ФП 2009-2
ISSN 1995-6134

УДК 35.078.3
В.М. АБАКУМОВ, Запорізький національний університет

СУБ'ЄКТИ ІНФОРМАЦІЙНИХ ВІЙН: ПОНЯТТЯ ТА ВИДИ

Ключові слова: *інформаційні війни, суб'єкти*

Інформаційна зброя, що постає основним засобом ведення інформаційної війни, не може використовуватися самостійно, обов'язково існують суб'єкти, що прагнуть використовувати в корисних та злочинних цілях позитивні властивості інформації та інформаційних технологій, які створювалися на користь людині, суспільству та державі. На нашу думку, розуміння шкідливості та деструктивної сили інформаційних війн вимагає більш ґрунтовного дослідження цього феномену з правової точки зору, у першу чергу це стосується діяльності тих суб'єктів, що своїми діями створюють суттєву загрозу інформаційній безпеці держави, суспільства, населення, окремих груп населення та, власне, людини – суб'єктів інформаційних війн.

Новизна роботи полягає у тому, що дана робота постає одним із перших комплексних досліджень такого невід'ємного елементу інформаційної війни як суб'єкти інформаційної війни, у роботі надано авторське визначення поняття «суб'єкти інформаційної війни», визначено структуру та ознаки цих суб'єктів, проаналізовано особливості використання ними інформаційної зброї як основного засобу ведення інформаційних війн, запропоновано окремі заходи, впровадження яких сприятиме належному забезпеченню інформаційної безпеки держави на належному рівні.

Перш ніж проаналізувати структуру суб'єктів інформаційних війн, визначити ознаки цих суб'єктів, їх роль у глобальних інформаційних війнах та особливості використання ними інформаційної зброї, вважаємо за доцільне визначитися із тим, що ж власне будемо розуміти під суб'єктами інформаційних війн. У результаті вивчення наукових праць, присвячених дослідженню питань ведення інформаційних війн [1-9], автор дійшов висновку про відсутність будь-якої узгодженої позиції щодо існування визначення поняття «суб'єкти інформаційних війн». На нашу думку, така ситуація зумовлена тим фактом, що формування понятійного апарату у сфері інформаційних відносин ще остаточно не завершено. Звісно, така ситуація призводить як до виникнення суперечок серед науковців, так і до виникнення певних непорозумінь на законодавчому рівні, оскільки відсутність закріплення у національному законодавстві ключових моментів, що загрожують інформаційній безпеці держави (таких як інформаційні війни, інформаційна зброя, суб'єкти інформаційних війн), призводить до неможливості вироблення чіткої державної стратегії боротьби з інформаційними війнами, розробки ефективного механізму впровадження організаційно-правових заходів, спрямованих на протидію інформаційним війнам, неналежному використанню інформаційної зброї різними суб'єктами.

У роботі під інформаційною війною розуміється сукупність методів та способів цілеспрямованого впливу суб'єктів-агресорів в умовах інформаційної відкритості на соціальні відносини (відносини людей між собою, відносини в суспільстві та державі), інформаційні ресурси, інформаційно-аналітичні та інформаційно-технічні системи, системи формування масової свідомості та психіки окремої людини, з використанням усіх властивостей інформації, інформаційних ресурсів та новітніх інформаційно-телекомунікаційних технологій з метою штучного створення факторів гальмування розвитку людини, суспільства та держави, встановлення контролю над інформаційними ресурсами потенційного супротивника задля отримання переваг у пріоритетних сферах суспільного життя.

Таким чином, виходячи із наданого визначення поняття інформаційної війни, під суб'єктами інформаційної війни будемо ро-

ISSN 1995-6134

зуміти людей, окремі групи людей, об'єднані спільними інтересами або іншими ознаками (національністю, мовою, професією, територіальним розташуванням тощо), держави, групи держав, міжнародні організації, що мають суттєві суперечки з іншими людьми, групами людей, державами, групами держав або міжнародними організаціями, які переходять до фази конкурентної боротьби з використанням усіх властивостей інформації, інформаційних ресурсів та новітніх інформаційно-телекомунікаційних технологій (інформаційної зброї).

