. Співробітники Міністерства отримали право повністю копіювати зміст таких пристроїв, а якщо він закодований, то вимагати від власника пароль доступу. У разі неотримання пароля служба безпеки може вилучати комп'ютер і залишати його для з'ясування обставин на невизначений термін. А між тим, люди везуть із собою масу найрізноманітнішої інформації - економічної, фінансової, технологічної, приватної, конфіденційної й т.д. Уся вона або чимала її частина в кінці кінців стає надбанням розвідувальних служб США [76, с.65].

У ФБР сконструйовано спеціальний пристрій для виявлення мобільників і стеження за господарями без дозволу суду. Новітня технологія дозволяє створювати фальшиві базові станції так, що стільникові телефони, які знаходяться неподалік, приєднуються до них і видають усі належні для їхньої ідентифікації дані. Апаратура може знаходитися в режимі очікування, поки в поле її досяжності не потрапить мобільник потрібної людини, або просто збирає ідентифікатори всіх телефонів, що опинилися поблизу, для подальшого аналізу.

Процес криміналізації комп'ютерних злочинів був об'єктивно викликаний стрімким розвитком комп'ютерних технологій і формуванням інформаційних відносин у західних країнах у 50-60-х роках XX століття. Так, перший у світі зареєстрований комп'ютерний злочин був скоєний у 1958 році, і з подальшим розвитком комп'ютерних технологій кількість злочинів у цій сфері та збитки від них стали неухильно збільшуватися [134, с.13].

Слід зазначити, що на даний час закони окремих держав щодо електронного шпіонажу серйозно різняться та погано сумісні. Наприклад, у Норвегії, Сінгапурі, Словаччині, Філіппінах, Південній Кореї, Україні криміналом вважається лише несанкціонований доступ у захищені комп'ютерні системи, зараження вірусами, протиправне використання комп'ютерних систем й інформації. У Данії, Швеції, Швейцарії, Франції, Японії до комп'ютерних злочинів віднесені дії, які заподіюють шкоду чужому майну, включаючи електронні дані. Нарешті, у США, Великобританії, ФРН, Нідерландах кримінальними вважаються дії, пов'язані не тільки з майновим збитком і загрозою національній безпеці, але й з порушенням прав особистості.

23 червня 2011 р. в американському конгресі почалися слухання щодо законопроекту про кібербезпеку, внесеного адміністрацією Барака Обами. Президент США запропонував збільшити термін тюремного ув'язнення для хакерів до 20 років. До полювання на комп'ютерних зломщиків підключилося і НАТО. У відповідь хакери, серед яких немало вихідців із Країн СНД, оголосили урядам війну. Головний сенс внесеного президентом США в конгрес законопроекту - різке збільшення покарання за комп'ютерні злочини. У разі схвалення пропозиції Барака Обами максимальний термін тюремного ув'язнення для хакерів збільшиться з теперішніх 10 до 20 років. Виступити з такою ініціативою президента США спонукала діяльність міжнародної хакерської групи Lulz Security,

яка здійснила за останній місяць ряд атак на ресурси великих комерційних й урядових структур. Хакерам вдалося зламати або обвалити інтернет-ресурси ФБР, ЦРУ і сенату США, Міжнародного валютного фонду, кількох банків, компаній Nintendo і Sony, британського Агентства з боротьби із оргзлочинністю й адміністрації президента Бразилії, а також ряду американських ЗМІ. Група Lulz Security утворилася на базі руху "хактивістів" (зломщиків із політичним підтекстом) Anonymous, які об'єдналися в віртуальне співтовариство заради боротьби з ворогами скандально відомого сайту WikiLeaks. У рядах "анонімів" чимало вихідців із країн СНД. А ось про склад Lulz Security майже нічого не відомо. Назву групи можна умовно перекласти як "глузування над безпекою". Вважається, що, на відміну від більшості "анонімів", складається вона зі справжніх хакерів-профі. За деякими даними, ядро групи становлять 6-10 осіб із різних країн, більшості з яких по 16-25 років, але один одного вони знають лише віртуально [114].

В Україні процес масової комп'ютеризації розпочався пізніше, ніж у США і Західній Європі, в кінці 1980-х - першій половині 1990-х років. Розвивався ринок комп'ютерів і програмного забезпечення, підвищувався рівень професійної підготовки користувачів, розширювалися потреби організацій у вдосконаленні технологій виробництва даних. Комп'ютер став практично обов'язковим елементом робочого столу не тільки керівників, а й рядових співробітників. Одним із наслідків цього процесу стала криміналізація сфери обігу комп'ютерної інформації.

Що стосується законодавства України, то 12 жовтня 2010 р. Президент України Віктор Янукович підписав Закон «Про внесення змін до Закону України "Про ратифікацію Конвенції про кіберзлочинність".

Конвенція про кіберзлочинність була укладена 23 листопада 2001 року в Будапешті. Україна ратифікувала її 7 вересня 2005 року.

Даним законом передбачено, що в Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних із комп'ютерними системами і даними, переслідуванні осіб, які обвинувачуються у скоєнні таких злочинів, а також зборі доказів у електронній формі, є Міністерство внутрішніх справ України.

Крім того, в законі зазначено, що цілодобовий контактний пункт із питань протидії кіберзлочинності буде створений на базі Міністерства внутрішніх справ у межах його штатної чисельності (Про ратифікацію Конвенції про кіберзлочинність). Відповідно до цього закону на МВС України покладаються повноваження щодо створення та забезпечення працездатності цілодобової контактної мережі - інфраструктури, передбаченої будапештською угодою (текст у перекладі доступний на сайті MediaLaw.ru). Наявність такого національного механізму дозволить здійснювати централізований збір інформації про кіберзлочини; надавати допомогу в розслідуваннях, що проводяться учасниками Конвенції; своєчасно виявляти зловживання та закликати правопорушників до відповідальності.

Отже, проблема кіберзлочинності, електронного шпіонажу турбує всі країни. В кінці червня 2011 р., група фахівців з Інтернет-безпеки провела в Сінгапурі зустріч, на якій обговорювався запуск нової глобальної системи для захисту інформації в Інтернеті від кіберзлочинців, повідомляє The New York Times. Фахівці назвали цю систему "променем світла", який зайнявся на тлі атак, що почастішали останнім часом, на різні інформаційні системи. "Не важливо, в якій точці світу ви будете перебувати, ви зможете переконатися в достовірності кого-завгодно і чого-завгодно", - сказав один із інженерів проекту Ден Каменські. Вчені розробляють спеціальну систему числових кодів, які дозволять захистити

мережевий трафік від шкідливих програм, тобто перевіряти всю інформацію, що надходить на комп'ютер із Інтернету та навпаки. Ця програма розробляється вже рік. Система числових кодів буде зберігатися у трьох центрах обробки даних, які облаштуються в Сінгапурі, Цюріху та Сан-Хосе. Ці центри, у свою чергу, будуть обладнані п'ятьма рівнями захисту [43].

Комунікаційна сфера взагалі та ЗМІ зокрема завжди були активними учасниками збройних конфліктів. У цьому контексті вельми символічно виглядає факт, який 60 років тому став приводом для Другої світової війни - напад на радіостанцію в Глейвіце. Історики відзначають, що Б. Муссоліні, на думку його ж соратників, при плануванні військових операцій більше уваги приділяв тому, які заголовки з'являться в газетах, ніж військовій доцільності. Однак у Другій світовій війні зазнали поразки саме ті держави, у яких досягнення в інформаційно-пропагандистській сфері були найбільш переконливими. Використання ЗМІ в той час мало порівняно невелике значення для військового успіху [189].

Про роль засобів масової інформації та комунікації в інформаційній війні в наступному підрозділі.

2.3. Засоби масової інформації та комунікації в інформаційній війні

Значна частина світу перетворилася в єдину аудиторію, яка отримує одну й ту ж інформацію і яку хвилюють одні й ті ж події. Мабуть, немає такого віддаленого куточка, мешканці якого б не мали можливості практично відразу ж дізнаватися про те, що відбувається в інших місцях:

вироблені у величезних кількостях і недорогі транзисторні приймачі є повсюдно, навіть у селах країн третього світу, які знаходяться далеко від центрів політичної влади [7, с.112]. Засоби масової інформації - газети, радіо, телебачення, журнали, а тепер ще й Інтернет, відіграють важливу роль в інтернаціоналізації установок і цінностей на планеті.

У наш час навіть виникнення таких понять як «інформаційна війна», «медіа-агресія», «інформаційна безпека» свідчить не тільки про тісний зв'язок мас-медіа з конфліктними ситуаціями, а й про те, що у збройних конфліктах сучасності боротьба на інформаційному полі не менш важлива, ніж безпосередньо військові дії. Якщо до недавнього часу війна впливала переважно на інформаційну сферу, зокрема на журналістику (наприклад, Перша світова війна стала стимулом для появи та розвитку в США аналітичної журналістики, так як американці не могли збагнути, яким чином убивство ерцгерцога Фердинанда послужило причиною такого конфлікту), то останнім часом спостерігається зворотний зв'язок, причому як на макро- так і на мікрорівні [189].

Як пише німецький філософ М. Больц, історія сучасної війни багато в чому збігається з історією нових медіа. «Застосування Наполеоном оптичного телеграфу та винахід наручних годинників для координації руху військ в англо-бурській війні - це лише анекдотичні поодинокі приклади. Манфред Шнайдер резюмує: «Можна без зусиль побачити, що великі військові події (наприклад, насильницькі реорганізації політичних просторів) у ході старої та нової історії були пов'язані з дестабілізацією тимчасових і постійних інститутів за допомогою нових технік комунікації та зберігання інформації: створення Римської імперії та папірус, хрестові походи і папір, Тридцятирічна війна і друк, революційні війни та нові техніки швидкого друку, Перша світова війна й телефон, Друга світова війна і радіо, В'єтнамська війна та телебачення». Кінцевим пунктом цього

розвитку стала сьогоднішня єдність наказу, комунікації, контролю та знання [24, с.65].

Роль ЗМК і ЗМІ в інформаційній війні зумовлена їхніми можливостями формувати медіапорядок денний у політичному дискурсі та впливати на механізми прийняття рішень. Як пише В. Євдокимов, «Найчастіше мас-медіа в ході інформаційної війни використовують реальні та вигадані дані, розраховані на прикрашання ролі того чи іншого суб'єкта в політичному процесі. Утворюється химерна суміш правдивої інформації та майстерної брехні. Ведення інформаційної війни забирає у її учасників час і енергію, які необхідні для досягнення інших цілей, наприклад, реалізації програм соціально-економічного розвитку територій» [74, с.104].

ЗМІ та ЗМК сьогодні стали найпотужнішим елементом механізму цілеспрямованого конструювання політичних порядків, засобом вибудовування необхідних владі зв'язків і відносин із громадськістю. Інформація, яка надається ЗМІ, ніколи не буває нейтральною, вона являє собою спроби пануючих еліт створити таке зображення дійсності, яке вигідне їм, та «виправдовує» їхню практичну політику, «упаковану» в стереотипні точки зору, що вигідні владі та виносять на передній план лише частину того, що відбувається в дійсності [78, с.10].

Ф. Уебстер пише, що «В ситуації, коли «ворог» може мати лише дуже обмежений доступ до каналів розповсюдження інформації (через надзвичайну ситуацію з її організаційними, етичними та політичними особливостями), коли ми прагнемо до перемоги (а не до тріумфу істини), з'являється маса можливостей для спотворення та введення в оману, та й мотиви, через які вдаються до брехні, загалом-то легко зрозуміти. У подібній ситуації і політики, і військові розглядають ЗМІ як засіб боротьби з ворогом, тобто це є зброя пропаганди» [212, с.268].

У даний час інформація пронизує всі сфери сучасного життя і для переважної більшості населення найважливішим засобом зв'язку з зовнішнім світом стали Інтернет, телебачення, радіо та преса. Цим зумовлена та особлива важливість інформаційної зброї, сфера застосування якої настільки широка, що сьогодні ряд фахівців й експертів беруть на себе сміливість стверджувати, що лише однією цією зброєю можна вигравати та програвати війни. За словами Дениса Богуша, віце-президента Української ліги зі зв'язків із громадськістю: «60% інформаційних атак припадає на телебачення, на другому місці - Інтернет. Наприклад, для «правильного» висвітлення газового конфлікту Газпрому й України, російською стороною було створено 8 сайтів, де щодня (навіть 31 грудня та 1 січня) розміщувалися якісь новини» [182].

«Поширюючи ті чи інші повідомлення та матеріали, ЗМІ створюють певну громадську думку, настрій, формуючи погляди і поведінку окремих особистостей, соціальних груп, а, у підсумку - всього суспільства. Іншими словами, повідомляючи своїм читачам, слухачам або глядачам певну інформацію, ЗМІ викликають у них певні почуття, відповідно до яких у людей формуються й певні моделі поведінки. Враховуючи, що споживачем масової інформації є практично кожна людина, схожі процеси подібним чином можна сформувати у всього суспільства в цілому або у переважної його частини» [187].

Ситуація складається така, що засоби масової інформації фактично перестають відображати дійсність, а самі створюють образи та симулякри, які й визначають реальність нашої дійсності, або, користуючись термінологією Ж. Бодрійяра, «гіперреальність», яка виявляється більш реальною, ніж сама реальність. Навіть війна в сучасному постмодерністському розумінні, завдяки засобам мас-медіа, перетворилася на тотальну симуляцію. Досягнення цієї видимості здійснюється не за допомогою дії реальних військових технологій, а за допомогою каналів

комунікації: текстів, що промовляються з екранів телевізорів, надруковані у газетах - війну намагаються виграти нетиповими для класичного розуміння засобами, тими ж, що й передвиборчі кампанії [1, с.8].

Ефективність Інтернету як засобу поширення інформації підтверджується ступенем охоплення аудиторії Інтернетом. Так, за наявними даними нових досліджень у липні 2010 р., кількість користувачів Інтернету в Україні становила більше 12 мільйонів чоловік. З 12000000 8,6 мільйона припадає на міста з населенням більше 50 000 чоловік. Ще близько 3,5 мільйона припадає на міста з населенням менше 50 тисяч осіб. Таким чином, враховуючи, що населення України становить 46 мільйонів жителів, рівень проникнення Інтернету в країні склав 25% [44].

Для порівняння, світовий Інтернет-трафік, як показало дослідження компанії TeleGeography, виріс за 2010 рік на 62%. У порівнянні з результатом минулого року (74%) спостерігається невелике уповільнення темпів зростання мережевих комунікацій, проте в цілому тенденція залишається у силі. Найбільша активність спостерігається у Східній Європі, а також у Південно-Східній Азії та Індії. Майже 100-відсотковий приріст трафіку зафіксований і на Близькому Сході. При цьому TeleGeography зазначає, що й у регіонах, де Інтернет освоєний найкраще - Західній Європі та Північній Америці - спостерігається стійке зростання: понад 50% на рік. "Провайдерам доводиться впроваджувати та встановлювати величезну кількість нового обладнання, щоб впоратися з таким зростанням трафіку", - прокоментував ситуацію голова компанії TeleGeography Алан Молдін.

У дослідженні також наголошується, що між розвиненими та країнами, що розвиваються, як і раніше зберігається величезний розрив із точки зору розвитку Інтернет-технологій. Так, наприклад, в Австрії, населення якої становить близько 8 мільйонів чоловік, кількість

користувачів Інтернету перевищує число жителів Африки, які мають доступ до всесвітньої мережі [30].

Рівень охоплення населення України державними програмами телерадіомовлення становив: УТ-1 - 94,4%, УТ-2 - 89,4%, УТ-3 -83,3%, обласного мовлення - 61,2%; УР-1 - 98, 8%, УР-2 - 7,8%, УР-3 - 8,3%, обласного радіомовлення - 52,3%. П'ята частина українських родин користується послугами кабельного телебачення [94].

Доводиться визнати, що ЗМК не завжди прагнуть відображати інтереси суспільства та надавати людям об'єктивну інформацію. Цим обумовлена потреба держави й суспільства впливати на їхню інформаційну діяльність, задавати через ЗМК власні пріоритети у висуванні та тлумаченні політичних проблем.

Щоб вести інформаційну війну протягом більш-менш тривалого періоду, суб'єкту необхідні відчутні ресурси, в якості яких використовуються мас-медіа. Такими володіють органи влади, впливові політичні партії, а також великі корпорації й окремі підприємці. Спостерігаючи наслідки таких війн, деякі дослідники оцінюють роль мас-медіа як класичної інформаційної зброї, яка належить тому, хто платить, тобто правлячій верхівці, та застосовується для управління власним народом за замовленням [185, с, 157].

Дослідники відзначають, що в даний час спостерігається боротьба за посилення впливу у сфері ЗМІ. Г. Бакулєв справедливо зауважує, що «Медіаіндустрія, яка змінюється сама, змушує змінюватися й інші громадські інститути, включаючи політичні, релігійні, ділові, військові та освітні. Тому не дивно, що їхні керівники постійно б'ють тривогу з приводу надмірної влади та шкідливого впливу медіа. Як тільки з'являються нові медіа, критики всіляко прагнуть затримати їхнє зростання або поставити їх під свій контроль» [17, с.79].

У зв'язку з цим у більшості країн Західної Європи запроваджений контроль за злиттям підприємств друку та введені обмеження питомої ваги загального тиражу видавництв на ринку. Так, у Німеччині встановлена гранично допустима питома вага загального тиражу. У Швеції проводиться політика економічної підтримки дрібних і середніх видавництв. У Франції в 1984 р. Національні збори прийняли Закон «Про обмеження концентрації й забезпечення фінансової ясності та плюралізму підприємств друку» [135, с.433].

Також у багатьох країнах робляться спроби поставити під контроль Інтернет. За результатами дослідження міжнародної правозахисної організації Freedom House, у списку країн із середнім рівнем свободи в Інтернеті опинилися Росія, Кенія, Мексика, Південна Корея, Грузія, Нігерія й інші. Найгірша ситуація зі свободою слова в Інтернеті в Китаї, Білорусі, М'янмі, Кубі, Саудівській Аравії та Ірані, який зайняв останнє місце у списку. Україна в дослідженні участі не брала.

Як відзначають дослідники, «З одного боку, відбувається саморегуляція мережної взаємодії - з'являються правила та норми спілкування на форумах і блогах, які розробляються учасниками мережевої комунікації, всередині мережевих спільнот; виникає модераторство при спілкуванні на різних сервісах і т.д. З іншого боку, держава намагається законодавчо регулювати інформаційну мережеву взаємодію; створюються технології управління мережевим доступом і наданням контенту, наприклад цензура та блокування певних сайтів (Китай, Білорусь й ін.). Мабуть, необхідна взаємодія держави й мережевих спільнот для вироблення та закріплення норм і правил мережевої комунікації, розробки етики мережевого спілкування» [180].

Влітку 2010 р. про свій намір розпочати боротьбу з незаконними матеріалами в Інтернеті повідомило і МВС України. Уточнювалося, що будуть перевірені всі сторінки «ВКонтакте» на наявність порнографії. У

першу чергу міліція буде шукати фотографії та відеозаписи з дитячою порнографією, сценами вбивств і насильства. А вже потім із їх розповсюдженням буде боротися особливий департамент.

Однак, як вважають експерти, наміри МВС спочатку спрямовані на встановлення повного контролю над мережею. "Боротьба з порно - це привід для повного контролю користувачів мережі. Якщо вони отримають контроль над акаунтами, то отримають і загальний доступ до мережі, який зможуть використовувати вже так, як їм захочеться, навіть у політичних цілях", - припускає керівник компанії Proloject у складі групи компаній Advanter Group Антон Білецький. На даний момент близько 80% інтернет-користувачів є учасниками соціальних мереж. При цьому "ВКонтакте" прописалися 70% від загального їх числа. Отже, отримавши контроль над одним сайтом, МВС візьме під свій контроль практично всіх українських інтернет-користувачів [141].

Ситуація зі свободою інтернету була вивчена організацією Freedom House у 37 країнах. Експерти прийшли до висновку, що разом із зростанням числа користувачів мережі, уряди багатьох країн намагаються знайти способи контролювати активність своїх громадян в Інтернеті. «Антидемократичні режими приділяють все більше уваги та ресурсів на те, щоб обмежити суспільну дискусію онлайн» - йдеться у звіті. Приміром, у 2000-х роках у Росії Інтернет став популярним для неї місцем, оскільки, на відміну від ЗМІ, не піддавався цензурі.

У кожній із 37 представлених у рейтингу країн намагалися простежити чи створюються для доступу в Інтернет певні бар'єри, чи порушуються права користувачів у мережі, як лімітується доступний контент і чи впливає місцева влада на відомих громадських активістів, блогерів й інтернет-журналістів.

Так, наприклад, однією з серйозних проблем у сфері онлайн-свободи в Росії експерти називають кіберзлочинність: 9% усіх інтернет-атак у світі

в 2010 році були здійснені з території цієї країни. Громадяни Росії рідше користуються антивірусними програмами, і їхні комп'ютери легко перетворюються у «ботнети».

Країнами з найвищим рівнем інтернет-свободи визнані Естонія, США та Німеччина. Замикають рейтинг Китай, Куба, М'янма й Іран [139].

Слід зазначити, що Інтернет контролювати набагато складніше у порівнянні з друкованими ЗМІ та телебаченням. Це пояснюється тим, що аудиторія Інтернету є і споживачем, і виробником, тобто в порівнянні з пасивною аудиторією друкованих ЗМІ та телебачення (які мають обмежену кількість продуктів) активна.

Дж. Макнамара зазначає, що «Мас-медіа регулярно претендують на незалежність і об'єктивність. Найчастіше ця претензія безапеляційна та необґрунтована. Якщо вірити заявам журналістів і редакторів, то ними рухають виключно прихильність правді та справедливість. Часом ЗМІ зі своєю моральною перевагою та самопроголошеною праведністю здаються надто наївними» [131]. Проте, як пишуть автори підручника «Політичні комунікації», «Будучи головними «розігрівачами» громадської думки, стимулюючими її активність щодо суспільно значущих питань політичного розвитку, ЗМК у рівній мірі можуть як спровокувати масовий протест, політичний скандал, кризу у відносинах влади та суспільства, так і запобігти розвитку конфлікту, зробивши, наприклад, доступною для суспільства певну інформацію» [174, с.73].

Класичним прикладом ключової ролі ЗМІ у запобіганні міжнародному конфлікту є Карибська криза в жовтні 1962 року, коли світ перебував на межі ядерної війни. Уникнути військового зіткнення між СРСР і США вдалося за безпосередньої участі Московського міжнародного радіо (нині «Голос Росії»). Тоді заяву радянського уряду, яка зняла гостроту ситуації, було передано по радіо до того, як вона була офіційно отримана у Вашингтоні [190].

