Міністерство освіти і науки України
Національний університет «Києво-Могилянська академія»
Факультет соціальних наук і соціальних технологій
Кафедра соціології

Кваліфікаційна робота

освітній ступінь – магістр

на тему:

«ДІЯЛЬНІСТЬ І СТРУКТУРА УКРАЇНСЬКИХ ХАКЕРСЬКИХ ТА OSINT СПІЛЬНОТ ПІД ЧАС РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ 2022-2023 РР.»

Виконав: студент 2-го року навчання

спеціальності 054 «Соціологія»
Міщенко Євгеній Євгенійович

Керівник: Артикуца С.С.,
Магістр,
Старший викладач

Рецензент:

Кваліфікаційна робота захищена з оцінкою «_____»

Секретар ЕК:
«_____»_____2023р

Київ – 2023

ВСТУП

Сучасна війна має певні відмінності від тієї, що можна було спостерігати у минулому. Новітні технології змінили як саме поле бою, так і шляхи, якими можна долучитися до участі в конфлікті. Широке застосування обчислювальної техніки на військових, інфраструктурних та інших об’єктах зробило можливим заподіювати шкоду виключно через інтернет. Хакерство в певному сенсі стало різновидом зброї. За його допомогою можна робити економічну шкоду, ускладнювати логістику або викривати секретні дані.

Проте, не вся інформація потребує хакінгу, щоб бути встановленою. Таким чином, розвідка сьогодні може відбуватися на основі відкритих джерел. Таке явище отримало назву Open-Source Intelligence. Метою такої розвідки є отримання певної інформації без використання розвідувальних апаратів, шпіонажу тощо. Натомість всі дані знаходяться у відкритих публікаціях, а вже на їх основі робляться висновки.

Змінилися й шляхи того, як люди можуть долучатися до будь-якої активності. Адже з появою інтернету з’явилася можливість вдаватися до дій онлайн. Подібне долучення має парасолькову назву “кіберактивізм”. Відповідно, люди отримали можливість вести в тому числі й воєнну діяльність через кіберактивізм: використовуючи хакінг, OSINT або інші методи. Для цього люди можуть об’єднуватися у спільноти та вести подібну діяльність організовано.

Саме подібні хакерські та OSINT спільноти стали **об’єктом** нашого дослідження. **Предметом** дослідження є діяльність та структура українських хакерських та OSINT спільнот під час російсько-української війни 2022-2023 рр. **Метою** дослідження є виявити особливості структури та діяльності таких спільнот.

Актуальність цього дослідження обумовлена збільшенням значущості та впливовості OSINT та хакінгу, що пов’язано з початком повномасштабного нападу. Хакерські та OSINT групи долучаються до спротиву, українська держава й сама створює подібні спільноти. Українські спеціалісти роблять внесок у переслідування військових злочинців, пошук місць дислокації збройних сил РФ, викриття інформації, руйнування російської військової, виробничої інфраструктури тощо. Проте, питання структури та інших принципів функціонування таких груп, як і питання безпосередньо самої їхньої діяльності потребують подальшої розробки.

Для того, щоб досягти поставленої мети, необхідно виконати такі **завдання**:

1. Оглянути основні теоретичні доробки, що стосуються вивчення явищ, кіберактивізму, хактивізму, OSINT, волонтерства, девіантної поведінки та субполітики.
2. Визначити особливості діяльності українських хакерських та OSINT спільнот в рамках повномасштабного нападу на Україну у 2022-2023 роках.
3. Встановити особливості структури організації таких спільнот.
4. З’ясувати можливі складові мотивації до такої діяльності.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ВИВЧЕННЯ ЯВИЩ ХАКТИВІЗМУ, OSINT, СУБПОЛІТИКИ, КІБЕРАКТИВІЗМУ ТА ВОЛОНТЕРСТВА

Явища хактивізму (hacktivism) та OSINT є важливими для нашого дослідження. Їхнє визначення буде описувати діяльність наших респондентів. Обидва ці терміни можна назвати “парасольковим”, адже вони описують скоріше певну категорію видів людської діяльності ніж конкретний її вид. Розробкою цих тем займалися й інші вчені в різних контекстах, в тому числі й у військовому, адже обидва явища можна певним чином віднести також й до поняття “cyber warfare”.