Хотілося б акцентувати увагу, що суб'єктам інформаційної війни притаманна низка ознак, що істотно відрізняють їх від інших суб'єктів. Так, зокрема, В.К. Бутранець [8] до таких ознак відносить:

- розробку інформаційної зброї, засобів її доставки, маскування або володіння інформаційною зброєю;
- наявність у складі суб'єкта спеціальних сил або структур, що функціонально уповноважені на ведення інформаційної війни;
- наявність у суб'єкта власних інтересів в інформаційній сфері та інших сферах життєдіяльності;
- контроль суб'єктом тієї частини інформаційного простору, в межах якої він наділений першочерговим правом встановлювати норми регулювання відносин;
- існування в офіційній ідеології положень, що дозволяють суб'єкту прямо чи опосередковано брати участь в інформаційній війні.

Підтримуючи загалом наведений перелік ознак суб'єктів інформаційної війни, хотілося би додати ще декілька, на нашу думку, суттєвих ознак зазначених суб'єктів, а саме:

- комплексний характер засобів, методів та стратегій ведення інформаційної війни, у тому числі розробка декількох варіантів форм інформаційних нападів, що не піддаються прогнозуванню;
- наявність ефективної системи захисту від інформаційної агресії з урахуванням усіх існуючих варіантів нападу від різних суб'єктів;
- наявність висококваліфікованих кадрів, найсучаснішої техніки, необмежених матеріальних можливостей (звісно ця ознака не є необхідною, але за наявності значної кількості матеріальних можливостей безпосередньо залежить наявність висококваліфікованих фахівців та найсучаснішої техніки, що, у свою чергу, постає одним із необхідних факторів успіху в інформаційній війні).

До числі суб'єктів інформаційних війн, що ведуться по всьому світу, відносяться:

- держави, їх союзи та коаліції;
- міжнародній організації;
- недержавні незаконні (у тому числі незаконні міжнародні) збройні формування та організації терористичної, екстремістської, радикальної політичної, радикальної релігійної спрямованості;
- транснаціональні корпорації;
- віртуальні соціальні спільноти;
- медіа-корпорації;
- віртуальні коаліції [1, с.281].

У роботі вважалося за доцільне коротко зупинитися на аналізі кожного суб'єкта інформаційних війн, оскільки такий аналіз постає вельми актуальним у зв'язку із необхідністю вироблення виваженої як державної, так і міжнародної стратегії боротьби з інформаційними війнами, розробки на державному та міжнародному рівнях ефективного механізму впровадження організаційно-правових заходів, спрямованих на протидію інформаційним війнам, неналежному використанню інформаційної зброї різними суб'єктами, максимального наближення діяльності суб'єктів інформаційних війн до меж правового поля з метою нанесення мінімальної шкоди діяльності міжнародних і державних інституцій, належному функціонуванню усієї світової спільноти, держави, суспільства, груп населення та окремих індивідуумів.

Так, держави, їх союзи та коаліції, як одні із найкрупніших суб'єктів інформаційних війн, характеризуються наявністю стабільних інтересів в інформаційному просторі. З метою постійного підтримання власних інтересів в інформаційній сфері, недопущення виникнення для них суттєвої загрози або бо-

ISSN 1995-6134

ротьби з недоторканість цих інтересів держави, їх союзи та коаліції розробляють та реалізовують низку заходів, серед яких першочергове місце належить:

- формування власного інформаційного простору (державного, союзного або коаліційного), що інтегровано до глобального інформаційного простору;
- контроль за належним функціонуванням інформаційного простору;
- розробка відповідної нормативно-правової, концептуальної, ідеологічної бази, що регламентує випадки участі в інформаційній війні, визначає основні принципи та форми участі в інформаційній війні даного суб'єкта;
- створення спеціальних структурних підрозділів (як у складі силових структур, так і у складі цивільних державних установ), основним призначенням яких постає ведення інформаційної війни;
- розробка різноманітних засобів ведення інформаційної війни (інформаційної зброї) або, у разі неможливості вироблення інформаційної зброї власними силами, її придбання (легальним або нелегальним шляхом) за кордоном.