Сьогодні ЗМІ - вже не стільки джерело максимально повної та достовірної інформації про ті чи інші події, скільки відображення інтересів, стереотипів, ідеологічних установок, конкуруючих/конфліктуючих сил. Саме в цьому проявляється їхній кризовий/конфліктний потенціал. Здатність ЗМІ провокувати ескалацію насильства яскраво показав «карикатурний скандал», який викликав у ряді країн зіткнення та погроми. «Карикатурний скандал» продемонстрував широке, а в разі радіо, телебачення й Інтернету практично всеосяжне охоплення аудиторії і, що особливо важливо, наявність зворотного зв'язку з нею. Публікація карикатур у данській газеті та хвиля масових маніфестацій протесту, що пішла за цим в арабських і мусульманських країнах, призвели у глобальному медіапросторі ефект вибуху бомби: новини з заголовками «карикатурний скандал» і «карикатурна війна» миттєво опинилися на верхніх щаблях новинних стрічок світових інформаційних агентств.

Карикатури на пророка Мухаммеда були передруковані у 132 виданнях 56 країн, що ще сильніше «підігріло» увагу світової аудиторії до світового скандалу та спровокувало ще більше обурення арабів і мусульман у всьому світі. Так за допомогою ЗМІ «карикатурний скандал» не просто отримав глобальне освітлення, надовго зайнявши лідируючі позиції в рейтингу за кількістю публікацій, а й сформував конфліктний дискурс у світовому масштабі. Тим самим було зайвий раз продемонстровано, що можливість передавати інформацію на значні відстані й охоплювати широку аудиторію робить світові ЗМІ впливовим гравцем на міжнародній арені та визначає їхній кризовий потенціал, - здатність провокувати і «підігрівати» конфлікти/кризи у глобальному й локальному масштабах у тих сферах, які найбільш схильні до впливу громадської думки [106, с.39].

Багато кампаній розпочинаються з висвітлення будь-яких сенсаційних, скандальних фактів, щоб надати громадській думці потрібного організаторам акції напрямку. Журналісти не зупиняються перед спотворенням фактів, втручанням в особисте життя, оприлюдненням конфіденційних матеріалів. У сучасній політичній практиці є чимало прикладів використання компроматів проти високопосадових осіб із метою їх усунення з посади. Так, наприклад, в Ірані скомпрометували міністра внутрішніх справ Ірану - Кордана, який вважався найосвіченішим політиком в оточенні президента Махмуда Ахмаді-Нежада. В якості компромату слугувала інформація про те, що його диплом доктора юриспруденції Оксфордського університету фальшивий, і це стало однією з причин відсторонення його від посади. Жертвами компрометації були міністр праці Греції - Цитурідіс у кабінеті К. Караманліса, М. Салін як головний претендент-жінка на пост прем'єр-міністра Швеції, міністр освіти Д. Бланкетт і міністр торгівлі та промисловості Мандельсон у кабінеті Т. Блера [144]. У ході президентської виборчої кампанії в США 2008 р. прихильники тоді ще кандидата в президенти Б. Обами поширювали інформацію про Дж. Маккейні стосовно його зради в період перебування у в'єтнамському полоні. Не залишалися в боргу і прихильники Дж. Маккейна, які звинувачували кандидата у президенти Б. Обаму в отриманні грошових коштів від нелегалів. У цей же період великим тиражем була випущена фальшива «Нью-Йорк Таймс», в якій публікувалися сфабриковані вибачення К. Райс за війну в Іраку, а Дж. Буш обвинувачувався у державній зраді. Широко висвітлювалися в засобах масової інформації й захоплення американського президента Б. Клінтона.

Яскравим прикладом використання засобів масової комунікації (ЗМК) в інформаційній війні стала вже не раз нами згадана «Буря в пустелі». Комітет начальників штабів ВС США розробив спеціальний

план заходів із дезінформації, реалізація якого здійснювалась через ЗМК. Поширювалися відомості, що не відповідають дійсності, про характер підготовки збройних сил до можливих бойових дій проти Іраку. Головна частина дезінформаційної операції була реалізована у другій половині серпня 1990 року - в момент інтенсивного нарощування угруповання американських військ у Саудівській Аравії. Засоби масової комунікації передавали, що в регіон перекинуто величезну кількість військових і техніки, це повинно було налякати Ірак і змусити його відмовитися від опору. Слід зазначити, що військово-політичне керівництво та командування багатонаціональними силами (БНС) блискуче впоралося з завданням координації діяльності всіх ЗМК, задіяних в інформаційній війні. Так, наприклад, коли було необхідно, поширення офіційної інформації було припинене.

«Командування об'єднаного штабу ввело жорсткий 48-годинний мораторій на повідомлення ЗМК й окремі обмеження на будь-яку інформацію, що стосувалася змісту оперативних планів і місця розташування угруповань військ. І лише через дві доби, з досягненням перших позитивних результатів наступальної операції, ЗМК була знову надана можливість широкого висвітлення подій. Спеціально створена радіостанція «Голос затоки» не тільки ретранслювала програми «Бі-бі-сі» та «Голосу Америки», але протягом майже двох місяців по 18 годин на добу вела власні передачі з наземних станцій на території Туреччини та Саудівської Аравії, а також зі спеціально обладнаних під ретранслятори літаків ЄС-130. Для забезпечення оперативності в підготовці та розповсюдженні репортажів активно були задіяні транспортні вертольоти сухопутних військ і морської піхоти США, що доставляли в розташування військ кореспондентів провідних інформагентств США та їхніх союзників» [168].

Аналіз інформаційних кампаній національних американських ЗМІ під час двох військових операцій США в Іраку (2.08.1990-28.02.1991) і 12.09.2002-1.05.2003), показав широке застосування ними інформаційно-комунікаційних технологій і методів впливу на аудиторію. При цьому було характерне не переважання якоїсь однієї технології над іншими, а їх симбіоз у рамках кампанії, організованої з урахуванням традицій освітлення виборчих і спортивних кампаній. У числі використовуваних прийомів - циклічність обігу інформації, зумовлена тими чи іншими подійними періодами, наростання інтенсивності інформаційного обміну до певного терміну (наприклад, день закінчення ультиматуму), наявність безперечного лідера (президент США Дж. Буш-мол.), який бореться з супротивником-антагоністом (президент Іраку С. Хусейн), динамічне підкріплення інформаційного висвітлення результатами соціологічних опитувань і рейтингів тощо.

Американські ЗМІ застосовували маркетингові та немаркетингові технології інформаційного впливу на суспільства. Зокрема, вони використовували не тільки прийоми та маніпуляції, які сприяють просуванню офіційної пропаганди, а й PR-технології, створюючи емоційно-оцінний контекст відповідно до комунікаційної стратегії адміністрації США. У другій кампанії слово «пропаганда» набуло позитивну оцінну характеристику в контексті наслідків терактів 11 вересня 2001 р. (боротьба проти міжнародного тероризму), коли критика дій уряду США не віталася суспільством і сприймалося більшістю американців як прояв непатріотичної позиції.

Завдяки революції в телерадіомовному обладнанні іракські конфлікти змінили не тільки правила журналістики, вони вплинули на проведення світової політики й інформаційних кампаній у глобальному просторі. Вперше в 1990-1991 рр.. президенти США й Іраку використовували єдину на той час супутникову телекомпанію Сі-Ен-Ен

для звернення один до одного і народів, залучених у конфлікт країн. Показ у прямому ефірі телерепортажів й інтерв'ю впливав на перебіг і результат криз. Практика організації прямих трансляцій у момент звершення подій отримала назву «ефект Сі-Ен-Ен», тобто феномен значного впливу ЗМІ на процес прийняття урядових рішень. У ході першого конфлікту Сі-Ен-Ен показувала події в прямому ефірі, що дозволяло президентам і простим громадянам одночасно спостерігати одні й ті ж події. У другому конфлікті трансляція подій в режимі реального часу велася вже не тільки в телеефірі, а й на Інтернет-сайтах усіх великих ЗМІ США. Тим самим, ЗМІ підштовхували політиків і військових до прийняття важливих рішень у рамках новинного циклу (до певного часу - виходу з друку тиражу газети або до виходу в ефір випуску новин).

Емоційний вплив ЗМІ, пригнічуючи розум і раціональність людини, призводить до високої ефективності використання ЗМІ з метою маніпулювання - прихованого управління свідомістю та поведінкою людей із метою примусити їх діяти в тому числі й всупереч власним інтересам. Переваги цього - непомітність для керованих, відсутність жертв, економічність. Інформаційна «наркотизація» сприяє нав'язуванню ілюзорних ідей і міфів, які сприймаються без раціонального осмислення. Для укорінення міфів існує безліч розроблених спеціальних прийомів лінгвістичного маніпулювання та методів впливу на людей з урахуванням закономірностей масової психології [135, с. 434].

Політтехнологи справедливо відзначають, що вся публічна політика сьогодні будується переважно на емоціях: саме збуджені емоції стають провідником більшості маніпулятивних впливів. Емоціями, які найбільш часто експлуатуються політиками, є: потреба в любові та схваленні, відчуття небезпеки, страх перед невизначеністю; престижні цінності, сексуальні інстинкти, почуття обов'язку та справедливості, почуття провини.

С. Беннет виділяє чотири різновиди спотворення новин: персоналізація, драматизація, фрагментація і нормалізація. Персоналізація новин має на увазі акцентування уваги на конкретних особистостях під час розповіді про процеси, події або явища. Драматизація виникає, коли новинний матеріал відбирається, виходячи з його високого драматичного або розважального значення, а не через його важливість для суспільства. Фрагментація передбачає передачу новин окремими стислими зведеннями (випусками новин, спецпрограмами або рубриками), їх дрібнення. Нормалізація передбачає подачу новини як проблеми, яка може бути вирішена відповідно до існуючих у суспільстві норм [25, с.157].

«Основна функція стратегії управління новинами полягає в контролі над новинним порядком денним у ЗМІ з метою впливу на громадську думку. Хоча це передбачає наявність прямого зв'язку між новинним порядком денним ЗМІ та громадською думкою, про що йдуть суперечки, основна ідея полягає в тому, що якщо спосіб висвітлення подій у даному ЗМІ максимально позитивно сприймається громадськістю, то найімовірніше, партія, уряд чи організація отримує її підтримку. Всі організації, зацікавлені в якомусь питанні, намагаються отримати контроль над новинним порядком денним» [127. с.184].

Як пише Н. Больц, «Хоча журналісти неохоче в цьому зізнаються, війна - найкраща тема для медіа. Постійно йдуть новини, всім цікаво і всіх зачіпає. Не випадково наші війська висаджуються у прайм-тайм. Люди дивляться війну у прямому ефірі, перебуваючи в той же час у безпеці. Але найважливіші питання про співвідношення війни та її висвітлення мас-медіа не можна ось так відразу критично, палаючи обуренням, перевести в тупик маніпуляцій. Занадто різні ефекти світових новин, щоб їх можна було просто вписати в схему легітимування та виправдання» [24, с.73].

Дослідники виділяють наступні вербальні та невербальні засоби впливу, що застосовуються американськими ЗМІ: встановлення новинного

порядку денного; підбір джерел інформації; символізація подій, людей і явищ, створення та використання особливої лексики; посилена візуалізація інформаційних матеріалів, проведення історичних аналогій; персоналізація подій; фрагментація. ЗМІ активно зверталися до сили символів, міфів, особливої мови, ритуалів й ідеології при описі подій навколо іракської проблеми, воліючи при цьому висвітлювати тільки дипломатичну сторону конфлікту, а не показувати суспільству реальне життя в регіоні конфліктів. Результатом усіх цих використовуваних ними прийомів стала не тільки концентрація уваги громадськості на конфліктах і силовому способі їх урегулювання, але й єднання американської нації перед обличчям зовнішньої загрози.

Факти маніпулювання з боку засобів масової інформації, використання їх для проведення спеціальних інформаційних операцій, необ'єктивність і упередженість у висвітленні суспільно-політичних подій ведуть до падіння довіри до ЗМІ з боку населення. В цьому зв'язку можна згадати відоме зауваження Н. Лумана, яким він розпочинає свою книгу «Реальність засобів масової інформації»: «Все, що ми знаємо стосовно нашого суспільства й навіть світу, в якому ми живемо, ми знаємо через засоби масової інформації... І, навпаки, ми знаємо так багато про засоби масової інформації, що нездатні їм довіряти як джерелу інформації» [262, с.9].

Як відомо, основою інформаційної війни є маніпулювання. Відомий фахівець у галузі політичного маніпулювання О. Чумиков розкриває механізм маніпуляції за допомогою ЗМІ, виділяючи три основні етапи інформаційного впливу:

- на першому етапі формується несистематизований і масштабний інформаційний потік («інформаційний вал»), який регулярно направляється на цільові аудиторії;

- на другому етапі, коли довіра до різноманітних інформаційних матеріалів стає відчутною, інформація починає носити вибірковий, дозований характер («сегментування інформаційного потоку»);

- на третьому етапі відбувається розширений обмін інформацією зі «своїми» суб'єктами інформаційного поля й обмежується інформаційний потік для «чужих» («інформаційне партнерство», «інформаційна закритість») [223, с, 656].

З метою штучного конструювання політичних реакцій і запитів населення крім маніпулювання використовуються дезінформація та фальсифікація відомостей. Дезінформація може виступати складовою частиною маніпулятивних технологій як особливого виду інформаційного впливу, спрямованого на приховування комунікатором власних цілей, але при цьому збуджуючи у реципієнта наміри, що збігаються не з його власними бажаннями, а з інтересами даного комунікатора.

Термін «дезінформація» був введений вищим командуванням німецької армії в роки Першої світової війни для позначення тієї частини польової тактики роботи з супротивником, метою якої було введення його в оману. Ця тактика мала на увазі прямий обман супротивника, використання брехні, наклепів, напівправди, які приховують часом не тільки справжній зміст явищ і фактів, а й саме їх існування.

Політична історія дала множинні приклади використання дезінформації не тільки як часткової технології, але й як масштабного інформаційного курсу держави, що забезпечує здійснення великих політичних цілей. Наприклад, система свідомо сфабрикованих і цілеспрямовано поширюваних помилкових повідомлень прикривала початок військових дій нацистів проти СРСР, сприяла розгрому вищого військового командування в країні перед Другою світовою війною і т.д.

У даний час подібні прийоми широко використовуються не тільки у сфері міждержавних відносин як прикриття справжніх цілей тих чи інших

країн, а й на внутрішньому політичному ринку у вигляді брехливих повідомлень про наміри конкурентів і відомостей про неіснуючі у них цілі, у формі приховування відомостей про події, що відбулися, у вигляді тенденційної оцінки та упередженого коментування фактів, що приховує їхню суть, і т.д. У цьому сенсі найвитонченішою технологією дезінформування є часткове, дозоване використання правдивої інформації, яке дозволяє представити подію в потрібному та спотвореному вигляді.

Залежно від цілей ретельного приховуваного управління мисленням і поведінкою контрагента обираються й відповідні інформаційні прийоми, наприклад, уривчасте і вибіркове інформування, коли реципієнту дається неповна інформація про події, а також «вал інформації», який не дозволяє людині відрізняти суттєве від несуттєвого, «зминає» будь-які орієнтири та пріоритети свідомості й кидає її в стан розгубленості. До найбільш показових прийомів маніпулювання можна віднести й клішування інформації, тобто використання готових образів, значень і стереотипів, які не потребують смислової обробки і тому викликають однозначно програмовану реакцію, що знижує поріг критично сприйнятої інформації. Наприклад, за радянських часів негативне значення мали образи капіталізму, приватної власності, а позитивне - соціалізм, з яким асоціювався цілий набір позитивних якостей і моментів: мир, стабільність, ясність світогляду й т.д. Такі клішовані образи, що тяжіють до чорно-білого зображення світу політики, часто використовують для розпалювання соціальної, національної та релігійної ворожнечі між людьми.

Найбільш характерними та широко використовуваними прийомами й техніками маніпулятивного типу є «навішування ярликів», тобто присвоювання окремим особам або їхнім діям однозначно позитивних чи негативних оцінок; використання «подвійних стандартів» при оцінці дій союзників і супротивників, «помилкова аналогія», коли порівнюються два

по суті різних, але зовні схожих явища та ін. Для маніпулятивних технологій характерні також відмова від розгорнутої аргументації, підміна її технікою психологічного навіювання. В цей інформаційний арсенал входять акції, що впливають на больові соціальні точки, наприклад, традиції конфронтації між різними групами населення, сумніви в щирості влади або союзників і т.д. Такі акції мимоволі викликають у людей страх, тривогу, ненависть. Вельми поширена і дифамація, тобто оприлюднення ганебних відомостей про когось, «гра цифрами», які передбачають комбінування статичних даних і здатні «обґрунтувати висновки, прямо протилежні існуючим реаліям».

У сучасній дослідницькій практиці утвердилася думка про те, що Інтернет кинув виклик традиційним ЗМІ, запропонувавши принципово нові форми ведення інформаційної війни. Разом із тим складно заперечувати й те, що Інтернет, по суті, запозичив багато інструментів емоційного впливу, властивих традиційним ЗМІ. Так, австралійський дослідник Е. Лоу зазначає, що специфіка обробки фактів для Інтернет-сайту залишається приблизно такою ж, що і для будь-якого аудіовізуального ЗМІ. Змінюється лише спосіб передачі інформації, стверджує він, але не специфіка самої інформації. Однак, на відміну від будь-яких інших ЗМІ, що функціонують в умовах вже розробленої законодавчої бази, Інтернет як і раніше в цьому відношенні залишається «темною конячкою». Правове оформлення поки що не встигає за розвитком нових технологій. За справедливим твердженням Д. Маквейла, британського фахівця в галузі масових комунікацій, Інтернет сьогодні функціонує, по суті, на напівлегальній основі. До сих пір немає жодної країни, де б він став предметом самостійного правового регулювання. Правда, відзначає Д. Маквейл, користувачі Інтернету повинні апріорі дотримуватися законів і регулюючих актів у сфері інформації, що діють на даній території. Однак такий підхід є занадто загальним для розуміння

правових орієнтирів мережевої загрози та наслідків за скоєні діяння (в тому випадку, якщо сторона, яка «відбороняється», все ж публічно заявить про наявність такої загрози) [110].

Ряд небезпек пов'язаний зі спробами певних політичних сил використовувати інформаційні можливості Мережі для формування громадської думки, впливу на маси з метою досягнення своїх інтересів. Безумовно, такого інформаційного впливу у вищій мірі зазнає найбільш масова й активна частина аудиторії Інтернету - молодь. Вона привертає сьогодні особливу увагу політиків і лідерів громадської думки. Всі вони хочуть знати, яку роль готова (або не готова) грати молодь у розвитку демократії, ринкової економіки, громадянського суспільства та правової держави. На молодих людей буквально обвалюється потік інформації, значну частину якої вони просто не в змозі адекватно сприйняти. Інформація, яка подається у спотвореному вигляді, здатна призвести до моральних деформацій, породити агресію, прагнення до прояву насильства.

Виступаючи перед студентами Кембриджського університету, Джуліан Ассанж заявив, що Інтернет не сприяє свободі слова, правам людини та громадянській активності, а скоріше є "технологією, яку можна використовувати для створення тоталітарного шпигунського режиму, якого ми досі не бачили", цитує The Guardian [12].

Стає очевидним, що суто інформаційна спрямованість мережі Інтернет поступово замінюється явно вираженим агітаційним, популістським, а іноді й агресивним підходом. Проникнення матеріалів з Інтернету у традиційні засоби масової інформації стало звичайним явищем, незважаючи на те, що в глобальній Мережі може бути опубліковане все, що завгодно. Інтернет-ЗМІ відрізняються від звичайних засобів масової інформації тим, що там можна публікувати новини не тільки дешево й оперативно, а й що дуже важливо - анонімно.

Так, відсутність налагоджених правових механізмів впливу на подану в комп'ютерних мережах інформацію дозволяє розміщувати тут матеріали відверто націоналістичного, фашистського, расистського змісту, порнографічну продукцію з елементами насильства, рецепти виробництва наркотичних і вибухових речовин і т.д. У ряді країн відзначається поява сайтів, що належать організованим злочинним угрупованням і терористичним організаціям, через які ведеться не тільки обмін інформацією, а й пропаганда відповідних ідей і способу життя.

Аналізуючи вплив мережевих інформаційних ресурсів на формування життєвих установок молоді, допустимо розглядати Інтернет у якості специфічного середовища прояву суспільних відносин. У цьому середовищі представлені практично всі соціальні верстви та вікові групи населення, тут знайшла втілення в тій чи іншій формі більшість видів діяльності суспільства (політична, фінансово-економічна, комерційна, освітня, культурна і т.д.), на основі спільності інтересів створюються численні «віртуальні» групи територіально відокремлених суб'єктів. У таких групах складається своя внутрішня соціальна ієрархія, з'являються формальні та неформальні лідери.

Безумовно, в сучасних умовах не можна, та й непотрібно ізолювати молоду людину від використання мережевих ресурсів. Однак повинні бути продумані шляхи нейтралізації негативного інформаційного впливу комп'ютерних мереж. Можна сказати, що вже назріла необхідність визначення жорстких критеріїв допустимості розміщення в мережах певних видів інформації. Слід виробити працюючі механізми обмеження доступу до окремих сайтів для різних вікових категорій аудиторії Інтернету. Потрібно законодавчо закріпити відповідальність власників сайтів за зміст розміщуваних інформаційних матеріалів. І дуже важливо, щоб протиправні процеси, які відбуваються в глобальних комп'ютерних мережах, отримували адекватну протидію з боку правоохоронних органів.

