РАДА ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

Державна служба спеціального зв'язку та захисту інформації України

КІБЕРАТАКИ, АРТИЛЕРІЯ, ПРОПАГАНДА

Загальний аналіз вимірів російської військової агресії

2022

ЗМІСТ

Автори дослідження відстежили координацію ракетних атак на місцеве самоврядування та кібератак на сервіси громади, чітке узгодження ракетних та кібератак на медіа та центри зв'язку, підготовку та реалізацію кібератак на інституції, які допомагають Україні (логістика, підтримка біженців та навіть культурні акції) тощо.

- Російська війна проти України має багато вимірів: конвенційний, економічний, кібер, інформаційний, культурний. Лише розуміння взаємодії цих вимірів дозволяє адекватно оцінити дії держави-агресора.

- Перша в світі масштабна кібервійна не продемонструвала нових "видів озброєння" в кіберпросторі. Всі атаки відбуваються за допомогою відомих раніше механізмів. Застосовувані Росією типи атак вже давно категоризовані і мають зрозумілі рецепти протистояння.

- Кібератаки повною мірою відповідають загальній військовій стратегії Росії. Кібератаки часто узгоджуються з іншими атаками: конвенційними на полі бою, а також з інформаційно-психологічними та пропагандистськими операціями. Найбільш яскраво це проявилося восени і взимку 2022 року, коли після серії кібератак на енергетику, РФ запустила декілька хвиль ракетних атак на енергетичну інфраструктуру та одночасно розпочала пропагандистську кампанію з метою перекласти відповідальність за наслідки (відключення електроенергії) на українські органи державної влади, місцеве самоврядування чи великий український бізнес.

- Таке узгодження атак у різних вимірах агресії проявляється дуже часто, хоч координація не є безумовним правилом.

- Доктринально РФ часто розглядає кібер та інформаційний виміри як єдиний домен "інформаційного протиборства". Це протистояння може включати або суто інформаційні кампанії, або ж щось складніше. Проте метою у будь-якому разі є інформаційна маніпуляція, до якої природно вразливі всі демократичні режими.

- Кібератаки, як і конвенційні атаки РФ, не визнають жодних правил — під ударом інфраструктура, гуманітарні організації, приватні та державні компанії. Російські хакери не приймають обмежень та не визнають кордонів, атакуючи різні держави, якщо вони допомагають Україні.

- Немає підстав вважати, що інтенсивність кібератак буде зменшуватися. Питання лише в тому, на чому вони будуть фокусуватися.

- Дослідження демонструє, що для ефективної протидії Росії та іншим авторитарним режимам необхідно:

  — адаптувати воєнні доктрини до сучасних викликів, використовуючи уроки українсько-російської війни для прогнозування і моделювання;

  — змінити правові підходи до визначення агресії, значно розширивши відповідні юридичні тлумачення;

  — обмежувати авторитарним режимам доступ до сучасних технологій шляхом посилення санкції, включаючи санкції проти найважливіших сфер економіки таких режимів.

Багатовимірність російської агресії проявила себе ще до повномасштабного вторгнення. Прикладами є так звані “економічні війни” і потужні ворожі пропагандистські кампанії. Але саме з 24 лютого 2022 року кореляція між різними видами атак набула системного характеру.

Ця тактика відпрацьовувалася Росією у попередніх збройних конфліктах (наприклад, під час агресії проти Грузії)[1]. Тобто, якщо її не вивчати і ефективно їй не протистояти — ця тактика буде використана в майбутньому проти інших держав. Якщо Росія не отримає гідної відповіді на всі свої агресивні дії сьогодні, завтра вона повернеться з ще більш зухвалими атаками, які не будуть обмежуватися Україною, чи навіть нашим регіоном.

Необхідність захисту від багатовимірної агресії створює запит на:

— багатовимірну інформацію та багатовимірні (а не ізольовані) прогнози;

— багатовимірні стратегії протидії атакам;
— багатовимірну юридичну відповідальність агресора.

> Окреме важливе питання — необхідність повної економічної ізоляції держави-агресора. Перш за все, йдеться про обмеження доступу до всіх сучасних технологій. Адже всі вони використовуються Росією як зброя.

На жаль, поки що міжнародне співтовариство не має жодного з цих компонентів, необхідних для успіху. Більшість напрацювань достатньо не систематизовані. Тому необхідно змінювати всі підходи вже зараз.

Прийнято вважати, що кібератаки — зброя майбутнього. Проте війна в Україні довела, що це майбутнє вже настало. Оборонні доктрини та міжнародне право мають швидко адаптуватися.

Багатовимірність війн — новий безпековий виклик (який можна було спрогнозувати, проте до якого все одно належним чином не готувалися). Немає сумнівів, що Росія — не єдина загроза для міжнародної безпеки. Інші авторитарні режими робитимуть висновки і використовуватимуть ці підходи в майбутньому.

Як би це парадоксально не звучало, але конвенційні атаки з часом можуть поступатися у своїх негативних наслідках кібератакам. Уже сьогодні на прикладі російської агресії можна побачити, що хакери атакують будь-які об'єкти. Проте у пріоритеті:

— державні інституції (як центри ухвалення рішень, відповідальні за підтримку стабільності всередині країни);

— цивільна і енергетична інфраструктура (тому що Росія — терорист, який хоче збільшувати страждання цивільних, не маючи успіхів та полі бою);

— медіа і зв'язок (ці атаки посилюють російську пропаганду, яка є перевіреною зброєю путінського режиму).

Основна мета російських хакерів із початком війни змінилась. Якщо напередодні вторгнення та в перший місяць війни кібератаки були скеровані на комунікації, які мали обмежити функціональність військових і влади в Україні, то після перших невдач на фронті російський агресор сконцентрувався на завданні максимальної шкоди цивільному населенню. Ця зміна стратегії простежується у всіх вимірах агресії. Атака на енергетичну інфраструктуру — найкращий приклад. Ця атака була гарно продуманою і з точки зору часу, і з точки зору об'єктів. Адже саме під час похолодання сталися перші масовані удари на енергетичну інфраструктуру для того, щоб завдати додаткового тиску саме на цивільне населення, яке адаптується до незручностей набагато гірше, ніж військові.

Отже, основне завдання як для України, так і для наших міжнародних партнерів — виявити всі кореляції у діях РФ, а також розробити всеохоплюючу стратегію протидії цим атакам.

ВЗАЄМОЗВ'ЯЗКИ МІЖ ПОДІЯМИ РІЗНИХ ВИМІРІВ РОСІЙСЬКОЇ АГРЕСІЇ

Конвенційному повномасштабному вторгненню передувало посилення масштабних кібератак.

