Кібервійни та кібербезпека в сучасному світі

доцент Горбенко В.І.
ауд.19, корп.1

Кібермиротворча діяльність

Як відновити і зберегти мир після кібервійни?
Яка концепція кібермиротворчої діяльності?

На міжнародному рівні визначення миротворчої діяльності зустрічається з деякими трактуваннями. Під “миротворчістю” розуміється “активне підтримання перемир’я між народами чи громадами, із можливим застосуванням міжнародної військової сили”. Термін підтримка миру часто вживається вільно, а інколи як ярлик для легітимізації сумнівної військової діяльності.

Визначення ООН з питань миротворчості таке: «Дії, спрямовані на збереження миру, хоч і неміцного, де бойові дії припинені та сприяння виконанню домовленостей, досягнутих миротворцями». Деякі країни віддають вестфальську перевагу перед миротворчою теорією, тобто є думка, що світ складається з суверенних держав, які не визнають вищої влади. Інші держави та організації не повинні втручатися у питання всередині цієї держави, якщо їх не запросять. Інші країни віддають перевагу поствестфальському порядку - держава може користуватися суверенітетом та невтручанням у внутрішні справи, доки вона захищає добробут своїх громадян. Якщо ця відповідальність за захист не вдається, міжнародна спільнота може і повинна втрутитись.

Кібермиротворча діяльність

Сьогодні ООН визначає два типи миротворчих операцій, які вона може здійснити: традиційну та багатовимірну.

• Традиційні: операції, які суворо дотримуються традиційних цілей спостереження, моніторингу та звітування.

• Багатовимірні: Більш складні операції, які включають підтримку миру, але також поширюються на побудову миру, наприклад реформування сектору безпеки держави та знешкодження мін.

Миротворча діяльність - це діяльність, яка перекривається із більш широким набором мирних заходів:

• Запобігання конфліктам: раннє втручання для запобігання ескалації суперечки.
• Миротворчість: дипломатичні заходи, спрямовані на припинення вогню.
• Застосування миру: Відновлення миру без згоди сторін.
• Розбудова миру: заснування фундаменту довгострокового миру та запобігання повторним конфліктам.

Кібермиротворчі операції можуть вплинути на попередження конфліктів, миротворчість та забезпечення миру.

Кібермиротворча діяльність

Миротворча діяльність ООН керується низкою основних принципів:

Згода сторін: Миротворчі операції повинні розгортатися лише за згодою основних конфліктуючих сторін. Це надає операції законності діяти як фізично, так і політично в районі. Без згоди всіх сторін операція ризикує втягнутись у конфлікт.

Безсторонність: Виконання мандата без надання переваги жодній із залучених сторін. Операція повинна розглядатися як неупереджена, щоб залишатися законною в очах сторін, що погодилися. Але неупередженість не є виправданням бездіяльності з метою запобігання загрозам миру.

Невикористання сили, за винятком самооборони та захисту мандату: Застосування сили має бути крайнім заходом. Сила може бути використана для захисту мандата, тобто силу можна застосовувати проти тих, хто твердо вирішив підірвати мирний процес.

Кібермиротворча діяльність

Шість заходів, які повинні проводити кібермиротворчі операції:

Управління кібермежами: Визначення мережевих з’єднань, доступних учасникам бойових дій. Наявність можливості виявляти атаки, що проходять через ці зв’язки, і закріплювати ці межі для атак.

Моніторинг та перевірка: Моніторинг інтернет-трафіку. Використання підпису та виявлення аномалій для моніторингу інцидентів.

Кантонне місто: кантонне місце - це притулок для учасників бойових дій під час припинення вогню. Запропоновано два підтипи: віртуальний кіберконтон, за допомогою якого проводиться профілювання, щоб визначити, що робить кожен учасник бойових дій і на кого вони націлені, та фізичний кіберконтонмент, за допомогою якого учасникам бойових дій надаються облікові записи в Інтернеті, які відокремлюються від їхніх колишніх ворогів і суворо контролюються.