Нових підходів потребує організація взаємодії і ЗМІ, в тому числі й у сфері протидії негативному інформаційному впливові. Правомірність такого підходу підтверджує закордонний досвід інформаційної політики в збройних конфліктах. Так, в останні два десятиліття керівництво НАТО позначило ряд проблем, які необхідно враховувати при інформаційній протидії в умовах криз:

- високі суспільні очікування «чистої, високотехнологічної війни». Наприклад, під час операції на Балканах у 1999 р. НАТО скинуло 23 тис. бомб, з яких тільки близько 30 не вразили намічені цілі (це одна десята відсотка, раніше недосяжна ступінь точності). Але ЗМІ та громадська думка в цілому були шоковані: вони ігнорували 99,9% успішних дій, а з 0,1% промахів зробили центральну драму і мірило оцінки військової та моральної ефективності НАТО;

- широке використання цензури та контрпропаганди, як у теле-радіоефірі, так і в Інтернеті. Наприклад, у США й інших країнах НАТО досить чітко відпрацьований механізм і принципи інформаційної політики під час збройного конфлікту. Для журналістів й інших представників ЗМІ відпрацьовуються спеціальні правила керівництва для роботи з висвітлення бойових дій. Із цього приводу Е. Месснер писав: «Агітація під час війни повинна бути дволикою: одна напівправда для своїх, інша для ворога. Але одного лукавства мало - потрібна, так би мовити, багатоликість: для кожного рівня свідомості, для кожної категорії характерів, схильностей, інтересів - особлива логіка, щирість або лукавство. Це змістовна відмінність, але не менше різноманіття існує й у варіантах каналів комунікації, які повинні донести обране повідомлення до цільової аудиторії;

- прагнення ЗМІ до безпосереднього наочного висвітлення подій. ЗМІ зацікавлені у новинах, причому в яскравих новинах, підкріплених «картинкою». Представники США під час війни в Іраку щодня витрачали

тисячі слів, щоб роз'яснити, що відбувається, але багатьом словам не вірили, оскільки не були представлені фотографічні свідоцтва;

- фрагментарність у висвітленні подій, які багато в чому спеціально організовуються військовим командуванням. ЗМІ відображають конфлікт як серію окремих яскравих інцидентів. При цьому втрачається або стирається загальний контекст, фундаментальна динаміка події. Люди виявляються недостатньо поінформованими про дипломатичні та політичні зусилля;

- непідготовленість прес-служб до ситуацій, коли конфлікт набуває дещо затяжного характеру. У цьому плані цікава думка колишнього міністра оборони США Д. Рамсфелда, висловлена ним на зустрічі з редакторами газет: варто готувати фахівців у різних регіонах зі знанням мови та культури, їх слід винагороджувати за ці знання, а не карати, оскільки це певне відхилення від нормальної армійської кар'єри. Тут важлива увага до зняття опору військового середовища для такого типу фахівця [52. с.25].

Концентрація та монополізація ЗМІ, утворення потужних національних і транснаціональних корпорацій, які контролюють інформаційний простір, перехід основних засобів ЗМІ під контроль зарубіжних, транснаціональних угруповань або «місцевих» груп, неорієнтованих на загальнонаціональні інтереси, полегшує культурно-інформаційну експансію інформаційних корпорацій Заходу, посилення впровадження нових інформаційних технологій, а також засобів і методів інформаційної війни. Наслідком цього стає створення та розгортання плацдарму для інформаційного домінування Заходу в світовому інформаційному просторі.

Для України, де йде активний процес становлення вітчизняних ЗМІ в атмосфері жорсткої конкуренції та при нестачі можливостей його контролю в умовах ідеологічної, фінансової та організаційної

незабезпеченості національно-державного сектора ЗМІ, проблема захисту від західного інформаційного домінування набуває загостреного характеру.

Одночасно з процесом монополізації вітчизняних ЗМІ фінансовими угрупованнями йде також процес розриву єдиного інформаційного простору України. Центральна преса втрачає провідні позиції в ньому. Різко скорочується річний тираж періодики за рахунок зменшення числа передплатників, в основному центральних видань. Падіння тиражу центральних ЗМІ ставить під питання збереження єдиного інформаційного простору України.

З розвитком телекомунікаційних і комп'ютерних технологій у даний час стають доступними за своєю вартістю такі апаратурні засоби, які дозволяють створювати базові конфігурації вузлів радіо- і телемовлення, видавництв газет і журналів, провайдерських вузлів міжнародних комп'ютерних мереж.

Новою тенденцією стало використання з метою інформаційної війни технологій мобільного зв'язку. «Через еволюцію мобільного зв'язку з'являються все нові способи інформаційно-психологічного впливу. До нових способів інформаційної війни на сучасному етапі можна віднести використання WAP-порталів та SMS-повідомлень. Ефективність матеріалів різної спрямованості може багаторазово посилюватися при повторенні в блогах, форумах, SMS-повідомленнях. Популярність подібного мобільного спілкування серед молоді призводить до того, що повідомлення безконтрольно поширюється з ресурсу на ресурс, обростає додатковими коментарями й охоплює в підсумку величезну аудиторію. Мобільні інтернет-портали та SMS-простір володіють величезним потенціалом для використання в інтересах спецслужб, який не обмежується тільки трансляцією новин певного напряму або організацією мобільних форумів із заданою тематикою обговорення, а й включає можливість сприяння зборові мас людей у необхідному місці в потрібний

час. Беручи до уваги схильність молоді до розваг й участі в різного роду подіях, у світі впевнено набирає популярність явище flash-mob (миттєвий натовп), у свою чергу, виключно залежне від попереднього сигналу, який передається за допомогою тих же SMS-повідомлень. Розсилка закликів до мітингів і демонстрацій сьогодні також здійснюється через мобільний зв'язок» [92].

У зв'язку з викладеним можна зробити висновок про існування реальної загрози розповсюдження спрямованої інформації, яка може спричинити шкоду національним інтересам України.

Висновки до розділу 2

У результаті науково-технічного прогресу в галузі інформаційно-комунікаційних технологій, розвитку засобів масової комунікації створені безпрецедентні можливості для агресивного інформаційного впливу на населення інших держав із метою нав'язування принципів устрою та життя суспільства, знищення національних духовних цінностей, зниження економічного й військового потенціалу держав шляхом впливу на індивідуальну, групову і масову свідомість.

Багато країн світу зараз активно розробляють і застосовують комплекс заходів щодо захисту свого суспільства від «інформаційної інтервенції», що здійснюється, як відомо, з боку «монополістів» у цій галузі - США, Китаю, Японії, країн Європи. Сучасні держави розглядають перевагу в інформаційній сфері як один із важливих факторів досягнення цілей своєї національної стратегії. Про це свідчить та увага, яка надається створенню спеціалізованих підрозділів у структурах збройних сил і спеціальних служб, розробці концептуальних документів, що

регламентуватимуть питання підготовки та ведення інформаційних операцій.

Інформаційна війна як агресивна взаємодія протиборчих сторін в інформаційній сфері негативно відбивається на стані політичних комунікацій суспільства в цілому. Застосування таких кампаній політичними акторами пов'язане зі збільшенням ризиків, результатом чого є швидка зміна статусів і позицій у відносинах влади. Через високу інтенсивність суперечок інформаційні війни погано піддаються управлінню та свідомому регулюванню й тому виступають як двосічна зброя для протиборчих сторін. Досягнення цілей подібними способами посилює політичну конфронтацію, знижує можливість поширення консенсусної культури, підриває стабільність у суспільстві.

Завдяки новим технічним засобам сьогодні можна охопити пропагандою мільйони людей одночасно. З'явилися й організації, здатні ставити небачені раніше за масштабами політичні спектаклі у вигляді масових видовищ або кривавих провокацій. Виникли дивні види мистецтва, які спричиняють сильний вплив на психіку (наприклад, перформанс, що перетворює буденну реальність у зачаровуючий спектакль). До проведення інформаційних війн сьогодні активно залучаються Голівуд, CNN й інші «медійні монстри».

Стратегія інформаційної війни офіційно взята на озброєння Пентагоном. Вона дозволяє захоплювати чужі території та встановлювати над ними американський контроль без використання звичайних озброєнь. Тому до інформаційної війни слід ставитися з усією серйозністю.

Одним із прийомів інформаційної війни, завдяки якому США має можливість контролювати цілі країни у своїх інтересах, є створення громадських організацій, які пропагують у суспільстві цінності західної культури. Саме такий процес сьогодні активно розвивається на

пострадянському просторі. Таким чином, іноземні спецслужби розхитують загальнонаціональні духовні цінності.

Зроблено висновок про те, що для зниження рівня розвитку електронного шпіонажу потрібна розробка безлічі заходів, починаючи з прийняття адекватного законодавства та закінчуючи рішенням суто технологічних питань. Головне ж завдання полягає в тому, щоб на міжнародному рівні, наприклад, в рамках ООН, розробити комплексну програму, що включатиме в себе всі можливі форми та методи боротьби з електронним шпіонажем - юридичні, програмні, технологічні, організаційні, економічні, політичні і т.д. Ці дії матимуть успіх лише в тому випадку, якщо будуть спиратися на систему постійного моніторингу електронного шпіонажу на загальнопланетарному та національному рівнях.

Політичне керівництво України в 1990-х роках не приділяло достатньо уваги ролі засобів масової інформації, особливо телебачення, в сучасній світовій політиці. Органи державного та військового управління далеко не повністю розуміли, що від позиції ЗМІ все частіше залежить, чи виглядає політична акція перемогою або поразкою, і практично не враховували це при плануванні реальних політичних дій. Така недооцінка організаційних аспектів взаємодії держави та ЗМІ вкрай негативно позначалася на міжнародному іміджі України, знижуючи ефективність її зовнішньополітичної активності.

РОЗДІЛ 3
УКРАЇНА В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

Об'єктивно зростаюча глобальність інформаційної сфери веде до того, що створювана інформаційно-комунікаційна інфраструктура країни та національні інформаційні ресурси виявляються об'єктами, вельми уразливими для впливу з боку геополітичних конкурентів, терористичних організацій, кримінальних груп і окремих зловмисників. Із урахуванням цих чинників інформаційний розвиток України, який помітно відстає від провідних промислово-розвинених країн, має здійснюватися в рамках системної та збалансованої державної інформаційної політики, спрямованої на активну протидію інформаційній агресії.

У даному розділі аналізуються причини та наслідки інформаційних війн у сучасній українській політиці.

Оскільки формування міжнародного іміджу держави розглядається автором як один із способів протидії інформаційним атакам, направленим

проти України, дану проблему слід аналізувати в двох аспектах: по-перше, який є імідж Україні і яким він повинен бути, по-друге, як затвердити імідж України як інформаційний продукт у сучасному інформаційному просторі?

3.1. Причини та наслідки інформаційних війн у сучасній українській політиці

Не секрет, що останнім часом, у політиці все більшу роль відіграє інформаційно-психологічний фактор. Цьому є декілька причин. В Україні демократизувалася система соціально-політичних відносин, завдяки чому Україна стала інформаційно відкритою країною, як для інших держав, так і всередині самої себе. Важливим підтвердженням цього є підписання Президентом України 3 лютого 2011 року Законів України «Про доступ до публічної інформації» та «Про інформацію». Закон «Про доступ до публічної інформації» передбачає 5-денний термін відповіді на інформаційний запит або ж 48-годинний - у разі надзвичайної ситуації. Крім того, ці закони передбачають необхідність створення підрозділів або відповідальних у різних установах державної влади.

Відповідно до закону, доступ до інформації про діяльність та рішення суб'єктів владних повноважень повинен здійснюватися таким чином: оприлюднення інформації в засобах масової інформації та в офіційних друкованих виданнях, надання інформації за запитами; розміщення інформації на офіційному веб-сайті, надання інформації через інформаційні служби суб'єктів владних повноважень.

Документ встановлює, що «обов'язковому оприлюдненню суб'єктами владних повноважень підлягають: інформація про діяльність суб'єктів

владних повноважень». Закон також передбачає контроль за забезпеченням доступу до публічної інформації, що здійснюватиметься спеціальними органами, які визначають Верховна Рада та Президент України. Документ забороняє створення органів державної влади, установ, введення посад, на які покладаються повноваження щодо здійснення контролю за змістом інформації, поширюваної засобами масової інформації.

Також передбачено, що зумисне перешкоджання законній професійній діяльності журналістів та/або переслідування журналіста за виконання професійних обов'язків, за критику, здійснювані посадовою особою або групою осіб за попередньою змовою, тягнуть за собою відповідальність, передбачену законами України.

Закон примітний тим, що визначає принципи діяльності ЗМІ та порядок акредитації журналістів [83].

В умовах демократизації суспільства відкриваються його інформаційні кордони. А це значить, що все більш доступними для негативного зовнішнього інформаційного впливу стають масова свідомість, соціальна психіка, мораль і моральність як головні цілі нанесення інформаційно-психологічних ударів.

Інформаційні атаки проти України проводить не тільки Росія, але й інші країни, наприклад, Румунія, Бельгія і, звичайно ж, США.

Як відзначають дослідники, сам характер інформаційної війни часто не дозволяє об'єктивно оцінити те, що відбувається, не тільки пересічним громадянам, а й фахівцям. Примітна думка російського дослідника В. Коровіна, яку дозволимо собі процитувати повністю: «Мережева війна ніколи не ведеться прямим чином. Замовник ніколи прямо не пов'язаний із виконавцем. І навіть якщо провести лінію через безліч посередників від виконавців до замовника – прямої не вийде. І кривої не вийде. Сукупність проведених ліній утворює мережу. Якщо у вас вийшла пряма або навіть крива - то перед вами не мережева операція, а звичайна, класична операція

епохи модерну, в якій зв'язок між замовником і виконавцем, навіть при відсутності деяких проміжних елементів, цілком можна встановити. Звичайно, між США та багатьма подіями по всьому світу можна встановити зв'язок, недвозначно визначивши замовника того чи іншого процесу. Але цей зв'язок буде суто умоглядним. Сучасний інформаційний контекст такий, що Америці можна пред'явити все, що завгодно, починаючи від «помаранчевої» революції в Україні та закінчуючи руйнівним цунамі в Південно-Східній Азії. І навіть якщо всі фактори будуть на користь пред'явлених версій, вам, у кращому випадку, розсміються в обличчя або відправлять у божевільню, бо у вас не буде жодного прямого факту, а всі докази та ланцюги будуть відводити вас у нескінченні нетрі мереж, переплітаючись, сходячись і розходячись у довільному порядку. Мережева війна ведеться на більш тонкому рівні, з використанням інформаційних технологій, дипломатичних мереж, неурядових організацій, із підключенням журналістів, політиків, ЗМІ. Це багаторівнева операція, в якій звичайній зброї немає місця, але, тим не менш, результатом її стає відторгнення територій - конкретна «військова» перемога» [116, с.55, 114].

У ряді досліджень передбачається, що так звані «оксамитові» революції є результатом інформаційних війн. «Немає формальних підстав стверджувати, що події 1989-1990 років, що ввійшли в історію під назвою «оксамитових» революцій, були ініційовані з-за кордону. Однак перебіг подій, гасла, тактика, застосовувана в даних подіях, дивно нагадують те, що мало місце в період руху «Солідарності». У подальшому сценарії, що ведуть до зміни влади, були успішно реалізовані в Сербії, Грузії й Україні. Не можна не звернути увагу на те, що всі ці події розвивалися за одним і тим же сценарієм, наче під копірку. Очевидно, в недалекому майбутньому стануть відомі достовірні факти, які розкриють справжніх ініціаторів усіх

«оксамитових» і «кольорових» революцій, але відомо, що події у Тбілісі та Києві фінансував фонд Сороса» [243, с.266-270].

Цікава точка зору британського вченого Марка Алмонда щодо моделі «помаранчевої» революції в Україні: «Будь-яка політика коштує грошей, а сцени за участю натовпу, які щодня передаються з Києва, коштують великих грошей. Ринкова економіка, можливо, і перемогла, але якби Мілтон Фридман нагадав тим, хто на майдані Незалежності задарма отримує їжу та напої, що «не існує такої речі, як безкоштовний ланч», його, безсумнівно, охрестили б сталіністом. Здається, лише одиниці цікавляться питанням, чого хочуть люди, які платять за «владу народу» в обмін на спонсорування всіх цих рок-концертів. Являючись старим кур'єром холодної війни, який перевіз десятки тисяч доларів дисидентам радянського блоку, а також і куди більш шанованим ученим, я мабуть, зможу пролити світло на те, що один мій румунський приятель називає «нашим таємним періодом» [13, с.13]. Як вважає О. Афанасьєва, «І Ющенко, і Саакашвілі, і Карзай в Афганістані, і нинішній формальний глава Іраку - аж ніяк не самостійні політики, які стали президентами завдяки власним зусиллям. Вони агенти, менеджери - називайте, як хочете, - яких просунули на президентські пости («демократичними» передвиборними сценаріями або військовою силою - вже технічні деталі). Робота цих персонажів - точно та беззаперечно виконувати отримані інструкції, інакше той же сценарій, який привів у президентські крісла їх самих, буде запущений знову, але вже проти них [13, с.30].

Відомо, що задовго до виборів в Україні у західних засобах масової інформації розпочалася масована інформаційна кампанія за участю провідних західних експертів і лідерів громадської думки, в тому числі й колишніх голів держав. Метою цієї інформаційної кампанії було переконати світову громадську думку в тому, що правлячий режим у країні є недемократичним, корумпованим, авторитарним і має намір

сфальсифікувати майбутні вибори заради утримання влади. Чесних виборів при такому режимі в Україні бути не може за визначенням, тому що на чесних виборах корумпований режим не переможе. Щоб запобігти фальсифікації Захід повинен чинити тиск на владу України, аж до погроз конфіскації зарубіжних активів і власності лідерів режиму та членів їхніх сімей, заборони на видачу їм віз. Після виборів, у яких офіційно переміг провладний кандидат, місії міжнародних спостерігачів (ОБСЄ, ПАРЄ, західні НУО) виступають із офіційними заявами, в яких вибори оголошуються недемократичними, несправедливими та не відповідають міжнародним стандартам. Це є підставою для офіційних заяв влади США та керівництва ЄС про невизнання оголошених результатів голосування в Україні та необхідності проведення нових «чесних виборів». Цей ключовий момент - невизнання результатів виборів провідними державами світу - перетворює Україну та її владну еліту в міжнародних ізгоїв. Конституційна влада у країні стає теж нелегітимною, а її повалення, в тому числі насильницьке, - цілком виправданим [225, с.29-31].

Виходячи з вищевикладеного, можна зробити висновок про глобальний характер інформаційної війни, розгорнутої проти України в період «помаранчевої революції». Однак, як видається, правильніше буде називати таку інформаційну війну глобально-державною. Оскільки паралельно з зовнішньою, велася і внутрішня інформаційна війна. Під гаслом «Чесних виборів при злочинній владі бути не може» опозиція вела виборчу кампанію, результат якої вже заздалегідь відомий і запрограмований: вибори будуть сфальсифіковані, перемога влади офіційно оголошена, але в дійсності опозиція знає, що перемогла вона. Цей висновок тиражується на всіх рівнях і у всіх форматах, в тому числі за допомогою контрольованих опозицією ЗМІ. Юристи опозиції подають до виборчкомів і судів усіх інстанцій позови щодо найнезначніших відхилень від виборчого законодавства. Інформація про нібито численні порушення

тиражується як доказ масової фальсифікації, що готується. Ключовим моментом є швидке оголошення результатів виборів за даними екзит-полів, у яких фіксується впевнена перемога опозиції. Розбіжність цих даних із попередніми результатами Центрвиборчкому на користь влади використовується як підстава для звернення опозиції до своїх прихильників із закликом вийти на вулицю та блокувати урядові будівлі (при цьому технології «виходу на вулицю» відпрацьовуються заздалегідь).

На президентських виборах в Україні восени 2004 р. усі традиційні передвиборчі процедури - спостереження за ходом виборів, юридичний супровід, оскарження результатів, «конвеєр скарг», кампанії у ЗМІ - вперше були задіяні як єдина система, що забезпечує тотальну мобілізацію ресурсів для досягнення потрібного результату - визнання не легітимності виборів. «Вторгнення в інформаційний простір країни прозахідних, у першу чергу американських, ЗМІ або спонсорованих за рахунок західних грошей джерел інформації і, з іншого боку, російських ЗМІ справило серйозний вплив на хід виборчої кампанії. Про вторгнення говорити буде навіть не вірно, оскільки більшість із цих джерел масової інформації перебували в Україні і раніше, але у вирішальний період кінця 2004 року вони заробили на повну потужність для досягнення єдиної мети, у кожної сторони - природно своєї, що і стало "інформаційною агресією"» [119].

Звичайно, В. Путін не став президентом Росії за допомогою інформаційних технологій Заходу, але, в той же час, не можна не помітити агресивне використання інформаційних технологій внутрішніми політичними силами. На зміну відносно ліберальному Б. Єльцину приходить людина зі спецслужб із протилежними ідеологічними установками. Це стало можливим із декількох причин. Історія виборів показує, що російські виборці традиційно голосують за кандидата, запропонованого владою. Однак й інформаційні технології, ЗМІ безумовно зіграли свою роль. Чого тільки варті кадри з Путіним на підводному човні,

на винищувачі, в костюмі дзюдоїста в спортивному залі, на лижах на гірському трампліні і т.д. І все це на тлі старіючого та немічного Б. Єльцина.

Таким чином, можна зробити висновок, що В. Путін став Президентом Росії у результаті застосування технологій інформаційної війни, розгорнутої оточенням Б. Єльцина, так званою «Сім'єю» з метою власної безпеки та самозбереження.

Про факт інформаційного впливу на Україну з боку Росії, пише український дослідник Г. Перепелиця. На його думку, з метою російської політики - повернути Україну в лоно російської державності, з боку Росії активно застосовуються засоби інформаційної війни, яка має переваги зважаючи на прихований характер використання її основних інструментів: їх легко замаскувати або надати їм вигляду боротьби ідей, висловлювань, приватних поглядів, конструктивної критики.

Г. Перепелиця пояснює пріоритетність застосування засобів інформаційної війни тим, що Росія має всі технічні, мовні та ментальні можливості для інформаційного впливу на населення України. «І не випадково, що законодавче закріплення в Україні української мови як державної розглядається багатьма в РФ як загроза її національним інтересам. Адже поширення української мови скорочує використання російської як засобу спілкування в Україні і таким чином звужує поле російського інформаційного впливу. Це, до речі, є однією з причин того, що Росія так наполегливо домагається впровадження в Україні російської мови як державної. Що ж до проявів інформвійни з боку Росії, то неважко помітити, як за допомогою передач ОРТ останнім часом створювався негативний політичний імідж керівництва України, дискредитувалися ідеї української державності» [168].

Однак інформаційна війна ведеться не тільки одними державами проти інших.

Ще не так давно існування «інформаційних війн» у медійному просторі України ставилося під сумнів. Однак політичні події показують, що інформаційні війни в Україні ведуться.

Можна констатувати, що останнім часом політико-інформаційний простір України став місцем проведення інформаційних атак, викликаних протистоянням політичних опонентів і олігархів. Досить згадати протистояння Президента та прем'єра, влади й опозиції, взаємини України та Росії, російсько-грузинський конфлікт, паливно-енергетичні питання і т.д.

Таким чином, характерною особливістю сучасного українського інформаційного простору стала наявність внутрішніх інформаційних війн.

