BRIEFING

European Parliament

Війна Росії проти України: хронологія кібератак

ОГЛЯД

Росія почала війну проти України 24 лютого 2022 року, але російські кібератаки проти України тривають із моменту незаконної анексії Росією Криму у 2014 році, посилившись безпосередньо перед повномасштабним вторгненням у 2022 році. За цей період найбільше постраждали державний, енергетичний, медійний, фінансовий, бізнесовий та некомерційний сектори України. Починаючи з 24 лютого поодинокі російські кібератаки ускладнили розподіл медикаментів, харчових продуктів та надзвичайної допомоги. Ці атаки мали різні наслідки – від перешкоджання доступу до основних послуг до крадіжки даних та поширення дезінформації, у тому числі за допомогою технології «діпфейк». До інших видів зловмисної кібердіяльності належать розсилка фішингових електронних листів, розподілені атаки «відмова в обслуговуванні», використання шкідливого програмного забезпечення для знищення даних, бекдорів, програмного забезпечення для стеження та викрадення інформації.

Організації та уряди в усьому світі не залишилися байдужими до гібридних ризиків, що пов'язані з цією кібердіяльністю. Під проводом ЄС, США та НАТО реалізуються ініціативи, спрямовані на нейтралізацію кіберзагроз та захист життєво важливої інфраструктури. У рамках цих ініціатив ЄС активізував роботу своїх команд швидкого реагування на кіберінциденти (проєкт у межах Постійного структурованого співробітництва (PESCO) у сфері політики безпеки та оборони) для посилення кібероборони України. Неурядові та приватні структури підтримують Україну за допомогою проведення різних заходів для досягнення кіберстійкості. Від початку вторгнення незалежні хакери здійснили значну кількість контратак, які вразили державну, безпекову, банківську та медійну системи РФ.

Європейський парламент закликав посилити допомогу Україні у сфері кібербезпеки та повною мірою використовувати режими кіберсанкцій ЄС проти осіб, організацій та установ, відповідальних за різні кібератаки на Україну або причетних до них.

У ЦЬОМУ БРИФІНГУ

ДСЄП | Дослідницька служба Європейського парламенту

Автор: Якуб Пшетачник із Сімоною Тарповою
Дослідницька служба євродепутатів

PE 733.549 – жовтень 2022 року

UK

Загальна інформація

Принаймні з 2014 року Україна постійно зазнає російських кібератак. Як зазначається в матеріалі *Politico*, тисячі атак відбуваються щомісяця, що робить Україну «ідеальною пісочницею для тих, хто хоче випробувати нову кіберзброю, тактику та інструменти». Починаючи з 24 лютого 2022 року, атаки мали обмежений масштаб, а очікувана, проте невдала, атака на електромережі відбулася лише протягом другого місяця війни. Експерти висловлюють різні припущення щодо причини такої «показової відсутності» кібератак. Пояснення варіюються від високого рівня захисту української інформаційно-технологічної (IT) мережі до залежності російських збройних сил від української IT-інфраструктури. Деякі експерти зазначають, що російські наступальні кіберможливості могли бути переоцінені, натомість інші припускають, що, можливо, Росія просто вичікує слушного моменту для проведення масованих атак. Масштабна кібератака може швидко поширитися й на інші країни. 21 березня 2022 року президент США Джо Байден закликав керівників бізнесу в США зміцнювати свої кібероборонні можливості, підкресливши, що використання Росією її повного спектра кіберможливостей становить ризик як для України, так і для інших країн. ЄС вжив низку заходів для підтримки кіберстійкості України та працює над зміцненням власної кіберстійкості.