1.1. Зміст явищ кіберактивізму та хактивізму

Одним з більш ранніх досліджень явища кіберактивізму є розділ “Classifying Forms of Online Activism: The Case of Cyberprotests Against the World Bank” за авторством Sandor Vegh зі збірки “Cyberactivism Online Activism in Theory and Practice”. Там автор дає таке визначення онлайн активізму: “...politically motivated movement relying on the internet” (Ayers et al., 2003). Також він додає, що вважає інтернет лише ще одним майданчиком, де активісти намагаються досягти своїх традиційних цілей та використовують традиційні техніки пропаганди. Але зазначає, що інтернет також може використовуватися для впровадження активності, яка можлива лише онлайн. В цій же статті вчений робить спробу категоризації онлайн активізму та виділяє три основні зони: інформування/пропаганда, організація/мобілізація та дія/реакція.

Перша зона, інформування/пропаганда, описує тип дистрибуції інформації. На думку автора, інтернет стає майданчиком для надання актуальної до події інформації, якій приділяють недостатньо уваги мейнстримні ЗМІ. Водночас взаємодія з такими ЗМІ потребує, зазначає автор, лояльності до них від видань, в той час, як в інтернеті розповсюдження інформації відбувається

завдяки індивідуальній дії або дії незалежних організацій. Крім того, як пише Vegh, розповсюдження інформації слугує для налагодження зв'язків, що потім можуть бути використані для мобілізації/організації.

Така мережа розповсюдження інформації також превалює, пише автор, в невеликих групах протестно налаштованих людей (Sandor Vegh пише про закриті державні режими), а роль таких груп подвійна. Перша це розповсюдження інформації, яка піддається цензуруванню, а друга це створення майданчиків для обговорення (автор наводить приклад обговорення проблем із правами людини, насиллям або цензурою) проблем, про які іноді стає відомою широкому загалу саме через такі майданчики, що призводить до офлайн акцій.

Пропаганда ж несе в собі ціллю залучити до дії людей зі схожими переконаннями та цілями. Автор наводить приклад антиглобалізаційного руху, який використовував інтернет, переважно, для координації. Інтернет, пише автор, дає можливість організувати велику кількість індивідуальних та групових учасників і лише інтернет дозволяє проводити організацію та інформування такого масштабу. Для інформування використовуються централізовані вебсайти та e-mail розсилки. Варто зазначити, що стаття опублікована у 2004 році й тоді ще не існувало Facebook, Telegram та інших соціальних мереж. тому автор не розглядає їх в контексті онлайн активізму.

Організація/мобілізація може проходити у три різні способи, вважає автор статті. Перший спосіб, це заклик до офлайн активності, другий це заклик до дій, які зазвичай виконуються офлайн, проте можуть бути більш ефективно впроваджені онлайн (заклик надсилати листи через email до конгресменів). Третій спосіб це заклик до онлайн-дій, які можуть бути впроваджені виключно онлайн (масовий спам, ping-attack або DDoS). Найбільш ефективними кампаніями автор вважає такі, що вправно поєднують пропаганду (інформування

з метою привернути на свій бік або залучити тих, хто вже має схожу думку, проте не залучений до активності) та мобілізацію.

Остання категорія, дія/реакція, охоплює, як пише автор, у дуже загальних рисах онлайн атаки, впроваджені “хакерами”. При цьому автор зазначає, що розуміння слова “хакер” має викривлений характер. Насправді ж, стверджує він, це спосіб використання інтернету може мати як фінансові, так і політичні мотиви. У цьому розділі статті автор згадує явище “хактивізму”, як перший приклад якого наводить рух Сапатистів. Організація під назвою “Electronic Disturbance Theatre” вчинила атаку на антисапатистські організації Мексики. Також автор описує спеціальне програмне забезпечення, що використовується для об’єднання малих зусиль різних людей для DoS-атак, наводячи приклад атак на сайт Всесвітньої Торгової Організації. (WTO). Автор називає чотири категорії політичної вмотивованості кібератак. Це може бути відповідь на події чи обставини, частина вже наявного конфлікту, частина в наявній мілітаристичній кампанії чи частина традиційної війни. Саме перші дві категорії автор називає такими, що відповідають духу хактивізму. Інші дві він відносить, скоріше, до категорії кібервійни.

