Вісник Львівського університету. Серія філос.-політолог. студії. 2014. Випуск 5

УДК: 316.77 : 355.43(477)

ФОРМУВАННЯ ДЕРЖАВНОЇ СТРАТЕГІЇ ІНФОРМАЦІЙНОЇ ВІЙНИ УКРАЇНИ

Анна Руднєва

Запорізький національний університет, кафедра політології
вул. Жуковського 66, м. Запоріжжя, Україна
e-mail: fisun2009@yandex.ru

Осмислено сутність формування стратегії державної інформаційної війни. Виокремлено рівні інформаційної політики в умовах розв'язання інформаційної війни. Сформовано принципи «інформаційної гігієни» для кожної людини. Визначено нагальність створення й окреслено коло завдань органу з питань ведення інформаційної війни України.

Ключові слова: інформаційна війна, інформаційна політика, інформаційна безпека, державна інформаційна стратегія, інформація.

Динамічна природа сучасної інформаційної цивілізації сприяє формуванню багатополюсного світу, який характеризується появою кількох центрів тяжіння й одночасним посиленням конфлікту інтересів. В умовах щільності світового життєвого та інформаційного простору підвищуються вимоги до мирного співіснування, ускладнюються процеси вирішення протиріч між глобальними акторами, що особливо відображається на геополітичних амбіціях й пов'язуються із поширенням феномену інформаційної війни. За таких умов актуалізується питання захисту від інформаційної агресії, необхідності пошуку ефективних механізмів геополітичного розвитку і мирного співіснування.

Питання інформаційної війни досліджують видатні українські вчені В. Ліпкан, О. Литвиненко, Г. Ложкін, Т. Ніколаєва, Ю. Ноєв, В. Остроухов, Г. Почепцов, М. Сенченко, М. Требін, В. Фомін та ін. Однак нагальною залишається проблема вироблення практичних рекомендацій із розроблення державної стратегії інформаційної війни Українською державою. Відповідно до проблемної ситуації ми маємо на меті проаналізувати державну стратегію оборонної та наступальної інформаційної війни України.

Стратегія інформаційної війни Української держави повинна містити оборонну і наступальну складові. Перша спрямована на фізичний та психологічний захист населення, військ, органів влади, інформаційної інфраструктури й інформаційно-політичного простору. Вона повинна охоплювати: організацію діяльності з формування системи оборони у випадку розв'язання іноземними державами інформаційної війни; протидію акціям і заходам інформаційно-політичної агресії, операціям інформаційно-психологічної війни; залучення ЗМІ та віртуальних соціальних спільнот до інформаційного протиборства. У зв'язку з розв'язанням проти Української держави

відкритої інформаційної агресії та війни, котрі ми маємо у відносинах із Російською Федерацією з кінця 2013 р., актуалізуються оперативність і швидкість реагування на всілякі виклики та загрози. Дії держави у зазначених умовах можна розподілити на три рівні: перший, геополітичний, сприяє викриттю інформаційного агресора й обмеження інтенсивності та сили його нападу; другий, державний, містить захист цілісності й дієздатності системи управління, інформаційної інфраструктури, інформаційних ресурсів; третій, суспільний, спрямований на захист стабільності та безперервності розвитку суспільно-політичних відносин, свідомості громадян, цілісності кожного індивіда.

Інструменти інформаційної політики, пов'язані з першим рівнем, містять:

– залучення світової спільноти і світової суспільної думки з метою викриття інформаційного агресора, його деструктивних впливів;

– інформування світової громади про напади й об'єктивний стан речей у власній країні, що є ефективним механізмом збереження власного статус-кво, цілісності іміджу та бренду країни, котрі агресивна сторона має на меті дискредитувати; крім того, названий механізм знизить ризик успішної реалізації протиборчою стороною дезінформаційних приводів, які виправдовують ті чи інші її експансіоністські наміри і дії; яскравий приклад – провокації РФ стосовно вбивств і дискримінації російських громадян «бандерівцями» на Кримському півострові в лютому – березні 2014 р. з використанням відверто сфабрикованих відеороликів та репортажів;

– посилення контрпропагандистської та розвідувальної діяльності; комплексний стратегічний аналіз світового й національного просторів, формування оперативних центрів інформації;

– заборона на власній території ЗМІ, що належать інформаційному агресорові, з метою уникнення пропаганди і деструктивного впливу на громадян;

– збереження статусу стабільності, підтримання позитивного конструктивного іміджу України й образу могутньої держави;

– взаємодія й обмін досвідом із міжнародними організаціями протидії кібератакам та інформаційним нападам на державні інформаційні ресурси.