Атаки з 24 лютого 2022 року

Після початку війни Росії проти України серед перших прикладів кібервійни були: атака на системи зв'язку газети «Kyiv Post» та супутникову мережу «KA-SAT» за годину до вторгнення (24 лютого), атака IssacWiper на урядові вебсайти (25 лютого), кібератака на пункт прикордонного контролю з метою перешкоджання виїзду біженців до Румунії (25 лютого) та атаки на цифрову інфраструктуру України, що призвело до блокування доступу до фінансових послуг та енергетичних ресурсів (28 лютого). 10 травня верховний представник ЄС засудив атаку проти KA-SAT, яка призвела до перебоїв зі зв'язком для приватних осіб та державних і комерційних структур України. Верховний представник назвав це «ще одним черговим прикладом безвідповідальної поведінки Росії в кіберпросторі», додавши, що кібератаки, націлені на Україну, «можуть поширитися на інші країни та спричинити системні наслідки, загрожуючи безпеці європейських громадян». У березні продовжилися кібератаки з використанням шкідливого програмного забезпечення на урядові та фінансові сайти, а також на неурядові, благодійні та гуманітарні організації, що перешкоджало розповсюдженню медикаментів, харчових продуктів та надзвичайної допомоги. Крім того, здійснювалися фішингові атаки на громадян і державні служби, а також атаки на постачальників телекомунікаційних послуг, що призводило до порушення функціонування українських мереж. 14 березня шкідливе програмне забезпечення CaddyWiper, як повідомляється, проникло в системи кількох українських організацій державного та фінансового сектору. Через два дні в ефірі одного з українських телеканалів з'явилося неправдиве повідомлення, нібито Президент України Володимир Зеленський закликав населення до капітуляції. Крім того, діпфейкове відео із Зеленським було поширено через один з Telegram-каналів.

Кібератаки на Україну з кінця березня включають фішингові електронні листи, націлені на уряд і збройні сили (17 березня) та різні організації (18 березня), а також використання бекдору LoadEdge для встановлення програмного забезпечення для стеження (20 березня). Кібернапади на сайти Укртелекому та WordPress спричинили перебої зі зв'язком та обмеження доступу до фінансових та урядових сайтів (28 березня). 30 березня за допомогою викрадача інформації MarsStealer було отримано доступ до облікових даних українських громадян та організацій.

Подібним способом у квітні хакери витягнули конфіденційну інформацію та облікові дані користувачів в українських урядових установах (2 та 7 квітня) та медіаструктурах (7 квітня). Вони також заволоділи банківськими та платіжними даними громадян за допомогою троянської програми (14 квітня) та шахрайського опитування через сторінки в соціальних

мережах (19 квітня). Інші кібератаки мали на меті заподіяти шкоду населенню. Одним із прикладів таких атак була спроба перешкодити роботі електростанцій та припинити постачання електроенергії мільйонам людей (8 квітня). У результаті останньої атаки вдалося зупинити роботу української поштової служби під час випуску серії поштових марок, присвячених війні (22 квітня).

У травні воєнні дії супроводжувалися кібератаками на урядові сайти, телекомунікаційні послуги та інфраструктуру. Наприклад, атака на Одеську міську раду відбулася під час ракетного обстрілу житлових кварталів міста (7 травня). Хакери також здійснили розподілену атаку «відмова в обслуговуванні» (DDoS-атаку) на деяких українських телекомунікаційних операторів із метою фільтрації та перенаправлення інтернет-трафіку на окуповані території (9 травня).

Попередні атаки у 2022 році

На початку 2022 року різко зросла кількість кібератак. Наприклад, 13 січня компанія Microsoft повідомила, що було виявлено шкідливе програмне забезпечення, націлене на уряд України та декілька некомерційних та IT-організацій. Наступного дня під тимчасовим контролем хакерів опинилися 70 урядових сайтів, зокрема сайти Кабінету Міністрів, міністерств оборони, закордонних справ, освіти та науки. Міністерство цифрової трансформації України поклало відповідальність за цю атаку на Росію.

У середині лютого DDoS-атака на кілька годин повалила сайти кількох державних установ, банків і радіостанцій. Кілька країн звинуватили Росію в тому, що вона розпочала атаку, щоб посіяти серед українців паніку і спричинити розгубленість. 23 лютого ті самі сайти, у тому числі сайт Кабінету Міністрів та кількох міністерств знову зазнали атак. Крім того, проти 100 організацій із фінансового, IT та авіаційного секторів було запущено шкідливе програмне забезпечення для знищення даних HermeticWiper.

