Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Протидія інформаційним загрозам в умовах антитерористичної операції

Албул Сергій Володимирович
кандидат юридичних наук, доцент,
перший проректор Одеського державногоуніверситету внутрішніх справ

Україна сьогодні зіткнулася з невідомою досі агресією з боку РФ, яка отримала назву гібридно-месіанської війни [2, с. 16]. Ключову роль в цій війні Росія відводить телевізійним формам подачі інформації. Інформаційна кампанія є невід'ємною складовою агресії РФ в Україні. Тобто первинною є мета керівництва Росії ослабити Україну та залишити її у сфері свого безпосереднього впливу. Для цього використовується увесь наявний арсенал інструментів впливу: економічних, інформаційних, дипломатичних, військових, політичних тощо.

Інформаційні впливи на масову свідомість існували завжди. Як технологію його використовували ще шамани і жерці, коли вони намагалися «конструювати майбутнє» в тому чи іншому напрямку.

Інформаційна війна – це комунікативна технологія по впливу на інформацію та інформаційні системи супротивника з метою досягнення інформаційної переваги в інтересах національної стратегії, при одночасному захисті власної інформації і своїх інформаційних систем [4, с. 116]. Інформаційна чи комунікаційна компонента є однією з найважливіших складових загальної стратегії та не існує відокремлено від інших компонент [1, с. 4; 3, с. 237]. Це важливо для розуміння неможливості відокремлено «виграти інформаційну війну». Комунікації, інформаційна компонента є складовою політики, але вони не можуть замінити собою політику. На сьогоднішній день супротивник використовує широке коло комунікаційних та інформаційних методів та технологій, сповідуючи принцип «мета виправдовує засоби». Важливо, що російські спецслужби швидко адаптують для своїх цілей будь-який інструментарій: маркетингові (рекламні) ходи; соціальні мережі та чутки; вигадані постановочні сюжети тощо. Крім цього, чітко сегментується й аудиторії впливу: власні громадяни; громадяни України на окупованому Сході; громадяни неокупованої території України; іноземна аудиторія (яка, за можливості, також сегментується географічно) тощо.

Для дестабілізації ситуації РФ використовує усі доступні канали комунікації: телебачення, Інтернет, радіо, пресу, чутки, дипломатію, експертне середовище. Слід, на наш погляд, виділити сильні сторони такої кампанії, з тим, щоб враховувати їх у заходах протидії. До таких, сильних сторін можна віднести: глобальність та системність задуму; чітку централізовану виконавчу вертикаль; залучення значних матеріальних та людських ресурсів; високий рівень медіавиробництва; високий технологічний рівень; чудові навики маніпуляції емоціями та почуттями (психологічне супроводження).

Російська інформаційна війна проти України продемонструвала, що пропаганда може бути різновидом зброї «масового ураження», яка атакує людську психіку, позбавляючи мільйони здатності до об'єктивного і критичного мислення.

Засоби, що їх використовують в інформаційній війні, швидко прогресують. Сьогодні дослідники вже говорять про перехід від першого до другого покоління моделей інформаційної боротьби. При цьому засоби інформаційної боротьби першого покоління – це:

• у воєнний час або за умов «гібридної війни» – збройне придушення тих чи тих елементів інфраструктури державного та військового управління;

• одержання розвідувальної інформації через перехоплення інформаційних потоків, які сьогодні є вельми різноманітними;

• несанкціонований доступ до інформаційних ресурсів, їх фальсифікація чи викрадення;

• масове подання в інформаційних каналах та глобальних мережах дезінформації для впливу як на осіб, які приймають рішення, так і на населення з метою викликати паніку.

Інформаційна боротьба другого покоління включає більш глибинні процеси:

• створення атмосфери бездуховності й аморальності, негативного ставлення до культурної спадщини противника;

• маніпулювання свідомістю соціальних груп населення з метою створення політичної напруженості та хаосу;

• дестабілізація відносин між партіями й рухами для провокації конфліктів, недовіри, репресій проти опозиції;

• погіршення стану інформаційного забезпечення органів влади, провокування помилкових управлінських рішень;

• дезінформація населення про роботу державних органів, їх дискредитація;

• підрив міжнародного авторитету держави в очах урядів та населення інших країн;

• спотворення інформації про життєво важливі інтереси держави в політичній, економічній, оборонній та інших сферах.