Другий рівень поєднує і систему державного управління, і національну інформаційну інфраструктуру, від ефективності функціонування котрих залежить загальний стан обороноздатності країни, її здатності протистояти агресивним нападам і зберігати інформаційну, територіальну, економічну, соціально-політичну, культурну цілісність. До основних методів інформаційної політики на зазначеному рівні ми зараховуємо:

– створення єдиного координаційного органу, центру прийняття рішень і керування державною інформаційною політикою та безпекою, однієї ефективної системи, міцної вертикалі органів та інститутів;

– підготовка фахівців з питань ведення інформаційної війни та реалізації державної інформаційної стратегії – політологів, аналітиків і прогнозистів, спеціалістів з інформаційних технологій, кібербезпеки, інформаційно-психологічної безпеки,

управління ризиками, практичних психологів з питань допомоги жертвам інформаційної агресії та ін.;

– навчання держслужбовців принципам, методам захисту інформації, так званої інформаційної грамотності й основам інформаційної безпеки, психологічний захист свідомості та зміцнення «інформаційного імунітету»;

– формування спеціалізованого органу кібербезпеки і протидії хакерських атак із залученням ІТ-спеціалістів. В даному випадку можемо говорити про створення спеціалізованих інформаційних військ;

– контролювання внутрішнього і постійний аналіз зовнішніх інформаційних полів. Вдосконалення інституційної складової моніторингу інформації та законодавче закріплення відповідної діяльності, відповідальності за протиправні дії в цій сфері;

– вироблення єдиного інформаційного центру опрацювання новин за певний період з метою виявлення джерел дезінформації; розвиток ринку новин і громадських медіа; посилення новинних ресурсів політичних організацій;

– ефективне використання державних інформаційних ресурсів і гарантування безпеки функціонування національної інформаційної інфраструктури через залучення фахових кадрів, інноваційних технологій з одержання, поширення та використання інформації; шифрування інформації та посилений контроль до її доступу; надійне технічне і програмне забезпечення, максимально національного виробника, а також антивірусна підтримка;

– заборона володіння національними медіа закордонним власникам. Посилення юридичної відповідальності ЗМІ за поширення деструктивної інформації, агресивних закликів, стану ворожнечі, нетерпимості та ін.;

– інформаційно-психологічний захист військового командування й армії від деморалізуючої пропаганди; навчання методам інформаційного захисту, принципам активної та оборонної інформаційної війни, особливостям реалізації інформаційної зброї.

Для третього рівня – суспільного – вагома діяльність, спрямована на підтримку стабільності соціально-політичного розвитку, консолідації та психологічної безпеки індивідуальної, масової свідомості. Тому серед принципів інформаційної політики ми вирізняємо:

– забезпечення громадян суспільно значущою інформацією, повідомлення громадськості про інформаційну небезпеку та зброю інформаційної війни і технічного і психологічного характеру;

– розвиток незалежних, соціально орієнтованих ЗМІ. Трансляція позитивно орієнтуючих програм, національного здобутку, героїчного минулого, перспектив і переваг розвитку країни з метою зміцнення національної гідності, патріотизму, пошани до власної Вітчизни;

– залучення віртуальних соціальних спільнот і ЗМІ до захисту національного інформаційного простору, так званої віртуальної колективної системи безпеки, зниження загального стану соціальної напруженості;

– захист духовного потенціалу суспільства від нав'язування ворожих цінностей, посилений захист свідомості дітей і молоді;

– вироблення консолідуючої символіки та єдиної консолідуючої ідеології, ґрунтованої на принципах поваги, єдності, компромісу, солідарності; створення соціальних роликів, реклами, мемів, суть котрих повинна бути спрямована на психологічний захист громадян;

– виховання політичної нації зі сформованою громадянською політичною культурою.

Хоча зауважимо: кожна людина є захисником власної свідомості від негативних наслідків інформаційної війни. Для цього сформуємо рекомендації стосовно здатності самостійно протистояти або хоча б зменшувати негативні наслідки інформаційних впливів. Безсумнівно, для інформаційної агресії характерним є виникнення сильної емоційної напруженості, збудженості, тому від людини вимагається докладання значних зусиль, щоб не піддаватися емоційним викликам та спрямовувати дії в раціональному напрямі. Серед основних принципів дій «інформаційної гігієни» ми вирізняємо:

1. Альтернативність джерел отримання інформації – намагатися отримувати її в об'єктивнішому стані, для чого потрібно звертатись до різних медіа, порівнювати характер отриманої інформації.