Роззброєння та демобілізація: Роззброєння військ кібервійни. Є припущення, що це буде включати кінетичний моніторинг та інспекції з метою виявлення кіберзброї.

Кібермиротворча діяльність

Поінформованість про загрози та попереджаюче усунення загроз: підтримка передових технологій та знань для забезпечення того, щоб кібермиротворці завжди мали вищі технічні можливості над тими, за якими вони стежать.

Самоохорона миротворця: Забезпечення того, щоб кібермиротворчі сили були невразливі до загроз, яким вони призначені запобігати. Сюди входить захист як від кібернетичних, так і від кінетичних атак.

Кібермиротворчі операції будуть потрібні в майбутньому: "запобігання кібер-конфліктам, пом'якшення наслідків, стримування наслідків та реабілітація з акцентом на деескалацію конфліктів та цивільну безпеку".

Кібермиротворча діяльність повинна мати шість цілей:
1) Захист цивільних осіб.
2) Збільшити довіру та безпеку в кіберпросторі.
3) Запобігання кібератакам та ескалації кіберконфліктів.
4) пом'якшення шкоди від конфліктів.
5) Утримання наслідків.
6) реабілітація.

Кібермиротворча діяльність

Кібермиротворча діяльність повинна відігравати певну роль на етапах доконфліктних, конфліктних та постконфліктних ситуацій.
На передконфліктній стадії кібермиротворці проводять заходи щодо підтримання та зміцнення міжнародного миру. Якщо спалахне конфлікт, ролі змінюються на захист цивільного населення від нападу.
Пропонується два практичні варіанти здійснення кібермиротворчої діяльності - Відділ швидкого реагування (RRD) та Відділ довгострокової стабільності та допомоги (LSRD).
Основна увага RRD спрямована на захист "безпечного шару кіберпростору". Це визначається як "заздалегідь визначена, мінімально необхідна критична інфраструктура, необхідна для цивільної безпеки".
У разі кіберконфлікту РРД вживає негайних заходів для захисту та забезпечення доступності цього безпечного шару. LSRD застосовує більш довгостроковий підхід, працюючи над зміцненням спроможності та захисту, щоб забезпечити більш тривалий мир.
Майбутні зусилля будуть зосереджені на встановленні того, як повинен виглядати рівень безпечного кіберпростору, та на зборі відгуків від зацікавлених сторін щодо того, чи є їх пропозиції життєздатними.

Кібермиротворча діяльність

Якщо такі події, як крах держави, гуманітарні страждання та порушення прав людини, є загрозою міжнародному миру та безпеці, то можна стверджувати, що кібератаки також є загрозою через їх потенціал ініціювати, складати або продовжувати такі події. Використовуючи це обґрунтування, кібератаки, що використовуються під час кібервійни, можуть розглядатися як загроза міжнародному миру та безпеці. Як приклад, кібератаки можуть принаймні сприяти розвалу держави, якщо вони ініціюють або продовжують вихід з ладу критичної національної інфраструктури. Нації стають залежними від кібердомену, щоб надавати послуги, що забезпечують функціонування нації: електромережі, водопостачання, зв'язок, транспорт та фінанси все більше стають кіберзалежними. Війна, яка спричиняє відключення електроенергії, припиняє постачання безпечної питної води, робить подорожі небезпечними або дестабілізує національну економіку, однозначно загрожує стабільності нації і, отже, загрожує міжнародному миру та безпеці.

Кібермиротворча діяльність

Подібні аргументи можна наводити щодо інших подій, таких як порушення прав людини.
У найбільш критичному кінці спектру національне відключення або токсичне водопостачання може загрожувати мільйонам цивільних прав людини на життя.
Менш серйозним, але все ж важливим є право кожної людини шукати, отримувати та передавати інформацію та ідеї через будь-які засоби масової інформації та незалежно від кордонів. Це права людини, які явно ризикують під час кібервійни, і слід зазначити, що ООН проявляє активну зацікавленість у подоланні таких порушень. Як приклад, коли уряд Камеруну припинив доступ до Інтернету до переважно англомовних частин країни, ООН заявила, що це "жахливе порушення їх права на свободу вираження поглядів". Це засвідчує той факт, що ООН вважає, що правам людини можуть загрожувати в кібердомені, і тому додає ваги аргументу, що кібервійна може потенційно становити загрозу міжнародному миру та безпеці.