Загалом автор визначає хактивізм наступним чином: “Hacktivism is a politically motivated single-incident online action, or a campaign thereof, taken by nonstate actors in retaliation to express disapproval or to call attention to an issue advocated by the activists” (Ayers et al., 2003, p. 83). Також автор наводить цитату іншого дослідника, соціолога Тіма Джордана, що називає хактивізмом суспільний рух, нову форму прямої дії, засновану на інтернеті активність, зосереджену на віртуальній політиці.

У статті “From clicktivism to hacktivism: Understanding digital activism” (George & Leidner, 2019), автори визначають хактивізм як хакінг, метою якого є досягнення політичних або соціальних цілей. Далі у статті наводиться

категоризація хактивізму, яка стане помічною і для нашого дослідження: кібертероризм, громадянський хакінг та патріотичний хакінг (cyberterrorists, civic hackers, and patriotic hackers). До першої категорії автори відносять низьку прямих дії, таких як розповсюдження вірусів або атаку Denial of Service (DoS або DDoS). Громадянський хакінг дослідники описують так: “loosely organized groups that perform IS actions…for the good of the community and in a legal manner”. Патріотичний хакінг полягає у діях спрямованих проти “ворожих” держав та їх громадян. Патріотичні хакери зазвичай не фінансуються державою і натомість “діють там, де не може держава”.

Одним з таких дослідників є James Andrew Lewis з Центру стратегічних та міжнародних досліджень, який у тексті статті “Compelling Opponents to Our Will (Kenneth, 2015a). The Role of Cyber Warfare in Ukraine” називає такі можливості кібератак: *“...manipulation of software, data, knowledge, and opinion…”*. Серед потенційних цілей або ефектів які мають подібні атаки він називає таке “…*to degrade performance and produce political or psychological effect”*. Самі ж кібератаки автор описує як такі, що підходять під сучасні політико-мілітарні реалії, адже вони, на його думку, можуть завдавати шкоди порівнянною з такою у кінетичної зброї. Проте основною метою кібератак він називає політичний та психологічний вплив: дезінформацію та маніпулювання громадською думкою.

Далі James Andrew Lewis дивиться на те, як подібні дії в кіберпросторі застосовувалися під час російсько-української війни, що почалася у 2014 році. Проте, він приділяє увагу переважно тому, як cyber warfare були використані проти України, а не нею самою. На думку Lewis, Росія обмежено використовувала свої можливості у кіберпросторі. На його думку, російські кібероперації полягали переважно у спробах створити “фашистський” образ України, звинуватити її у злочинах, тобто “manipulation of opinion”, який автор описував на початку статті.

Згідно зі згаданими текстами, хактивізм може вважатися одним з різновидів кіберактивізму. Автори виділяють різноманіття цього явища. Зокрема, вони пропонують такі його різновиди, як кібертероризм, патріотичний хакінг тощо. Робилися категоризації кіберактивізму як на основі методів, так і на основі цілей. Кіберактивізм загалом та хактивізм і зокрема розглядалися вченими у різних формах їхнього прояву. Явище хакінгу досліджувалося як у контексті цивільного протесту, так і як складова cyber warfare. Останній контекст знаходив відображення в тому числі й у дослідженнях російсько-українського конфлікту загалом та повномасштабного вторгнення зокрема. Оцінка ефективності цього методу може бути різною, проте деякі автори додавали ремарки про складність вимірювання такої ефективності.

1.2. Поняття OSINT та його прояви

OSINT розшифровується як Open-Source Intelligence та може описувати будь-який пошук інформації. Це можуть бути розслідування про осіб та організації, пошук місць дислокації ворога тощо. Цей інструмент може використовуватися в різних контекстах, але центральним для нас є його використання у просторі війни.

Колектив дослідників в огляді літератури “Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence” (Evangelista et al., 2020) пропонує систематичний огляд літератури з теми. Там вони, посилаючись своєю чергою на Glassman & Kang визначають OSINT наступним чином:
“Open Source Intelligence (OSINT) is the concept used to describe the search and acquisition of information from publicly available sources, as well as the techniques and tools used” (Evangelista et al., 2020, p. 2).

Автори зазначають, що під час подібних розвідувальних дій може використовуватися будь-яка публічна інформація. Це можуть бути публікації у

соціальних мережах, наукові публікації, супутникові знімки тощо. Вони додають, що цей спосіб є ефективним безпековим способом. А тому його використовують зокрема FBI, CIA та Europol. На думку дослідників, раніше цей спосіб розвідки був прерогативою державних інституцій, проте зараз його можуть використовувати й приватні особи.