За межами своєї держави це може бути «образ ворога» чи «не ми», а всередині - будь-хто, хто протистоїть або недостатньо підтримує керівництво («лідера»), яке управляє засобами інформаційної війни. Якщо члени групи не підтримують цілі «лідера» в ході бойових дій, внутрішня інформаційна війна (яка включає пропаганду, брехню, терористичні акти та чутки) може бути використана для їх примусу бути більш лояльними по відношенню до «лідера» і його цілей [34].

Така ситуація, звичайно ж, характерна не тільки для України, але й для інших пострадянських держав, зокрема Росії. Як зазначає російський дослідник С. Ткаченко, іноді політична еліта використовує інформаційну війну проти власного народу. Як приклад він наводить вибори в Росії, за допомогою яких правлячим політичним силам вдається зберігати політичну владу й одночасно проводити політику, що прямо суперечить інтересам більшості населення. «Свідомість, а значить, і політичний вибір російських виборців зазнає справжньої інформаційної атаки. Для досягнення сприятливого результату застосовуються навіть методи нейролінгвістичного програмування (НЛП), які дозволяють впливати на підсвідомість, минаючи розум. Так, крок за кроком нормальне мислення

російського виборця блокується, а потім і повністю руйнується. Люди втрачають можливість об'єктивно оцінювати політичне життя й адекватно реагувати на події в ньому» [207, с.19]. У результаті цього виборчий процес перетворюється в дійство, яке не передбачає ніякого вільного вибору. ЗМІ ж тільки сприяють тому, що довіра пересічних громадян до політичних інститутів і політиків продовжує падати. Проте це не бентежить апологетів існуючої російської політичної влади, до яких відносяться і політичні експерти, і так звані дослідники, які роблять вигляд, що все в порядку. Вони наполегливо переконують громадськість у тому, що вибори в Росії «перестали бути фіктивною процедурою. Постійною практикою стала наявність декількох кандидатів на виборні посади та реальна боротьба між ними» [142, с.4]. Така свідома брехня є елементом інформаційної війни.

Як пише С. Ткаченко, «Така інформаційна війна реалізується за рахунок підміни та руйнації національних духовних цінностей: одні з них штучно занижуються, а роль інших навпаки, перебільшується. Мета подібних дій одна - маніпулювати людьми, змушуючи їх діяти всупереч власним інтересам. В арсенал інформаційної війни, яка ведеться проти росіян власною владою, входять такі методи як повалення громадських авторитетів, носіїв культури та моралі, а також навіювання чужих ідей за допомогою масового гіпнозу. Все частіше в засобах масової інформації застосовуються різні психоаналітичні технології, спрямовані на маніпулювання свідомістю телеглядачів, читачів або слухачів. Для «зомбування» населення використовуються навіть такі заборонені та небезпечні технічні засоби, як 25-й кадр [207, с.21].

Тому закономірно, що термін «інформаційна війна» став звичним як в засобах масової інформації, так і в лексиці політичних сил. Часто цей термін сприймається як «злив компромату», якому в чималому ступені сприяє новий засіб масової комунікації - Інтернет. Саме через Інтернет

безконтрольно поширюються компрометуючі матеріали, «вкидається» в суспільство потрібна та своєчасна інформація, яку друковані й електронні ЗМІ тиражують, уже посилаючись на джерела в Інтернеті.

Як вважає А. Єрмолаєв, оцінюючи діяльність попередньої влади, «Поверхневе і негативне ставлення до України породила, перш за все, сама Україна. Українська влада, українські політики виглядають в очах наших партнерів лукавими, непослідовними, скандальними й у багатьох питаннях просто некомпетентними. І тому в наявності розчарування в Україні, не в країні як такої, а в її державній політиці. Другий аспект пов'язаний із українською економікою. Українська економіка вважається однією з найбільш корумпованих, однією з найбільш конфліктних для ведення бізнесу. Про це говорять зараз практично всі великі західні інвестори, які працюють в Україні. Українські громадяни, особливо та їх частина, яка займається дрібною торгівлею, так само не є зразком громадянської культури.

Я, на жаль, неодноразово чув неформальні репліки дипломатів європейських країн, які визнавали, що у нас багато розмов про «європейськість», але немає європейської практики як такої, і це проявляється на всіх рівнях.

П'ять років тому були сподівання, що нова влада зможе запропонувати нові формати, нові стандарти розвитку. Але цього не сталося. Наша держава, навпаки, деградувала. Деградувала у сфері бізнесу, не наблизилася до існуючих соціокультурних стандартів. І як результат - негативний фон навколо України. Шукати тут якусь змову безглуздо. Тому, що ця ситуація «народжена» нашими політиками, тією частиною представників України, які розглядали Захід як місце втечі або Клондайк» [113].

Розглянемо проблеми, які роблять Українську державу вразливою в інформаційній війні.

По-перше, глобальні інформаційні мережі, що знаходяться поза контролем, продовжують стрімко розвиватися. Буквально щодня з'являються нові електронні ресурси, серед яких засоби масової інформації, сайти різних радикальних угрупувань й ін.

По-друге, вдосконалюються засоби та способи доставки інформаційно-пропагандистських матеріалів до аудиторії в ході інформаційно-психологічних операцій. З цією метою все більш активно використовуються такі нові медійні засоби як супутникове телебачення та радіо, цифрове телебачення, електронна пошта, засоби віртуальної реальності й ін.

По-третє, збільшується число засобів спеціального програмно-математичного впливу на ресурси інформаційних систем, при цьому самі ці засоби з розвитком глобальних мереж стали широко доступні, що веде до зростання числа хакерських атак на інформаційні системи Міністерства оборони та інших органів влади. У багато разів збільшилася кількість комп'ютерних вірусів, існуюча антивірусна промисловість уже не в повному обсязі справляється зі збільшеним навантаженням.

По-четверте, з’являється все більше систем супутникового зв'язку, технічні характеристики яких все більше удосконалюються. Зростає й число операторів супутникового зв'язку.

По-п'яте, розвиваються науково-дослідні програми зі створення технічних засобів маніпулювання свідомістю. За заявою ряду інформаційних агентств, в останні роки отримано ряд позитивних результатів зі створення технічних засобів дистанційного управління тваринами (включаючи і людину), що в найближчій перспективі загрожує появою нового класу загроз, пов'язаних із прихованим впливом на підсвідомість вищого військового та політичного керівництва країни.

По-шосте, недостатньо ефективною є підготовка випускників вищих навчальних закладів за спеціальностями, пов'язаними з інформаційними

технологіями. Крім того, спостерігається їх масовий виїзд за кордон. У результаті цього Україна може втратити кваліфікованих фахівців, які займаються розробкою та впровадженням нових інформаційних технологій у систему оборони країни.

По-сьоме, низький рівень розвитку комунікацій. Падіння рівня промислового виробництва, у тому числі інформаційних технологій в Україні, спричинило різке скорочення можливості створення конкурентоспроможних вітчизняних засобів інформатизації. В результаті українські засоби обчислювальної техніки не тільки не отримали місця на міжнародному ринку, а й у самій Україні в переважній більшості використовуються апаратно-програмні засоби та зв'язне устаткування, вироблене за кордоном. У підсумку для України в даний час стала актуальною проблема використання виключно іноземних інформаційних засобів і технологій.

Як відзначають дослідники, використання компрометуючої інформації для дискредитації конкурентів, супротивників, суперників і опонентів у ході політичної боротьби є не тільки об'єктивною реальністю сучасного політичного процесу, найважливішим елементом політичних технологій і політичних комунікацій, компонентом «public relations», а й основою такого відносно нового явища як «війна компроматів», що набуло широкого поширення в політичній практиці. З найбільшою інтенсивністю та гостротою «війна компроматів» розгорається в період виборчих кампаній як регіонального, так і національного рівнів. Суть цієї війни полягає в тому, що кандидати, які бажають будь-якою ціною потрапити в ту чи іншу виборну державну структуру, у своєму прагненні «втопити» супротивника зливають потужний потік негативної інформації не тільки один на одного, але й, що більш небезпечно, на потенційних виборців [144].

Негатив - це засіб, який використовують у комунікації з метою виділити слабкі сторони в аргументах опонентів, їх поведінці, індивідуальних якостях або якостях, необхідних для роботи в уряді. Поняття негативу тісно пов'язане з нападками (різкою критикою) на адресу опонентів на виборах, що підриває позиції кандидата або партії. В основі цих нападок лежить припущення, що їх ініціатор може працювати краще, ніж його опонент [127, с.176].

Як пише Даррен Дж. Ліллекер, «Більшості кандидатів під час передвиборчої гонки довелося вдаватися до негативної реклами, або чорного піару, щодо своїх опонентів. Прем'єр-міністр Великобританії Бенджамін Дизраелі говорив, що його опонент, представник Ліберальної партії Вільям Гледстоун, - це «аморальний маніяк... незвичайна суміш заздрості, мстивості, лицемірства та забобонів» і, що, напевно, було найгіршим в умовах вікторіанського британського суспільства, це людина, «яка ніколи не була джентльменом». На відміну від особистих нападок, критика на адресу держави завжди була корисним знаряддям у руках кожного, хто претендує на те, щоб називатися радикалом або революціонером. Російський лідер революції Ленін і обраний демократичним шляхом Прем'єр-міністр Росії Борис Єльцин (Президент Росії - О.М.), які працювали з розривом майже в сто років, обидва виступали з критикою помилок царизму, в першому випадку, і комунізму - у другому. Критика Гітлера була спрямована на слабкість уряду Веймара, у той час як Кастро вів пропагандистську війну проти кубинського уряду Батисти. Однак систематичне використання негативу в демократичному контексті - це щось нове, і вперше цю практику стали використовувати в американській моделі проведення кампаній [127. с.177].

Прагнення обіграти суперника, зайняти більш вигідні позиції в політичній сфері, підвищити свою ресурсну оснащеність змушує політичних акторів застосовувати технології інформаційних війн у зоні

порогових значень громадської думки. Тобто, нехтуючи правилами суспільної моралі та діючими в суспільній свідомості стандартами сприйняття інформації, такі політичні сили, схильні до використання «військових» технологій у своїх прийомах впливу на масову свідомість, нерідко переходять обмеження психіки, для сприйняття повідомлення впливаючи на підкіркові механізми людини.

Базовими способами організації дій у рамках інформаційних війн стають активізація підсвідомих механізмів сприйняття політично важливих відомостей, розмивання раціональних підвалин оцінок і суджень громадян, маніпуляція їхніми почуттями та емоціями. Наслідками застосування такого роду прийомів і технік є хаотизація групових і масових уявлень, розмивання цілісних вражень про світ і посилення залежності громадян від політичних сил, які розгорнули інформаційну війну між собою [174, с.260].

Слід зазначити, що використання тих чи інших видів компромату як засобу боротьби за політичну владу відоме давно і не є особливою характеристикою сучасного політичного життя або виключно українським винаходом.

Ключова роль у поширенні компрометуючої політиків інформації як достовірної, так і помилкової належить ЗМІ. При публічному поширенні найчастіше використовуються друковані видання, теле-, радіо-, відеопрограми або інші форми періодичного поширення. Широко використовуються у процесі політичної боротьби й можливості віртуального простору. Маса повідомлень компрометуючого характеру виходить у друкованих виданнях, спеціально створених штабами кандидатів на виборні посади. Однак пряма фальсифікація відомостей однозначно переслідується законом. Тому в більшості випадків для дискредитації конкурента використовуються факти або натяки, що неоднозначно трактуються [123, с.178].

Одним із факторів того, що Україна не завжди виходить переможцем в інформаційній війні є те, що Україна не контролює частотний ресурс біля власних кордонів. За наявними даними, третина населення отримує інформацію з джерел, не легалізованих в Україні. Серед експертів даної сфери сформувалися дві позиції стосовно інформаційної політики в Україні: 1) українська влада вивчає ситуацію в інформаційному просторі та пропонує зміни в регулюванні інформаційної політики в Україні, щоб привести медіа у відповідність до національного законодавства; 2) в Україні не існує інформаційної політики, оскільки влада не займається медіа. Через те, що влада вчасно не визначила пріоритети, Україна втратила частотний ресурс. Уздовж кордону України функціонують передавачі іноземних держав. Турецькі, болгарські, російські компанії ведуть мовлення на Україну, в той же час українські медіа не можуть досягти своїх громадян [88].

Як вважають фахівці, оцінюючи активність України в інформаційному просторі у період висвітлення війни в Грузії (8.08 - 13.08.2008), Україна програла інформаційну війну. Причому, на думку експертів, Україна навіть не помітила розгорнутої проти неї інформаційної війни. В українських медіа переважав російський дискурс. А українські засоби масової інформації, замість того, щоб висловлювати власний погляд на події, в основному посилалися на російські джерела. Таким чином, українським телеканалам бракувало власного контенту. Обравши більш легкий шлях для отримання інформації, вітчизняні ЗМІ переважно використовували інформацію російських засобів масової інформації, яку в порівнянні з англійськими інформаційними джерелами легше перекласти. Не треба бути професіоналом, щоб зрозуміти, що не тільки грузинсько-російський конфлікт, а й інші інформаційні приводи висвітлюються українськими журналістами на низькому рівні. У зв'язку з цим представляється доцільним знизити залежність українських ЗМІ від

російських медіа, що, втім, не означає посилення залежності від англомовних джерел. Мова йде про те, що за кордоном необхідно розвивати власну потужну кореспондентську мережу, а професійний рівень українських журналістів підвищувати [88].

Як справедливо стверджує З. Циренжапов, «В умовах інформаційних війн об'єктами руйнування стають ціннісні орієнтири суспільства, національний менталітет, суспільний ідеал. Одним із основних інструментів деструктивного інформаційного впливу стають мас-медіа. У зв'язку з цим однією з найважливіших цілей державної інформаційної політики слід визнати формування механізмів інформаційно-комунікативної протидії негативному впливу ззовні» [229, с.3].

Наприклад, телевізійні, друковані та рекламні інформаційні потоки у Французькій республіці суворо нормуються. В репертуарі кінотеатрів частка французьких фільмів повинна становити не менше 40%. На телебаченні частка іншомовної музичної продукції також обмежується до 60% і є вимога супроводжувати її субтитрами. Більше того, телеканали зобов'язані направляти фіксовану частину свого прибутку на виробництво кінопродукції французькою мовою. Зовнішня реклама без перекладу також суворо лімітується. Це лише елементи цілого комплексу заходів, що здійснюється французькою владою для захисту свого інформаційного простору [121].

Доводиться визнати, що деякі позиції концепції культурного імперіалізму справедливі. Як відомо, прихильники концепції зазначають, що функціонування західних ЗМК в інформаційному просторі країн неминуче веде до посилення соціально-економічної, політичної та культурної залежності останніх. Це призводить до руйнування їхньої національної ідентичності, до формування привілейованих умов для реалізації інтересів «вестернізованої» еліти, до створення в суспільстві

країн, що розвиваються, психологічної атмосфери, яка передбачає реалізацію проектів, пов'язаних із миттєвим споживанням.

Концепція культурного імперіалізму набула в 80-і-90-і рр. певного розвитку. Акцент був зроблений на аналізі домінування не стільки США (як провідної наддержави), скільки на вирішальній ролі транснаціональних корпорацій, їхнього широкого залучення в управління світовими політико-економічними та культурними процесами. В даний час існує не так вже й багато прихильників ідеї культурного імперіалізму в чистому вигляді, проте в цілому вплив цієї «парадигми» залишається вельми істотним.

Звичайно ж, найкращі можливості та ресурси зі зниження соціальної небезпеки інформаційної війни знаходяться в розпорядженні держави. Проте інформаційна політика України поки ще не орієнтована на якісний захист українського суспільства від руйнівного впливу інформаційної війни. Однією з причин цього є те, що українське суспільство не готове чинити активний опір будь-яким спробам маніпулювання суспільною свідомістю. «У той час як в масовій свідомості громадян ще тільки формується розуміння тієї загрози, яку можуть нести сучасні інформаційно-психологічні війни, технології інформаційно-психологічної війни вже впливають не тільки на свідомість, а й на підсвідомість» [138, с.312].

У науковій літературі під інформаційною політикою розуміється «сукупність цілей, що відображає національні інтереси в інформаційній сфері, стратегії, тактиці, завданнях державного управління, управлінських рішеннях і методах їх реалізації, що розробляються та реалізуються державною владою для регулювання та вдосконалення як власне процесів інформаційної взаємодії в суспільно-політичному житті та соціально-економічній сфері життєдіяльності суспільства й держави, так і процесів, що забезпечують таку взаємодію». Підкреслюється, що для усунення

«дефіциту довіри до влади» державна інформаційна політика повинна спрямовуватися не тільки на надання населенню необхідної інформації в зручній формі й оптимальним для споживача чином, вона повинна також стимулювати прямий діалог влади з громадськістю, «ініціатором якого повинна виступати сама державна влада» [154. с.23].

Інформаційну політику України необхідно адаптувати до нових умов, суть яких полягає в тому, що як постійне соціальне явище інформаційну війну на даному етапі розвитку суспільства усунути не можна, але можна контролювати на певному рівні соціальної небезпеки за допомогою державного регулювання.

Неодмінною умовою успішності будь-яких акцій інформаційних війн є інституціалізація даного роду комунікацій. Причому кожен політичний актор використовує для цього власні можливості. Найкраще становище в цьому сенсі в держави, в розпорядженні якої знаходиться розгалужена система інститутів, здатних організувати та підтримати кампанії в форматі інформаційних війн. До таких інститутів слід віднести:

- керівні та координуючі структури (різні державні органи, агентства національної безпеки, силові структури);

- інформаційні агентства, контрольовані державою та використовувані нею для просування своїх інформаційних цілей як всередині країни, так і на міжнародній арені;

- мережа джерел постійного інформування на певній території (резидентура або інші джерела інформування, що постійно перебувають за межами країни);

- окремі ЗМІ, що знаходяться під контролем уряду та беруть участь у забезпеченні його інформаційних цілей;

- вітчизняні та зарубіжні групи інтересів;

- агенти впливу;

- наукові конференції, використовувані як механізм вираження думок експертного співтовариства для захисту інтересів держави; окремі міжнародні організації, що знаходяться під контролем окремої національної держави.

Злагоджена та скоординована робота такого типу інститутів забезпечує високу ефективність досягнення політичних цілей держави, їхнє інформаційне забезпечення [174, с.261-262].

У ситуації, коли інформаційна війна стає перманентною, державна інформаційна політика повинна бути спрямована на пошук закономірностей, принципів, форм і методів політичного регулювання [137].

На думку А. Манойло, це дозволить: «підготувати суспільство до активної протидії інформаційно-психологічній війні; протидіяти інформаційно-психологічній війні на державному рівні з активною участю інститутів громадянського суспільства; здійснювати цілепокладання, формування організаційної структури, методичне та ресурсне забезпечення системи державного управління за критеріями: випереджаючого розвитку в порівнянні з системою здійснення інформаційно-психологічної агресії (війни); адекватно протистояти інформаційно-психологічній війні як постійному соціальному явищу (конфлікту)» [137].

Дослідниками помічено, що специфіка формування політичного іміджу держави на початку XXI століття багато в чому залежить від доступності будь-якої інформації про державу в глобальному інформаційному просторі. В умовах сучасного стану глобального інформаційного простору, з практично необмеженими можливостями інформаційного обміну, рівень міжнародного іміджу буде відігравати велику роль у всіх політичних процесах держави [1, с. 15-16].

Таким чином, з метою просування позитивного образу України за кордоном необхідна цілеспрямована, послідовна та систематична робота. Ігнорування інформаційного забезпечення зовнішньополітичної діяльності може призвести до втрати міжнародних позицій Української держави.

Як відомо, за допомогою інформаційної зброї ряд неурядових організацій, підтримуваних з-за кордону, формує негативний образ України. У зв'язку з цим Україна застосовує певні заходи для протидії інформаційній зброї, що застосовується ззовні.

Про формування міжнародного позитивного іміджу України в наступному підрозділі.

3.2. Формування позитивного іміджу України за кордоном як протидія інформаційній зброї

Як справедливо зазначають дослідники, образ країни можна розглядати не тільки як засіб, інструмент управління, але й як об'єкт цілеспрямованих інформаційно-психологічних атак [140, с.8]. Створення міжнародного іміджу держави, під яким у науковій літературі розуміється «сукупність характеристик державного механізму, зав'язаного в єдину взаємозалежну систему, що сформувалася в результаті історичного процесу розвитку суспільства, державних інститутів, ефективність взаємодій яких визначає тенденції політичних, економічних, соціальних, громадських й інших процесів всередині самої держави» [1, с.15], є дуже важливим питанням.

Саме міжнародний імідж держави впливає на те, «яку репутацію отримала або отримає держава у свідомості глобальної громадськості в

результаті взаємодії тих державних компонентів, які співвідносяться з навколишнім світом у глобальному інформаційному просторі» [1, с.15].

Не варто сперечатися з тезою про те, що від того, якою бачать Україну у світі - надійним або непередбачуваним партнером - залежить розвиток міжнародного співробітництва в економічній, політичній і соціальній сферах. Також не викликає сумнівів те, що складність процесу інтеграції України в міжнародне співтовариство визначається, в першу чергу, особливостями економічного та політичного процесів, політико-культурними відмінностями. З іншого боку, позитивні образи країни всередині України - це запорука стабільного стійкого внутрішнього розвитку, відсутність громадянських конфліктів, гарантія підтримки населення. Своє незадоволення іміджевою діяльністю уряду висловив Президент України Віктор Янукович. У зв'язку з цим він поставив уряду завдання створити іміджеву програму Україні. «Ми не вміємо подати те, що маємо», сказав він. «Коли ми їздимо за кордон, ми бачимо, як нас здивовано слухають партнери, наче ми приїхали з якоїсь Тьмутаракані й у центрі Європи немає такої країни» [252].

Україна, як одна з демократичних держав світу, що динамічно розвиваються, завжди буде залишатися об'єктом для впливів у прагненні країн на світове лідерство. Підтвердженням цьому є спроби окремих держав сформувати у широких кіл світової громадськості негативний образ Української держави. Відчутні складнощі, що виникають зі сприйняттям України на Заході, багато в чому пояснюються не ворожими підступами, а неготовністю західної аудиторії до позитивної інформації про нашу країну. Завдяки інформаційній кон'юнктурі, що склалася, інтерес до сучасної України дуже обмежений і формується в чітко негативному ключі. Між тим у сьогоднішніх умовах сприяння об'єктивному сприйняттю України за кордоном на основі достовірної інформації - це проблема не тільки міжнародного престижу, а й національної безпеки.