Кібермиротворча діяльність

Хоча існують аргументи як за, так і проти існування кібермиротворчої діяльності, є вагомі докази того, що кібервійна може загрожувати міжнародному миру та безпеці.
Подібно до того, як міномет може спричинити травми та смерть, кібератака на водоочисну станцію, електростанцію або фінансові мережі країни здатна завдати непропорційну та нерозбірливу фізичну, психологічну та економічну шкоду цивільному населенню. Без будь-якого плану відновлення цих систем після війни, ці страждання можуть мати довгостроковий характер, оскільки країни борються за безпечне повернення інфраструктури в Інтернет. Протягом цього часу існує ризик краху держави, гуманітарних криз та порушень прав людини, що все вже розглядається як загроза міжнародному миру та безпеці. Відомо, що кібермиротворча діяльність сьогодні не потрібна, але вона буде потрібна найближчим часом. Отже, розпочинати дискусію та закладати основи досліджень у цій галузі є виправданим, щоб миротворчі організації могли якнайкраще підготуватися до своєї майбутньої ролі у кібердомені.

Кібермиротворча діяльність

Визначення 1. Кібермиротворча діяльність ООН. Застосування кіберздатності для збереження миру, хоч і неміцного, де припинено бойові дії та сприяння виконанню домовленостей, досягнутих миротворцями.

Основна сила визначення полягає в тому, що воно ґрунтується на формулюванні, яке вже склалося у міжнародному співтоваристві. Визначення ООН щодо миротворчості та пристосовує його, щоб обмежити „дію” в кібердомені. Потенційною слабкістю у визначенні є те, що вимагає виконання дії у кіберпросторі, щоб вважати її кібермиротворчою діяльністю, означає, що діяльність, яка вимагає кібернетичних знань, але має кінетичний характер (наприклад, навчання або допомога у проведенні політичних реформ), не може розглядатися як кібермиротворча діяльність.

Визначення 2. Кібер-миротворець. Особа, яка здійснює кібермиротворчу діяльність.

Кібермиротворча діяльність

Кібермиротворчі операції можна розглядати як унікальну концепцію, а комплекс заходів можна розробити з нуля.

Можна вивчити налагоджену миротворчу діяльність ООН та обговорити її придатність до кібермиротворчої діяльності.

Останній підхід приносить ряд переваг:

• Адаптація: кібермиротворчі операції відповідають встановленим рамкам.

• Всебічність: існуюча доктрина стосується питань, які є важливими для миротворчих операцій.

• Інтеграція: поділяючи загальний підхід, кібермиротворча діяльність має гнучкість, щоб діяти як окрема подія, так і поряд з кінетичною миротворчістю як частина більш широкої операції.

Кібермиротворча діяльність

Спостереження, моніторинг та звітування (ОМР) є однією з основних видів діяльності, що здійснюється під час миротворчої операції ООН. Ця діяльність приносить користь завдяки забезпеченню неупередженої звітності про дотримання угод про припинення вогню, порушення прав людини та іншу інформацію, де довіра до її правильності є критичною для збереження миру. Персонал ООН прагне спостерігати, контролювати та звітувати про:

1) Дії, що порушують мирні угоди.
2) Порушення прав людини.
3) Зміни рельєфу, розташування та цивільна діяльність.

Розглядаючи питання про те, як ОМР може застосовуватися до кібердомену, одразу слід зазначити, що концепція спостереження, моніторингу та звітування в кіберпросторі не є новою. Кібератаки на підприємства та уряди спонукають до досліджень того, як можна покращити спостереження, моніторинг та звітність у кіберпросторі.