Хотілося б звернути увагу на той факт, що ведення інформаційної війни між державами їх союзами та коаліціями постає дуже небезпечною справою, оскільки під час цієї війни суттєво страждає економіка країн-учасниць, їх політичне, культурне та соціальне життя, посилюються глобальні процеси конфліктів інформаційного характеру, що, у свою чергу, створює загрозу не лише інформаційній безпеці країн-учасниць, а й національній безпеці. Вважаємо, що інформаційній війни між державами, їх союзами та коаліціями можуть вестися тільки у виняткових випадках, коли одна сторона завдає або може завдати значну шкоду іншій стороні, що значно перевищує ту шкоду, яка буде нанесена відносинам в усіх пріоритетних сферах життя під час ведення інформаційної війни.

Міжнародні організації також мають власні стабільні інтереси в інформаційному просторі, частково контролюють інформаційні простори держав-учасниць конкретних міжнародних організацій та беруть активну участь у формуванні глобального світового інформаційного простору, з метою чого здійснюють цілу низку організаційно-правових заходів, а саме:

- за допомогою відповідного ресурсного потенціалу держав-учасниць конкретної міжнародної організації ведуть інформаційні війни;
- у разі необхідності забезпечують створення та функціонування власних структур, основним призначенням яких постає ведення інформаційної війни;
- розроблюють відповідну нормативно-правову, концептуальну, ідеологічну базу, що регламентує випадки участі в інформаційній війні, визначає основні принципи та форми участі в інформаційній війні міжнародної організації;
- створюють шляхом ретельного підбору у країнах-членах конкретної міжнародної організації власний науково-технічний потенціал;
- розроблюють різноманітні засоби ведення інформаційної війни (інформаційної зброї), використовуючи потенціал держав, що інтегровані до цієї міжнародної організації, або, у разі неможливості вироблення інформаційної зброї власними силами чи у разі гострої необхідності, придбає її (легальним або нелегальним шляхом) у третіх осіб тощо.

Зважаючи на значний (в окремих випадках вирішальний) вплив міжнародних організацій на процес прийняття рішень в державах-членах відповідних міжнародних організацій, а також і по всьому світу (особливо якщо мова йде про крупну міжнародну організацію, наприклад, Європейський Союз, Рада Європи, НАТО, Співдружність Незалежних Держав та ін.), хотілося б акцентувати увагу на подвійній значущості й небезпеці ведення міжнародними організаціями інформаційних війн (у порівнянні з державами, їх союзами та коаліціями) та необхідності вироблення виваженої міжнародної інформаційної політики в цьому напрямку.

Недержавні незаконні (у тому числі незаконні міжнародні) збройні формування та

ISSN 1995-6134

організації терористичної, екстремістської, радикальної політичної, радикальної релігійної спрямованості, ведення інформаційної війни якими постає однією із основних складових їх діяльності, у напрямку підготовки до ведення інформаційної війни з різними суб'єктами здійснюють наступні заходи:

- створюють власний (частіше за все закритий) сегмент інформаційного простору, що прагне до захоплення чи контролю, руйнації та заміни на власний сегментів національного та/або глобального інформаційного простору;

- створюють в рамках власних або союзних структур сили, до функцій та звань яких відноситься ведення інформаційної війни;

- створюють та використовують власний науково-технічний потенціал або використовують науково-технічний потенціал союзників та держав, що їх підтримують, які пов'язані з діяльність цього суб'єкта інформаційних війн або (гласно або таємно) підтримують її, для розробки засобів ведення інформаційної війни – інформаційної зброї, засобів доставки та маскування інформаційної зброї чи придбають (частіше за все таємно) у разі необхідності зазначені засоби у союзників чи у третьої сторони;

- розроблюють відповідну нормативно-правову, концептуальну, ідеологічну базу, що обґрунтовує необхідність ведення інформаційної війни, визначає основні принципи та форми участі в інформаційній війні даного суб'єкта [1, с.283-284].

Так, у результаті аналізу наведених заходів, що розроблюють та впроваджують недержавні незаконні (у тому числі незаконні міжнародні) збройні формування та організації терористичної, екстремістської, радикальної політичної, радикальної релігійної спрямованості можна дійти висновку, про агресивність даної категорії суб'єктів інформаційних війн, про спрямованість їхньої діяльності за нанесення реальної суттєвої шкоди іншим суб'єктам, у тому числі і тим, що функціонують в інформаційній сфері.