В контексті повномасштабного вторгнення одним з можливих застосувань OSINT є пошук інформації про військових злочинців, збір доказової бази, персональних даних тощо. У своєму тексті "OSINT як один з інструментів для збирання інформації про воєнні злочини Російської Федерації в Україні", що був презентований на конференції "Modern Science: Innovations and Prospects" Комісарчук та Черевко описують його як один з головних інструментів збору подібної інформації. Вони додають, що інструмент є "базовим" (Комісарчук, 2022).

Американський автор Stephen C. Mercado у статті під назвою "Sailing the Sea of OSINT in the Information Age" надає свою оцінку цьому явищу. На його думку, цей метод здатний "суттєво покращити програми по збору секретних даних" (Mercado, 2004). Стаття була написана у 2004 році, на думку автора, на той момент ставлення до OSINT було "несерйозне" і деякі розвідники не ставилися до нього як до розвідки взагалі.

До уваги дослідників також потрапляла структура OSINT-діяльності. Одним з прикладів подібного аналізу є робота "Current Status and Security Trend of OSINT" за авторством колективу вчених з Південної Кореї та Сполучених Штатів (Hwang et al., 2022). Першим кроком, на їхню думку, є "Identifying the source". Цей крок включає до себе роботу по відбору слушних даних з загального масиву доступних. Другим кроком колектив називає "Data collection". Він, своєю чергою, поділяється на два типи: "активний" та "пасивний". Активним називається такий пошук (collection), який реалізується за допомогою скриптів

або програм, які напряму звертаються до джерел. Натомість пасивний залучає сторонні ресурси (third-party), такі як Google, Whois, Shodan тощо. Відмінність полягає у тому, що пасивний спосіб не залишає по собі логів, які, наприклад, можуть бути використані адміністратором інтернет-джерел з метою ідентифікації пошукача. Третім кроком є “Processing”. Він полягає у “сортуванні” великого масиву даних, що був зібраний на попередньому етапі. На думку дослідників, така робота вимагає великого досвіду та високого рівня навичок. Четвертим етапом є “Analysis”, який полягає безпосередньо в аналізі зібраних та відсортованих даних. Фіналом всього процесу є “Reporting”. Це певне підсумовування даних, аналізу, висновків, приведення інформації до “читабельного” виду. Також автори описують недоліки та переваги OSINT.

У звіті організації Institute of Post-Information society наводяться різноманітні приклади використання OSINT в контексті повномасштабного вторгнення (Укрінформ, 2023). Одним з них є журналістські розслідування. Автори наводять зокрема приклад програми “Схеми”, яка за допомогою інструменту MarineTrafic змогла навести аргументи на користь факту оминання Росією санкцій. Крім цього, низька осіб та спільнот публікує списки російських військових, які так чи інакше беруть участь у війні проти України. Згідно зі звітом, подібний список є й на сайті Головного Управління Розвідки.

Інше поле використання OSINT, яке наводиться у звіті - громадська сфера. На думку авторів, цей інструмент допомагає забезпечити прозорість дій державних органів. Крім цього, OSINT може бути використаним в адвокації та під час протестних кампаній. В оборонному секторі подібна розвідка також може принести користь. На думку Інституту, це може бути різноманітне заподіювання шкоди ворогу не бойовими методами. Наприклад, це можуть бути “інформаційно-психологічні операції”, підвищення обізнаності про склад військових частин противника тощо. Також у звіті наводиться перелік можливих

інструментів, серед яких, крім згаданого MarineTrafic є FlightRadar, RadarBox, Himera тощо.

OSINT як метод може мати різноманітне застосування. Сам по собі він не є характерним лише для однієї сфери суспільного буття. Він може бути використаний як під час військових дій, так і як складова громадського протесту. Цей метод застосовується в тому числі й під час повномасштабного вторгнення. За його допомогою може відбуватися, наприклад, юридична підтримка (як от збір доказів про злочини), пошук місць дислокації ворога. Інструментарій такої діяльності також є різноманітним. Крім цього, деякі автори стверджували відносну доступність такого методу, легкість його застосування у порівнянні з більш “традиційними” методами розвідки та збору даних.