Кібермиротворча діяльність

Дії, що порушують мирні угоди

Війни майбутнього будуть містити елементи кібервійни. Тоді майбутні мирні угоди будуть містити умови кібервійни. Чи є технічно доцільним та цінним для кібермиротворчих операцій спостерігати за діями, що порушують мирні угоди? З точки зору цінності, очікується, що моніторинг порушень кібертермінів принесе високу цінність тому, що це внесе впевненість у мирний процес і дозволить нейтральній третій стороні здійснювати незалежний моніторинг. Наприклад, якщо країна А погодиться не нападати на електромережу країни В, моніторинг кібермиротворців був би цінним, якщо виступатиме третьою стороною, якій довіряють, щоб контролювати дотримання цієї угоди.

З точки зору технічної доцільності базову можливість моніторингу можливо встановити, використовуючи наявні знання, але є значні проблеми. По-перше, слід дотримуватися обережності, коли узгоджуються кібер умови. Заявляючи, що країна А припинить усі кібератаки на країну Б, буде важко відстежувати. Причиною цього є те, що просити будь-яку організацію контролювати кожну мережу в країні нереально: для цього просто знадобиться така кількість ресурсів (як людських, так і апаратних), які було б неможливо забезпечити в контексті миротворчої операції. Тому передбачається, що мирні угоди містять перелік конкретних мереж, напад на які буде вважатись порушенням мірних угод.

Кібермиротворча діяльність

Найважливішою технічною перешкодою є проблема атрибуції. Хоча можна буде спостерігати атаку на мережу, важко буде довести, звідки ця атака відбулася, хто її організував та провів. Дослідження проблеми атрибуції тривають, але, ймовірно, це буде перешкодою для спостереження за діями, які порушують мирні угоди.

Це є потенційною перешкодою на шляху до здійсненності, оскільки це робить значні наслідки у заяві про те, що певна сторона порушила мирну угоду.

Природа кібермиротворчої діяльності представляє потенційно нове рішення. Кібермиротворча діяльність має потенціал у формі кібер-миротворців-резервістів. Це люди, які працюють у магістральних провайдерів Інтернет і зможуть бути активними тоді, коли це потрібно, швидко виконувати відстеження через організаційні кордони.

Кібермиротворча діяльність

Порушення прав людини

Права людини - це проблема, яка завжди була основою миротворчої діяльності, і тому контроль за порушеннями прав людини є другою ціллю спостереження. Перше питання порушення прав людини з точки зору кібервійни - чи можна їх порушувати в кіберпросторі ?
Права людини, які викладено у Загальній декларації прав людини (ЗДПЛ), має три вразливі до загрози в кіберпросторі пункти:

Стаття 3. Кожна людина має право на життя, свободу та особисту безпеку.

Стаття 12. Ніхто не може піддаватися свавільному втручанню в його приватне життя, сім'ю, будинок або листування, а також нападкам на його честь і репутацію. Кожен має право на захист закону від такого втручання або нападу.

Стаття 19. Кожна людина має право на свободу думки та вираження поглядів; це право включає свободу дотримуватися думок без втручання та шукати, отримувати та передавати інформацію та ідеї через будь-які засоби масової інформації та незалежно від кордонів.

Кібермиротворча діяльність

Спостереження за порушеннями приватного життя (стаття 12) буде технічно важко здійсненним та технічно складним тому, що перегляд мережевого трафіку є пасивною діяльністю, яку важко виявити технічно. Наприклад, уряд може перевірити весь трафік, що проходить через контрольований урядом ISP, або змусити регіональні технологічні фірми надати доступ до даних клієнтів, таких як електронні листи. Це такі дії, що порушують права, які важко виявити за допомогою технічного рішення. Політична доцільність спостереження за порушеннями статті 12 також буде низькою. Кібермиротворці діятимуть за згодою приймаючої країни, і ця згода може бути поставлена під загрозу, якщо приймаюча сторона підозрює або виявляє, що кібермиротворці намагаються виявити порушення конфіденційності.