15 лютого, російські хакери розпочали найпотужнішу в історії України DDoS-атаку, яка, серед іншого, була спрямована на фінансовий сектор (DDoS-атака на 15 банківських сайтів, сайтів з доменом gov.ua, також сайтів Міноборони, Збройних сил та Міністерства з питань реінтеграції тимчасово окупованих територій, що тривала близько 5 годин). 23 лютого, перед початком російського вторгнення в Україну було повторно атаковано низку державних сайтів та банківських сайтів. За даними державного оператора системи передачі електроенергії Укренерго, пік кібератак проти енергетичного сектора припав на момент підключення української електромережі до європейської ENTSO-E (тобто на 23-24 лютого). Під час деяких атак на Укренерго російські хакери навіть не намагались ховати своє походження і використовували російські IP-адреси для сканування мережі державного енергетичного оператора.

> Таким чином, кібератаки були покликані збільшити хаос від конвенційного вторгнення, зменшити керованість країни, а також нанести шкоду критичній інфраструктурі.

ЛЮТИЙ

24 лютого

Масштабна кібератака порушила супутниковий доступ до Інтернету.[2] Хакери відключили модеми, які зв'язуються із супутником KA-SAT компанії Viasat, що забезпечують доступ в Інтернет для клієнтів в Європі, включаючи Україну.[3]

24 лютого

24 лютого російські війська розпочали широкомасштабне вторгнення на територію України, що супроводжувалося ракетним обстрілом цивільних та військових об'єктів.

Із початком конвенційного повномасштабного вторгнення також посилилися інформаційні атаки. [4] Зокрема, до 16 лютого інформаційних атак майже не фіксувалося. З 17 до 23 лютого було незначне збільшення таких атак, а 24 лютого був пік активності – було зафіксовано 23 маніпулятивні кейси (які сіяли паніку, закликали до капітуляції тощо). Висока активність інформаційних атак продовжувала спостерігатися протягом усього березня.

Хакерська атака на службу супутникового інтернету почалася 24 лютого між 05:00 і 09:00, саме в той момент, коли російські війська почали обстрілювати українські міста і заходити на територію країни.

Колишній технолог командування спеціальних операцій США Пабло Брейер сказав, що відключення супутникового інтернет-з'єднання може ускладнити боротьбу України з російськими військами. "*Якщо ви використовуєте сучасні інтелектуальні системи, інтелектуальну зброю, намагаєтеся виконувати загальновійськові маневри, то ви повинні покладатися на ці супутники*", — **уточнив Брейер.**[5]

В подальшому США, Великобританія та Європейський Союз звинуватили Росію у масштабній кібератаці по Україні напередодні повномасштабного вторгнення російських військ, яка була спрямована на мережу супутникового зв'язку. На думку експертів, основною метою, безперечно, були силові структури України, однак у результаті кібератаки також постраждали українські підприємства та приватні особи, які використовують обладнання Viasat. Кібератака також торкнулася об'єктів за межами України. Так, у Німеччині було виведено з ладу майже 6 000 вітряних турбін, робота яких залежала від маршрутизаторів Viasat.[6]

ВИСНОВКИ

1. Потужні кібератаки можуть передувати масштабним конвенційним атакам.
2. Кібератаки використовуються Росією для послаблення України та її здатності ефективно протистояти конвенційній агресії.
3. Державі-агресору байдуже до так званих «супутніх збитків»; кібератаки Росії у війні з Україною створюють загрози для цивільного населення всього світу, перш за все – Європи.
4. Інформаційні атаки супроводжують конвенційну агресію і значно посилюються одночасно зі збільшенням інтенсивності бойових дій.

БЕРЕЗЕНЬ

1 березня

Запущено шкідливе програмне забезпечення DesertBlade проти українських телекомпаній.[7] Київська медіакомпанія стикнулася з деструктивними атаками та викраденням даних.[8]

1 березня

Успішна ракетна атака проти телевишки у Києві[9].

Користуючись тим, що була порушена нормальна робота телебачення, агресор вдався до посилення інформаційних атак[10]. Зокрема, Служба безпеки України спростувала повідомлення, яке ширять у соцмережах, що російські військові встановлюють обладнання мобільного зв'язку, яке нібито може перебивати українські мережі. А Центр протидії дезінформації при РНБО попередив, що окупанти почали інформаційну атаку на жителів України, здебільшого на літніх людей, використовуючи при цьому телефонні дзвінки для поширення панічних настроїв.

ВИСНОВКИ

1. Кібератаки та конвенційні атаки можуть завдаватися одночасно по одному об'єкту.
2. Кібератаки та конвенційні атаки можуть мати на меті здобування переваги в інформаційному просторі (тобто позбавлення цивільного населення доступу до правдивої інформації).
3. Коли конвенційні атаки на засоби доступу до інформації є вдалими (наприклад, коли пошкоджено телевишки, а телекомпанії зазнають кібератак), агресор може посилювати руйнівний ефект шляхом поширення дезінформації й панічних настроїв (телефоном, в Інтернеті тощо).

2 березня

Посольство України в Лондоні зазнало кібератаки через вторгнення Росії в Україну[11].

Початок березня

Пік української активності на міжнародній арені; посольство в Британії опікується багатьма питаннями (від санкцій до гуманітарної допомоги).

1 березня почав діяти потужний пакет санкцій, запроваджених Британією проти Росії за повномасштабне вторгнення[12].

Олівер Пінсон-Роксбург, генеральний директор Bulletproof і Defense.com зазначив: «Кібератака на посольство в Лондоні демонструє, що події в Україні відбуваються не у вакуумі. Підприємства в усьому світі мають бути готові до боротьби із загрозами, що швидко розвиваються, особливо з огляду на нові типи зловмисних програм, які наразі націлені на українські мережі та хакерів». США попередили свої банки, щоб вони починали готуватися до кібератак на тлі суворих санкцій проти Росії. До цього Британія та ЄС опублікували подібні попередження своїм фінансовим установам[13].

ВИСНОВКИ

1. Кібератаки не мають географічних меж і тим самим масштабують війну в Україні до конфлікту без кордонів.

2. Атаки у кіберпросторі можуть бути спрямовані проти успішних дій України на дипломатичному фронті (а також співпадати у часі з рішеннями міжнародних партнерів України щодо посилення санкцій).

16 березня

Червоний Хрест України повідомив про злам свого сайту, який того ж дня було відновлено. На веб-сайті не зберігалися персональні дані бенефіціарів. Постраждала лише інформаційна складова сайту[14].