Як зазначає А.В. Манойло [1, с.286], транснаціональні корпорації під час підготовки до ведення інформаційних війн або розробки заходів, спрямованих на нейтралізації загроз, що несуть у собі інформаційні війни, здійснюють практично ті ж самі заходи, що і міжнародні організації у цьому напрямку. Звісно власники інформаційно-комунікаційних мереж та розробники найсучасніших мережевих технологій серед інших представників транснаціональних корпорацій під час ведення інформаційних війн (в ролі будь-якої із сторін учасниць) відіграють особливу роль в зв'язку з тим, що за умов сучасного інформаційного суспільства умови диктує той, хто є власником інформаційних мереж, ресурсів та технологій. Звісно, транснаціональні корпорації також можуть підлягати впливу, особливо з боку органів державної влади тих країн, на території яких знаходяться їх офіційні представництва, але, у випадку, якщо така корпорація має значну чисельність філіалів на території декількох крупних держав та забезпечує переважну кількість населення та всі органи державної влади цих країн інформаційними ресурсами, то вплив з боку однієї країни на діяльність корпорації може привести до суттєвих збитків політичним та економічним інтересам інших країн, що, у свою чергу, призведе до суттєвих небажаних ускладнень зовнішньополітичних стосунків. Таким чином, можна дійти висновку, що транснаціональні корпорації, особливо ті, що спеціалізуються на виготовленні інформаційного продукту, дуже рідко можуть поставати стороною, у бік якої розпочато інформаційну війну. Частіше за все така корпорація сама буде агресором інформаційної війни.

Наступним суб'єктом інформаційної війни, діяльність якого щодо ведення інформаційної війни або протидії їй та усуненню негативних наслідків, схожа з діяльністю у цьому напрямку міжнародних організацій та транснаціональних корпорації є віртуальні соціальні спільноти. За умов сучасного інформаційного суспільства відбувається становлення нових соціальних формацій, що набувають принципово нових можливостей здійснення цілеспрямованого впливу на тради-

ISSN 1995-6134

ційні державні та суспільні структури. До числа таких нових формацій відносяться віртуальні соціальні спільноти, що являють собою соціальні системи, які включають до себе усю сукупність соціальних системи різних типів та їх окремих елементів, сегментів інформаційного простору, джерел інтелектуальних і матеріальних ресурсів, розподілених по земній кулі та об'єднаних у рамках досягнення загальної мети єдиною для усіх елементів віртуальної системи ідеологією [1, с.288].

Перш за хотілося б акцентувати увагу на тому, що віртуальна соціальна спільнота в якості реального об'єкту існує виключно в уявленні її членів (окремих громадян, груп людей, колективів та соціальних структур), а всі відносини, що пов'язують членів цієї спільноти здійснюються без встановлення обов'язкового особистого контакту (віртуально) і постають такою формою відносин, що притаманна виключно інформаційному суспільству. У разі, якщо така віртуальна спільнота буде позбавлена інформаційно-телекомунікаційних технологій, за допомогою яких налагоджується зв'язок між її членами, то така спільнота просто припинить своє існування. Звісно, існування таких віртуальних формацій не відноситься до традиційних уявлень ведення будь-якої діяльності та реалізації соціальної активності суспільства, але, заважаючи на стрімкий розвиток інформаційно-комунікаційних технологій не є чимось непередбачуваним та нереальним.

Як вже зазначалося у роботі, діяльність транснаціональних корпорації та віртуальних соціальних спільнот щодо ведення інформаційної війни або протидії їй та усуненню негативних наслідків багато в чому схожа між собою, але, хотілося б акцентувати увагу на такій відмінності як використання інформаційної зброї: транснаціональні корпорації під час ведення інформаційної війни частіше за все використовують власний інформаційний потенціал та інформаційні ресурси у той час, як віртуальні спільноти використовуються під час боротьби чужі матеріальні та інтелектуальні ресурси.