Як показала так звана "газова війна" з Росією, інформаційна політика України продемонструвала повну «беззубість». На тлі інформаційної активності Росії українська сторона виглядала пасивно та мляво. Доводиться визнати, що в якійсь мірі зусиллями експертів, дипломатів і політиків, Росії вдалося дискредитувати Україну в очах західної громадськості.

Ця ситуація є одним із яскравих прикладів того, що поки ще Україні не вдалося організувати ефективну комунікацію з зовнішнім світом.

Колишній Надзвичайний і Повноважний Посол України у США Юрій Щербак сказав, що "якщо є хтось, хто займається PR України від правлячої групи, вони повинні за голову схопитися та бути дуже стурбованими. Йде усюди системна надзвичайно негативна інформація про Україну". За його спостереженням, західна преса, західні інститути стурбовані згортанням демократичних процесів у країні та відзначають відсутність реформ. "Цей режим починають називати авторитарним, йде велика стурбованість із приводу повернення в радянське минуле... Це надзвичайно погана реклама України... Ми не виконуємо своїх міжнародних зобов'язань", - сказав екс-посол [248].

Згідно з наявними даними, Україна не часто привертає увагу впливових іноземних ЗМІ. Окремі американські та західноєвропейські видання приділяють увагу Україні на більш-менш регулярній основі, причому більшість матеріалів має критичну спрямованість. У публікаціях переважають головним чином сенсаційні повідомлення - про корупцію, злочинність, економічні катаклізми і т.п. Українська проблематика в східноєвропейських ЗМІ висвітлюється більш активно, що зумовлено зацікавленістю в розвитку міждержавних відносин [239, с.119].

Імідж держави в науковій літературі визначається як спрощений символічний образ усієї сукупності інститутів влади держави, заснований як на їхній реальній діяльності, так і створюваний стихійно або

цілеспрямовано на основі міфів і стереотипів масової свідомості, тим самим формуючи стійкі політичні мотивації людей. Імідж держави включає в себе зовнішньополітичну та внутрішньополітичну складові [140, с.12].

Смислове наповнення образу країни залежить від об'єктивних і суб'єктивних факторів. Об'єктивні чинники, що впливають на смисловий зміст образу країни у масовій свідомості, формуються під впливом уявлень про неї в сусідніх країнах, її відносин із ближніми сусідами, геополітичних устремлінь, уявлень про зарубіжний світ. Суб'єктивні чинники є основою самосприйняття громадянами своєї Батьківщини, їх уявлень про свою країну, її місце у світі, служать певною психологічною компенсацією, дозволяють офарбити економічні, політичні інтереси країни в кольори культурної спільності, ментальної близькості. У результаті смислової трансформації образу країни в імідж і бренд держава позиціонує себе в міжнародних інформаційних потоках [4, с.17].

Технології конструювання образу країни (регіону, міста), оцінка їхньої ефективності та способи її підвищення знаходяться в центрі пильної уваги експертно-аналітичного співтовариства та діяльності консалтингових структур. Регулярно проводиться порівняльний рейтинг "брендів" держав світу. Такі дослідження мають суто прикладний характер, їхнє завдання - забезпечити розробку технологій просування позитивного сприйняття. Замовниками виступають державні відомства, зокрема, міністерства закордонних справ. Образ країни розглядається в контексті розвитку маркетингових стратегій національного бізнесу, просування відповідних марок і залучення іноземних інвестицій. Конкурентоспроможність країни не вичерпується економічним потенціалом, вона включає в себе політичний імідж, соціальний клімат і культурну спадщину. Сама держава позиціонується в рамках такого підходу як "бренд", що працює на конкурентоспроможність країни у

глобальному світі. В якості інструментів аналізу адаптуються звичні для маркетингу термінологія (образ бренду, його конкурентоспроможність, позиціонування й ін.) і відповідний аналітичний інструментарій; з їх допомогою позиціонування країни обґрунтовується подібно позиціонуванню товару. [193, с.14].

Інформаційний простір, у якому формується сприйняття країни в світі, складається під впливом процесів глобалізації, але вони не задають односпрямований вектор динаміки національного образу. Останній зберігає статичні характеристики, відтворює укорінені розхожі уявлення, але не розмивається. Більше того, універсалізація побуту та стандартів споживання підсилює прагнення національної спільноти зберегти і підтримати впізнаване обличчя - носій унікального культурного досвіду. Відкритий простір інформації та комунікації розширює можливості участі в такому досвіді (через туризм, канали гуманітарного обміну і т.п.). Ці можливості успішно використовують, наприклад, такі не найпривабливіші з точки зору багатств культурної спадщини країни як Фінляндія, Нова Зеландія або Ірландія. Тут цілеспрямовано підтримують образи національної культурної самобутності, заробляючи іміджевий капітал і на новітніх інформаційних технологіях, і на етнокультурних традиціях.

У минулому багато країн намагалися змінити існуючі уявлення про себе в світі, для того щоб позначити таким чином зміну політичного режиму, перетворення державного ладу, проведення нових реформ.

Більшість урядів світових держав усвідомлює і багато з них намагаються керувати своєю репутацією, що дало назву цілому напрямку в маркетингу - reputation management.

Деякі країни досягли в цьому великих успіхів: Ірландія, Іспанія, Нова Зеландія, Австралія, ПАР у порівняно короткі терміни істотно поліпшили свій імідж, у результаті чого економіка, зовнішньополітичні відносини та повага з боку міжнародного співтовариства значно

зміцнилися. Інші країни, як, наприклад, Малайзія, Польща, Латвія, Китай, тільки вступили на шлях поліпшення іміджу країни [222, с.12].

Не буде перебільшеною думка про те, що сьогодні на кону міжнародний імідж України. У Європі пильно спостерігають за подіями в Україні та не приховують, що втомилися від непрогнозованості розвитку подій, де замість проведення ефективних політичних й економічних реформ політики вирішують свої власні проблеми.

Про устремління української держави до зміцнення свого міжнародного іміджу та пошуки власного курсу на реформи заявив, виступаючи у Верховній Раді, Президент України Віктор Янукович: «Нас повинні об'єднувати ідеї глибоких реформ в економіці та соціальній сфері, модернізація країни, створення ефективної системи національної безпеки, зміцнення авторитету України на зовнішній арені». Він підкреслив, що завдання України дуже складне: "увійти в коло країн - лідерів розвитку, знайти та пройти власний шлях і знайти методи бути сучасними, конкурентоспроможними, сильними". Глава держави також запевнив, що Україна остаточно «візьме курс на модернізацію суспільства, на формалізацію відносин, на асоціацію з Європейським Союзом» [2].

Одним із ефективних резервів формування іміджу України є врахування громадської думки в інших країнах. Механізми взаємосприйняття України та решти світу мають на меті дослідження причин виникнення стійко негативних стереотипів, зміни самоіміджу, виправлення деформацій, а потім технологічного просування нової країнної ідентичності та країнної індивідуальності.

У зв'язку з цим цікаві результати досліджень Інституту світової політики, який, опитавши по 30-50 експертів у Білорусі, Грузії, Молдові, Польщі, Росії та Румунії, представив «тридцятку» асоціацій з Україною в цих країнах. З'ясувалося, що в усіх країнах, окрім Польщі, Україна сприймається в позитивних асоціаціях.

Перше місце серед асоціацій польських експертів зайняли такі асоціації як корупція, дефіцит демократії, олігархи. Як вважають дослідники, свою роль зіграли розчарування, пов'язані з Помаранчевою революцією. Польські експерти також асоціювали Україну з загальною історією (зокрема, трагедія на Волині), з гостинним народом, невизначеністю в геополітичному векторі.

У білоруських експертів Україна асоціюється з Помаранчевою революцією, Кримом, із дружньою країною, з українською мовою та Києвом. Дослідники відзначають, що для білоруських експертів Україна є зразком демократії. Їх вражають Помаранчева революція, свобода ЗМІ, незалежність. На думку заступника директора Інституту світової політики Е. Зарембо, для білоруських експертів особливе значення мало те, що в Україні єдина державна мова.

У Грузії Україна асоціюється з такими поняттями як «дружня країна», «велика країна», «стратегічний партнер і союзник», «національна кухня та культура» й «Помаранчева революція».

Експерти Молдови асоціюють Україну з загальною історією, національною кухнею, великою державою, з Києвом і буфером-рятівником між Сходом і Заходом.

Як вважають українські дослідники, несподіваними були відповіді російських експертів. У них Україна асоціюється з літом, відпочинком, канікулами, фруктами... Також зустрічаються асоціації з родичами, друзями. Друга асоціація - Київ, наступна - не Росія. Російські експерти також асоціюють Україну з «близькою країною».

Результати опитування експертів із Румунії показали, що в цій країні присутній інформаційний вакуум щодо України. Деякі експерти надавали лише одну асоціацію. Інші - дві. В Румунії на перше місце вийшла асоціація з українською історією. Конкретно - з українськими козаками, Запорізькою Січчю, з Богданом Хмельницьким. Як виявилося, в

румунській колективній пам'яті Україна як самодостатня держава сприймається саме в період Запорізької Січі.

Метою Інституту світової політики стала розробка відповідних рекомендацій для уряду для посилення іміджевої діяльності в цих країнах [202].

Чи існують способи змінити тенденцію та кардинально поліпшити імідж України, насамперед у країнах Заходу? Доводиться визнати, що в рамках пануючих уявлень, традиційно обмежуючих поняття іміджу державними рамками, образ української держави завжди буде заручником проведеної ним політики. Небезпека його погіршення зберігатиметься постійно, навіть за найсприятливіших зовнішньополітичних обставин. Окрім того, в очах зарубіжної громадськості образ держави занадто часто асоціюється (а деколи просто зливається) з портретом правлячого режиму. В умовах панування медійних структур, це потенційне джерело дискредитації. Спроби включити до державного іміджу громадську складову проблеми не вирішують. Образ української держави також досить уразливий, оскільки не вписується в західні уявлення з їхніми високими стандартами демократії, правової захищеності, соціального благополуччя та матеріального достатку. Непрості справи і з іміджем держави, що економічно успішна та динамічно розвивається.

Європейські партнери дають зрозуміти, що для поліпшення свого іміджу Україні необхідно провести широкі реформи в судовій системі. Таку думку озвучив європейський комісар Гюнтер Оттінгер у ході дебатів щодо українського питання "Справа Тимошенко й інших членів колишнього уряду" 9 червня 2011 р. у Страсбурзі. Єврокомісар заявив, що якщо Україна хоче досягти політичної асоціації й економічної інтеграції з Європейським союзом, ЄС, у свою чергу, хоче бачити в Україні незалежну судову систему. "Це - одна з умов, яка дозволить просуватися в інших сферах. Ми чекаємо, що Україна змінить свою систему (судову), і буде

об'єктивне правосуддя, яке буде гарантоване Конституцією", - зазначив він. "І я вірю, що подальший прогрес України на шляху до ЄС буде залежати від цього. Це (подальший прогрес) буде залежати від поваги до прав людини, принципів демократії та верховенства права", - додав єврокомісар. Оттінгер зазначив, що дана позиція є також і частиною Європейської політики сусідства. За словами єврокомісара, найближчим часом пройде Рада зі співробітництва, в рамках якої Україні буде поставлений "ряд важливих питань". "І буде чіткий меседж про те, що ми чекаємо бачити в реформі у цій сфері. Ми схвалюємо той факт, що Україна хоче завершити переговори щодо Угоди про асоціацію до кінця того року. Але Україна має зробити необхідні кроки для реформування судової системи, боротьби з корупцією", - підкреслив він.

Оттінгер також запевнив, що в цьому відношенні Україна не залишається одна і ЄС надасть їй свою підтримку. Він запевнив присутніх депутатів у тому, що Європейська комісія стежить за розвитком в Україні з великою увагою та нагадав про те, що недавно ЄК оприлюднила свою доповідь щодо України. "Нічого серйозно не змінилося, все ще є необхідність у проведенні широких реформ у судовій системі", - сказав єврокомісар. Оттінгер також зазначив, що "будь-яке інше використання кримінального права (не за прямим призначенням, у тому числі, в політичних цілях) дає серйозні причини для занепокоєння" [221].

Не поліпшує імідж країні й та обставина, що Україну вважають одним із кращих прикладів олігархії у Європі. Про це заявив дипломатичний радник голови Європарламенту Єжи Бузека Арнольдас Пранцкевічус. "У вас відбулося практично повне злиття політики та бізнесу, їх майже неможливо відокремити одне від одного", - заявив він. При цьому він зазначив, що "подібна ситуація була характерна і для інших ваших урядів, не тільки чинного". "Звідси висновок: українські олігархи мають значний вплив на політику або безпосередньо займаються нею,

змішуючи політичні та бізнес-інтереси", - сказав Пранцкевічус. За його спостереженнями, з точки зору ЄС і з урахуванням досвіду євроінтеграції в Центральній і Східній Європі, такі процеси дуже небезпечні та багато в чому можуть вплинути на "здоров'я" демократичних структур. Як зазначив радник голови Європарламенту, в нормальному демократичному суспільстві має існувати чіткий поділ між держслужбовцями, політичними лідерами та бізнесом. "Звичайно, необхідна їх співпраця, це дуже важливо. Проте, коли все це знаходиться в одних руках, відповідальність розмивається, звітність перед суспільством практично зникає. Потенційно це несе великі проблеми, пов'язані з Конституцією," здоров'ям "політичних партій, яким не вистачає політичної ідеології та які часто керуються економічними інтересами, інтересами олігарха або приватними інтересами своїх лідерів" - зауважив радник Бузека.

"Така проблема існувала у багатьох країнах Центральної та Східної Європи, які приєдналися до ЄС у 2004 та 2007 роках. І вона до цих пір існує. Її подолання потребує багато часу. Втім, чим раніше ви почнете займатися цим, тим простіше буде впоратися", - підкреслив Пранцкевічус. Нещодавно в Брюсселі була представлена доповідь Інституту Горшеніна "Великий український бізнес і уряд України", в якому зазначалося, що більшість членів українського уряду - мільйонери [31].

І все ж, слід шукати пріоритети, що утворюють своєрідний ресурс іміджевої стратегії. Стійкий позитивний імідж вимагає фундаментального обґрунтування, яке апелює до внутрішніх джерел існування країни та народу, що розкривають і пояснюють місце України в ряду інших країн світу. Подібні підстави повинні бути звільнені від ідеологічного навантаження й, за можливістю, від питань поточної політики, але при цьому, затверджувати національне буття, тобто громадянську єдність, суверенітет і територіальну цілісність країни.

У зв'язку з цим підвищується відповідальність українських ЗМІ, безпосередньо причетних до формування національного іміджу. Вони служать провідниками найбільш стійких уявлень, що вкорінюються як усередині країни, так і за її межами. При цьому особливо важливо, щоб вони відповідали поведінковим стандартам, починаючи з елементарних понять і форм мовленнєвої культури. Мова вітчизняних ЗМІ іноді рясніє двозначними мовними зворотами, які породжують сумніви, скажімо, в цілісності та стабільності українського політичного простору.

Зарубіжні вчені У. Оллінс і С. Анхольт, говорячи про образ тієї чи іншої держави, ввели поняття country branding, яке можна перевести як «національний або країнний бренд», - загальне сприйняття країни громадянами, засноване на шести складових: туризм; експорт; населення; уряд; культура, історія та традиції; інвестиції й імміграція [253].

Як справедливо зазначає З. Циренжапов, просування позитивного зовнішнього іміджу держави в міжнародному інформаційно-комунікативному просторі повинне вестися з використанням іміджевого потенціалу країни. Елементами іміджевого потенціалу держави є: природна, культурна й історична спадщина, досягнення культури, науки, спорту, туристична привабливість регіонів країни [229, с.17]. Проаналізуємо іміджевий потенціал України.

Туризм міг би стати напрямком не тільки брендинговим, а й економічно вигідним. А в основі брендингу якраз могла б бути багатогранна культура українського народу. Якщо будь-який імідж складається зі стереотипів, то імідж культури - фактично «стереотип у стереотипі». Завдяки своїй стереотипності культура надає найширші можливості для іміджмейкерства. Формування іміджу передбачає створення репрезентативно-образної конструкції, яка повинна не тільки описувати, а й пояснювати об'єкт, що цікавить, за допомогою колективних уявлень. Отже, збагачення іміджу культурними стереотипами розширює

коло можливих оцінок і, тим самим, підриває негативні установки, позбавляючи уявлення однозначності [201, с.23].

На замовлення Міністерства культури й туризму на провідному міжнародному телеканалі CNN демонструється ролик, який рекламує туристичні пам'ятки України.

Які ж експортні бренди могла б запропонувати Україна? Думається, що за умов удосконалення технологій, Україна могла б виробляти більш сучасну військову техніку, конкурентоспроможну сільськогосподарську продукцію, якісний метал.

Важливим фактором у формуванні позитивного міжнародного іміджу стали президентські вибори 2010 р., які були названі спостерігачами на президентських виборах в Україні від ПАРЄ «блискучими та прекрасними». "Вибори можуть бути збудливими для кандидатів, важливими для виборців і повинні бути нудними для спостерігачів. Це були блискучі та прекрасні вибори, добре організовані, мирні й тихі. Вітання Україні", - сказав Матіас Еорші в Страсбурзі, виступаючи з попередньою доповіддю відносно проведення президентських виборів в Україні. У той же час, депутат ПАРЄ зробив висновок, що вибори "були прекрасні не завдяки, а всупереч". "Українські політики повинні зобов'язатися провести другий раунд відповідно до виборчого коду. Це були добре організовані вибори, але політичні виклики в Україні залишаються невирішеними. Багато людей в Україні вважають, що країною керують олігархи, а не вільно обрані політики - це має бути змінено. Також в Україні українські політики вважають за краще грати з правилами, замість того, щоб грати за правилами. Вони повинні врахувати, щоб це було по-іншому", - заявив Еорші. Відзначивши, що "сьогодні нам не відомо, хто буде обраний президентом України", депутат ПАРЄ особливо підкреслив, що "ця ситуація не застосовна для всіх сусідніх країн". "Ми сподіваємося, що другий раунд 7 лютого буде навіть кращим.

Привітання ПАРЄ з допомогою Україні в подорожі до демократії", - сказав він [166].

Ще один фактор, який впливає на бренд - громадяни держави. Так склалося, що найбільш відомі за кордоном громадяни України - це артисти шоу-бізнесу, спортсмени, олігархи та політики. Таким чином, саме їхня поведінка перебуває під пильною увагою іноземної громадськості. Звичайно ж, має значення й поведінка багатьох співвітчизників, які працюють за кордоном.

Пан Айхеліс, розробник стратегій поліпшення іміджу деяких країн Європи й Азії, акцентував увагу на привабливості українського напряму для багатьох категорій виробників завдяки дешевизні робочої сили, близькості держави до Європи, багатому науково-промисловому та кадровому потенціалу [96].

Що стосується інвестицій, то їх обсяг залежить від того, наскільки сприятливим буде інвестиційний клімат. За певних умов інвестори могли б взяти участь, наприклад, у модернізації промислових підприємств, аграрному секторі української економіки й ін.

Слід зазначити, що певні кроки з боку держави для формування іміджу України за кордоном робляться, і навіть виділяються на це кошти. Так, у 2010 році Міністерству закордонних справ виділено 9,2 мільйона гривень на створення позитивного іміджу України за кордоном. Як зазначив прес-секретар прем'єр-міністра Віталій Лук'яненко, "Ідея показати світові нашу країну з кращого боку, щоб залучити інвесторів і туристів з-за кордону, виникла ще у 2004 році, коли президентом був Леонід Кучма, а країна була на підйомі. Але тоді втілити в життя її не встигли". І далі: «Фактично ця програма поновилася з 2007 року, але вона хронічно не виконувалася. Були постійні скандали, гроші, виділені на рекламу країни, зникали... Звичайно, зараз грошей виділено небагато, але

це реальні гроші. Їх витрачання проконтролює КРУ та Рахункова палата» [62].

З метою формування позитивного образу держави, серед іншого, планується:

- видати два подарункових фотоальбоми накладом до 1000 штук, один із яких розповість про Україну загалом, а інший буде рекламувати туристичні визначні пам'ятки країни, її привабливість для бізнесу. Їх роздаватимуть послам, міністрам й іншим високопосадовим гостям країни;

- зняти та запустити в ефір 3-хвилинний ролик під умовною назвою "Пізнай Україну". Його планують показувати на Euronews, CNN та інших. Крім того, буде знятий 15-хвилинний відеофільм про Україну для презентації на виставках, конференціях, ярмарках;

- оновити веб-сайти МЗС і дипломатичних установ за кордоном - на них розмістять інформацію про Україну іноземними мовами.

В Україні стратегія інформаційно-роз'яснювальної роботи розробляється МЗС України (Управління інформації, прес-служба, Управління політичного аналізу та планування) відповідно до доручення Президента України та зовнішньополітичного курсу держави. Зазначені відділи розробляють, моделюють і рекомендують стратегії зовнішньої політики, забезпечують аналіз зовнішньополітичної ситуації та розробляють прогнози на підставі інформації, що надходить в інформаційно-аналітичне управління [239, с.117].

Крім того, в останні роки до роботи над іміджем України залучаються відомі західні PR-агенції. Так, відомо, що за замовленням Міністерства закордонних справ України візуальну концепцію України, а також стратегію позиціонування країни в світі, розробила компанія CFC Consulting, яка ініціює загальнонаціональне обговорення документа. «Сьогодні в суспільстві панує думка про те, що розроблена стратегія

складається з двох символів та логотипу», - зазначив партнер CFC Consulting Василь Мірошниченко, - «разом з тим, громадськість мало ознайомлена з іншими розділами документу - ключовими повідомленнями, системою цінностей, інформаційними кампаніями та спеціальними проектами, які заслуговують вивчення й обговорення».

Головним майданчиком суспільної дискусії стратегії компанія CFC Consulting планує зробити соціальні мережі та нові медіа. Для цього в Facebook, Twitter і LiveJournal створені спеціальні групи і сторінки, які мають загальну назву BrandUkraine, де кожен бажаючий користувач може долучитися до обговорення та висловити свою думку.

Основними компонентами стратегії, розробленої у вигляді бренд-буку та розміщеної на однойменному сайті www.brandukraine.org є: дослідження сприйняття бренду України за кордоном, формулювання стратегії (система цінностей і ключові повідомлення), візуальні рішення, паспорт стандартів, інформаційні кампанії, а також спеціальні події та проекти.

Окрім інформаційної кампанії "Ukraine. All About U", яка вже реалізовується, проектна частина стратегії містить більше десяти масштабних акцій, систематичних заходів, орієнтованих на іноземних інвесторів, туристів, політиків і чиновників міжнародних організацій. Серед них - проекти з популяризації української моди, культурні заходи в адміністративних центрах Євросоюзу - Брюсселі і Страсбурзі, а також технологічні проекти в мережі Інтернет [188].