2. Авторитетність і надійність медіа – намагатися обирати найоб'єктивніші й достовірні ЗМІ, проте все одно перевіряти подані факти й висвітлювані події.

3. Використання офіційних документів, законів та нормативних актів.

4. Виокремлювати й уникати «фейкових» джерел інформації, які неприкрито поширюють деструктивну інформацію. Зазвичай вони використовують емоційно-забарвлені заголовки (наприклад, «шок», «ти не повіриш»), нерідко сфабриковані світлини, маскуються під відомі аналітичні чи новинні медіа з метою привернути максимальну увагу. Це стосується також фото- і відео- сенсацій, котрі можуть не мати нічного спільного зі зображеними подіями. Прикладів достатньо, наприклад, коли російські медіа в репортажі про затори на українсько-російському кордоні внаслідок масової втечі українських громадян у Росію, транслювали, насправді, кордон «Шегині» у Львівській області.

5. Недовіра до чуток – перевіряти поширену інформацію, не піддаватися емоційному оцінюванню інформації. Стати «самому собі журналістом», розвивати критичне мислення і рефлексію.

6. Вирізнення фактів від емоційних оцінок журналістів, політиків, лідерів думок – уникати нав'язування певних емоцій і поглядів. Кожна ситуація може висвітлюватись по-різному. Наприклад, факт жорстокого знущання силовиків «Беркута» над мітингуючим чоловіком» [2] та факт урятування «Беркутом» майдану того ж чоловіка від самоспалення» [1] – дві різні думки про одну й ту ж саму подію.

7. Непіддавання суспільній паніці, ескалації емоційного напруження. Зберігати емоційну стабільність до новин сенсаційного характеру, так званих інформаційних блискавок, котрі мають гіперболізований характер і спрямовані переважно на спричинення емоцій.

8. Власне підсумовування явищ, ситуацій, рішень – аналітично і критично мислити, уникаючи побутово-забарвлених висновків.

9. Відлучення від інформаційних потоків – давати мозку відпочити аби уникнути забруднення інформаційним шумом, поновлювати здатність раціонально й аналітично мислити; зосередитись на позитивних враженнях, емоціях, фізичному та духовному відпочинку. Позитивно мислити, що допомагає уникнути панічного стану, страху, невизначеності, розчарування та інших негативних соціально-психологічних наслідків.

На окрему увагу заслуговують соціальні мережі, які, починаючи з «арабської весни», стають все могутнішим інструментом інформаційної війни та полем інформаційних баталій. У цьому сенсі, важлива підтримка певного балансу між виявами свободи слова, що соціальні мережі максимально репрезентують, і різними провокаціями, дестабілізацією соціально-політичного порядку, сепаратизму. Ввести державну цензуру в цій сфері – фактично, порушити цілісність принципу свободи слова і думок. Залишити все на саморегулювання – виникає серйозна погроза суспільної нестабільності в реальному світі й соціально-психологічному здоров'ю громадян, особливо молоді.

Вважаємо за необхідне сформувати певні рекомендації для кожної людини, так звані принципи інформаційної гігієни стосовно поведінки у соціальних мережах, одного з головних просторів інформаційної війни. По-перше, треба зрозуміти їхню сутність, як засобу комунікацій, а не як авторитетного джерела інформації, що дає змогу кожному учасникові висловлювати свої думки незалежно від адекватності безвідповідальності за наслідки. По-друге, небажано поширювати інформацію (репост) без її осмислення та перевірки на достовірність. Наскільки ця інформація вагома? Яку користь суспільству чи конкретній людині вона принесе? Чи можна довіряти такій інформації? Обов'язково необхідно дати на ці питання. По-третє, не варто довіряти фактам, у котрих порушено причинно-наслідкові зв'язки. По-четверте, не можна залишати детальну інформацію про факти свого життя. По-п'яте, батьки повинні навчити дітей правилам безпеки користування ресурсом, повідомляти про небезпеки і ризики, які їх можуть очікувати у соціальних мережах.

Наступальна складова інформаційної війни спрямована на розроблення превентивних заходів захисту від небезпеки негативних наслідків інформаційних впливів і дієвого механізму ведення власної інформаційної війни, що стає сьогодні природним засобом комунікації на геополітичному рівні. Головна мета – формування єдиної системи інформаційної політики на всіх рівнях: від національного до місцевого. Це передбачає, по-перше, формування єдиної системи законодавства, механізму створення, опрацювання та збереження інформаційних ресурсів; по-друге – створення державного органу, відповідального за ведення інформаційної війни на всіх етапах.