Через численні воєнні злочини та окупацію значної території України, гуманітарна ситуації стрімко погіршується. Роль Червоного Хреста України зростає. Крім того, напередодні, 14 березня відбулася зустріч керівництва Червоного Хреста України (ТЧХУ) з Делегацією Міжнародний Комітет Червоного Хреста в Україні (МКЧХ)[15]. ТЧХУ виступало своєрідним посередником між МКЧХ та українським урядом (що було особливо важливо на тлі критики МКЧХ, яка лише посилювалася в березні).

Кібератака проти Червоного Хреста супроводжувалася інформаційними атаками[16]. Зокрема, у соцмережах почали поширювати інформацію з посиланням нібито на дані Міжнародного Комітету Червоного Хреста та звіти Міністерства оборони України, що Україна «зазнає колосальних втрат у живій силі». Також почали поширюватися фейки про те, що Червоний Хрест України видає довідки, які дозволяють безперешкодно перетинати кордон.

ВИСНОВКИ

1. Цілями атак Росії стають і міжнародні гуманітарні організації.

2. Геноцидний характер конвенційної війни обумовлює спроби кібератак проти організацій, які могли б зменшити гуманітарну кризу чи страждання цивільного населення.

3. Інформаційні атаки проти міжнародних гуманітарних організацій, які посилюють кібератаки, спрямовані на руйнування іміджу таких організацій, зменшення

довіри цивільного населення (яке, відповідно, втрачатиме можливість отримати гуманітарну допомогу через недовіру чи небажання звертатися до відповідних організацій).

28 березня

Хакери здійснили потужну кібератаку на інфраструктуру одного з найбільших українських провайдерів – Укртелеком. Укртелеком спостерігає зростання кількості кібератак на свою інфраструктуру від самого початку вторгнення в Україну. Атака, яка відбулась 28 березня, була потужною та складною. Вона відбувалась у два етапи. Першою була стадія дослідження (discovery). Другим етапом стала кібератака 28 березня, під час якої хакери намагались вивести з ладу обладнання та сервіси компанії, а також отримати контроль над мережею та обладнанням Укртелекому. Другий етап кібератаки був зафіксований протягом 15 хвилин від початку. IT-фахівці Укртелекому невідкладно вжили заходів з протидії кібератаці. Доступ до інтернету для клієнтів почали відновлювати ввечері 28 березня. Наступного дня сервіси Укртелекому стали майже повністю доступними для всіх споживачів.

Наприкінці березня конвенційна війна характеризувалася двома тенденціями. З одного боку, продовжувалася й загострювалася активна фаза війни. З іншого боку, російському керівництву вже стали очевидними великі невдачі на фронті (перш за все – в контексті провалу плану захоплення Києва).

ВИСНОВКИ

1. Потужні кібератаки можуть використовуватися як певний компенсатор невдач у конвенційній війні.

2. Зв’язок — основна ціль ворога, атаки проти якої можуть здійснюватися у будь-який момент.

3. Росія здатна до складних багатокрокових кібератак, проте такі атаки можуть бути організовані зовсім не часто (через великий ресурс, необхідний для підготовки).

КВІТЕНЬ

8 квітня

Кібератака на об'єкти енергетики України[17].

За словами українських чиновників, атака мала початися ввечері 8 квітня, коли громадяни поверталися додому з роботи, і могла унеможливити їхнє повсякденне життя або отримання доступу до інформації про хід війни. Якби атака була успішною, вона позбавила б електроенергії приблизно два мільйони людей і ускладнила б відновлення електропостачання[18].

8 квітня

Окупанти завдали ракетного удару по залізничному вокзалу Краматорська. Удар призвів до численних людських жертв.

ВИСНОВКИ

1. Держава-агресор може комбінувати конвенційні атаки і кібератаки для посилення панічних атак серед цивільного населення.

2. Воєнні злочини можуть скоюватися як конвенційно, так і в кіберпросторі. Тероризм РФ також є багатовимірним.

11 квітня

Кібератаки на три європейські компанії вітрової енергетики. Хакери намагалися спричинити хаос у секторі, який збирається отримати вигоду від зусиль, спрямованих на зменшення залежності від російської нафти та газу. Час атак свідчить про потенційні зв'язки з прихильниками вторгнення Росії в Україну.

За повідомленням Deutsche Windtechnik AG, постраждали системи дистанційного керування для приблизно 2000 вітряних турбін у Німеччині, відновлення підключень до дистанційного моніторингу даних до вітрових турбін було здійснено через 1-2 дні. Діяльність з оперативного обслуговування клієнтів відновилася 14 квітня (через 3 дні після атаки) і працювала лише з незначними обмеженнями.

11 квітня

Заяви ряду держав про готовність відмовитися від російської нафти і газу:

- Фінляндія готова відмовитися від газу і нафти з Росії.
- Франція готова ухвалити рішення про заборону на російську нафту.
- Японська енергетична компанія Kyushu Electric Power відмовляється від закупівель російського вугілля. А японські страхові компанії не укладатимуть контракти з компаніями, що працюють у РФ.

ВИСНОВКИ

1. Енергетична сфера є ключовою для російської економіки; крім того, це основний елемент залежності Європи від РФ. Тому хакерські атаки спрямовуються на зелену енергетику, яка може похитнути позиції Росії в енергетичній сфері.
2. Хакерські атаки можуть бути відповіддю на політичні заяви держав про готовність відмовлятися від російського газу і нафти.
3. Хакерські атаки також спрямовані на те, щоб продемонструвати “крихкість” та нестабільність зеленої енергетики.

14 квітня

У CERT-UA повідомили про масове поширення серед громадян України шкідливих XLS-документів. Після відкриття вони завантажували і спочатку запускали «GzipLoader», а потім зловмисне програмне забезпечення «IcedID». “IcedID” також відомий як “BankBot”, банківський троян, який може збирати облікові дані користувача.

14 квітня

Іноземні онлайн-магазини та їхні банки-еквайєри блокують платежі за випущеними в РФ картками китайської UnionPay[20].

ВИСНОВКИ

1. Росія здатна робити нескладні, проте швидкі дзеркальні кібератаки.
2. “Дзеркальні кібератаки” можуть охоплювати будь-яку сферу, зокрема і банківську.

ТРАВЕНЬ

1 травня

Кібератаки на сервіси онлайн-продажу та лінію підтримки Укрзалізниці[21].

Протягом тижня атак від російських і проросійських угрупувань також зазнали České dráhy (Чеська залізниця), деякі регіональні аеропорти та сервер державної служби Чехії, державні ресурси Естонії, Молдови та Румунії, а також компанія Coca-Cola.

1 травня

Повідомляють про стягнення окупантами до прикордонних з Україною районів залізничними шляхами знятого зі зберігання у Західному, Центральному, Східному військових округах та північному флоті озброєння і військової техніки[22].