Моніторинг порушень свободи вираження поглядів та доступу до інформації (стаття 19) також є складною з технічної точки зору. Існує сценарій, коли певна країна починає блокувати доступ до певної інформації або забороняти доступ до Інтернету людям з певними поглядами. Відсутність доступу до неупередженої інформації з міжнародних джерел може призвести до заворушень і дозволити пропаганді поширювати дезінформацію про конфлікт. Якщо підрозділ з питань кібермиротворчої діяльності може забезпечити доступ до національного постачальника послуг Інтернету (ISP), існує можливість спостерігати та повідомляти про блокування вмісту та інші обмеження доступу.

Кібермиротворча діяльність

Спостереження за загрозами життю, свободі та безпеці особи (стаття 3) має високий потенціал на здійснення з технічної точки зору та є дуже цінним. Кібератаки на критичну інфраструктуру, таку як громадське водопостачання або контроль повітряного руху, потенційно можуть загрожувати життю та безпеці цивільного населення, і його можна відстежувати, виявляти наявність загроз за умови надання згоди на їх контроль.

Незважаючи на те, що кіберпростір створює перешкоди для спостереження за порушеннями прав людини, він також надає нові потенційні можливості. Соціальні медіа стали засобом для моніторингу прав людини у всьому світі, надаючи жертвам порушень метод звітування, який раніше був недоступний. Беручи до уваги цей момент, кібермиротворці можуть спостерігати за соціальними мережами та контролювати не лише порушення, що відбуваються в кіберпросторі, а й у соціальних мережах. Багато благодійних організацій, таких як Privacy International та Human Rights Watch, вже проводять такий моніторинг.

Кібермиротворча діяльність

На додаток до прав, викладених в ЗДПЛ, прикладають певні зусилля до розробки набору прав людини у віртуальному просторі, метою яких є забезпечення нового набору прав, таких як право на доступ. Якби світ прийняв такий набір прав, можна сперечатися, що кібермиротворці мали б повноваження захищати їх. Поки такі права не узгоджено, важко робити прогнози щодо їх цінності та доцільності.

Таким чином, значення моніторингу за порушення прав людини є високим або середнім. Універсальні права, такі як приватність, свобода вираження поглядів, життя та безпека, можуть бути під загрозою в кіберпросторі, і спостереження за порушеннями сприятиме миру та безпеці. Однак доцільність цього відрізняється. Очікується, що моніторинг порушень конфіденційності буде складним. Очікується, що моніторинг порушень права на пошук та розповсюдження інформації, а також загрози життю та безпеці буде більш здійсненним за умови забезпечення необхідної згоди приймаючої країни. Моніторинг загрози життю є найбільш здійсненним із трьох, а також, мабуть, найціннішим.

Кібермиротворча діяльність

Зміни рельєфу, розташування та цивільна діяльність

Кінцевою метою спостереження є моніторинг та звітування про зміни рельєфу, розподіл сил та цивільну діяльність. Повідомлення про зміни місцевості дозволяє миротворчим силам постійно оновлювати місцеві карти з основними особливостями місцевості, що може допомогти інформувати, де слід проводити патрулювання та потенційні осередки конфлікту.
Під “змінами рельєфу місцевості” в контексті кіберпростору слід розуміти, що кібермиротворці повинні стежити за змінами в структурі мережі. Наприклад, раптова недоступність серверів або додавання нових пристроїв є цінними змінами, на які слід звернути увагу. Слід зазначити, однак, що мережі, природно, можуть змінюватися в звичайних умовах: таблиці маршрутизації можуть змінюватися залежно від мережевих умов, і сервери можуть бути недоступними для виправлення та обслуговування. Тому дуже важливо, щоб кібермиротворці формували розуміння того, що є нормальним, а що ненормальним, ефективно проводячи виявлення аномалій в мережі. Кінцева мета - покращити ситуаційну обізнаність щодо структури кібердомену в регіоні та використовувати цю обізнаність з якоюсь цінною метою.