Головним об'єктом ураження залишається людина, прихований вплив на яку здійснюється через її нервову систему та психіку, здебільшого на підсвідомому рівні. При цьому використовується подвійна психобіологічна природа інформації. Так, «комфортна» на рівні психобіологічного сприйняття інформація може спричинити шкоду на психосоціальному рівні чи навпаки, «цікава» - призвести до неусвідомлюваних психобіологічних негараздів, стимулюючи девіантну поведінку особи та руйнувати позитивні соціальні тенденції в суспільстві.

Цілеспрямований інформаційний вплив на населення передбачає пануюче становище суб'єкта інформаційної війни у всіх сферах життєдіяльності іншої держави: економічній, політичній, психологічній, релігійній, науково-технічній, мистецькій, а також міжнаціональних і міжнародних зв'язків. Зростання ефективності заходів безпосереднього підриву, зокрема інформаційної війни, досягається за рахунок встановлення контролю над інформаційним простором іноземної країни, точності та цілеспрямованості таких акцій з урахуванням необхідного обсягу та рівня достовірності інформації, що доводиться, ступеня диференціації населення за системами матеріальних і духовних цінностей, здатності адекватно сприймати відомості та реагувати на них, а також політичної, економічної, етнорелігійної та іншої ситуації в державі й регіоні.

На наш погляд, система контрзаходів передбачає, що одну глобальну задачу із протидії інформаційним загрозам слід поділити на менші підзадачі, виконання яких є абсолютно реалістичним. Такими під задачами виступають:

1) Правоохоронна діяльність із захисту демократичних засад держави. Сюди належить контррозвідувальна, оперативно-розшукова та процесуальна робота спрямована на фіксацію та руйнування системи поширення різноманітних закликів (незаконне захоплення влади, дії, направлені на зміну територіальної цілісності, міжнаціональна ворожнеча тощо). В умовах загострення загроз особливо важлива роль тут належить РНБО як органу, що координує діяльність правоохоронного та безпекового сектору держави та знаходиться під контролем Глави держави [4, с. 114]. Саме цей орган має усі потрібні організаційні важелі для об’єднання розрізнених зусиль відомств (Прокуратура, СБУ, МВС, фіскальні органи) з протидії єдиній ворожій системі пропаганди.

2) Робота з контентом, тобто зі змістом інформації, яка формує картину світу для людини. Передбачає впровадження стимулюючих заходів для створення власного інформаційного продукту, зробленого на власному історичному досвіді, з урахуванням власних цінностей та характеристик.

3) Постійний розвиток власної інформаційної інфраструктури. Окремо необхідно підкреслити важливість зменшення залежності українського інформаційного простору від російського сегменту Інтернет: виведення України з під юрисдикції московських офісів Гугл, Фейсбук, тощо.

4) Реалізація «стратегічних комунікацій» системи влади. Фактично, це прямий обов’язок з інформування громадськості та форма звітності перед замовником-громадянином. Стратегічні комунікації передбачають чітко сформульовану мету та постійний пакет інформації на тему того, як ми досягаємо поставленої мети. Наразі за цим напрямом немає проблем у різних консультантах, а існують лише «підводні камені» в процесі узгодження позицій різних політичних сил.

Підсумовуючи викладене, слід зазначити, що протидія інформаційним загрозам в умовах антитерористичної операції має базуватися на наступному:

1. Протидію інформаційній агресії Росії організаційно доцільно здійснювати через інструментарій РНБО під єдиним керівництвом Глави держави.

2. Система включає як заходи з протидії протиправній діяльності, так і заходи зі стимулювання розвитку відповідних вітчизняних галузей. Протидія спрацьовує через притягнення до відповідальності та регуляторні заходи, стимулювання розвитку – через економічні та організаційні заходи.

3. Уся система повинна охоплюватись єдиним задумом, бути керованою та пов’язаною з громадянським суспільством за допомогою мережі стратегічних комунікацій.

Література:

1. Албул С.В. Кримінальна розвідка як функція оперативно-розшукової діяльності: Європейський досвід та Українські перспективи // EuropeanReformsBulletin: internationalscientificpeer-reviewedjournal: GrandDuchyofLuxembourg. – 2015. – № 2. – P. 2-6.

2. Березовець Т.В. Анексія: острів Крим. Хроніки «гібридної війни» / Т.В. Березовець. – Брайт Букс, 2015. – 584 с.

3. Захаров В.П. Інформаційна розвідка як перспективний напрям розвитку правоохоронної діяльності у боротьбі зі злочинністю / В.П. Захаров // Вісник Львів. держ. ун-ту внутр. справ (юридична серія). – 2006. – № 2 – С. 236-242.