Атаки в період 2016–2021 років

У період із 2016 до 2021 року кібератаки на Україну значно посилилися. Найпомітнішою з них був запуск шкідливого програмного забезпечення NotPetya через бухгалтерське програмне забезпечення в червні 2017 року — найбільш руйнівна, як вважається, кібератака в історії. NotPetya вразив Чорнобильську атомну електростанцію та орієнтовно 13 000 пристроїв, якими користувалися державні установи, банки, поштові служби, газети, об'єкти транспортної інфраструктури та підприємства. Були знищені накопичувачі комп'ютерів, що унеможливило відновлення даних після шифрування вірусом. Це шкідливе програмне забезпечення спричинило глобальні наслідки, вразивши 65 країн і орієнтовно 50 000 систем, зокрема європейські та американські компанії FedEx, Maersk та Merck, і завдавши збитків на суму понад 10 мільярдів доларів США.

У 2018 та 2021 роках відбулися дві спроби масштабних кібератак. Перша була спрямована на Аульську хлороперелівну станцію, продукція якої використовується у 23 областях України, а друга — на вебсайти Служби безпеки України. Атака на систему електронної взаємодії, яку використовували органи виконавчої влади, виявилася невдалою, але завдала шкоди роботі системи.

Атаки у 2014 і 2015 роках

13 березня 2014 року, за три дні до референдуму щодо статусу Криму, Росія здійснила восьмихвилинну DDoS-атаку, спрямовану на дестабілізацію українських комп'ютерних мереж і комунікацій, щоб відвернути увагу громадськості від присутності російських військ у Криму. У травні 2014 року, незадовго до президентських виборів в Україні, проросійська група хактивістів здійснила низку кібератак із метою маніпулювання голосуванням. Хакери «КіберБеркута», атакуючи Центральну виборчу комісію, проникли в мережу та видалили

файли, намагаючись змінити результати виборів. Атака не вдалася, оскільки шкідливе програмне забезпечення було видалено за 40 хвилин до початку виборів (25 травня). Проте хакерам вдалося затримати підрахунок голосів.

Протягом наступних кількох років українська влада пов'язала з Росією дві кібератаки на електромережі. 23 грудня 2015 року від чергової DDoS-атаки постраждали кол-центри та мережа трьох енергорозподільчих компаній. У результаті понад 230 000 споживачів у Західній Україні зазнали відключень електроенергії від однієї до шести годин. Крім того, групі Sandworm, фінансованій, ймовірно, Росією, вдалося завадити роботі систем 16 електричних підстанцій. Подібна кібератака була здійснена у 2016 році. Перебої на київській підстанції призвели до припинення подачі електроенергії, що тривало одну годину, але спроба повністю вивести обладнання з ладу не вдалася.

Рис.1. Хронологія кібератак на Україну

Джерело: дані,зібрані ДСЄП; графіка: Люсіль Кіллмаєр.

Протидія кібератакам

Хоча Україна має обмежені можливості протидії кібератакам, вона намагається посилити свою кібероборону за допомогою зовнішньої допомоги. Уряд залучив волонтерів зі всього світу, щоб сформувати ІТ-армію. У відповідь на російські атаки ІТ-команда, створена Міністром цифрової трансформації, здійснила кілька DDoS-атак та атак wiper. Перші порушують роботу серверів, штучно створюючи великий обсяг трафіку, а другі призводять до видалення даних. Серед цілей атак — уряд Росії, медіасистеми, фінансові установи, оборонні об'єкти, електромережі та залізниці.

У рамах протидії кібератакам незалежні хакери з усього світу викрали та оприлюднили російські урядові та фінансові дані, у тому числі електронні листи, інформацію про банківську діяльність, виробництво енергії та пропагандистські кампанії, а також дані про військовослужбовців та агентів Федеральної служби безпеки (ФСБ). Повідомляється, що ця конфіденційна інформація потім передається міжнародним активістам, щоб покарати Росію за її злочини в Україні. Вторинним ефектом останніх дій хакерів є їхній успіх стосовно створення хаосу в російських кіберсистемах і руйнування переконань про неприступність кібероборони Росії.