ВИСНОВКИ

1. Кібератаки можуть здійснюватися проти об'єктів, які синхронно використовуються державою-агресором для власних потреб.

2. Під час активізації конвенційних операцій посилюються кібератаки на залізницю, оскільки вона слугує як об'єктом для евакуації та перевезення гуманітарних вантажів, так і важливою транспортною артерією, яка забезпечує військо (зокрема, й іноземними поставками).

3. Кіберагресія Росії здійснюється не лише проти України, РФ атакує й інші демократичні країни ЄС із метою політичного тиску на уряди, а також з метою зменшення допомоги Україні.

9 травня

Кібератака на провідні телекомунікаційні компанії України. кібератака на провідні телекомунікаційні компанії України[23].

9 травня

Масований ракетний обстріл Одеси. Голова Євроради Шарль Мішель під час візиту до Одеси був змушений піти у бомбосховище через повітряну тривогу і високу ймовірність ракетного удару[24].

ВИСНОВКИ

1. У дати, які є важливими для російської пропаганди, є вірогідними атаки на комунікаційні системи. Кібератаки можуть використовуватися для посилення пропаганди.

2. І ракетні обстріли, і кібератаки використовуються як помста за успіхи України, а також як інструмент відволікання уваги від невдач РФ. Наприклад, традиційний парад у Москві був менш помпезним, у ньому не брала участі авіації. Путінський режим використовує різнорівневі атаки проти України для того, щоб продемонструвати свої успіхи і силу російським громадянам.

13 травня

Масова кібератака на мережі львівської мерії.

Під час російської кібератаки на мережі мерії викрали частину робочих файлів міста та опублікували її на ворожих телеграм-каналах[25].

15 травня

Обстріл Львова.

4 ракети влучили у військовий об'єкт у Яворівському районі.
Його повністю знищено[26].

ВИСНОВКИ

1. Конвенційні й кібератаки можуть повністю співпадати географічно.
2. Одночасні кібератаки і ракетні обстріли одного міста використовуються для посилення паніки і збільшення негативних наслідків для цивільного населення.
3. Кібератаки проти місцевих органів влади, які передують обстрілам, можуть використовуватися для дискредитації українських інституцій.

14-15 травня

Італійські правоохоронці відбивали кібератаки проросійських груп під час пісенного конкурсу «Євробачення» у Турині, де перемогу здобули українські виконавці.

Український гурт Kalush Orchestra переміг у фіналі «Євробачення-2022» з піснею «Стефанія». Після виступу гурт зі сцени звернувся до світу із закликом врятувати захисників Маріуполя із «Азовсталі» (у цей час оборона Азовсталі тривала).

ВИСНОВКИ

1. Росія здійснює кібератаки для нанесення іміджевих втрат важливим для Європи культурним проєктам (тобто це прояв гуманітарної агресії).

2. Кібератаки також можуть бути прогностичними, тобто протидіяти можливим українським інформаційним кампаніям. Було очевидно, що в України великі шанси перемогти. Зважаючи на те, що порятунок захисників Азовсталі був пріоритетом для українського суспільства, акції на підтримку українських військовослужбовців були прогнозованими. Тому держава-агресор використовує всі засоби (зокрема - і кібератаки) для недопущення привернення уваги до її воєнних злочинів.

ЧЕРВЕНЬ

2 червня

Кібератака на державні організації України з використанням шкідливої програми Cobalt Strike Beacon та експлойтів до вразливостей CVE-2021-40444 і CVE-2022-30190.

Урядовою командою реагування на комп'ютерні надзвичайні події України (CERT-UA) виявлено файл "зміни оплата праці з нарахуваннями.docx", що розповсюджувався серед державних організацій України засобами електронної пошти (ураження комп'ютера шкідливою програмою Cobalt Strike Beacon).

1-2 червня

Відстежується активність українських посадових осіб з візитами, промовами, коментарями, виступами тощо (активність під час Всеукраїнського форуму до Дня захисту дітей).

ВИСНОВКИ

1. Нескладні, проте масові кібератаки проти державних службовців використовуються державою-агресором, щоб зменшити медійну активність українських державних органів.

2. Агресор може прораховувати, що у певні дати (міжнародні свята, пам'ятні дні тощо) українські посадовці робитимуть багато заяв, відбуватимуться адвокаційні кампанії тощо. Тому до цих дат готуються кібератаки.

10 червня

Масована кібератака на медійні організації України з використанням шкідливої програми CrescentImp.

Відбулося масове розсилання електронних листів, зокрема, серед медійних організацій України (радіостанції, газети, новинні агенції та інші) з темою "СПИСОК посилань на інтерактивні карти". Встановлено більше 500 електронних адрес отримувачів.

Приблизно у цей час відбувається низка важливих міжнародних подій:

- Засідання Парламентського Комітету Асоціації Україна-ЄС.
- Парламентський Комітет Асоціації Україна-ЄС проводить дводенне засідання у Страсбурзі.[28]
- Європарламент закликає європейські інституції надати Україні статус кандидата на вступ до ЄС.[29]
- Саміт ЄС: євродепутати вітають посилення санкцій проти Росії.[30]

ВИСНОВКИ

1. "Міжнародний фронт" - важливий елемент успіху України. Саме тому кібератаки проти медіа можуть відбуватися у періоди, коли запланована активна міжнародна діяльність.
2. Міжнародна адвокація неможлива без медійного висвітлення. Тому кібератаки проти медіа використовуються РФ для зменшення впливу відповідних міжнародних подій.

20 червня

Кібератака групи UAC-0098 на об'єкти критичної інфраструктури України.

Виявлено шкідливий документ "Накладення штрафних санкцій.docx", відкриття якого призведе до завантаження HTML-файлу та виконання JavaScript-коду (CVE-2022-30190), який забезпечить завантаження та запуск шкідливої програми Cobalt Strike Beacon.

20-21 червня

Масові авіаудари по цивільний інфраструктурі країни:

- Авіаудари по об'єктах інфраструктури неподалік Богородичного, Устинівки, Гірського та Лисичанська, в районі Нью-Йорка; Щербаків (Курахівський напрямок); в районі Очакова та Куцуруба на Миколаївщині. [31]
- Удар по депо Харківському метрополітену. [32]
- Руйнування цивільних об'єктів Донеччини. [33]
- Руйнувань зазнали 54 цивільних об'єкти – житлові будинки та інфраструктура. [34]
- Вдень 21 червня ворог атакував Індустріальний район Харкова. [35]

ВИСНОВКИ

1. Атаки на цивільну інфраструктуру можуть одночасно відбуватися у кількох вимірах, зокрема у кібер та конвенційному.
2. Кібератаки використовуються державою агресором, щоб примножити негативні наслідки від ракетних обстрілів та збільшити страждання цивільного населення.