Кібермиротворча діяльність

Ситуативна обізнаність передбачає чотири конкретні етапи:

1) отримання інформації з навколишнього середовища;
2) Інтеграція інформації з відповідними внутрішніми знаннями для створення ментальної картини поточної ситуації;
3) Використання цієї картини для спрямування подальших досліджень сприйняття у постійному перцептивному циклі;
4) Передбачення майбутніх подій.

Спостереження за змінами в структурі мережі в кібермиротворчих операціях виконується у ці чотири кроки. Кібермиротворці спостерігають за кіберсередовищем, створюють його уявлення, визначають райони, де потрібні подальші дослідження, а потім використовують цю інформацію для передбачення майбутніх подій. Тому спостереження за змінами в структурі мережі може принести користь наступними способами:
1) Надання законних пояснень щодо змін трафіку, які в іншому випадку викликали б тривогу.
2) Виділення нових потенційних цілей атаки або видалення старих.
3) Вказівки на порушення, яке ще не було виявлено іншими способами.

Кібермиротворча діяльність

Перша перешкода полягає в тому, що спостереження за кіберзброєю та кіберкомбатами є складним завданням. Кіберзброя може бути не зрозумілою і в повній мірі не визначеною. Кіберкомбатам не потрібно фізично переселятись або об’єднуватися в групи, щоб здійснити ефективні атаки.

Альтернативний підхід полягає в розгляді цілей моніторингу розпоряджень, а потім у розгляді способу досягнення цих цілей у кіберпросторі.

Цілями моніторингу розпорядження є наступні:

- Визначення потенційних точок конфлікту (наприклад, незвичне нарощування сил у певного ресурсу).
- Визначення зростання чи спаду боєздатності (наприклад, кібермиротворці, що працюють у мережі, можуть стежити за вдосконаленням методів кібербезпеки, що застосовуються місцевим персоналом на місцях, де вони розміщені, і робити висновки щодо рівня їх кібер спроможності).

Кібермиротворча діяльність

Спостереження за цивільною діяльністю є показником рівня миру та безпеки, який відчуває місцеве населення. Будь-яка зміна звичних моделей цивільного життя може вказувати на зміну місцевої ситуації, яку варто вивчити далі.

У кібердомені ця мета спостереження може бути перетворена на зміни в мережевому трафіку, за допомогою яких кібермиротворці будують базовий рівень для нормального трафіку і згодом шукають відхилення від цього базового рівня.

Це мало б значення для миротворчого процесу, попереджаючи про потенційні зараження шкідливим програмним забезпеченням, атаки відмови в обслуговуванні, вилучення даних та несанкціонований доступ до захищених миротворчих мереж.

Кібермиротворча діяльність

Перешкоди

По-перше, це питання опору на всіх рівнях (місцевому, регіональному та національному). Хоча дві сторони протиборства можуть погодитися на мир на найвищому рівні, це не може призвести до автоматичного дотримання і сприймання кібермиротворців. Кібермиротворці можуть виявити, що власники мереж неохоче відкривають свої мережі для моніторингу, навіть якщо це одна з визначених критично важливих мереж, і доступ узгодили політичні лідери. Це особливо актуально, якщо мережею є приватна компанія, така як Інтернет-провайдер. Кібермиротворці мають бути готовими зустріти опір на всіх рівнях, і це слід очікувати і планувати. Крім того, можна передбачити, що спротив виникне навіть на найвищих рівнях при розгляді високочутливих мереж, таких як критична національна інфраструктура (CNI).
Другою перешкодою є технічні проблеми, які представляє CNI. Такі об'єкти, як електростанції та водні об'єкти, мають властивості, які роблять спостереження та моніторинг більш складними, ніж стандартні методи моніторингу мережі. Використання власних протоколів та цілодобова доступність означають, що виконання OMR на цих системах вимагатиме спеціального набору навичок. Іншими потенційними перешкодами є одинокі нападники кібервовків та проблема спойлерів.