Савчук Аліна Валентинівна,

Донецький національний університет імені Василя Стуса

Як  Україна  може  ефективно  використати  статус  партнера з розширеними  можливостями  НАТО  у  процесі  забезпечення національної безпеки у кіберпросторі?

Внаслідок швидкого розвитку технологічних можливостей людства майже всі сфери людського життя пов’язані з кіберпростором. Держави активно переорієнтовуються на використання інформаційно-комунікаційних технологій, створюючи нову інформаційну інфраструктуру. Вирішення проблем інформаційної безпеки сильно пов’язане з захистом національного інформаційного простору, підвищенням ролі інтелектуальної власності та розвитком інформаційно-комунікаційної системи для забезпечення державної інформаційної політики.

Положення України в кіберпросторі досить нестабільне та вразливе. Законодавство не здатне захистити український інформаційний простір повною мірою, хоча кіберзлочини не є рідкісним явищем. З початком військової агресії Російської Федерації Україна почала все частіше відчувати на собі наслідки недосконалості системи національної кібербезпеки. Починаючи з 2014 року, було здійснено чимало кібератак на стратегічно-важливі об’єкти української інфраструктури. Хакерські групи, що підконтрольні владі Російської Федерації, постійно розробляють нові та ще більш небезпечні віруси і шкідливе програмне забезпечення, яке згодом тестується на території України. А українська влада в свою чергу не може забезпечити попередження цих загроз своєчасно. Варто лише згадати віруси «Uroboros» чи «Petya.A», який в 2017 році був запущений з метою підірвати фінансову систему України та своєрідні «війни» між хакерськими групами обох сторін, адже до захисту державних інтересів та прав громадян вдаються не лише державні структури, а й IT-фахівці з почуттям патріотизму. Треба також усвідомлювати, що вражаючи одну систему, існує величезний ризик поширення збоїв і на інші системи. Саме так сталося з вірусом «Petya.A», адже він вразив не лише комп’ютерні системи України, а й Данії, Індії, Сполучених Штатів.

Україні все ж варто скористатися статусом партнера з розширеними можливостями НАТО для розвитку національної кібербезпеки, адже РФ, схоже, не планує заспокоюватись, що видно з нових спроб російських хакерів втрутитись в хід президентських виборів США, атакуючи одну з головних консультаційних фірм кандидата в президенти від Демократичної партії Джо Байдена. Ще одною причиною для прискорення дій є оголошений президентом Володимиром Зеленським режим paperless у який Україна почне входити в 2021 році. Ймовірно, для когось це стане величезною спокусою для викрадення інформаційних масивів з систем управління України і не складе великої проблеми, якщо не буде належного захисту.

Насправді, Україна вже кілька років діє з метою консолідації зусиль для пришвидшення впровадження стандартів НАТО у сфері приєднання до колективної системи забезпечення кіберзахисту. Але цей процес все ж є досить повільним, що свідчить про недосконалість існуючої системи протидії загрозам у кіберпросторі та зовнішнім кібератакам у сучасних умовах. Проте, проаналізувавши показники Global Сybersecurity Index з 2014 по 2018 роки, можна побачити, що Україна не стоїть на місці, особливо в останні роки, коли прослідковується активізація співпраці з Альянсом. Якщо в 2014 – 2016 вона трималася на 70 місці у світовому рейтингу, мавши показник 0,353, то вже в 2017 році цей показник збільшився майже вдвічі, досягнувши показника 0,501, і віддав Україні 59 місце в світі. Наступного року показник ще збільшився - 0.661 (max. 1) і на 2018 Україна посідала 54 місце в рейтингу. Відповідно до позитивної динаміки можна припустити, що показник за 2019 рік покращиться ще більше, а Україна підніметься на вищий щабель у світовому рейтингу.

На мою думку, співпраця між Україною і НАТО раніше була дещо формальною. Безперечно, основи співпраці існували і таким прикладом є Трастовий фонд Україна – НАТО, який «спрямований на підтримку України у розвитку її оборонних можливостей у галузі кібернетичної безпеки, пропонуючи обладнання, програмне забезпечення, технічну допомогу, консультативні послуги та проведення навчальних тренінгів»[[1]](#footnote-1). Отримане комп’ютерне обладнання призначене для аналізу великих обсягів даних (ідентифікаторів) про підготовку та здійснення кібератак на інформаційно-телекомунікаційні системи державних органів України, і мабуть це найбільш вагомий крок у розбудові кібербезпеки за допомогою НАТО. Крім того, організовувались тренінги, які спрямовуються на персонал центрів реагування на інциденти в кіберпросторі, щоправда, оборонного характеру. Усі заходи фінансуються виключно з бюджету Фонду. З реалізації заходів, що проводяться Трастовим Фондом, і Україна, і НАТО отримують користь для себе. Україна в свою чергу зміцнює кібербезпеку, а Альянс має змогу випробувати технічні та організаційні рішення в реальних умовах.