24 червня

Кібератака щодо **операторів телекомунікацій України** з використанням шкідливої програми DarkCrystal RAT.

Відбулося розповсюдження електронних листів з електронної адреси в домені gov.ua (вірогідно, скомпрометованої).

У разі відкриття документу та активації макросу було виконано Power-Shell-команду, яка забезпечувала завантаження та запуск .NET-завантажувача "MSCommondll.exe". Згаданий виконуваний файл, у свою чергу, здійснював завантаження та **запуск шкідливої програми DarkCrystal RAT.**

Припускається, що атака була спрямована на операторів та провайдерів телекомунікацій України.

Відбувається ника важливих подій:

- Суттєве просування ворога на більшості напрямків, обстріли, авіаудари. [36]
- Україна отримала статус кандидата в члени Європейського Союзу.[37]
- Поява фейків та маніпуляцій з боку Росії щодо кандидатури на членство в ЄС.

ВИСНОВКИ

1. Атаки проти операторів телекомунікацій можуть використовуватися для посилення успіхів держави-агресора на фронті (тому що зв'язок має ключове значення).
2. Кібератаки на операторів телекомунікацій також співпадають з інформаційними атаками і цілеспрямованим поширенням фейків щодо важливих геополітичних подій (таким чином, посилюється вплив фейків).

23 червня

Російські спецслужби атакували сервер електронної пошти Миколаївської ОДА. Внаслідок цього був отриманий доступ до поштової скриньки прес-служби облдержадміністрації.

22 червня

Російська армія обстріляла південне місто України — Миколаїв.
По місту було випущено сім ракет.

ВИСНОВКИ

1. Конвенційні і кібератаки можуть співпадати регіонально (географічно).
2. Одночасність різних атак збільшує негативний вплив на цивільне населення, посилює паніку.

ЛИПЕНЬ

1 липня

Кібератака на ІТ-інфраструктуру групи ДТЕК. Це кібератака на найбільшу приватну енергетичну компанію України (яка була здійснена разом із ракетними атаками на Криворізьку електростанцію на сході України).

Увечері 28 червня російські окупанти атакували Криворізьку ТЕЦ. Російські пропагандисти анонсували цю атаку напередодні, адже міноборони держави-агресора заявило про нібито українських військових на ТЕЦ.[39]

ВИСНОВКИ

1. Влітку РФ фактично “тестувала” атаки на енергетичну інфраструктуру, які стали масовими восени. Крім того, влітку держава-агресор намагалася знайти виправдання своїм атакам, прямо не визнаючи, що її ціль - цивільна інфраструктура. Восени атаки на енергетику публічно визнаються.
2. Одночасність кібератак і ракетних ударів проти енергетичної інфраструктури покликана масштабувати негативні наслідки та збільшити шкоду від атаки.

6, 11 липня

Кібератака UAC-0056 на державні організації України з використанням Cobalt Strike Beaco.

Ці атаки співпали з важливими міжнародними подіями. 4-5 липня в швейцарському місті Лугано проходила масштабна Міжнародна конференція з питань відновлення України [40]. 11 липня Голова Комітету з питань інтеграції України до ЄС взяла участь у Конференції голів парламентських комітетів з європейських питань держав-членів Європейського Союзу (COSAC). [41]

ВИСНОВКИ

1. Кібератаки на державні органи часто співпадають з піками активності українських високопосадовців на міжнародній арені.

2. Кібератаки спрямовані на зменшення ефективності міжнародної адвокації.

21 липня

У радіохолдингу TAVR Media заявили, що на мережу радіостанцій здійснили кібератаку, в результаті якої в ефірі прозвучало повідомлення про нібито тяжкий стан президента Володимира Зеленського. [42]

21 липня

у ГУР заявили, що росіяни планують провести так звані “референдуми” чи іншим шляхом приєднати окуповані території до Росії, зокрема Херсонщини та Запорізької області. [43]

ВИСНОВКИ

1. Кібератаки на медіа, спрямовані на поширення дезінформації, є постійним елементом російської агресії. Це також приклад поєднання кібер і інформаційних атак.

2. Дезінформації із закликами припинити боротьбу є частиною загальної політики, спрямованої на успішну анексію українських територій.

СЕРПЕНЬ

16 серпня

Відбулася найпотужніша від початку повномасштабного вторгнення рф хакерська атака на офіційний сайт ДП «НАЕК «Енергоатом».

16 серпня

Енергоатом опублікував інформацію про ризик порушення радіаційної небезпеки ЗАЕС. Також відбулася телефонна розмова Макрона та Зеленського стосовно пропозиції МАГАТЕ направити місію на Запорізьку АЕС.[44]

ВИСНОВКИ

1. Кібератаки можуть спрямовуватися щодо певного конкретного об'єкта, який також зазнає конвенційних атак і щодо якого ведуться важливі міжнародні переговори.
2. Ядерний тероризм РФ є багатовимірним і включає конвенційні, інформаційні та кібератаки.

18 серпня

Естонія зазнала наймасштабніших кібератак з 2007 року.[45]

16 серпня

За розпорядженням уряду Естонії у місті Нарва та його найближчих околицях було перенесено шість монументів із радянською військовою символікою.

ВИСНОВКИ

1. Кібератаки використовуються РФ для послаблення союзників України.

2. Російська агресія має також культурний вимір. Мета путінського режиму – збереження і поширення власної світоглядної парадигми (“русский мир”). Тому кібератаки є відповіддю на спроби будь-якої держави ставити під сумнів російські міфи.

21 серпня

Російські хакери закликають атакувати Мінцифри.[46]

21 серпня

Після вбивства Дугіної російські пропагандисти закликають здійснювати удари по центрам ухвалення рішень у Києві.[47]

ВИСНОВКИ

1. Органи державної влади – одні з найбільш поширених цілей для хакерських атак Росії. Це доводить, що мета агресії – послаблення, а потім знищення української держави.

2. Не наважуючись здійснювати конвенційні атаки на центральні органи влади України, Росія вдається до кібератак (які часто є своєрідною помстою).

ВЕРЕСЕНЬ

16 вересня

Monobank, один з провідних банків України, зазнав потужної DDoS-атаки.[48]

13 вересня

Monobank вирішив відмовитися від російської мови у додатку і анонсував, що із сервісу зникне підтримка мови окупанта.[49]

ВИСНОВКИ

1. Основна перевага України над Росією – згуртованість громадянського суспільства і бізнесу заради спільної мети. Тому проукраїнський патріотичний бізнес – потенційна мішень для хакерів.

2. Атаки Росії проти українського бізнесу доводять, що економічний вимір війни має суттєве значення.