Усвідомлюючи усю небезпеку діяльності віртуальних соціальних спільнот як потенційних агресорів інформаційної війни, хотілося б висвітлити найбільш небезпечні моменти:

- висока мобільність сил та засобів таких соціальних систем до ведення та відбиття інформаційного нападу;
- висока здатність поповнювати сили, засоби, втрати інтелектуальних та матеріальних ресурсів, беручи їх безпосередньо із держав із розвиненою інформаційно-комунікаційної інфраструктурою, що до цього не брали участі в конкретній інформаційній війні;
- здатність у найкоротші строки повністю змінити свій вигляд та форму існування в інформаційному просторі, структуру та методи діяльності, що ускладнює вироблення дієвих санкцій;
- юридична складність встановити віртуальний зв'язок між елементами віртуальної спільноти, оскільки віртуальні відносини не залишають слідів, що створює певні труднощі для притягнення до відповідальності учасників та організаторів такої спільноти.

Засоби масової інформації та масової комунікації, як повноправні суб'єкти інформаційних війн, мають стабільні інтереси в інформаційному просторі, приймають активну участь у формуванні глобального інформаційного простору, здійснюють частковий контроль (намагаючись перейти до повного) за формуванням та функціонуванням національних сегментів інформаційного простору. Засоби масової інформації та масової комунікації прийнято розділяти на державні і недержавні.

Основним призначенням державних засобів масової інформації постає інформування населення про діяльність органів державної влади і місцевого самоврядування, тобто засоби масової інформації постають своєрідним посередником у встановленні суспільних зв'язків між населенням та органами влади і місцевого самоврядування. Під час налагодження такого виду зв'язку засоби масової інформації мають безпосередньо неупереджено висвітлювати ту інформацію, що

ISSN 1995-6134

вони отримують від органів державної влади та місцевого самоврядування, але, насправді, можна спостерігати зовсім іншу картину, коли засоби масової інформації свідомо змінюють, редагують отриману інформацію, підтасовують факти тощо. Усі вказані діяння відносяться до інформаційної війни, яку можуть вести засоби масової інформації як за власною ініціативою (неупереджене журналістське розслідування), так і за замовленням окремих (державних чи приватних) структур.

Говорячи про тісний зв'язкою засобів масової інформації та органів державної влади і місцевого самоврядування, хотілося б навести приклад такої взаємодії – електронне врядування. Зміст електронного врядування, зважаючи на прагнення України досягти європейських стандартів, одним із яких постає служіння держави, перш за все, народові та надання якісних адміністративних послуг, полягає у спрощеній процедурі спілкування населення з органами державної влади і місцевого самоврядування. Електронне врядування сприяє забезпеченню високого ступеню інформаційної прозорості діяльності органів державної влади і місцевого самоврядування (але, все ж таки, зважаючи на прагнення самого органу бути відкритим до громадськості та надання доступу до інформації).

Що ж стосується недержавних засобів масової інформації, що частіше за все належать крупним фінансово-промисловим структурам, які тісно взаємодіють з політичною елітою (або знаходяться у її складі), то слід підкреслити, що засоби масової інформації ведуть власну політику здійснення впливу на індивідуальну та масову свідомість суспільства в політичних та економічних інтересах їх власників. Таким чином, можна дійти висновку, що за таких умов діяльності недержавних засобів масової інформації їх діяльність не може поставати незалежною й об'єктивною.

Загальновідомим постає твердження про те, що засоби масової інформації з четвертою владою в країні (зважаючи на прийнятий розподіл влади на три гілки – законодавча, виконавча і судова). На нашу думку, така теза виникла у зв'язку із очевидним прагненням засобів масової інформації бути на одному рівні з органами державної влади і місцевого самоврядування, здійснювати безпосередній контроль за потоками інформації, що стосується діяльності органів державної влади і місцевого самоврядування, та здійснювати вплив на населення в результаті перекручення отриманої інформації. Вважаємо, що саме завдяки добре налагодженому електронному врядуванню буде можливо уникнути свідомого викривлення вихідної інформації у відповідності до політики, якої притримується конкретний засіб масової інформації або його власник.