У розробці стратегії просування того чи іншого продукту часто пропонують вигаданих персонажів, які будуть втілювати ті людські якості, до яких хотілося б прив'язати бренд. Держави та великі корпорації є основними прихильниками такого підходу - адже через упізнаваного персонажа (дядько Сем, Рональд Макдональд, Бібендум тощо) легко передаються емоції та складні зв'язки.

Не стала винятком й українська візуальна концепція. Для просування Української держави в світі було обрано двох персонажів - Спритка та Гарнюню.

Проте дані образи викликали неоднозначну реакцію у широкої громадськості. Як відзначили експерти, обидва ці образи не є релевантними реальному населенню України, а також не є цікавими для потенційних гостей країни. Це змусило Міністерство закордонних справ відмовитися від використання Спритка та Гарнюні для іміджевих кампаній України.

Це не дивно, оскільки, як видається, «імідж держави, який позитивно сприймається та транслюється в різних аудиторіях, повинен будуватися на серйозній ідеологічній основі, тобто являти собою набір певних смислів і зрозумілих формул, які враховують культурні особливості, ціннісні установки, прийняті в даному соціумі. Для цього потрібно знати та брати до уваги національні особливості як країни-виробника, так і держав-споживачів іміджевого продукту. З цим завданням здатні впоратися фахівці в галузі міжкультурної комунікації та вчені-регіоноведи, які займаються об'єктивними дослідженнями в цій сфері, чиї фундаментальні знання сьогодні не надто затребувані суспільством споживання і масової культури» [222, с.16].

Отже, Україна - країна з високим рівнем накопичення інтелектуального капіталу, багатющою культурною спадщиною, унікальним природним середовищем - має величезний потенціал зростання якості життя, але він використовується поки що більш ніж неефективно. Серйозні перешкоди на цьому шляху - слабка сприйнятливість соціальних інститутів до стратегій інноваційного розвитку, низький рівень довіри за межами малих соціальних груп. Це викликає труднощі в конвертації індивідуального творчого досвіду в макросоціальні стратегії розвитку. Розрив між уявленнями про ресурсний

потенціал України і якістю життя її населення, між можливостями розвитку та потребами людей підкріплюється даними про соціальну диференціацію і бідність. У результаті надлишкова нерівність і супутні їй соціальні проблеми підтримують інерцію негативного бачення перспектив розвитку країни, яку лише частково стримують показники економічного зростання.

Висновки до розділу 3

На основі викладеного можна виявити характерну особливість українського інформаційного простору - наявність внутрішніх інформаційних війн: інформаційні війни між олігархами, інформаційна війна між владою й опозицією, інформаційні війни, інсценовані протистоянням різних сегментів влади.

Виявлено політичні чинники розгортання інформаційної війни всередині країни: провал у державному управлінні, який проявляється, насамперед, у кризі ідей відносно модернізації внутрішньої та зовнішньої політики; прагматизм політичних партій, який прийшовши на зміну ідеології, став причиною розмивання відмінностей між ними. Результатом цього стає абсентеїзм, коли електорат виявляє до виборів байдужість і відсутність інтересу. А основним завданням державної політики стає не прогресивний розвиток, а підтримання існуючого порядку будь-якими засобами.

Дослідження показало, що ситуація, яка склалася в сучасному світі та в Україні, змушує до прийняття відповідних заходів протидії іноземній інформаційній експансії. Зокрема, необхідно:

- підвищити ефективність політики інформаційної безпеки в галузі оборони, для чого удосконалити відповідні структури;

- перешкоджати маніпулятивним технологіям, застосовуваним для впливу на суспільну свідомість;

- активно розробляти власні інформаційні технології;

- вдосконалювати методи безпеки інформаційних і телекомунікаційних систем, а також систем і засобів інформатизації озброєння та військової техніки, систем управління військами і зброєю;

- готувати фахівців у галузі ведення інформаційної війни.

Викладене дозволяє зробити висновок, що через відставання у сфері інформаційно-комунікаційних технологій Україна поки що програє в інформаційній війні найбільш розвиненим країнам світу, і найбільше в цій ситуації наноситься шкоди міжнародному іміджу України.

Аналіз соціокультурних механізмів дозволяє виділити універсальні позитивні характеристики, що впливають на формування позитивного сприйняття країни як всередині самого національного співтовариства, так і за його межами. Це перш за все рівень соціального самопочуття національної спільноти. Ключовою складовою тут є оцінка особистого майбутнього в контексті перспектив розвитку країни. У зв'язку з цим постає питання про суб'єктів інноваційного розвитку на надіндивідуальному рівні та про необхідність створення і підтримки стимулюючого розвиток інституційного середовища, соціальних й економічних умов, сприятливих для розвитку креативних практик. Мова йде не стільки про художню творчість, яка може стати «візитною карткою» країни за умови створення нових значущих образів і форм, скільки про розвиток інноваційної економіки, наукового потенціалу і, головне, різних форм соціальної творчості.

Поки що в української влади немає якоїсь єдиної стратегії інформаційного супроводу реалізованих країною внутрішньо- і

зовнішньополітичних заходів. Очевидно, що це пов'язано з недооцінкою із боку українського керівництва політики інформаційної війни як засобу, здатного протистояти опонентам як ззовні, так і всередині країни.

На думку автора, назріла нагальна необхідність у створенні спеціальної державної структури відповідальної за формування позитивного образу України на міжнародній арені.

Зовнішній імідж сучасної України потребує суттєвого зміцнення. Ця обставина, безумовно, впливає на сприйняття українських політичних лідерів за кордоном, яке викривлюється через призму далеко не завжди позитивних уявлень про українські реалії. Це необхідно враховувати в зовнішньополітичній інформаційно-пропагандистській роботі з закордонними аудиторіями, до яких слід доносити не лише історичні та соціокультурні особливості країни, але і її реальні досягнення й успіхи в різних сферах життя суспільства, мирної та відкритої зовнішньої політики.

ВИСНОВОК

Аналіз ступеня розробленості проблеми показав, що питання інформаційних війн досліджуються в економічному, управлінському, організаційно-технічному, психологічному, правовому, культурологічному й інших аспектах. Однак, враховуючи, що останнім часом у політичному просторі як окремих країн, так і всього світу інформаційні технології та інформація отримали визначальне значення, політичний аспект вивчення інформаційних війн зайняв домінуючу позицію.

Незважаючи на те, що у вітчизняній політичній науці запропоновано чимало ідей теоретичного та практичного характеру, що стосуються збору, використання й поширення інформації, інформаційних засобів і технологій у політичних цілях, у той же час відчувається дефіцит комплексних досліджень, присвячених проблемам інформаційної війни. Розгляд наукових робіт зарубіжних авторів дозволив отримати актуальну інформацію з досліджуваної проблеми, зіставити зміст систем інформаційного протиборства в різних країнах.

Дослідження основних концепцій і підходів до розуміння природи процесів інформаційної війни показало, що деякі з класичних теорій, наприклад Г. Лассуела, в даний час здаються трохи наївними, проте свого часу вони повністю відповідали парадигмальним теоретичним поглядам у соціології та психології.

Сучасний досвід розвитку політичних систем дійсно продемонстрував певні тенденції до зростання ролі техніко-інформаційних засобів в організації політичного життя, насамперед в індустріально розвинених державах. Завдяки новим технічним засобам сьогодні можна охопити пропагандою мільйони людей одночасно. З'явилися й організації, здатні ставити неймовірні раніше за масштабами політичні спектаклі у вигляді масових видовищ або кривавих провокацій.

Поки що в теорії політичної науки не сформувалося єдине універсальне поняття інформаційної війни. Однак на основі сучасного досвіду ведення інформаційних війн ясно, що інформаційна війна є не тільки особливим способом «несилового» ураження супротивника, але і самостійною формою політичної боротьби.

Інформаційна війна - це, перш за все, сукупність певних ідей, які руйнують національну самосвідомість цілого народу. Саме в цьому полягає її стратегія. В інформаційної війни, порівняно з війною звичайною, набагато більше тактичних прийомів, вивертів, способів і хитрувань.

Порівняння понять «інформаційна війна» й «інформаційно-психологічна війна» дозволило зробити висновок про те, що в інформаційній війні об'єктом впливу стають комп'ютери та інформаційні системи; в інформаційно-психологічній війні до інформаційного напрямку приєднується психологічний - об'єктом впливу стає індивідуальна і масова свідомість. В результаті цього не тільки руйнується наявна інформаційна система, а й проводиться зміна комунікативної установки в суспільстві.

Інформаційні війни ведуться давно, проте до XXI століття їхні прийоми стали набагато витонченішими, а тому небезпечнішими. Адже сьогодні ті, хто планує та здійснює інформаційні атаки, озброєні сучасними знаннями в галузі психології. Це дозволяє їм впливати на підсвідомість і таким чином керувати вчинками людей. На зміну

прямолінійній пропаганді приходить масовий гіпноз, котрому піддаються цілі країни та народи. Методи, що дозволяють досягати подібних результатів, виникли й удосконалювалися протягом усієї історії людства, ставали все більш ефективними. Так від шаманських танців людство перейшло до психотехнологій, за допомогою яких здійснюється прихований вплив на поведінку людини. Зазнавши подібного впливу, людина навіть не усвідомлює не тільки його мету, але й те, що він взагалі відбувається. В результаті прихованого інформаційного впливу людина може перетворитися на справжнього зомбі, який безвідмовно виконуватиме будь-які вимоги свого володаря. При цьому зовні така людина не буде відрізнятися від оточуючих, а сама не усвідомлюватиме, що піддалася «програмуванню».

На сьогодні провідні країни світу знаходяться у стані перехідного періоду від індустріального етапу свого розвитку до індустріально-інформаційного, на якому головним стратегічним національним ресурсом стають інформація, мережева інфраструктура й інформаційні технології. Завершення цього періоду очікується у другому десятилітті XXI століття, але вже сьогодні інформаційна залежність усіх сфер життєдіяльності особистості, суспільства та держави надзвичайно велика. Дослідження досвіду зарубіжних країн у розвитку технологій політичної інформаційної війни показало, що в даний час у світі розроблено й апробовано на практиці широкий спектр засобів і методів інформаційного впливу. Практично всі сторони, які здійснюють інформаційний вплив у своїх інтересах, формують стратегію і тактику інформаційної війни, конкретний зміст інформаційно-психологічних операцій у відповідності до своїх інтересів, цілей, завдань та наявних можливостей. На основі досвіду багатьох держав можна зробити висновок, що інформаційна війна є не тільки функцією Збройних сил, а й інших інститутів держави. Активну роботу в цьому напрямку ведуть спецслужби.

Зроблено висновок про те, що на сьогодні електронний шпіонаж став суворою реальністю. Загальну кількість операцій електронного шпіонажу, що відбуваються у світі, навіть важко підрахувати, оскільки в силу різних причин не всі вони стають надбанням гласності. Комп'ютери перетворилися на найпотужнішу зброю електронного шпіонажу. Для ліквідації електронного шпіонажу потрібна розробка безлічі заходів, починаючи з прийняття адекватного законодавства та закінчуючи вирішенням суто технічних питань. Наприклад, із метою зниження або нейтралізації існуючих і майбутніх небезпек для суспільства необхідно контролювати Інтернет. Однак при цьому слід прагнути до того, щоб не порушити природу Інтернету, цієї складної динамічної системи, що розвивається абсолютно вільно на основі власних законів еволюції та самоорганізації. Головне ж завдання полягає в тому, щоб на міжнародному рівні, наприклад ООН, розробити комплексну програму, що включатиме в себе можливі форми та методи боротьби з електронним шпіонажем - юридичні, програмні, технологічні, організаційні, економічні, політичні і т.д. Ці дії принесуть успіх лише у випадку, якщо будуть спиратися на систему постійного моніторингу електронного шпіонажу на загальнопланетарному та національному рівнях.

Зроблено висновок про те, що на даному етапі найважливіша роль в інформаційній війні, як і раніше належить ЗМІ, особливо електронним. Суттєвою проблемою сучасного етапу політичного розвитку є те, що багато ЗМІ (які в основному займаються «викривальною» журналістикою та доводять до громадської думки відомості про афери, тіньове життя політиків) часто нехтують суспільною мораллю. Практикований цими ЗМІ стиль критики опонентів нерідко порушує прийняті в суспільстві норми пристойності, а іноді й правові обмеження. Одним із найпоширеніших прикладів такого порушення норм, у тому числі і правового характеру, є надмірно докладне висвітлення журналістами ситуацій із захопленням

заручників, що нерідко використовується для критики або окремих політичних діячів, або уряду в цілому. Щоб зняти такого роду конфлікти та запобігти соціальним чварам, розпалюванню національної ворожнечі та іншим негативним наслідкам дій журналістів, у демократичних державах приймаються закони про ЗМІ, які регламентують їхню діяльність і встановлюють суворі обмеження на поширення публічного слова.

У результаті дослідження зроблено висновок про те, що технології інформаційної війни застосовуються не тільки в інтересах військово-політичного керівництва іноземних держав, а й з метою політичної боротьби всередині якої-небудь держави. У зв'язку з цим були розглянуті причини та наслідки інформаційних війн у сучасній українській політиці.

Інформаційна війна ставить перед Україною дві взаємопов'язані проблеми. Одна з них полягає в тому, що включення в світові процеси інформатизації, інтеграція в інформаційний простір є факторами подальшого розвитку всіх сфер суспільного життя, формування позитивного іміджу у світовому співтоваристві. З іншого боку, поширення інформаційних технологій, які не знають кордонів і практично не мають бар'єрів, веде до виникнення нових загроз безпеці особистості, суспільства і держави в Україні.

Доводиться констатувати, що поки ще українська політична еліта недооцінює роль інформаційної війни в умовах стрімкого розвитку глобальної економічної та геополітичної конкуренції в сучасному світі. Думається, що багато в чому геополітичне та геоекономічне значення України буде залежати від того, чи зможе вона створити ефективну систему інформаційної війни, в яку повинні входити потужні інформаційно-аналітичні й інформаційно-пропагандистські структури. Така система повинна одночасно вирішувати дві важливі задачі: організація жорсткого опору інформаційним акціям супротивника й обмеження сфери розповсюджуваних ним відомостей, особливо тих, що

можуть нанести політичний збиток країні. Таким чином, необхідно контролювати власні інформаційні потоки й обмежувати можливості супротивника щодо проведення інформаційних атак.

Не секрет, що в Україні серйозні проблеми створює діяльність зарубіжних ЗМІ. Масовий інформаційний продукт сьогодні часом суперечить деяким вітчизняним традиціям і відносинам. Інформаційний простір України знаходиться під впливом масової культури, яка захоплює все населення України. Поряд із посиленням і навіть підвищенням деяких культурних стандартів (особливо у сфері споживання) завдяки їй людина політична стає людиною натовпу, яка діє за принципом «як усі», прагнучи не розуміти, а діяти. Таким чином, політичні сили повинні знайти спосіб адаптуватися до цієї інтернаціоналізації масових комунікацій, зберігши при цьому культурну специфіку свого суспільства.

Дослідження показало, що політичні сили України, які вдаються до технологій інформаційних війн, практично не дотримуються прийнятих у суспільстві норм, кожен раз демонструють інновації, ламаючи звичні стандарти публічного спілкування. Однак вони, як правило, перекладають відповідальність за це на опонента або пояснюють необхідність подібних дій екстраординарними обставинами.

Україна порівняно нещодавно почала активно формувати власний імідж для позиціонування себе як сучасної держави, що динамічно розвивається. Поліпшення образу Української держави в світі є одним із пріоритетних напрямів зовнішньої політики. Розгляд механізмів формування позитивного образу України за кордоном показав, що на формуванні «зовнішнього» образу позначаються як стереотипи мислення укорінені в свідомості міфологеми сприйняття, так і політичні пріоритети тих, хто взаємодіє з Україною, а уявлення, які складаються на підставі оцінки різних сторін української дійсності, носять опосередкований характер. Тим не менше, між образом і реальністю простежується взаємна

залежність. Іміджеві технології вносять лише певні корективи і, скоріше, емоційне напруження в характер такого сприйняття.

Україні для того, щоб вигравати інформаційні війни, необхідні грамотна, активна інформаційна стратегія та стратегія культурної репрезентації за кордоном. Усе це міг би забезпечити спеціальний орган управління для ведення інформаційних війн, який відповідав би за зовнішньополітичну пропаганду.

Тільки це може стати гарантією того, що Україна не опиниться на задвірках світового інформаційного простору з дискредитованим, не без допомоги «дружніх» держав, іміджем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авсейков С.А. Политические аспекты влияния глобализации на развитие российских и зарубежных информационных сообществ : автореф. дис… канд. полит. наук : 23.00.04 – политические проблемы международных отношений и глобального развития / С.А. Авсейков. – М., 2007. – 21 с.

2. Авторитет Украины в мире должен расти – Янукович [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/power/2011/02/01/750586.html

3. Агамирзян И.Р. Управление Интернетом – вызов нового века или страх перед будущим? / И.Р. Агамирзян // Технологии информационного общества – Интернет и современное общество : труды VII Всероссийской объединенной конференции (Санкт-Петербург, 10–12 ноября 2004 г.). – СПб. : Изд-во Филологического фак-та СПб. ГУ, 2004. – С. 153–155.

4. Адилов В.А. Образ России в Казахстане: опыт проектирования имиджа страны во внешней среде : автореф. дис… канд. соц. наук : спец. 23.00.02 – политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии (социологические науки) / В.А. Адилов. – М., 2009. – 26 с.

5. Акопов Г. Internet – джин, выпущенный из бутылки [Електронний ресурс]. – Режим доступу: http://www.rau.su/observer/N12_2004/12_03.HTM

6. Алексеева А.О. Новые интерактивные медиа в контексте теорий информационного общества: дис… кандидата филол. наук: спец. 10.01.10 «Журналистика» / А.О. Алексеева. – М., 2006. – 169 с.

7. Алмонд Г. Сравнительная политология сегодня Мировой обзор / Г. Алмонд, Дж. Пауэлл, К. Стром, Р. Далтон. – М.: Аспект Пресс, 2002. - 537 с.

8. Андросова И.Г. Особенности политико-психологического манипулирования в современной России : автореф. дис… канд. полит. наук : Специальность: 23.00.02 – Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии / И.Г. Андросова. – М., 2008. – 30 с.

9. Анохин М.Г. Авангардные информационные технологии PR: возможности и перспективы / М.Г. Анохин, М.Ю. Павлютенкова // Связи с общественностью в политике и государственном управлении / Под общ. ред. В.С. Комаровского. – М.: Изд-во РАГС, 2001. С. 408–425.

10. Ануфриева А. Блоги, новые медиа и гражданская журналистика / А. Ануфриева [Электронный ресурс]. - Сайт LifeInternet. – Режим доступу: http://www.yashar.ru/post34272843/

11. Арапова Н.П. Социально-информациологический подход к теории информационных войн / Н.П. Арапова. – М.: РАГС, 2007. – 234 с.

12. Ассанж: Интернет содействует тоталитаризму, а не свободе слова [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/opinion/2011/03/16/758517.html.

13. Афанасьева Е. Государство или революция? / Е. Афанасьева. – М.: Европа, 2005. – 124 с.

14. Ашин Г.К. Вторжение без оружия: идеологическая борьба в современном мире и буржуазная “массовая культура” / Г.К. Ашин. – М.: Советская Россия, 1985. – 160 с.

15. Бабак М.П. Використання комунікативних методів побудови політичного іміджу в засобах масової інформації : автореф. дис… канд. філол. н. : спец. 10.01.08. – журналістика / М.П. Бабак. – К., 2007. – 21 с.

16. Багиров Р.З. Политическая коммуникация в обеспечении военной безопасности Российской федерации : автореф. дис. на соискание науч. степени канд. полит. наук наук : спец. 23.00.02 «Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии» / Р.З. Багиров. –М., 2009. – 21 с.

17. Бакулев Г.П. Массовая коммуникация: Западные теории и концепции: [учебное пособие для студентов вузов] / Г.П. Бакулев. – М.: Аспект Пресс, 2005. – 176 с.

18. Балуев Д.Г. Личностная и государственная безопасность: международно-политическое измерение / Д.Г. Балуев: Монография. Н. Новгород: Изд-во Нижегородского госуниверситета, 2004. – 231 с.

19. Барматова С. Изменение места и роли коммуникации в современном мире / С. Барматова // Социология: теория, методы, маркетинг. – 2009. - № 3. – С.161.

20. Бедрицкий А.В. Реализация концепции информационной войны военно-политическим руководством США на современном этапе : автореф. дис… канд. полит. наук : спец. 23.00.04 – политические проблемы международных отношений и глобального развития / А.В. Бедрицкий. – М., 2007. – 26 с.

21. Бехманн Г. Концепции информационного общества и социальная роль информации / Г. Бехман // Политическая наука. – 2008. - № 2. – С.10-28.

22. Богуш Д. Будущее имиджа Украины [Електронний ресурс]. – Режим доступу: http://pressing.net.ua/pressing/menu/Monitoring/Analitics/4783

23. Бойко Ю. Политика государства в информационной сфере. //Обозреватель. – 2006. – № 7. – С.24-26.

24. Больц Н. Азбука медиа / Н. Больц. – М.: Европа, 2011. – С.65 136 с.

25. Брайант Дж. Основы медиа-воздействия / Дж. Брайант, С. Томсон. – М., 2004. – 432 с.

26. Бритков В.Б. Информационные технологии в национальном и мировом развитии / В.Б. Бритков, С.В. Дубовский // Общественные науки и современность. – 2000. – № 1. – С. 146–150.

27. Брусницин Н.А. Информационная война и безопасность / И.А. Брусницин. – М.: Вита-Пресс, 2001. – 134 с.

28. Будылин К.Ю. Информационное противоборство в военной сфере (политологический анализ) : автореф. дис… канд. полит. наук : спец. 23.00.02 – политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии / К,Ю. Будылин. – М., 2009. – 16 с.

29. Быков И.А. Интернет-сайт как инструмент политической коммуникации / И.А. Быков [Электронный ресурс]. – Режим доступу: bykov.socionet.ru/public/Bykov_SitePolitPart.html

30. В 2010 году мировой интернет-трафик вырос на 60 процентов [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/internet/2010/10/08/721460.html.

31. В Европарламенте считают Украину показательным примером олигархии [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/power/2011/04/06/762557.html

32. Вершинин М.С. Политическая коммуникация в информационном обществе / М.С. Вершинин. – СПб.: Изд-во Михайлова В.А., 2001. – 252 с.