25 вересня

Кібератака на Київгаз.[50]

26 вересня

Серія вибухів на газопроводах північних потоків.[51]

ВИСНОВКИ

1. Події у кібервимірі і в конвенціному вимірі можуть синхронізуватися, тобто відбуватися в одній і тій же сфері.

2. Росія може використовувати кібератаки для посилення власної пропаганди або інформаційних атак.

30 вересня

Сайт британської контррозвідувальної служби, відомої як MI5, у п'ятницю зазнав кібератаки угруповання, яке назвалося Russian Anonymous.[52]

20 вересня

Велика Британія заявила про намір збільшити обсяг військової допомоги на 2023 рік. Про це було сказано у прес-релізі британського уряду.[53]

ВИСНОВКИ

1. РФ використовує кібератаки на західні держави як помсту за підтримку України.

2. Росія здійснює кібератаки навіть проти спецслужб ядерних держав (тобто кібератаки розглядаються як дієвий інструмент у випадку, коли конвенційні атаки є занадто ризикованими).

ЖОВТЕНЬ

8-11 жовтня

Кібератака на регіональні ділянки української залізниці.

11 жовтня – поширена інформація про кібератаку проти транспортних і логістичних організацій в Україні. [54]

11 жовтня – російські хакери атакували сайти американських аеропортів.[55]

8-11 жовтня

8 жовтня – успішна українська атака на “кримський міст”. [56]

10 жовтня – масштабний ракетний обстріл України, зокрема і Києва.[57]

ВИСНОВКИ

1. Нескладні кібератаки не потребують багато часу на підготовку, тому часто використовуються як швидка відповідь на успішні дії України.
2. Кібератаки Росії можуть віддзеркалювати дії України: тобто після успішної атаки на російську інфраструктуру можуть мати місце кібератаки на інфраструктуру України.
3. Кібератаки здійснюються Росією не лише проти України, але і проти її союзників. РФ боїться наносити конвенційні удари державам НАТО, про наважується здійснювати кібератаки навіть проти США.
4. Кібератаки і потужні ракетні атаки співпадають у часі, посилюючи негативні наслідки для України.

21 жовтня

Виявлено факт розповсюдження електронних листів, начебто, від імені пресслужби Генштабу ЗСУ з посиланням на сторонній веб-ресурс.[58]

20 жовтня

На тлі посилення ракетних обстрілів, Головнокомандувач Збройних сил України Валерій Залужний наголосив, що українська система ППО та ПРО ефективно працює завдяки професіоналізму українських воїнів та військовій допомозі від партнерів. Він закликав громадян зберігати спокій.[59]

ВИСНОВКИ

1. Головна мета атак проти цивільного населення – збільшення паніки. Тому будь-які спроби Генштабу протидіяти інформаційним атакам ворога спричиняють відповідь. У даному випадку була спроба знизити рівень довіри до заяв та повідомлень Генштабу.

2. Головнокомандувач Збройних сил України користується великою підтримкою і довірою громадян України. Саме тому, атаки проти нього є прогнозованими. Неконвенційні атаки у даному випадку мають на меті послабити військовий потенціал України.

27 жовтня

Маршалок Сенату Польщі Томаш Гродзький повідомив про потужну кібератаку на сервери верхньої палати польського парламенту.[60]

26 жовтня

Сенат Польщі одноголосно, 85 голосами, ухвалив резолюцію про визнання влади Російської Федерації терористичним режимом.

ВИСНОВКИ

1. РФ використовує кібератаки як помсту союзникам України за їхню підтримку.
2. РФ не обмежується політичними (або дипломатичними) відповідями на політичні рішення західних держав; відповіді РФ є непропорційними і ворожими.
3. Кібератаки проти органів влади іноземних держав демонструють, що РФ не визнає жодних обмежень для власних атак.

ЛИСТОПАД

24 листопада

Росія супроводжує свої ракетні удари по енергетичних об'єктах України потужними кібератаками, щоб спричинити максимальний «блекаут». За даними СБУ, опублікованими в листопаді, в середньому РФ здійснювала понад 10 кібератак на Україну за добу (проти об'єктів критичної інфраструктури). [61]

У листопаді продовжувалися масштабні ракетні обстріли енергетичної інфраструктури.

ВИСНОВКИ

1. Кібератаки на критичну інфраструктуру мають на меті посилення негативних наслідків ракетних обстрілів.
2. Кумулятивний ефект від різних атак на енергетичну інфраструктуру розглядається державою-агресором як інструмент збільшення страждання цивільного населення, а також посилення панічних настроїв.
3. Елементами політики геноциду є не лише конвенційні атаки, але і кібератаки. Кібератаки також можуть бути воєнними злочинами.

23 листопада

Президентка Європарламенту Роберта Метсола заявила, що сайт ЄП зазнав кібератаки з боку прокремлівських хакерів. [62]

23 листопада

Європарламент визнав Росію державою-спонсором тероризму.[63]

ВИСНОВКИ

1. Російські кібератаки не мають географічних кордонів. РФ не ризикує здійснювати конвенційні атаки на ЄС, проте здійснює атаки у кіберпросторі.

2. Кібератаки можуть бути відповіддю на будь-які політичні рішення на міжнародній арені, які шкодять інтересам РФ.

24 листопада

Офіційний сайт Української Греко-Католицької Церкви ugcc.ua був підданий DDoS-атаці[64] ворожих хакерів. За кілька годин було здійснено 5 млн запитів, 1 млн — щогодини. Завдяки вчасно вжитим заходам IT-спеціалістів Департаменту інформації УГКЦ кібератаку вдалося відбити. Робота сайту відновлена.

22-24 листопада

Служба безпеки України завершила контррозвідувальні (безпекові) заходи, які проводила на територіях Свято-Успенської Києво-Печерської Лаври у Києві, Корецького Свято-Троїцького монастиря та у приміщеннях Сарненсько-Поліської єпархії УПЦ на Рівненщині. У взаємодії зі співробітниками Нацполіції та Нацгвардії було ретельно перевірено понад 350 церковних споруд і 850 осіб.[65]

ВИСНОВКИ

1. Кібератаки Росії можуть бути відповіддю на успішні безпекові операції українських силових структур; тобто такі атаки не завжди плануються заздалегідь, а можуть бути своєрідною помстою.

2. Кібератаки, які використовуються як відповідь на успіхи України, є дзеркальними, тобто відбуваються щодо тієї самої сфери, що і конвенційні атаки.

3. Кібератаки проти церкви доводять, що Росія розглядає цей інститут як політичний інструмент гібридної агресії.

ТИПОЛОГІЯ КОРЕЛЯЦІЙ

СПІВПАДІННЯ ЗА ПРЕДМЕТОМ

Географічна кореляція

Різні атаки відбуваються щодо одного об'єкта або щодо одної територіальної одиниці.