Таким чином, хотілося б наголосити, що засоби масової інформації, за умов сучасного інформаційного суспільства, мають значні можливості з маніпулювання інформацією про діяльність органів державної влади і місцевого самоврядування, що робить їх одним із найнебезпечніших суб'єктів ведення інформаційної війни, але за умов існування електронного урядування можна значно зменшити вплив засобів масової інформації на свідомість громадян. Отже, вважаємо за доцільне запропонувати розробку та введення ефективної моделі електронного врядування, яка б враховувала особливості електронного врядування провідних країн світу, особливо країн-членів Європейського Союзу, зважаючи на прагнення України набути статусу повноправного члена цієї міжнародної організації.

Останній суб'єкт інформаційних війн – віртуальні коаліції, що можуть включати до свого складу усіх суб'єктів інформаційних війн, що були проаналізовані вище.

Таким чином, у роботі було визначено та коротко проаналізовано суб'єкти інформаційних війн, що дозволяє дійти нам наступного висновку. Враховуючи найвищий ступінь небезпеки, що несуть своєю діяльністю суб'єкти інформаційних війн усім державам (у вигляді їх органів державної влади), міжнародним організаціям необхідно виробити відповідну нормативно-правову базу з урахуванням усіх можливостей сучасних інформаційно-телекомунікаційних технологій; звернути першочергову увагу на вироблення та розви-

ISSN 1995-6134

ток інформаційно-телекомунікаційних технологій у сфері державного управління, підвищення здатності органів державної влади і місцевого самоврядування до використання ефективних технологій управління та організацію конструктивної взаємодії з громадськістю; звернути увагу на недостатній рівень підготовки кадрів в галузі створення та використання інформаційно-телекомунікаційних технологій та розробити низку заходів щодо підвищення зазначеного рівня.

ЛІТЕРАТУРА

1. Манойло А. В. Государственная информационная политика в особых условиях : монография / А. В. Манойло. – М. : МИФИ, 2003. – 388 с.
2. Кормич Б. А. Правові засади політики інформаційної безпеки України : монографія / Б. А. Кормич. – Одеса : Юридична література, 2003. – 472 с.
3. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – К. : КНТ, 2006. – 280 с.
4. Нижник Н. Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : навчальний посібник / Н. Р. Нижник, Г. П. Ситник, В. Т. Білоус ; за заг. ред. П. В. Мельника, Н.Р. Нижник. – Ірпінь, 2000. – 304 с.
5. Харченко Л. С. Інформаційна безпека України : глосарій / Л. С. Харченко, В. А. Ліпкан, О. В. Логінов ; за заг. ред. докт. юрид. наук, проф. Р. А. Калюжного. – К. : Текст, 2004. – 180 с.
6. Разуваев В. Э. Правовые средства противостояния информационным войнам : автореф. дис. на соискание науч. степ. канд. юрид. наук : спец. 12.00.14 / В. Э. Разуваев. – М., 2007. – 24 с.
7. Операции информационно-психологической войны : краткий энциклопедический словарь-справочник / под ред. А.И Петренко. – М. : Горячая линия-Телеком, 2005. – 495 с.
8. Бутранец В. К. Информационное противоборство: понятие, субъекты, цели / В. К. Бутранец. // Государственное управление и право. – 2008. – № 3 (28). – С. 104-109.
9. Почепцов Г. Г. Информационные войны / Г. Г. Почепцов. – К. : Ваклер, 2000. – 576 с.

Абакумов В. М. Суб'єкти інформаційних війн: поняття та види / В. М. Абакумов // Форум права. – 2009. – № 2. – С. 6–12 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2009-2/09avmptv.pdf

Визначаються поняття суб'єктів інформаційних війн, види та ознаки цих суб'єктів, особливості використання ними інформаційної зброї як основного засобу ведення інформаційних війн.

***

Абакумов В.М. Субъекты информационных войн: понятие и виды

Определяются понятие субъектов информационных войн, виды и признаки этих субъектов, особенности использования ими информационного оружия как основного средства ведения информационных войн.

***

Abakumov V.M. Subject of Information Wars: Concept and Kinds

The concept of subjects of information wars, kinds and attributes of these subjects, features of use by them of the information weapon as basic means of conducting information wars are defined.