1.3. Зміст явищ субактивізму, волонтерства девіантної поведінки

Враховуючи нелегальний характер певних хакерських дії, подібна діяльність може розглядатися як девіантна. Дослідник Роберт Мертон у роботі “Соціальна структура та аномія” наводить класифікацію видів людської поведінки (Merton, 1968). Вся класифікація відбувається через визначення відношення суб’єкта такої поведінки до суспільно схвалюваних цілей та таких само методів. Відхід від конформної поведінки (коли суб’єкт приймає як суспільно схвалювані цілі, так і такі ж шляхи досягнення цих цілей) за Мертоном пов’язаний з депривацією та неможливістю досягти мети інституційними методами. У випадку патріотичного хакінгу, цілі є, скоріше, суспільно схвалюваними, проте методи можуть бути розцінені як девіантні. Подібну комбінацію сам Мертон називає “Innovation”.

Проте, подібна класифікація може виступати лише як “приблизна”, або “схематична”. Вона не бере до уваги, так би мовити, “рівень схвальності” цілей, не бере до уваги контекст, мінливість та особливості поглядів, що панують у суспільстві. Враховуючи цей факт, подібна класифікація може бути адекватно

застосована лише з позиції, коли спостерігач знаходиться всередині суспільства, де відбувається поведінка. Або, принаймні, глибоко розуміє контекст різноманітних цілей та дій, особливий для цього суспільства. Адже методи або цілі, які всередині суспільства є нормою, схвалюються та вітаються, можуть "стати" відхиленням, девіацією, злочином, якщо спостерігач знаходиться в іншому суспільному та культурному контексті. Тому, ми звернемося до мертонівської класифікації, проте зробимо додаткові коментарі до неї, які розкривають особливості її використання в контексті об'єкта та предмета дослідження.

Дослідники Lindgren & Linde у статті **"The subpolitics of online piracy A Swedish case study"** згадують про онлайн піратство як про громадський рух (2012). Громадський рух вони, посилаючись на Eyerman and Jamison визначають наступним чином: "when a group of people are acting together to change society in some way and when this collective action is grounded in some kind of societal conflict".

В статті автори роблять спробу поєднати концепцію субполітики Бека та субактивізму Бакардьєвої з аналітичною рамкою Eyerman and Jamison, що розглядає громадські рухи як когнітивну практику. Концепцію субполітики вони пояснюють наступним чином: "politics that is expressed outside of the established and traditional system – often in relation to specific issues rather than to complete ideological packages – is labeled subpolitics by Beck". Як приклад субполітики автори наводять й хактивізм, посилаючись на McCaughey and Ayers (Ayers et al., 2003). Автори пишуть про те, що субполітика пояснює явище індивідуальної дії, яка здатна до агрегування, а інтернет, на їхню думку, є потужним помічником такої агрегації, завдяки якій ці дії можуть ставати значущими.

Сам Ульріх Бек, автор концепції субполітики, розповідає про неї в рамках ширших роздумів про індивідуалізацію політики, що проходить від модерну. На його думку, політика-як-процес "зміщується" від держави до приватних осіб, компаній, підприємств тощо (Beck, 2005). У сучасному капіталістичному

суспільстві саме там, на думку Бека, знаходяться decision makers. Саме для того, щоб підкреслити різницю між політикою що відбувається всередині державного апарату та політикою, що відбувається поза нею він вводить термін субполітика. За його версією, субполітикою можуть займатися різні верстви населення: технічна інтелігенція, професіонали, дослідницькі інститути, робітники, громадські ініціативи тощо. Також він додає, субполітику можуть творити не лише організовані групи, а й окремі люди. Як термін субполітики, так і сама концепція буде використана нами під час роботи з зібраними даними.

Явище волонтерства стало актуальним для України під час та після Євромайдану. В той момент з'явився простір для неї, у вигляді підняття протестних настроїв, а згодом, після окупації Криму та початку вторгнення на Донбас, й патріотичних, націоналістичних, проукраїнських або антиросійських. Волонтерські рухи України в контексті війни з Росією також потрапляли до уваги дослідників.

На волонтерський (в широкому сенсі) рух звертав увагу, зокрема, Emmanuel Karagiannis (Karagiannis, 2016) у свої статті "Ukrainian volunteer fighters in the eastern front: ideas, political-social norms and emotions as mobilization mechanisms". Стаття є презентацією польового дослідження, під час якого автор спілкувався з людьми, що пішли добровольцями на війну проти Росії. В тексті автор розглядає можливі механізми мобілізації людей, серед яких він називає такі категорії як ідеї (ideas), соціально-політичні норми (political-social norms) та емоції (emotions).