4. Словник ключових понять та абревіатур сектору безпеки: англо-українсько-російський (на матеріалах інтернет-джерел) / Л.Ф. Компанцева, О.В. Акульшин, Н.Т. Акульшина, Т.О. Дєдушкіна, Г.Ю. Зінченко, О.В. Завадська, І.О. Хома; за заг. ред. І.І. Мусієнка. – Х.: «Оберіг», 2014. – 428 с.

Адміністративно-правові заходи боротьби з кіберзлочинністю в Україні

Грохольський В.Л.
доктор юридичних наук, професор,
професор кафедри кібербезпеки
та інформаційногозабезпечення
Одеського державного університетувнутрішніхсправ

Інтеграція України до Європейського співтовариства, а ще краще до світового товариства, передбачає входження нашої держави до інформаційного суспільства, яке характеризується широким використанням переваг нових інформаційних технологій у всіх сферах виробництва, науки, культури, безпеки тощо.

В Україні, як і в інших державах світу, невпинно розвиваються якісно нові галузі економіки, що базуються передусім на використанні сучасних інформаційних технологій, локальних та глобальних комп'ютерних мереж, зокрема мережі Інтернет.

Наслідком розбудови інформаційного суспільства є те, що пропорційно розвитку інформаційних ресурсів зростає й кількість правопорушень з використанням комп'ютерних технологій. Наразі кіберзлочинність є однією з найбільш серйозних проблем багатьох держав, щорічні збитки від якої становлять мільярди доларів США.

Аналіз сучасних тенденцій розвитку нашої держави свідчить про те, що з'явилися нові загрози національній безпеці України – комп'ютерна злочинність та комп'ютерний тероризм.

Проблеми кіберзлочинності в контексті інформаційної безпеки як складової національної безпеки неодноразово розглядалися Верховною Радою України, Президентом України та Радою національної безпеки і оборони України, однак чітких і дієвих заходів протидії цим видам злочинів поки що не визначено.

Враховуючи вище викладене та інші обставини кіберзлочинності в Україні, вбачається за необхідне здійснити наступні кроки:

1. Криміногенна ситуація у сфері використання інформаційних технологій вимагає комплексного підходу як із боку правоохоронних органів, так і з боку інших зацікавлених відомств (органів). Але, сьогодні, на жаль, відсутня взаємодія між суб'єктами, які причетні до розробки комп'ютерних технологій і правоохоронними органами (підрозділами), які здійснюють боротьбу з кіберзлочинністю. На законодавчому рівні ще не створено умов, які б дозволяли ефективно взаємодіяти заради протидії кіберзлочинності.

2. Протидія злочинам у сфері використання інформаційних технологій вимагає якісного кадрового забезпечення. Адже зрозуміло, що не кожний працівник, наприклад, органів (підрозділів) Національної поліції у змозі виявляти і протидіяти особам, які вчиняють такі злочини. У зв'язку з цим, виникає проблема підбору і підготовки фахівців для протидії кіберзлочинності. На наш погляд, таких фахівців у навчальних закладах системи МВС України готувати досить складно, з різних причин, і це окрема тема. Але цю проблему необхідно вирішувати уже сьогодні. Тому вбачається за доцільне здійснювати відбір кадрів для боротьби з кіберзлочинністю, по-перше, - серед студентів-випускників вищих навчальних закладів, які готують фахівців для роботи у сфері інформаційних технологій, по-друге, - серед працівників, які уже працюють у сфері інформаційних технологій. Звичайно, слід враховувати, що висококваліфіковані фахівці такого напряму не будуть працювати за 4-5 тис. грн. Тому, необхідно приваблювати таких фахівців як достойною зарплатою, так і соціальними пакетами, які у нашій державі ще не розроблені і не використовуються, наприклад, – пільгові кредити для придбання житла, автомобіля, меблів тощо, право виходу на пенсію за вислугою років і т. ін.

3. Основна проблема боротьби з кіберзлочинністю сьогодні полягає у тому, що розвиток законодавчої бази і реагування на всі проблеми боротьби з кіберзлочинністю поки що відстає від розвитку інформаційних технологій. А відтак, відсутності дієві правові механізми контролю, необхідні для правозастосування.

4. Слід звернути увагу на те, що, сьогодні, майже увесь світ обговорює проблему боротьби з кіберзлочинністю, і Україна визнала, що кіберзлочинність загрожує національній безпеці, але Стратегії