Інформаційна війна, в загальному має дві глобальні складові – матеріальну, яка містить технічні засоби, в тому числі реальну зброю, та психологічну – свідомість і підсвідомість людини та суспільства, зокрема військової сили, армії. У стратегіях США та Китаю простежуємо багато інструментів впливу на духовно-психологічний стан армії супротивника, в основу чого покладено пропагандистські дії. Деморалізація людського

складової може завдавати більшої шкоди, ніж важка зброя. У цьому ми неодноразово переконувались під час проведення більшості кампаній НАТО на чолі зі США. Хоча також акцентується й на інформаційно-психологічному захисті власних армій, піднятті духу патріотизму, відваги та мужності.

Отже, враховуючи усе зазначене, вважаємо за необхідне окреслити коло завдань Органу з питань ведення інформаційної війни України, який має стратегічний характер діяльності:

1. Створення єдиного центру, але розширеної спеціалізованої структури Органу, що має фахівців з питань ведення інформаційної війни; відповідних підрозділів – пропаганди і контрпропаганди, розвідки, планування, спеціалістів соціальних мереж і под.

2. Визначення і класифікації інформаційних погроз та їхніх проявів, моніторинг; Розроблення методичних рекомендацій з виявлення ризиків і відстеження розвитку загрозливих ситуацій з метою підвищення ефективності роботи структур, котрі займаються гарантуванням інформаційної безпеки.

3. Здійснення інноваційної діяльності, пов'язаної з дослідженням інформаційно-психологічної зброї. Захист складу військ та підвищення його моральної стійкості, здатності протистояти деструктивним інформаційно-психологічним впливам; інновація методів інформаційного управління.

4. Захист військ і суспільства від деморалізуючої пропаганди іноземних суб'єктів; контрпропагандистська діяльність; інформування про особливості інформаційної війни, методів та засобів інформаційної зброї; освоєння тактик протидії зазначеним явищам і використання їх у реалізації висунутого завдання.

5. Організовування розвідувальної діяльності, використання тактик китайської інформаційної війни, пов'язаних із проникненням в органи влади і впливові структури інших країн з метою просування інтересів Української держави.

6. Діяльність представництва національних інтересів України в інформаційному, віртуальному просторі; поширення позитивної інформації про державу, створення сприятливого підґрунтя для співпраці з іншими країнами.

7. Формування і захист сприятливого образу нашої країни за допомогою інформаційних технологій, що охоплює, з одного боку, рекламну, просвітницьку, пропагандистську діяльність, створення та підтримку національного бренду, з іншого – моніторинг міжнародного інформаційного простору відносно формування іміджу країни іноземними ЗМІ, нейтралізацію інформаційних викликів, загроз і диверсій, іміджмейкерство.

8. Участь у світових інформаційних процесах, формування інформаційної стратегії у воєнній і соціальній сферах, загальнодержавної системи інформаційного протиборства.

9. Стимулювання наукових досліджень і розроблень у сфері оптимізації ефективності державної інформаційної політики та безпеки.

10. Міжнародне співробітництво у сфері протидії розвитку кіберзлочинності, створення колективної системи інформаційної безпеки; пошук шляхів інформаційно-технічного й інформаційно-психологічного захисту держави та суспільства.

На нашу думку, чільне місце в діяльності державного органу з питань ведення інформаційної війни України має посідати прогностична діяльність як передбачення і прогнозування розвитку подій на глобальному рівні, їхнього впливу на стан нашої країни. Ми вважаємо, що у наступальній інформаційній війні необхідно дотримуватися поміркованого характеру дій і виваженої стратегії. Антиподом цього є приклад російської інформаційної війни проти України, свідками якої ми стали. Відверта брехня та гіперболізований характер декотрих інформаційних атак спричинили зворотній ефект – вразили саму країну, знизили світові рейтинги, призвели до резонансу світової спільноти. Можемо казати про розумну інформаційну війну, яка повинна бути непомітною.