Відстежуючи історію мобілізації через емоції, Emmanuel Karagiannis згадує й про Організацію Українських Націоналістів (ОУН) та Українську Повстанську Армію (УПА). На його думку, саме через націоналістичні ідеї відбувалося залучення людей до цих організацій. В сучасній Україні, на думку автора, подібним способом користуються й партії "Свобода" та "Правий сектор",

які, за його словами, вважають себе ідеологічними послідовниками (ideological successors) ОУН та УПА.

Мобілізація через норми ж є похідним від ідеологічного. Таким чином, посилаючись на інших дослідників, автор наводить думку про те, що, на думку українських націоналістів, культура України та українців суттєво відрізняється від такої у Росії та росіян. Таке переконання, своєю чергою, задає певну рамку, виходячи з якої люди будують свою національну ідентичність. В такому випадку, мобілізація відбувається через думку про те, що саме так мають вчиняти люди з цієї (в цьому випадку, української) культури.

Емоції, як вважає Emmanuel Karagiannis також грають роль у процесі мобілізації. Його інформанти розповідали, що відчувають любов, солідарність, обов'язок, гордість тощо. Саме так респонденти раціоналізували свій вчинок.

Автор доходить висновку, що подібна мобілізація не може бути пояснена раціональним вибором. На його думку, інші фактори мобілізації (ideas, political-social norms, emotions) отримують недостатньо уваги з боку дослідників. Крім того, підкреслюється вплив націоналістичних ідей на респондентів, з якими спілкувався Emmanuel Karagiannis.

На думку деяких вчених, сучасна політика змістилася зі сфери інституційного до сфери індивідуального, особистого. Залучатися до такої політики можуть різні групи людей та окремі індивіди, юридичні особи тощо. Такий різновид політичного був описаних Ульріхом Беком під назвою "субполітика". Волонтерство розглядалося вченими в тому числі й у контексті російсько-української війни. Особисті особливості мобілізація до такої активності може бути різноманітною, вона може лежати поза раціональним, знаходячись натомість у полі емоційного, соціального, ідеологічного. Роберт Мертон робив спробу класифікації девіантної поведінки. Його класифікація відбувається через відношення актора до загальносхвалюваних цілей та таких само методів досягнення цих цілей.

1.4. Діяльність хакерського та OSINT спільнот під час війни з Росією

Термін “хакерство” у значенні, що ми його використовуємо описується низкою статей Кримінального Кодексу України. Зокрема, подібна діяльність згадується у статтях 361, 362 та 363 (Кримінальний кодекс України). У зазначених статтях є згадка про декілька типів незаконних дій, які можуть бути застосовані проти електронно-обчислювальної техніки. Наприклад, стаття 361 містить таке визначення: “Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж”. Крім цього, незаконним є створення та розповсюдження програмного забезпечення, що допомагає вчиняти подібне втручання. Стаття 362 описує незаконні дії, які можуть бути вчинені стосовно інформації, що зберігається на електронно-обчислювальній техніці. Стаття 363 описує, зокрема, вид діяльності, до якого належать і DDoS-атаки: “Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку”.

Акронім DDoS розшифровується як distributed denial-of-service attack. Цим терміном називають різновид DoS-атак (denial-of-service), при якому ресурси для атаки розподілені між певною кількістю техніки, не мають “загального центру”. Відповідно, успішним результатом такої атаки є “denial-of-service”, тобто відмова в обслуговуванні з боку сервера, яким користується об’єкт атаки. Це відбувається через надлишок кількості запитів, яка штучно збільшується нападником. Тобто їхній об’єм має бути достатнім для того, щоб серверна машина була не здатна їх обробити, щоб об’єм запитів був більшим за пропускну здатність сервера. Як результат це призводить, наприклад, до неможливості отримати доступ до сайту, додатку тощо. Автор Steve Mansfield-Devine у публікації “The growth and Evolution of DDoS” згадує про те, що наразі описані атаки можуть застосовуватися хактивістами. Він наводить приклад застосунку

Low-Orbit Ion Cannon (LOIC) (Mansfield-Devine, 2015). Даний застосунок дозволяє користувачам надати свої обчислювальні можливості для атаки на певний сервер. Для того, щоб доєднатися до такої атаки немає потреби в особливих технічних навичках. Такий тип атак може бути класифікований як одна з частин статті 363 ККУ.