Галузева кореляція

Різні атаки відбуваються щодо певної сфери; наприклад, щодо енергеритики, інфраструктури тощо.

ТЕМПОРАЛЬНІ СПІВПАДІННЯ

Підготовчі атаки

(кібератаки передують конвенційним атакам)

Синхронні атаки

(кібератаки посилюють негативні наслідки конвенційних атак)

Атаки-відповіді

- ***Атаки задля помсти***
- ***Атаки проти інших держав*** (щоб зупинити міжнародну допомогу Україні)

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Російська збройна агресія проти України, яка розпочалася у 2014 році, із самого початку була багатовимірною. Крім того, Росія постійно використовувала гібридні атаки (економічні війни, пропагандистські кампанії тощо) для досягнення власних цілей. Неконвенційна російська агресія триває не лише проти України, такі атаки здійснюються проти всіх «недружніх» держав. Тобто потенційно ці атаки створюють глобальні загрози. Тому кореляція між різними вимірами агресії потребує детального вивчення, а в ефективній протидії цим атакам зацікавлені всі світові держави (за винятком нечисленних союзників РФ).

РЕКОМЕНДАЦІЯ 1

Український досвід має систематизуватися і використовуватися для протидії не лише Росії, але й іншим авторитарним режимам.

Широкомасштабне вторгнення Росії продемонструвало багато логічних зв'язків між різними видами атак. Агресія, яку РФ здійснює проти України, не має аналогів у сучасній історії Європи. Водночас ця війна дуже добре вказує на підходи, які можуть використовуватися і в майбутніх збройних конфліктах.

Протистояння демократії й авторитаризму лише набирає обертів і буде визначальним для формування глобального порядку денного у найближчі десятиліття. Тому досвід України – це ключ до перемоги демократії. Головна слабкість авторитарних режимів у тому, що вони використовують досвід одне одного. Їхня централізованість і передбачуваність – це не сила, а Ахіллесова п'ята.

РЕКОМЕНДАЦІЯ 2

Оборонні доктрини мають адаптуватися до вимог часу. Логічні зв'язки між різними вимірами російської агресії можуть бути використані для прогнозування і моделювання.

Очевидно, що частина даних, що використовувалися для моделювання війн до 24 лютого 2022 року, були помилковими. І справа не лише у тому, що багато аналітиків недооцінили Україну і переоцінили Росію. Проблема також у тому, що багато

теоретичних припущень ніколи не перевірялися на практиці.

Оборонні доктрини мають враховувати той факт, що конвенційні атаки – не єдиний спосіб завдати значної шкоди супротивникам. Тому всі стратегічні документи мають враховувати багатовимірність сучасних війн.

РЕКОМЕНДАЦІЯ 3

Міжнародно-правові підходи до юридичного визначення агресії повинні змінитися (агресія у XXI сторіччі буває не лише конвенційною). Відповідальність має поширюватися на всі прояви агресії, а не лише на класичні.

Юридичне визначення агресії було сформульоване Резолюцією Генеральної Асамблеї Організації Об'єднаних Націй 3314 ще у 1974 році. З того часу міжнародне співтовариство не наважувалося поставити під сумнів актуальність цієї дефініції. Міжнародне право також майже цілком ігнорує поняття економічної агресії. І хоча Резолюція 3314 передбачає, що агресією є «застосування будь-якої зброї державою проти території іншої держави», наразі немає чіткої відповіді на запитання, чи включає «будь-яка зброя» економічну, інформаційну і кіберзброю. Більшість юристів матимуть сумніви. І саме цією двозначністю користується держава-агресор (і будуть користуватися інші авторитарні режими). Тому визначення агресії має бути оновлене.

РЕКОМЕНДАЦІЯ 4

Кібератаки можуть прирівнюватись до воєнних злочинів. Міжнародне гуманітарне право повинно встановити більш жорсткі рамки для неконвенційних атак.

Спроби Росії знищити українську енергосистему продемонстрували, що конвенційні атаки проти критичної інфраструктури часто супроводжуються кібератаками. При цьому теоретично кібератаки можуть приносити не менше шкоди і страждань цивільному населенню, ніж ракетні обстріли. Тому кібератаки можуть бути воєнними злочинами. Міжнародне гуманітарне право повинно стати більш прогностичним і запропонувати адекватне регулювання відповідних правовідносин.

РЕКОМЕНДАЦІЯ 5

Багатовимірність російської агресії доводить необхідність санкцій проти найважливіших сфер економіки. Санкції мають посилюватися, а міжнародні компанії мають йти з російського ринку. Сьогодні співучасть в агресії – це не лише продаж безпілотників, але і надання доступу до технологій.

Потужність неконвенційних атак ще більше загострює питання необхідності повної економічної ізоляції держави-агресора.

Крім того, неконвенційна агресія (перш за все – кібератаки Росії) не має географічних обмежень. Це означає, що західні компанії, які продовжують постачати РФ новітні технології, не лише сприяють продовженню агресії проти України. Вони підривають безпеку власних держав, адже ніхто не знає, проти кого буде здійснена російська атака завтра.

РАДА ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ ВИСЛОВЛЮЄ ПОДЯКУ

компанії TRUMAN та Управлінню стратегічних комунікацій Апарату Головнокомандувача Збройних Сил України за сприяння у зборі та аналізі інформації, необхідної для підготовки цього звіту

Автор:

Ілона Хмельова
провідна експертка, РЕБ

Незалежні консультанти:

Олена Юрченко
провідна аналітикиня, TRUMAN

Денис Гутик
проєктний менеджер, TRUMAN

МАТЕРІАЛИ ТА ЛІНКИ

1. https://journals.sagepub.com/doi/10.1177/0967010611431079
2. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details
3. https://www.rbc.ua/ukr/news/ssha-rassleduyut-kiberataku-sputnikovyy-internet-1647052748.html
4. https://disinfo.detector.media/
5. https://www.rbc.ua/ukr/news/ssha-rassleduyut-kiberataku-sputnikovyy-internet-1647052748.html
6. https://ukranews.com/ua/news/855983-za-godynu-do-vtorgnennya-rosiya-zavdala-masshtabnoyi-kiberataky-na-systemu-suputnykovogo-zv-yazku-v
7. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details
8. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
9. https://uk.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%BB%D1%96%D0%BA_%D1%80%D0%B0%D0%BA%D0%B5%D1%82%D0%BD%D0%B8%D1%85_%D1%83%D0%B4%D0%B0%D1%80%D1%96%D0%B2_%D0%BF%D1%96%D0%B4_%D1%87%D0%B0%D1%81_%D1%80%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%BE%D0%B3%D0%BE_%D0%B2%D1%82%D0%BE%D1%80%D0%B3%D0%BD%D0%B5%D0%BD%D0%BD%D1%8F_2022#%D0%91%D0%B5%D1%80%D0%B5%D0%B7%D0%B5%D0%BD%D1%8C
10. https://disinfo.detector.media/day/01-03-2022
11. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details
12. https://researchbriefings.files.parliament.uk/documents/CBP-9481/CBP-9481.pdf
13. https://cybernews.com/news/ukrainian-embassy-in-london-suffers-from-constant-cyber-attacks/
14. https://twitter.com/RedCrossUkraine/status/1504123401941790720
15. https://www.facebook.com/RedCrossUkraine/posts/1578656718837464/