33. Вершинин М.С. Политическая коммуникация в информационном обществе: перспективные направления исследований / М.С. Вершинин // Актуальные проблемы теории коммуникации : сборник научных трудов. – СПб.: Изд-во СПбГУ, 2004. – С.98-107.

34. В информационной войне превосходство в военной мощи не гарантирует от поражения [Електронний ресурс]. – Режим доступу: http://www.arms-expo.ru/049051124053053051052.html.

35. В Иране подумывают об альтернативе Интернету [Електронний ресурс]. – Режим доступа: http://podrobnosti.ua/internet/2011/05/30/772390.html.

36. В Китае массово закрывают интернет-сайты [Электронный ресурс]. - Сайт Подробности. - Режим доступу: http://podrobnosti.ua/internet/2009/01/27/578788.html

37. Вейман Г. Как современные террористы используют Интернет / Г. Вейман [Електронний ресурс]. – Режим доступу: http://nak.fsb.ru

38. Вирилио П. Информационная бомба. Стратегия обмана / П. Вирилио. – М.: Фонд науч. исслед. “Прагматика культуры”: Гнозис, 2002. – 190 с.

39. Власов А.И. Политические манипуляции: История и практика средств массовой информации США / А.И. Власов. – М.: Международные отношения, 1982. – 303 с.

40. Война в Южной Осетии перекинулась на Интернет. В последнем конфликте на Кавказе участвовали полки хакеров, вооруженных компьютерами [Електронний ресурс]. – Режим доступу: http://news.bbc.co.uk/hi/russian/international/newsid_7561000/7561201.stm)

41. В последнем конфликте на Кавказе участвовали полки хакеров, вооруженных компьютерами [Електронний ресурс]. – Режим доступу: http://news.bbc.co.uk/hi/russian/international/newsid_7561000/7561201.stm)

42. Воронцова Л.В. История и современность информационного противоборства / Л.В, Воронцова, Д.Б. Фролов. – М.: Горячая линия – Телеком, 2006. – 192 с.

43. В скором времени будет создана глобальная система кибербезопасности [Електронний ресурс]. - Режим доступу: http://podrobnosti.ua/internet/2011/06/25/777413.html

44. В Украине каждый четвертый является пользователем Сети [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/internet/2010/07/15/701012.html.

45. Гавра Д.П. Современные подходы к построению структурной модели внешнего имиджа государства / Д.П. Гавра [Электронный ресурс]. – Режим доступа: www.statebrand.ru/upload/files/doc_1222464362.doc)

46. Галумов Э.А. Имидж против имиджа /Э.А. Галумов. - М., 2005. – 176 с.

47. Галумов Э.А. Международный имидж России: стратегия формирования / Э.А. Галумов. – М., 2003. – 423 с

48. Головин И. Информационная война / И. Головин // Мир безопасности. – 1998. - № 8-9 (60). – С.79-85.

49. Голубєв В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / за заг. ред. Р. А. Калюжного, М. Я. Швеця / В. О Голубєв, В.Д Гавловський., В. С. Цимбалюк. — Запоріжжя: Просвіта, 2001.— 252 с.

50. Голубев В. Проблемы борьбы с кибертерроризмом в современных условиях / В. Голубев, Т. Сайтарлы [Електронний ресурс]. – Режим доступу: http://www.crime-research.ru/library/e-terrorism.htm.

51. Горбенко А.И. Информационное противоборство в политике современных государств : автореф. дис… канд. полит. наук : спец. 23.00.02 – «Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии» / А.И. Горбенко. – М., 2008. – 19 с.

52. Горбенко А. СМИ в сфере информационного противоборства / А. Горбенко / Власть. – 2008. - № 11. – С. 23-26.

53. Грачев Г. Информационно-психологическая безопасность личности [Электронный ресурс] / Г. Грачев, И. Мельник. – 2004. - URL: http://www.koob.ru/grachev_melnik/psy_defence

54. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты / Г.В. Грачев ; Рос. акад. гос. службы при Президенте Рос. Федерации. - М. : Изд-во РАГС, 1998. - 123 с. ; То же [Электронный ресурс]. – URL: http://www.i-u.ru/biblio/archive/grachev%5Finfo/ (16.01.08).

55. Грачев Г.В. Информационно-психологическая безопасность личности: теория и технология психологической защиты : автореф. дис. ... д-ра психол. наук / Г.В. Грачев ; [Рос. акад. гос. службы при Президенте Рос. Федерации]. - М., 2000. - 56 с.

56. Грачев Г.В. Личность и общество: информационно-психологическая безопасность и психологическая защита / Г.В. Грачев. - М. : ПЕР СЭ, 2003. - 303 с.

57. Гринберг Т.Э. Образ страны или имидж государства: поиск конструктивной модели / Т.Э. Гринберг [Електронний ресурс]. – Режим доступу: http://www.mediascope.ru/node/252.

58. Гриняев С. Война в четвертой сфере. Превосходство в киберпространстве будет определять победу в конфликтах XXI века / С. Гриняев [Електронний ресурс]. – Режим доступу: http://nvo.ng.ru/spforces/2000-11-10/7_war.html.

59. Гриняев С. Информационная война: история, день сегодняшний и перспектива / С. Гриняев [Електронний ресурс]. – Режим доступу: www.Agentura.ru

60. Гриняев С.Н. Концепции ведения информационной войны в некоторых странах мира / С.Н. Гриняев // Зарубежное военное обозрение. – 2002. - № 2. – С.5.

61. Губарев А.Б. Информационные войны как объект политологического исследования : автореф. дис… канд. полит. наук : спец. 23.00.02 / А.Б. Губарев. – Уссурийск, 2005. – 26 с.

62. 9 миллионов гривен потратят на рекламу Украины [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/power/2010/07/29/704643.html

63. Деньщиков А.Л. Информационная стратегия США (анализ, современность, перспективы) : автореф. дис…. канд. полит. наук : спец. 23.00.02 – политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии / А.Л. Деньщиков. – М.. 2007. – 26 с.

64. Джадан И. Искусство психологической войны. Психологические операции в эпоху незаконной миграции [Електронний ресурс]. – Режим доступу: http://www.apn.ru/publications/article21053.htm

65. Дзялошинский И.М. Манипулятивные технологии в масс-медиа. – Вестник МГУ. – Сер. Журналистика. - № 1-2.

66. Димлевич Н. Информационные войны в киберпространестве – Китай и Индия / Н. Димлевич [Електронний ресурс]. – Режим доступу: http://www.truenet.info/analitika/informatsionnye-voyny-v-kiberprostranstve-kitay-i-indiya.html

67. Дмитриев А.В. Массовая коммуникация: пределы политического влияния / А.В. Дмитриев, В.В. Латынов. – М.: Межведомственный научно-учебный центр комплексных проблем национальной политики (МНУЦ), 1999. – 111 с.

68. Дмитриева А.Г. Информационная война как феномен современной политики / А.Г. Дмитриева // SCHOLA-2009: Сборник научных статей факультета политологии Московского государственного университета имени М. В. Ломоносова / Под общ. ред. А. Ю. Шутова и А.

А. Ширинянца; сост. А. И. Волошин, Э. А. Козьменко. — М.: Издательство «Социально-политическая МЫСЛЬ», 2009. — С. 261–264.

69. Доповідь Секретаря РНБОУ Раїси Богатирьової щодо питання забезпечення національної безпеки в інформаційній сфері [Електронний ресурс]. – Режим доступу: http://www.bogatyrova.org.ua/press/news/47e757ea070f7/view_print/

70. Дремлюга Р.И. Интернет-преступность : автореф. дис… канд. юрид наук : спец. 12.00.08 – уголовное право и криминология; уголовно-исполнительное право / Р.И. Дремлюга. – Владивосток, 2007. – 25 с.

71. Дьякова Е.Г. Массовая коммуникация: модели влияния. Как формируется “повестка дня”? / Е.Г. Дьякова, А.Д. Трахтенберг. – Екатеринбург: Издательство Гуманитарного университета, 2001. – 130 с.

72. Дьякова Е.Г. Массовая политическая коммуникация в теории установления повестки дня: от эффекта к процессу/ Е.Г. Дьякова // Полис. – 2003. - № 3. – С.119

73. Дьякова Е. Массовая политическая коммуникация в теории установления повестки дня: от эффекта к процессу / Е. Дьякова // Полис. – 2003. - № 3. –

74. Евдокимов В. Информационная война как феномен политической коммуникации / В. Евдокимов // Актуальные проблемы образования и воспитания: международный опыт и перспективы сотрудничества. Сборник научных статей / научный ред. А.Э. Еремеев, отв. редактор О.В. Попова. – Омск: Издательство НОУ ВПО «Омская гуманитарная академия», 2009. – 188 с.

75. Еляков А. Интернет – Тотальная угроза обществу? / А. Еляков // Мировая экономика и международные отношения. – 2007. - № 11. – С. 92-95.

76. Еляков А. Электронный шпионаж / А. Еляков // Международная экономика и международные отношения. – 2009. - № 8. – С.62-68.

77. Емельянов Г.А. Информационная безопасность России. Основные понятия и определения : Учеб. пособие / Г.А. Емельянов, А.А, Стрельцов // Под общей ред. Проф. А. Прохожева. – М.: РАГС, 1999. – Ч.1. – С.34.

78. Ефимова С.С. Механизм формирования общественного мнения о власти в современной России : автореф. дис… канд. соц. наук : спец. 23.00.02 – Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии (социологические науки) / С.С. Ефимова. – Саратов, 2007. – 22 с.

79. Жуков В. Взгляды военного руководства США на ведение информационной войны / В. Жуков // Зарубежное военное обозрение. – 2001. - № 1. – С.2-9.

80. Забузов О.Н. Интернет как средство реализации военно-информационной политики Российского государства : автореф. дис. на соискание науч. степени канд. полит. наук наук : спец. 23.00.02 «Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии». – М., 2008. – 26 с.

81. Забузов О.Н. Сущность и структура политической коммуникации / О.Н. Забузов // Общество и безопасность: история, перспективы эволюции, современное состояние: Межвузовский сборник научных статей / под ред. Н.П. Шабанова – Саратов: СВИРХБЗ, «Научная книга», 2006. – С. 120–130.

82. Завадский И.И. Информационная война – что это такое? – М., 1999. – 153 с.

83. Закон України «Про доступ до публічної інформації» [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/T112939.html

84. Залєвська І.І. Інформаційна безпека: нові підходи до визначення поняття / І.І, Залєвська // Освіта регіону. – 2010. - № 4. – С.216-220.

85. Залєвська І.І. Нові інформаційні загрози національної безпеки / І.І. Залєвська // Політичний вісник. Зб. Наук. Праць – Вип.52. – К.: «ІНТА», 2011. – С.362-370.

86. Залєвська І.І. Принципи державної політики у сфері забезпечення інформаційної безпеки / І.І. Залєвська // Вісник державної академії керівних кадрів культури і мистецтв: наук. журнал. – К.: Міленіум, 2011. - № 1. – С.199-202.

87. Золина Г.Д. Формирование положительного образа Краснодарского края в средствах массовой информации : автореф. дис… канд. филол. наук : спец. 10.01.10. – Журналистика / Г.Д. Золина. – Краснодар, 2007. – 29 с.

88. Інтернет становить загрозу для інформаційної безпеки України [Електронний ресурс]. – Режим доступу: http://telekritika.kiev.ua/bezpeka/2008-10-24/41481

89. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навчальний посібник // За заг. ред. В. Б. Толубка. – К.: НАОУ, 2004. – 315 с.

90. Информационные войны в киберпространстве – США (часть 1) [Електронний ресурс]. – Режим доступу: http://mywebs.su/blog/politic/2869.html

91. Информационные вызовы национальной и международной безопасности / И.Ю. Алексеева и др. Под общей ред. А.В. Федорова В.Н. Цыгичко. – М.: ПИР-Центр, 2001. – 328 с.

92. Использование за рубежом сети Интернет в интересах ведения информационных войн [Електронний ресурс]. – Режим доступу: http://defpol.org.ua/site/index.php/ru/arhiv/alternativno/5986-2011-06-17-07-53-23

93. Іщенко М. Імідж України в контексті глобальних трансформаційних процесів / М. Іщенко, О. П'ецух // Політичний менеджмент. – 2008. - № 4 - С.158-164.

94. Каждый третий украинец является пользователем Интернета [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/internet/2011/02/17/753622.html)

95. Кара-Мурза С.Г. Манипуляция сознанием / С.Г. Кара-Мурза. – М., 2000.

96. Карпенко Н. Иллюзии и реалии бренда «Украина» / Н. Карпенко [Електронний ресурс]. – Режим доступу: http://propr.com.ua/ru/public/view/14724

97. Карякин В.В. Наступила эпоха следующего поколения войн – информационно-сетевых / В.В. Карякин [Електронний ресурс].- Режим доступу: http://nvo.ng.ru/concepts/2011-04-22/1_new_wars.html.

98. Кафтанчиков, Д.П. Как противостоять информационной агрессии /Д.П.Кафтанчиков, Д.Л. Цыбаков // Государственная служба. – 2008. – № 5. – С. 64–70.

99. Кашлев Ю. Информационное взаимодействие: реальность, перспективы и императивы / Ю. Кашлев, Т. Лебедева. – Прага Международная организация журналистов, 1990. – 368 с.

100. К 2056 году исчезновение украинского языка станет необратимым [Електронний ресурс]. - Режим доступу: http://podrobnosti.ua/society/2011/01/31/750479.html

101. Киберпреступность растет быстрее других видов преступности [Електронний ресурс]. – Режим доступу: http://antimalware.ru/news/2009-12-11/2076

102. Киберпространство: новые угрозы [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/newstext.php?news_id=60111

103. Китай начинает войну в Интернете [Электронный ресурс]. – Режим доступа http://podrobnosti.ua/internet/2010/05/03/683579.html

104. Кларк Р. Третья мировая война. Какой она будет / Р. Кларк, Р. Нейк. – СПб.: Питер, 2011. – 336 с.

105. Клинтон: США терпят поражение в информационной войне [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/opinion/2011/03/03/756262.html

106. Кобзева С.В. Медиа-мониторинг кризисов и конфликтов: методология и техники / С.В. Кобзева // Полис. – 2008. - № 1. – С.33-50.

107. Коляденко В.А. Інфокомунікаційні технології як засіб взаємодії органів влади і суспільства / В.А. Коляденко // Держава і право : зб. наук. пр. – вип. 17. – К.: Інститут держави і права ім.. В.М. Корецького, 2002. – С.494-498.

108. Коляденко В.А. Комунікаційні технології і політичний процес / В.А. Коляденко // Держава і право : зб. наук. пр. – вип. 17. – К.: Інститут держави і права ім.. В.М. Корецького, 2002. – С.477-481.

109. Коляденко В.А. Інфокомунікаційні технології як чинник політичної модернізації / В.А. Коляденко : автореф. дис. на здобуття науковой ступені канд. політ. наук : спец. 23.00.02 «Політичні інститути та процеси» / В.А. Коляденко. – Одеса, 2002. – 16 с.

110. Комлева Н.А. Интернет как ресурс сетевой войны /Н.А. Комлева, Г. Саймонс, Д.Л. Стровский // Журнал ПОЛИТЭКС. – 2010. - № 2. [Електронний ресурс]. – Режим доступу: http: // www.politex.info/content/view/702/30/.

111. Компьютерный абордаж военного спутника // Эхо планеты. – 1999. - № 10. – С.10-16.

112. Компьютерные технологии в юридической деятельности: учеб. и практ. пособие / К.Е. Зинченко, Л.Ю. Исмаилова, А.Н. Караханьян, Б.В. Киселев. - М.: Изд-во БЕК, 1994. - 303 с.

113. Кому нужна информационная война против Украины? [Електронний ресурс]. – Режим доступу: http://www.ukr-portal.com/index.php?nma=news&fla=stat&nums=2525

114. Конгресс США может решить, что хакерам положено 20 лет тюрьмы [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/internet/2011/06/23/776959.html

115. Контрразведка Британии обвинила Китай в электронном шпионаже [Електронний ресурс]. – Режим доступу: http://www.orientnews.ru/politic/5039-kontrrazvedka-britanii-obvinila-kitaj-v.html

116. Коровин В.М. Главная военная тайна США: сетевые войны / В.М. Коровин. – М.: Эксмо – 288 с.

117. Кравченко В.И. Власть и коммуникация в информационном обществе: проблемы теории и методологии : автореф. дис. на соискание науч. степени докт. полит. наук наук: спец. 23.00.02 «Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии» / В.И. Кравченко. – СПб., 2004. – С.48 с.

118. Кравченко В.И. Власть и коммуникация: проблемы взаимодействия в информационном обществе / В.И. Кравченко. – СПб.: Издательство Санкт-Петербургского государственного университета экономики и финансов, 2003. – 272 с.

119. Кракович Д. Проигрывает ли Украина в информационной войне на своей территории? / Д. Кракович [Електронний ресурс]. – Режим доступу: http://dialogs.org.ua/project_ua_full.php?m_id=9802

120. Кретов Б.Е. Средства массовой информации – элемент политической системы общества / Б.Е. Кретов // Социально-гуманитарные знания. – 2000. – № 1. – С. 101–115.

121. Круглый стол, посвященный проблеме информационных войн. (Сергей Миронов Президент Института "Справедливый мир" - Председатель Совета Федерации Федерального Собрания Российской Федерации) [Електронний ресурс]. – Режим доступу: http://www.sdrvdv.org/node/158

122. Крысько В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) / В.Г. Крысько. – Минск: Харвест, 1999. – 189 с.

123. Кудинов О. П. Большая книга выборов: Как проводятся выборы в России / О.П. Кудинов. - М.: Издательство «Арт Бизнес Центр», 2003. - 663 с.

124. Кучумов Д.О. Семантический анализ информационной войны (на примере осетино-ингушского конфликта) : автореф. дис… канд. полит. наук : спец.: 23.00.02 - политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии / Д.О. Кучумов. – Ростов-на-Дону, 2007 – 23 с.

125. Лассуэлл Г. Коммуникативный процесс и его структуры / Г. Лассуэл // Современные проблемы социальной коммуникации. – СПб., 1996. – 234 с.

126. Лассуэлл Г.-Д. Структура и функции коммуникации в обществе / Г.-Д. Лассуэл // Назаров М.М. Массовая коммуникация в современном мире: методология анализа и практика исследований. [пер. М.М. Назарова] – М.: Едиториал УРСС, 2000. – 240 с.

127. Лиллекер Д.Дж. Политическая коммуникация. Ключевые концепты / Д. Дж. Лиллекер. – Харьков: Гуманитарный центр, 2010. – 300 с.

128. Липпман У. Общественное мнение / У. Липпман. – М.: Институт Фонда “Общественное мнение”, 2004. – 384 с.

129. Лозовский Б.Н. Манипулятивные технологии управления средствами массовой информации / Б.Н. Лозовский. Учебное пособие. – Екатеринбург, 2007. – 166 с.

130. Лысенко Г.В. Взаимодействие власти и СМИ: стратегия и технологии ее реализации (региональный аспект) / Г.В. Лысенко // Социологические исследования. – 2008. - № 4. – С.73-78.

131. Макнамара Дж. Воздействие PR на СМИ / Дж. Макнамара [Електронний ресурс]. – Режим доступу: http://www.exlibris.ru/ru/media/show.html?page=articles/090417-prnasmi.html.

132. McAfee предупреждает о наступлении эпохи кибернетических войн [Електронний ресурс]. – Режим доступу: http://press-relizy.ru/archive/hi-tech/25859.html

133. Маліс О.В. Розвиток Інтернету як комунікативного засобу та його вплив на діяльність суб'єктів політичного процесу в Україні : автореф. дис. на здобуття наук. ступеня канд. політ. наук : спец. 23.00.02 «Політичні інститути та процеси» / А.В. Малис. - К., 2009. – 19 с.

134. Маляров А.И. Уголовно-правовые и криминологические аспекты международного сотрудничества в сфере защиты электронно-цифровой информации : автореф. дис… канд. юр. наук : 12.00.08 – уголовное право и криминология; уголовно-исполнительное право / А.И. Маляров. - Краснодар – 2008. – 24 с.

135. Манойло А.В. Государственная информационная политика в условиях информационно-психологической войны / А.В. Манойло, А.И. Петренко, Д.Б. Фролов. - М.: Горячая линия – Телеком, 2003.

136. Манойло А.В. Роль информационно-психологических технологий в разрешении современных конфликтов» : автореф. дис… докт. полит. наук : спец.23.00.04 – политические проблемы международных отношений и глобального развития / А.В. Манойло. – М., 2008. – 30 с.

137. Манойло А.В. Управление психологической войной в системе государственной информационной политики / А.В. Манойло [Електронний ресурс]. – Режим доступу: http://psyfactor.org/lib/psywar26.htm

138. Манойло А.В. Технологии несилового разрешения современных конфликтов / А.В. Манойло. – М.: Горячая линия – Телеком, 2008. – 392 с.

139. Маслакова А. Эксперты: свобода Интернета в России может ограничиваться / А. Маслакова [Електронний ресурс]. – Режим доступу: http://www.epochtimes.com.ua/ru/world/society/jeksperty-cvoboda-interneta-v-rossii-mozhet-ogranichivatsja-t23721.html

140. Медведева Н.Н. Внешнеполитический имидж России в контексте развития отношений с Европейским Союзом : автореф. дис… канд. полит. наук : спец. 23.00.04 - Политические проблемы международных отношений и глобального развития / Н.Н. Медведева. – М., 2008. – 26 с.

141. Милиция перечитает страницы пользователей "ВКонтакте" [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/internet/2010/07/07/698868.html

142. Минникес И.В. Выборы в истории русского государства Х1-ХУШ вв. / И.В. Минникес. – М.: Юридический центр Пресс, 2010. – 538 с.

143. Миру угрожает кибервойна [Електронний ресурс]. – Режим доступу: http://www.zavtra.com.ua/news/mir/57236/

144. Митрохина Т.Н. Компрометирующие материалы в прессе как средство борьбы / Т.Н. Митрохина, С.А. Федорова // Журнал ПОЛИТЭКС. – 2009. - № 3 [Електронний ресурс]. – Режим доступу: http://www.politex.info/content/view/604/30/

145. Михайлов В.А. Особенности развития информационно-коммуникативной среды современного общества / В.А. Михайлов, С.В.

Михайлов // Актуальные проблемы теории коммуникации. – СПб.: Изд-во СПбГПУ, 2004. – С.34-52.

