ВИКОРИСТАННЯ РОСІЙСЬКОЇ ВІЙСЬКОВОЇ ТЕХНІКИ У ІНФОРМАЦІЙНІЙ ВІЙНІ ПРОТИ УКРАЇНИ

Христенко В.Є., кандидат психологічних наук, доцент
Національний університет цивільного захисту України

Інформаційна війна поступово стає не менш важливою, ніж «традиційна» війна. І постає ця війна в самих різних формах. Згідно з сучасними поглядами, інформаційні операції (цей термін зараз використовується для заміни терміну «інформаційна війна») являють собою і захист своїх інформаційних систем, і одночасний вплив на інформаційні системи противника з метою утруднити чи зробити взагалі неможливим прийняття ним правильних рішень. Дуже часто інформаційні операції ділять на радіоелектронну боротьбу (РЕБ), психологічні операції, мережеві операції, заходи щодо оперативного маскування і по забезпеченню безпеки власних сил і засобів.

Російське керівництво вже давно зрозуміло важливість інформації під час воєнних дій. Наприкінці 2013 року російське керівництво офіційно заявило про створення військ інформаційних операцій. Тобто, інформація розглядається як зброя, яка має дуже великий потенціал. Прикладом цього є той факт, що в першу чергу під час вторгнення у 2014 році в Донецьку та Луганську області були захоплені телевізійні вишки.

Можна виділити наступні ключові особливості інформаційних операцій:

- порівняно низька вартість створення засобів інформаційного протиборства і інформаційної зброї, а відповідно - низькі фінансові та матеріальні витрати на проведення інформаційних операцій;
- ліквідація статусу традиційних державних кордонів при підготовці і проведенні інформаційних операцій;
- посилення ролі управління сприйняттям ситуації шляхом маніпулювання інформацією по її опису і контексту;
- зміна пріоритетів в діяльності стратегічної розвідки, які зміщуються в область завоювання і утримання інформаційної переваги;
- ускладнення завдання виявлення початку інформаційної операції;
- складність створення коаліції проти агресора, який проводить інформаційну операцію.

Як відомо, гібридна війна не має остаточного визначення. Але треба розуміти, що гібридна війна проводиться: без оголошення війни; за всіма можливими напрямками одночасно (у зовнішньополітичній сфері, у сфері державної безпеки, у воєнній сфері та сфері безпеки державного кордону України, у внутрішньополітичній сфері, в економічній сфері, у соціальній та гуманітарній сферах, у науково-технологічній сфері, в екологічній сфері, в інформаційній сфері). І все це проводиться приховано, із запереченням на офіційному і неофіційному рівнях з боку агресора.

Моніторингова місія ОБСЄ на сході України постійно повідомляє про новітні російські станції постановки радіоперешкод, комплекси радіоелектронної боротьби з безпілотними літальними апаратами, спеціальні комплекси для постановки радіоперешкод у мережах мобільного зв'язку, які з'являються на непідконтрольних України територіях. Саме комплекс «Леєр-3» призначений для проведення РЕБ у мережах сотового зв'язку стандарту GSM. Радіус дії цього комплексу біля 6 кілометрів. Цей комплекс для потреб збройних сил Росії серійно почав виготовлятися у 2015 році. І саме за допомогою цього засобу РЕБ у 2015 році почав відбуватися вплив на свідомість і психічний стан наших військових. Вплив відбувається у вигляді смс-повідомлень, які отримували наші захисники, знаходячись на передовій.

Повідомлення мали ознаки офіційних повідомлень від українських сотових операторів. Вони містили різноманітну коротку інформацію, яка мала вивести нашого захисника з емоційної рівноваги, зневіритися у правильності своїх дій, погрози розправи з ним або його рідними, а іноді і спонукали до переходу на бік супротивника. Ці смс-повідомлення були цілеспрямовані на мобільні телефони українських військових.

На мобільні телефони цивільних, які перебували поряд з військовими на передовій, надходили повідомлення дещо іншого змісту. Вони мали на мету викликати недовіру до українських військових, невдоволення українською владою. Також ці смс-повідомлення містили номера телефонів чи адреси інтернет сайтів, за якими можна передати інформацію щодо розташування підрозділів української армії.

Особливим класом в інформаційній війні є дезінформація, причому мова йде не тільки і не стільки про пряму брехню в повідомленнях ЗМІ, а про речі набагато більш складних і тонких.

Наприклад, найсучасніші методи РЕБ вже не зводяться до того, щоб «тупо задавити» перешкодами РЛС супротивника. Вищий клас тепер - це створити на екрані РЛС супротивника неправдиву картину повітряної обстановки, ворожий оператор повинен бачити цілі не там, де вони знаходяться насправді. Відповідно, ракети будуть наводитися на порожнє місце, в прямому сенсі опиняючись ракетами «земля-повітря». Такий метод отримав назву «неенергетичні перешкоди.

Не менш ефективними можуть бути такого ж роду мережеві операції. Йдеться про так званих семантичних атаках, коли інформаційна система противника зовні продовжує працювати в звичайному режимі. Однак вхідна інформація не є адекватною реальності. Подібним атакам можуть піддаватися найбільш популярні сайти, що викликають цілковиту довіру користувачів. Непомітна зміна їх змісту впливає і на психологічний стан населення ворожої і країни, і на рішення, що приймаються її керівництвом. Природно, що сторона, яка проводить такі операції, повинна бути впевнена, що сама не є об'єктом подібного впливу. Тому мережевий захист анітрохи не менш важливий, ніж мережевий напад.

Російські війська інформаційних операцій використовують будь-яку військову техніку, яка дозволяє досягти поставленої мети. Наприклад, для проведення пропаганди в окупованих районах, на першому етапі використовувалась військова техніка із арсеналу РЕБ для транслювання на телеканалах своїх програм. При цьому одночасно використовувалась апаратура для встановлення радіоелектронних перешкод для унеможливлювання перегляду на окупованій території українського телебачення.

Також за допомогою деяких засобів РЕБ в міські адміністрації, які розташовані поряд з лінією розмежування, через мережу Інтернет представники російських інформаційних військ «вкидають» неправдиву інформацію, що змушує керівників цих адміністрацій приймати неправильні рішення.

Таким чином, інформація в сучасному світі є дуже сильною зброєю, яку використовує російське керівництво проти України. На початку 21 століття засоби радіоелектронної боротьби призначалися в основному для протидії військовій техніці супротивника. Останнім часом засоби РЕБ російські військові використовують не тільки у межах військового протистояння, але й у «гуманітарному напрямку», який передбачає безпосередній вплив на психіку людини.