16. https://disinfo.detector.media/search?search_string=%D1%87%D0%B5%D1%80%D0%B2%D0%BE%D0%BD%D0%B8%D0%B9+%D1%85%D1%80%D0%B5%D1%81%D1%82&-search_tag=
17. https://cert.gov.ua/article/39518
18. https://www.nytimes.com/2022/04/12/us/politics/ukraine-russian-cyberattack.html?utm_source=pocket_mylist
19. https://www.epravda.com.ua/news/2022/04/10/685535/
https://www.epravda.com.ua/news/2022/04/10/685515/
https://www.epravda.com.ua/news/2022/04/10/685514/
20. https://www.epravda.com.ua/news/2022/04/13/685666/
21. https://t.me/UkrzalInfo/2251
22. https://uk.wikipedia.org/wiki/Хронологія_російського_вторгнення_в_Україну_(травень_2022)
23. https://ukranews.com/en/news/856131-russia-carried-out-large-scale-cyber-attack-on-ukrainian-telecom-operators-websites
24. https://www.pravda.com.ua/articles/2022/05/9/7344951/
25. https://city-adm.lviv.ua/news/government/291555-naslidky-kiberataky-na-lviv-vykradeno-chastynu-danykh
26. https://t.me/andriysadovyi/765
27. https://hromadske.ua/posts/prorosijski-hakeri-atakuvali-yevrobachennya-ta-namagalisya-zlamati-sistemu-golosuvannya
28. https://t.me/verkhovnaradaukrainy/25217
29. https://t.me/verkhovnaradaukrainy/25297
30. https://t.me/verkhovnaradaukrainy/25196
31. https://t.me/mvs_ukraine/14194

32. https://uk.wikipedia.org/wiki/%D0%A5%D1%80%D0%BE%D0%BD%D0%BE%D0%B-B%D0%BE%D0%B3%D1%96%D1%8F_%D1%80%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%BE%D0%B3%D0%BE_%D0%B2%D1%82-%D0%BE%D1%80%D0%B3%D0%BD%D0%B5%D0%BD%D0%BD%D1%8F_%D0%B2_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%83_(%D1%87%D0%B5%D1%80%D0%B2%D0%B5%D0%BD%D1%8C_2022)#/media/%D0%A4%D0%B0%D0%B9%D0%B-B:Kharkiv_Metro_depot_after_rocket_strike_on_20_June_2022_(02).jpg

33. https://t.me/mvs_ukraine/14202

34. https://t.me/mvs_ukraine/14238

35. https://t.me/mvs_ukraine/14260

36. https://t.me/mvs_ukraine/14329

37. https://t.me/verkhovnaradaukrainy/26789

38. https://t.me/mykolaivskaODA/1552

39. https://24tv.ua/udar-po-krivorizkiy-tets-golova-rva-pro-naslidki-ataki_n2052766

40. https://t.me/verkhovnaradaukrainy/28009

41. https://t.me/verkhovnaradaukrainy/28702

42. https://www.pravda.com.ua/news/2022/07/21/7359395/

43. https://www.pravda.com.ua/news/2022/07/21/7359429/

44. https://suspilne.media/271277-vtorgnenna-rosii-v-ukrainu-den-174-tekstovij-onlajn/

45. https://www.eurointegration.com.ua/news/2022/08/18/7145161/

46. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details

47. https://www.pravda.com.ua/news/2022/08/21/7364186/

48. https://life.fakty.com.ua/ua/tekhnolohii/monobank-zaznav-potuzhnoyi-ddos-ataky-gorohovskyj/

49. https://life.fakty.com.ua/ua/tekhnolohii/monobank-vidmovytsya-vid-rosijskoyi-movy-chas-perehodyty-na-derzhavnu/

50. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details

51. https://uk.wikipedia.org/wiki/%D0%A1%D0%B0%D0%B1%D0%BE%D1%82%D0%B0%D0%B6_%D0%BD%D0%B0_%D0%B3%D0%B0%D0%B7%D0%BE%D0%BF%D1%80%D0%BE%D0%B2%D0%BE%D0%B4%D1%96_%D0%9F%D1%96%D0%B2%D0%BD%D1%96%D1%87%D0%BD%D0%B8%D0%B9_%D0%BF%D0%BE%D1%82%D1%96%D0%BA

52. https://www.eurointegration.com.ua/news/2022/09/30/7147847/

53. https://www.gov.uk/government/news/uk-will-match-record-ukraine-support-in-2023

54. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details

55. https://www.ukrinform.ua/rubric-technology/3590532-rosijski-hakeri-atakuvali-saj-ti-amerikanskih-aeroportiv-cnn.html

56. https://www.bbc.com/ukrainian/features-63183830

57. https://suspilne.media/291732-rosijski-raketni-obstrili-ukraini-10-zovtna-so-vidomo/

58. https://cert.gov.ua/article/2394117

59. https://www.radiosvoboda.org/a/news-hzaluzhnyy-ppo/32092725.html

60. https://www.eurointegration.com.ua/news/2022/10/27/7149503/

61. https://armyinform.com.ua/2022/11/09/ponad-10-kiberatak-na-strategichni-obyekty/

62. https://www.ukrinform.ua/rubric-world/3620523-sajt-evroparlamentu-zaznav-kiberataki-pisla-viznanna-rosii-sponsorom-terorizmu.html

63. https://www.ukrinform.ua/rubric-world/3620523-sajt-evroparlamentu-zaznav-kiberataki-pisla-viznanna-rosii-sponsorom-terorizmu.html

64. https://ugcc.ua/data/na-ofitsiynyy-sayt-ugkts-zdiysnyly-kiberataku-1500/

65. https://ssu.gov.ua/novyny/sbu-znaishla-prorosiisku-literaturu-miliony-hotivky-u-riznii-valiuti-ta-sumnivnykh-hromadian-rf-pid-chas-bezpekovykh-zakhodiv-u-prymishchenniakh-upts-mp-video