У цьому ж контексті постає питання і про ефективність інформаційної політики у сфері ведення інформаційної війни. Визначити ефективність достатньо важко, але можемо вивести певні її критерії:

– відсоток зростання/падіння іміджу країни на світовому рівні за показниками привабливості загального бренду, її торговельної та партнерської привабливості, військової могутності;

– відсоток співвідношення реалізації запланованих національних інтересів і цілей до відсотка нереалізованих;

– загальний відсоток частоти (зростання/падіння) інформаційних провокацій, нападів, атак порівняно з певним підзвітним періодом (місяць, рік);

– відсоток співвідношення відсічених/пропущених інформаційних провокацій, нападів, атак за певний підзвітний період (місяць, півроку, рік);

– ступінь суспільного резонансу, тобто здатності зовнішніх впливів розбалансувати суспільство і призвести до суспільних хвилювань (за шкалою від 1 до 5);

– ступінь захищеності інформаційних ресурсів органів державної влади від зовнішніх нападів (за шкалою від 1 до 5) – відсоток відсічених/ефективно реалізованих інформаційних операцій;

– відсоток зростання/зменшення ризиків у інформаційно-політичному просторі держави та в її геополітичному положенні;

– відсоток успішно реалізованих інформаційних кампаній та операцій.

Отже, формула ефективності державної інформаційної війни у загальному сенсі дорівнює % росту іміджу + % реалізації національного інтересу + % частоти інформаційних нападів + % інформаційних провокацій + ступінь суспільного резонансу + ступінь захищеності інформаційних ресурсів + % ризиків у інформаційно-політичному просторі + % успішності інформаційних кампаній. Окрім того, показниками ефективності є безперервність процесу розвитку соціально-політичних процесів у суспільстві та їхня стійкість незалежно від зовнішніх деструктивних впливів; відповідність системи соціально-політичних відносин держави до розвитку інформаційної цивілізації, набуття нових якостей, демократизація суспільних процесів.

У підсумку, зазначимо, що ведення інформаційної війни в сучасному світі – природний закономірний процес комунікації, запорука геополітичної безпеки держави, а стосовно України – механізм національного захисту в умовах ескалації інформаційної експансії лідерів інформаційної цивілізації. Основною аксіомою XXI ст. стала давно відома істина: «Володієш інформацією – володієш світом».

Список використаної літератури

1. Беркут спас майдан от самосожжения [Электронный ресурс] // Укр. новости. – Режим доступа : http://ukrnovosti.net/?p=1683
2. В интернете появилось видео жестоких издевательств «Беркута» над митингующим [Электронный ресурс] // Сегодня. – Режим доступа : http://www.segodnya.ua/ukraine/v-internete-poyavilos-video-zhestokih-izdevatelstv-berkuta-nad-mitinguyushchim-490833.html
3. *Литвиненко О. В.* Інформаційні впливи та операції: теоретико-аналіт. нариси / О. В. Литвиненко. – К. : НІСД, 2003. – 240 с.
4. *Ліпкан В. А.* Інформаційна безпека України в умовах євроінтеграції : навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – К. : КНТ, 2006. – 280 с.
5. *Манойло А. В.* Государственная информационная политика в особых условиях / А. В. Манойло. – М. : МИФИ, 2003. – 388 с.

Стаття надійшла до редколегії 28.05.2014
Прийнята до друку 20.06.2014

Вісник Львівського університету. Серія філос.-політолог. студії. 2014. Випуск 5

FORMING OF STATE STRATEGY OF INFORMATION WARFARE OF UKRAINE

Anna Rudnieva

Zaporizhzhya national university, Department of political science
Zhukovsky street 66, Zaporizhzhya,Ukraine
e-mail: fisun2009@yandex.ru

Essence of forming of strategy of state information war is intelligent. The levels of informative politics are distinguished in the conditions of offensive of information warfare. Principles of «informative hygiene» are formed for everybody. Urgency of creation is certain and the circle of tasks of Organ is outlined on questions of prosecution of informative war of Ukraine.

Key words: information warfare, informative politics, informative safety, state informative strategy, information.

ФОРМИРОВАНИЕ ГОСУДАРСТВЕННОЙ СТРАТЕГИИ ИНФОРМАЦИОННОЙ ВОЙНЫ УКРАИНЫ

Анна Руднева

Запорожский национальный университет, кафедра политологии
ул. Жуковского 66, г. Запорожье, Украина
e-mail: fisun2009@yandex.ru

Осмыслено сущность формирования стратегии государственной информационной войны. Выделены уровни информационной политики в условиях наступления информационной войны. Сформированы принципы «информационной гигиены» для каждого человека. Определена неотложность создания и очерчен круг заданий органа по вопросам ведения информационной войны Украины.

Ключевые слова: информационная война, информационная политика, информационная безопасность, государственная информационная стратегия, информация.