Реакція ЄС та міжнародної спільноти

ЄС підтримав Україну в протидії кібератакам, започаткувавши кібердіалог між ЄС та Україною (червень 2021 р.), посиливши оперативну спроможність телекомунікаційних служб України та допомагаючи в боротьбі з дезінформацією. Крім того, на прохання українського уряду ЄС уперше в оперативному контексті активував команди швидкого реагування на кіберінциденти у межах PESCO (лютий 2022 р.). Експерти з кібербезпеки надаватимуть допомогу у виявленні, розпізнаванні та мінімізації загроз. Раніше, у липні 2020 року, ЄС запровадив перші в історії санкції проти організаторів кібератак, у тому числі NotPetya. Нещодавно схвалений Стратегічний компас має на меті посилити кіберстійкість ЄС (запропонувавши, зокрема, новий закон про кіберстійкість і подальше зміцнення інструментарію кібердипломатії) та східних партнерів ЄС завдяки співпраці у сфері протидії гібридним і кіберзагрозам, а також дезінформації.

У лютому 2022 року команда кіберкомандування США допомагала командам швидкого реагування на кіберінциденти шукати активні загрози. США зі свого боку з 2017 року виділили 40 мільйонів доларів на розвиток ІТ-сектору України. Країни-члени НАТО також інвестують у кібероборону України через обмін інформацією та підтримку на місцевому рівні. У березні 2022 року Україна стала учасником-контрибутором Об'єднаного центру передових технологій з кібероборони НАТО. Крім того, приватні компанії, як-от Microsoft, Amazon і Google, під час вторгнення допомагають Україні у виявленні кібератак та протидії їм. Європейський центр передового досвіду з протидії гібридним загрозам з початку війни також посилив співпрацю з Україною, спостерігаючи за ситуацією та організовуючи навчання.

Позиція Європарламенту

У резолюції від 1 березня 2022 року Парламент закликав до негайного та повного впровадження всіх рішень, які посилять внесок ЄС у зміцнення обороних спроможностей України, у тому числі у сфері кібербезпеки. Крім того, Парламент закликав ЄС, НАТО та інших зацікавлених партнерів посилити допомогу Україні у сфері кібербезпеки. Євродепутати закликали до повного застосування режиму кіберсанкцій ЄС проти фізичних, юридичних осіб та установ, відповідальних за кібератаки проти України або причетних до них.

У минулому Парламент неодноразово наполягав на тому, щоб ЄС надав Україні допомогу в протидії гібридним загрозам (наприклад, кібератакам та дезінформації); Парламент також підтримав збільшення інвестицій у кібербезпеку України. У своїй рекомендації від 8 червня 2022 року Парламент закликав до швидкого впровадження Стратегічного компаса, у тому

числі його кібераспектів; у тексті також рекомендувалося, щоб Рада ЄС та верховний представник ЄС із закордонних справ і політики безпеки / заступник Голови Комісії повною мірою використовували режими кіберсанкцій ЄС проти фізичних осіб, суб'єктів та органів, відповідальних за різні кібератаки або причетних до різних кібератак, спрямованих на Україну.

Резолюція Парламенту від 8 червня 2022 року про безпеку в регіоні Східного партнерства (СП) та роль спільної безпекової й оборонної політики містить кілька конкретних пропозицій. У резолюції визнається, що стратегічний інтерес ЄС може полягати у включенні асоційованих країн СП (країн, які мають угоди про асоціацію з ЄС, а саме України, Молдови та Грузії) в окремі проєкти PESCO, особливо у сферах гібридних загроз та кібербезпеки. У резолюції міститься заклик до вивчення варіантів для посилення кіберспроможностей країн Східного партнерства, а також пропонується започаткувати цивільні кібермісії. Щодо Консультативної місії Європейського Союзу (КМЄС) в Україні, то в резолюції наголошується на необхідності розширення її мандату, включивши до нього питання протидії гібридним загрозам, стратегічної комунікації, цифрових технологій та кібербезпеки.

ПОСИЛАННЯ НА ОСНОВНІ ДЖЕРЕЛА

A Strategic Compass for Security and Defence, EEAS, March 2022.

Activation of first capability developed under PESCO points to strength of cooperation in cyber defence, EDA, February 2022.