146. Михайлов М.И. История политической пропаганды / М.И. Михайлов. – К., 1990. – 223 с.

147. Михальченко И.А. Информационные войны и конфликты идеологий в условиях геополитических изменений конца XX века : автореф. дис… канд. полит. наук : спец.23.00.03 / И.А. Михальченко – Санкт-Петербург, 1998. – 26 с.

148. Морозова Е.Г. Политический рынок и политический маркетинг: концепции, модели, технологии / Е.Г. Морозова. – М.: Российская политическая энциклопедия (РОССПЭН), 1999. – 246 с.

149. Назаретян А. Психология массового стихийного поведения / А. Назаретян. – М.: ПЕР СЭ, 2001. – 112 с.

150. Недбай В.В. Социально-политические последствия развития информационного общества: Дис. … канд. полит. наук: 23.00.02; - Защищена 5 июля 2004 г. – О., 2004. – 202 с.:

151. Ненашев А.И. Информационное пространство современного общества: коммуникационный аспект: автореферат дис. на соискание науч. степени канд. фил. наук: спец. 09.00.11 «Социальная философия по философским наукам» / А.И. Ненашев. – Саратов, 2008. – 20 с.

152. Ненашев Д.А. Лоббирование посредством компьютерных сетей: новый инструмент политического влияния / Д.А. Ненашев // Политическая наука: сборник научных трудов. – 2002. № 1: Современное состояние. Тенденции и перспективы / отв. ред. и сост. Л.Н. Верченов. – М., 2002. С. 126–136.

153. Нисневич Ю.А. Информационно-коммуникационная стабилизация политической системы / Ю.А. Нисневич // Вестник Российского университета дружбы народов. – Серия: Политология. – 2006. – № 1 (6) – С. 68–80.

154. Нисневич Ю А. Информация и власть / Ю.А. Нисневич. - М.: Мысль - 2000 – 296 с.

155. Олехнович К.С. PR-технологии в региональных политических процессах (на примере Южного Федерального округа) : автореф. дис… канд. полит. наук : спец. 23.00.02 – политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии / К.С. Олехнович. - Ростов-на-Дону, 2007. – 28 с.

156. Ольшанский Д.В. Психология масс / Д.В. Ольшанский. – СПб.: Питер, 2001. – 363 с.

157. Павлютенкова М.Ю. Информационная война: реальная угроза или современный миф / М.Ю. Павлютенкова [Електронний ресурс]. – Режим доступу: http://www.x-libri.ru/elib/smi__352/00000001.htm

158. Панарин И.Н. Информационная война и власть. – М.: Мир безопасности, 2001. – 240 с.

159. Панарин И. Н. Информационная война и выборы / И.Н. Панарин. - М. : ОАО "Издательский Дом "Городец", 2003. – 411 с.

160. Панарин И.Н. Информационная война и дипломатия / И.Н. Панарин. – М.: Городец, 2004. – 528 с.

161. Панарин И.Н Информационная война, PR и мировая политика / И.Н. Панарин. – М.: Горячая линия – Телеком, 2006. – 352 с.

162. Панарин И.Н. Информационная война и Россия / И.Н. Панарин. – М.: Изд.дом Мир безопасности, 2000. – 160 с.

163. Панарин И.Н. Информационная война и Третий Рим / И.Н. Панарин. - М., 2003. - 244 с.

164. Панарин И.Н. Технология информационной войны / И.Н. Панарин. – М.: Изд-во КСП, 2003. - 320 с.

165. Паршин С.А. Кибервойны --- реальная угроза национальной безопасности? / С.А. Паршин, Ю.Е. Горбачев, Ю.А. Кожанов

[Електронний ресурс]. – Режим доступу: http://www.urss.ru/cgi-bin/db.pl?lang=Ru&blang=Ru&page=Book&id=119613

166. ПАСЕ: В Украине политики играют с правилами, а не по правилам [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/power/2010/01/25/660793.html

167. Пеньков И.А. Влияние защищенности российского сегмента глобальной сети Интернет на состояние информационной безопасности государства [Електронний ресурс]. – Режим доступу: http://www.budgetrf.ru/Publications/Magazines/VestnikSF/2005/vestniksf261-09/vestniksf261-09060.htm

168. Перепелица Г. Информационные войны / Г. Перепелица // Зеркало недели. - № 17. - 30 апреля 1999.

169. Петрик В. М. Информационно-психологическая безопасность в эпоху глобализации: Учеб. пособ. / В.М. Петрик, В.В. Остроухов, А.А. Штоквиш и др. // Под. ред. В. В. Остроухова. – К., 2008. – 544 с.

170. Петрик В.М. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій: Навчальний посібник / В.М. Петрик, В.В. Остроухов та ін.. – К.: Росава, 2006. – 208 с.

171. Пигров К.С. Телевидение как этап в развитии виртуального пространства. Виртуальное пространство культуры. Материалы научной конференции 11-13 апреля 2000 г. СПб.: Санкт-Петербургское философское общество, 2000. – С.31-36.

172. Пирумов В.С. Информационное противоборство. Четвертое измерение противостояния / В.С. Пирумов. - М., : Издательский дом «Оружие и технологии», 2003. - 544 с.

173. Пирумов В.С. Некоторые аспекты информационной борьбы в военных конфликтах / В.С, Пирумов, М.А. Родионов // Военная мысль. – 1997. - № 5. – С.44-47.

174. Политические коммуникации / ред. А.И. Соловьев. – М.: Аспект Пресс, 2004. – 332 с.

175. Порфімович О.Л. Імідж як складова політичної культури органу державної виконавчої влади України : автореф. дис… докт. політ. наук : спец. 23.00.03 – політична культура та ідеологія / О.Л. Порфімович. – К., 2006. – 34 с.

176. Почепцов Г.Г. Информационно-психологическая война / Г.Г. Почепцов. – М.: СИНТЕГ, 2000.

177. Почепцов Г.Г. Информационные войны / Г.Г. Почепцов. – М.: РефлБук, Киев: Ваклер, 2000.

178. Проект Концепції Державної програми формування позитивного міжнародного іміджу України на 2007-2010 роки [Електронний ресурс]. – Режим доступу: http://www.mfa.gov.ua/mfa/ua/publication/content/6652.htm.

179. Прокофьев В. Ф. Тайное оружие информационной войны / Прокофьев В. Ф. - М. : СИНТЕГ, 1999. - 152 с.

180. Прокудин Д.Е. Проблемы реализации прав человека в информационном обществе / Д.Е. Прокусин [Електронний ресурс]. – Режим доступу: http://www.politex.info/content/view/635/30/

181. Пюкке С.М. Социальные конфликты в информационной среде: соотношение понятий / С.М. Пюке. - М., 2004.

182. Работа над ошибками: практика «противодействия» Украины информационной агрессии России в «газовом» вопросе [Електронний ресурс]. – Режим доступу: http://www.press-release.com.ua/releases/view/11899/

183. Рада отменяет 50-процентную квоту украинской музыки на ТВ и радио [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/power/2011/02/02/750791.html

184. Разуваев В.Э. Правовые средства противостояния информационным войнам / В.Э. Разуваев : автореф. дис. ... канд. юрид. наук : спец. 12.00.14 / В.Э. Разуваев. - Москва, 2007. – 26 с.

185. Расторгуев С.П. Информационная война / С.П. Расторгуев. - М: Радио и связь, 1999. - 416 с.

186. Решетов Ю.А. Свобода информации: кому она принадлежит? / Ю.А. Решетов // Московский журнал международного права. - 2001. – № 2. - С. 97-101.

187. Робинов А.А. Ограничения свободы СМИ и борьба с терроризмом / А.А. Робинов [Електронний ресурс]. – Режим доступу: http://echr.ru/news/msg.asp?id_msg=166

188. Розробник стратегії поліпшення іміджу україни за кордоном ініціює суспільне обговорення документу [Електронний ресурс]. – Режим доступу: http://mystuff.su/blog/355.html

189. Роль СМИ в военно-политических конфликтах современности [Електронний ресурс]. – Режим доступу: http://www.fpsiholod.ru/smi.htm

190. Роль СМИ в предотвращении конфликтов [Електронний ресурс]. – Режим доступу: http://www.vremya.ru/2008/102/5/205948.html

191. Рост киберпреступности, кибертерроризма и электронного шпионажа тесно связан с вредоносными программами, направленными на хищение данных [Електронний ресурс]. – Режим доступу: http://b2blogger.com/pressroom/release/33978.html&usg=AFQjCNFQ0uZMpLJ59Z37xir8yHRxv1hTCQ.

192. Сапожникова А. Информационно-психологическая безопасность России: состояние и тенденции / А. Сапожникова // Власть, № 2, 2009. – С.54-58.

193. Семененко И.С. Образы и имиджи в дискурсе национальной идентичности / И.С. Семененко // Полис. - 2008. - № 5. - С. 7-18.

194. Сіленко А.О. Інформаційні технології створення образу політичного лідера / А.О. Сіленко // Наукові записки Інституту політичних і етнонаціональних досліджень ім. І.Ф.Кураса НАН України: Збірник наукових праць. – К., 2007. – Вип. 35. – С.52-67.

195. Сіленко А. Інформаційні технології – новий імпульс для пошуку парадигми майбутнього суспільства / А.О. Сіленко // Політичний менеджмент. – 2007. - № 3. – С.96-113.

196. Сіленко А.О. Соціально-політичні наслідки інформаційної революції / А.О. Сіленко // Політичний менеджмент. – 2005. - № 5. – С.61-75.

197. Соленикова Н.В. Интернет как канал распространения политической рекламы в предвыборный период / Н.В. Соленикова // Материалы Международной научно-практической конференции «Вторая мировая война в зеркале современности»: Ч. 2 /Ред.кол.: Дорожкин Ю.Н. и др. – Уфа: Изд-во УГНТУ, 2005. - С.351-360.

198. Соленикова Н.В. Политический Интернет в российских избирательных кампаниях: тенденции развития / Н.В. Соленикова // Общественные науки и современность. – 2007. № 5. – С. 69-74.

199. Соленикова Н.В. Опыт использования Интернет во время избирательной кампании на Украине / Н.В. Соленикова // Актуальные проблемы связей с общественностью в современном российском обществе: Сборник статей Всероссийской научно-практической конференции. – Пенза, 2005. - С. 114-116.

200. Соленикова Н.В. Основные этапы становления и развития политической рекламы в Интернет / Н.В. Соленикова // Материалы III Всероссийской научно-практической конференции «PR-технологии в информационном обществе». - Часть I Санкт-Петербург, 25-26 февраля 2006 г. СПб.: Изд-во СПбГПУ, 2006. - С. 198-200.

201. Соловьев Э.Г. Международный имидж современной России: дефицит привлекательности или дефицит идей? / Э.Г. Соловьев, А.Н. Смирнов. – Полис. – 2008. - № 5. – С. 19-33.

202. Соседи ассоциируют Украину с коррупцией и каникулами [Електронний ресурс]. - Режим доступу: http://podrobnosti.ua/society/2011/06/22/776845.html.

203. Степанова Н.С. Информационное противоборство между Японией и КНДР (политологические аспекты : автореф. дис… канд. полит. наук : спец. 23.00.04 - Политические проблемы международных отношений глобального и регионального развития / Н.С. Степанова. – М., 2010. – 30 с.

204. США-Канада: экономика, политика, культура. – 2007. - № 3. – С. 34-37.

205. Тараскин М.М. Взгляды Высшего военно-политического руководства ведущих иностранных государств на противодействие угрозам кибернетических войн / М.М. Тараскин, С.А. Чешуин [Електронний ресурс]. – Режим доступу: http://www.naukaxxi.ru/materials/171/

206. Терещук В.І. Електронний паблік рілейшнз як засіб формування зовнішньополітичного іміджу держави : автореф. дис… канд. політ. наук : спец. 23.00.04 — Політичні проблеми міжнародних систем та глобального розвитку / В.І. Терещук. – Чернівці, 2008. – 23 с.

207. Ткаченко С. Информационная война против России / С. Ткаченко. – СПб.: Питер, 2011. – 224 с.

208. Тоффлер Э. Метаморфозы власти: знание, богатство и сила на пороге XXI века [Пер. с англ.] / Э. Тоффлер. — М.: ООО «Издательство АСТ», 2003. – 669 с.

209. Турко Н.И. Основы информационной войны / Н.И. Турко // Анализ систем на пороге XX1 века: теория и практика. – М., 1996. – 312 с.

210. Туронок С.Г. Информационно-коммуникативная революция и новый спектр военно-политических конфликтов / С.Г. Туронок // Полис. – 2003. - № 1.- С.24-38.

211. Угроза кибершпионажа нарастает, предостерегает Оттава, не упоминая вслух о Китае [Електронний ресурс]. – Режим доступу: http://www.newsab.ru/incidents/id_72153/

212. Уэбстер Ф. Теории информационного общества. Пер. с англ. / Ф. Уэбстер. – М.: Аспект Пресс, 2004. – 400 с.

213. Уэст Д. Краткая история политической рекламы на телевидении / Д. Уэст // Политическое консультирование / под ред. Д. Перлматтера. – М.: Инфра М., 2002. – С.15-27.

214. Федорова С.А. Компрометирующие материалы как средство политической борьбы : автореф. дис. канд. полит. наук : спец. 23.00.02 – политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии (по политическим наукам) / С.А. Федорова. – Саратов, 2009. – 22 с.

215. Фимин А. Ю. Технология виртуальной реальности в современной рекламе / А. Ю. Фимин // Философское осмысление социально-экономических проблем: межвуз. сб. науч. тр. / ВолгГТУ. – Волгоград, 2005. – Вып. 9. – С. 82-85.

216. Хабермас Ю. Моральное сознание и коммуникативное действие / Ю. Хабермас. – СПб.: Наука, 2000. – 377 с.

217. Хлобустов О. Проблемы информационно-пропагандистского противодействия терроризму / О. Хлобустов // Власть. – 2006. – С.44-49.

218. Хлыстунов С.Ю. Средства массовой информации Российского общества в условиях идеологической глобализации: социологический подход : автореф. дис. на соискание научной степени докт. соц. наук : спец. 23.00.02 «Политические институты, этнополитическая конфликтология,

национальные и политические процессы и технологии (социологические науки)» / С.Ю. Хлыстунов. – Саратов, 2007. – 43 с.

219. Чергинец Н.И. Государственная политика в области информационной безопасности: состояние и перспективы развития / Н.И. Чергинец // Национальная безопасность: управленческие и информационные технологи обеспечения. – Минск, 2000. – С.14.

220. Чичановский А.А. В тенетах свободы: Политологические проблемы взаимодействия властных структур, средств массовой информации и общества в новых геополитических условиях / А.А. Чичановский. – М.: Славянский диалог, 1995. – 303 с.

221. Чтобы попасть в Европу надо реформировать суды – еврокомиссар [Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua/rus/news/2011/06/9/6284429/

222. Чумакова А.А. Информационно-имиджевая политика страны в культурологическом освещении (на материале российской и зарубежной прессы) : автореф. дис… канд. культурологи : спец. 24.00.01 – Теория и история культуры / А.А. Чумакова. – М., 2007. – 26 с.

223. Чумиков А.Н. Политическое манипулирование / А.Н. Чумиков // Политическая энциклопедия: в 2 т. – М., 1999. – Т.1. – 723 с.

224. Цветков О.М. Политическое манипулирование : автореф. дис… канд. филос. наук : спец. 23.00.03 / О.М. Цветков. – М., 1996. – 26 с.

225. Цыганов В. Информационные войны в бизнесе и политике. Теория и методология / В. Цыганов, С. Бухарин. – М,: Академический Проект, 2007. – 336 с.

226. Цыганов В.В. Основы теории, методологии, методы и технологии информационных войн // ХУ Международная конференция «Проблемы управления безопасностью сложных систем» [Електронний ресурс]. – Режим доступу: http://www.ipu.ru/period/pu/s0801/pb108_mk.pdf.

227. Цыганков П.А. Международные процессы в условиях глобализации: проблема эффективной коммуникации / П.А. Цыганков // Вестник Московского университета. – Сер. 18: Социология и политология. – 1999. – № 4. – С. 56–65.

228. Цымбал В.И. О концепции информационной войны / В.И. Цымбал // Информационный сборник «Безопасность». – М., 1995.

229. Цыренжапов З.О. Информационно-коммуникативный потенциал имиджа Российского государства : автореф. дис… канд. полит. наук : спец. 10.01.10. - Журналистика (политические науки) / З.О. Цыренжапов. – М., 2008. – 24 с.

230. Шамин И.В. Технологии «прямых» и «непрямых» действий и их применение в современном международно-политическом процессе : автореф. дис… докт. полит. наук : спец. 23.00.02 – политические институты, процессы и технологии / И.В. Шамин. – Нижний Новгород, 2011. – 58 с.

231. Шампань П. Делать мнение: новая политическая игра / П. Шампань. – М.: Socio-Logos, 1997. – 317 с.

232. Шамсуев М.Х. Теоретические аспекты изучения информационной безопасности [Електронний ресурс]. – Режим доступу: http://www.teoria-practica.ru/index.php/2010-2/215-politologia/485-2010-07-02-12-21-16

233. Шариков П.А. Политика США в области информационной безопасности : автореф. дис… канд. полит. наук : спец. 23.00.04 – политические проблемы международных отношений и международного развития / П.А. Шариков. – М., 2009. – 38 с.

234. Шарков Ф.И. Аудитория и мониторинг СМИ / Ф.И. Шарков, В.И. Баранова // Социологические исследования. – 2005. - № 10. – С.106-111.

235. Шарков Ф.И. Основы теории коммуникации Ф.И. Шарков. – М.: Социальные отношения, 2002. – 245 с.

236. Шафрански Р. Теория информационного оружия [Електронний ресурс]. – Режим доступу: http://lib.hive.kiev.ua/SECURITY/kvn/shafran.txt

237. Швец Д.Ю. Информационная безопасность России в современных международных отношениях : автореф. дис... канд. полит. наук : спец. 23.00.02 / Д.Ю. Швец. – М., 2005. – 26 с.

238. Швец Д.А. Информационное управление как технология обеспечения информационной безопасности / Д.А. Швец // Сб. «Массовая коммуникация и массовое сознание», М., МГИМО, 2003. – С.43.

239. Шевченко Е.В. PR-технологии формирования международного имиджа страны (на примере Украины) / Е.В. Шевченко // PR-технологии в информационном обществе: Материалы Всероссийской научно-практической конференции. Санкт-Петербург, 4-5 ноября 2003 г. СПб.: Изд-во СПбГПУ, 2003. - 214 с.

240. Шерковин Ю.А. Психологические проблемы массовых информационных процессов / Ю.А. Шеркович. – М.: Мысль, 1973. – 213 с.

241. Шестопал Е.Б. Политическая психология / Е.Б. Шестопал. – М.: ИНФРА–М, 2002. – 446 с.

242. Шипова А.В. Манипулирование сознанием и его специфика в современном обществе : автореф. дис. канд. филос. наук : спец. 09.00.11 – социальная философия / А.В. Шипова. – Ставрополь, 2007. – 28 с.

243. Ширяев Б.А. Внешняя политика США. Принципы, механизмы, методы : Курс лекций / Б.А. Ширяев. – СПб.: Издательский дом Санкт-Петербургского университета, 2007. – 442 с.

244. Шкурлатов Р. Государство будет ввергнуто в хаос если его «нервные центры» подвергнутся кибератакам /Р.Шкурлатов // Основы безопасности жизнедеятельности.- 2005.- № 9.- С.22-27.

245. Шомова С.А. Политическая коммуникация: социокультурные тенденции и механизмы С.А. Шомова. – М.: Издательство ИНИОН, 2004. – 246 с.

246. Шустеров Д.М. Средства массовой информации в региональном социально-политическом процессе современной России : автореф. дис… канд. полит. наук : спец. : 23.00.02 – политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии / Д.М. Шустеров. – Орел, 2009. –

247. Щербаков В. Киберспецназ атакует с территории Поднебесной [Електронний ресурс]. – Режим доступу: http://nvo.ng.ru/spforces/2008-07-04/12_china.html.

248. Эксперт: Запад обеспокоен возвратом Украины в советское прошлое [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/opinion/2010/08/20/709573.html

249. Эксперты НАТО: кибератака должна приравниваться к вооруженному нападению [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/newstext.php?news_id=67643

250. Южная Корея обвинила китайских хакеров в кибершпионаже [Електронний ресурс]. – Режим доступу: http://techfeed.ru/2010/10/yuzhnaya-koreya-obvinila-kitajskix-xakerov-v-kibershpionazhe/ë

251. Юдаев В.В. Информационные технологии в политическом процессе: теоретико-прикладной анализ : автореф. дис. на соискание науч. степени канд. полит. наук наук : спец. 23.00.02 «Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии» / В.В. Юдаев. - М., 2005. – 26 с.

252. Янукович накричав на Азарова, бо Україну в світі вважать Тьмутараканню [Електронний ресурс]. – Режим доступу: http://lypa.te.ua/archives/11517

253. Anholt–GMI. Nation Brands Index [Електронний ресурс]. – Режим доступу: www.anholt.com

254. Arquilla J. Networks, Netwar, and Information-Age Terrorism // The Changing Role of Information in Warfare. – Rand Corporation. – 1999. – P.88–89., Arquilla J., Ronfeldt D. The Advent of Netwar // In Athena's Camp. – Rand Corporation . – 1997. – P.275-279.

255. Szafranski R. Neocortical Warfare? The Acme of Skill. – Military Review, 1994, Nov.

256. Davis N. An Information-Based Revolution in Military Affairs. - Strategic Review, 1996, vol.24, № 1.

257. Hovard M. (ed.) Restraints of War. Studies in the Limitations of Armed Conflict. Oxford, 1979, p.8.

258. Lasswell H. D. Propaganda Technique in the World War /H. Lasswell. - N.Y., 1927. - P. 220-221. Цит. по: DeFleur. - P. 163.

259. Libicki M. What is Information Warfare. – National Defense University. ACIS paper 3. – August 1995.

260. Laquer W. Postmodern Terrorism / W. Laquer // Foreign Affairs. – 1996. - № 75. – P.35-44.

261. Lippmann W. Public Opinion / W. Lippmann / - N.Y., 1934. – 392 p.

262. Luhmann N. Die Realitat der Massenmedien / N. Luhmann – Opladen: Westdeutscher Verlag, 1996. - 223 p.

263. Toffler A., Toffler H. The New Intagibles. – Arquilla J., Ronfeldt D. (eds.) In Athena’s Camp: Preparing for Conflict in the Information Age/. Santa Monica.

264. Winn Schwartau. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994. - P.13-34.