Проте більш дієва співпраця прослідковується саме 3 - 4 останні роки. Якщо держава не може захистити свої стратегічно важливі об’єкти, в поле ще більшої небезпеки потрапляють громадяни. Раніше головна проблема України з підтримки кібербезпеки полягала в тому, що влада боролася з наслідками вже здійснених атак, а не працювала на випередження. Завдяки створеному відносно нещодавно Державному центру кіберзахисту та протидії кіберзагрозам (CERT-UA) за підтримки НАТО захист інформаційного простору

України піднявся на значно вищий рівень. Тепер виявлення загроз відбувається

на ранніх стадіях, що, напевне, є головним фактором успішного забезпечення безпеки. Крім того, допомога Альянсу цим не обмежується: CERT-UA активно співпрацює з аналогічними центрами НАТО. Насправді, це надзвичайно важливо, адже активний обмін досвідом та інформацією допомагає «новачкам швидше увійти в курс справи».

Відповідно до Річної національної програми під егідою Комісії Україна - НАТО на 2019 рік до кінця 2020 року заплановано чимало заходів, серед яких:

* покращення технічного обладнання;
* впровадження систем кіберзахисту «Єдиної інформаційної системи» та захисту інформації, яка в ній зберігалася і оброблялася;
* підготовка та перепідготовка фахівців у сфері кіберзахисту та кібербезпеки за міжнародними стандартами.

На мою думку, саме в останньому пункті можна скористатися статусом партнера з розширеними  можливостями  НАТО повною мірою. Китайська мудрість каже: «Дай людині рибу, і ти нагодуєш її лише раз. Навчи її ловити рибу, і вона буде годуватися нею все життя». Незважаючи на те, що за підтримки НАТО були створені і Ситуаційний центр забезпечення кібербезпеки Служби безпеки України, і Державний центр реагування на кібербезпеки CERT-UA, туди необхідні кваліфіковані працівники. Оскільки до переваг статусу розширеного партнера НАТО належать розширений доступ до програм взаємодії та навчань і обмін інформацією та отриманим досвідом, для України існує можливість отримати якісно підготовлені кадри для безпекових інституцій. Наприклад, чому б не скористатися нагодою і не влаштувати підготовку кадрів за підтримки Об'єднаного центру передових технологій з кібероборони НАТО, що знаходиться у Таллінні або Оборонного коледжу НАТО в Римі на постійній основі. Але підвищення кваліфікації за кордоном це, безперечно, дуже добре, але було б ще значно краще робити це не покидаючи країни. Тому, мені здається, що розбудові національної кібербезпеки ефективно посприяє створення і реалізація окремих урядових програм, які включали б в себе стипендіальні програми, літні школи, тощо. Це, насправді, може дати гарні можливості і талановитій молоді реалізувати свій потенціал, і державі забезпечити себе «розумами». І НАТО стає важливою складовою на початковому етапі цього процесу, аби передати необхідні навички та знання.

Ще одним фактором, який, мабуть, не береться особливо до уваги, це є діяльність хакерських груп. В Україні їх є чимало і вони активно діють в умовах військової агресії на території України, але, на жаль, самостійно. Так, наприклад, представники Української кібер-армії зламали системи відеоспостереження на окупованих територіях України і через них відслідковують пересування військ та техніки, а також вони блокують російські сайти. Було б доречно за підтримки НАТО консолідувати діяльність цих груп як в загальному укріпленні кібербезпеки України, так і в здійсненні моніторингу інформаційного простору держави локалізовано, адже центр не завжди може не впоратись самостійно у нагляді за периферією.

Безумовно надана Альянсом підтримка Україні свідчить про широкі перспективи відносин в майбутньому. Для України та НАТО важливо продовжувати взаємодію у кіберсфері і не тільки. На тлі розширення та поглиблення багатостороннього співробітництва між Україною та НАТО, покращення кібербезпеки України в контексті посилення її загальної спроможності до опору в різних сферах означатиме закриття іншої вразливої ​​зони європейського кіберпростору та появу додаткового щита, який захистить Європу від Сходу.

1. Стратегія кібербезпеки України від 15 березня 2016 року № 96/2016. *База даних «Законодавство України»*. [↑](#footnote-ref-1)