Antoniuk, D., *DDoS attacks hit Ukrainian government websites*, *The Record*, February 2022.

Attribution to Russia of malicious cyber activity against Ukraine, Australian government, February 2022.

Brumfield, C., *Russia-linked cyber-attacks on Ukraine: A timeline*, CSO, April 2022.

Cerulus, L., *How Ukraine became a test bed for cyberweaponry*, *Politico*, February 2019.

Cerulus, L., *Ukraine is getting pummeled with cyber-attacks. What's the West to do?*, *Politico*, February 2022.

Cimpanu, C., *Hackers deface Ukrainian government websites*, *The Record*, January 2022.

Cimpanu, C., *Ukraine reports cyber-attack on government document management system*, Zdnet, February 2021.

Clayton, M., *Russia Hammers Ukraine With Massive Cyber-Attack*, *Business Insider*, March 2014.

Deputy Secretary General stresses NATO will continue to increase Ukraine's cyber defences, NATO, January 2022.

EU imposes the first ever sanctions against cyber-attacks, Council of the European Union, July 2020.

Fendorf, K. and Miller, J., *Tracking Cyber Operations and Actors in the Russia-Ukraine War*, Council on Foreign Relations, March 2022.

Harding, L., *Ukraine hit by 'massive' cyber-attack on government websites*, *The Guardian*, January 2022.

Hern, A., *Ukrainian blackout caused by hackers that attacked media company, researchers say*, *The Guardian*, January 2016.

Holland, Steve. and Pearson J., *US, UK: Russia responsible for cyber-attack against Ukrainian banks*, Reuters, February 2022.

Hybrid CoE continues to work to support European security and Ukraine, Hybrid CoE, March 2022.

Ishak, N., *Is Russia holding back from cyberwar?*, Vox, March 2022.

Kagubare, I., *US, EU cyber investments in Ukraine pay off amid war*, *The Hill*, March 2022.

Madiega, T., *Russia's war on Ukraine: The digital dimension*, EPRS, March 2022.

Madnick, S., *What Russia's Ongoing Cyber-attacks in Ukraine Suggest About the Future of Cyber Warfare*, *Harvard Business Review*, March 2022.

Menn, J., *Hacking Russia was off-limits. The Ukraine war made it a free-for-all*, *Washington Post*, May 2022.

Miller, M., *Despite years of preparation, Ukraine's electric grid still an easy target for Russian hackers*, *Politico*, February 2022.

NotPetya, CyberLaw, May 2019.

NotPetya, Five Facts to Know About History's Most Destructive Cyber-attack, HYPR, June 2017.

Resolution of 1 March 2022 on the Russian aggression against Ukraine (2022/2564(RSP)), European Parliament, 1 March 2022.

Resolution of 11 February 2021 on the implementation of the EU Association Agreement with Ukraine (2019/2202(INI)), European Parliament, 11 February 2022.

Scroxton, A., *Ukraine joins Nato cyber knowledge hub*, *Computer Weekly*, March 2022.

UK assesses Russian involvement in cyber attacks on Ukraine, Foreign, Commonwealth & Development Office and National Cyber Security Centre, United Kingdom, February 2022.

Ukraine accuses Russian networks of new massive cyber attacks, Reuters, February 2022.

Ukraine power cut 'was cyber-attack', BBC, January 2017.

Ukraine: Timeline of Cyber-attacks on critical infrastructure and civilian objects, CyberPeace Institute, April 2022.

Vazquez, M., Judd D., Lyngaas S. and Cohen, Z., *Biden warns business leaders to prepare for Russian cyber attacks*, CNN Politics, March 2022.

What is a DDoS attack?, Cloud Flare.

Wiper Attacks, Firewalls Security Blog.

Wolff, J., *Why Russia Hasn't Launched Major Cyber Attacks Since the Invasion of Ukraine*, *Time*, March 2022.

ВІДМОВА ВІД ВІДПОВІДАЛЬНОСТІ ТА АВТОРСЬКЕ ПРАВО

eprs@ep.europa.eu (контакт)

www.eprs.ep.parl.union.eu (інтранет)

www.europarl.europa.eu/thinktank (інтернет)

http://epthinktank.eu (блог)