Патріотичні хакери та OSINT-спеціалісти представлені в Україні різноманітними спільнотами та індивідуальностями. При цьому хакінг не є новим явищем. Частина людей, що раніше займалися, наприклад, кібертероризмом (George & Leidner, 2019) до початку війни, додалися до категорії патріотичних хакерів. Відповідно, їхня діяльність продовжувалася й під час повномасштабного вторгнення. Проте, варто зауважити, що під час повномасштабного нападу з'явилися також низька нових спільнот.

Авторка Tetyana Lokot у своєму тексті "Public Networked Discourses in the Ukraine-Russia Conflict: 'Patriotic Hackers' and Digital Populism" описує результати етнографічного дослідження українських хакерських груп. Серед досліджуваних груп є Ukrainian Cyber Alliance, а зокрема Trinity, Falcons Flame, RUH8. Дослідниця описує Альянс як широке об'єднання різних людей та спільнот (Lokot, 2017). На її думку, Альянс не контролюється державою.

У згаданій перед цим статті Tetyana Lokot, авторка перелічує такі хакерські спільноти як RUH8, Falcon Flame та Trinity, які є учасниками Ukrainian Cyber Alliance. Український Кіберальянс (Ukrainian Cyber Alliance або UCA, або Кіберальянс) є юридичною особою та має статус громадської організації. Їхня присутність у медіапросторі проявляється через наявність акаунтів у таких соціальних мережах як Facebook, Telegram, Twitter. Одним з прикладів хакерських атак Альянсу у бік Російської Федерації є подія, що отримала назву "Surkov Leaks". Про це згадував, зокрема, Aric Toler, у статті "Crowdsourced and Patriotic Digital Forensics in the Ukrainian Conflict" (Toler, 2018). Ця подія полягала

у публікації документів, які, як заявляється, належали російському політику Владіславу Суркову. Вперше ці документи були проаналізовані та опубліковані іншим учасником Альянсу, спільнотою InformNapalm. Іншим прикладом подібної хакерської активності Aric Toler вважає публікацію документів з комп'ютера одного з командирів так званої "Донецької Народної Республіки" ("ДНР"), які доводили тісну кооперацію останньої з Російською Федерацією. У згаданій статті також наводяться й інші спільноти або особи, які вчиняли хакерську діяльність, спрямовану проти Росії або "ДНР". Серед них він називає, зокрема, такі імена чи назви як Necro Mancer, Askai707, sled_vzayt та інших.

Про створення IT-армії заявив Міністр цифрової трансформації Михайло Федоров (Fedorov 2022). Зробив він це у своєму Telegram-каналі. До свого повідомлення він прикріпив посилання на інший Telegram-канал де, за його словами, будуть публікуватися "усі оперативні завдання". IT-армія (або IT Army) має власний вебсайт (it Army of Ukraine), на якому, зокрема, публікує приклади своїх атак. Серед них є, наприклад, звіти про атаки на російські ЗМІ, митницю та інші державні та приватні установи. Сама IT Army на своєму сайті заявляє, що є "фахівцем у DDoS". Там само вони розповідають, що ведуть розробку програмного забезпечення для подібних атак. Це забезпечення працює подібним до згаданого застосунку LOIC чином. Воно надає можливість користувачам доєднатися до атаки.

Автор Nikolay Koval у "Revolution Hacking" вважає, що до Євромайдану, основним інструментом хактивістів був DDoS (Kenneth, 2015b). Як приклад його використання він наводить атаку на державні сайти після закриття торрент-трекера ex.ua. Після Євромайдану, на думку автора, хакерська діяльність почала ускладнюватися. З'явилися нові загрози, розпочалося протистояння з російськими та проросійськими хакерами. Як приклад других він наводить КіберБеркут та вже згадану атаку на лічильну комісію. На думку автора, саме КіберБеркут стояв за цим.

Згадані вище приклади хакерських спільнот, що працюють або працювали з метою зашкодити Росії не являють собою вичерпного списку подібних спільнот. Існують і інші, інформацію про які можна знайти у різноманітних наукових і публіцистичних матеріалах. Проте, наведені вище події ілюструють наявність хакерського контексту в рамках як повномасштабного вторгнення, так і всього російсько-українського конфлікту загалом.

OSINT як інструмент також застосовується вже певний час. Відповідно, після початку бойових дій, цей інструмент почав використовуватися в контексті війни. Як вже зазначалося, це може бути різноманітна розвідка, фіксація воєнних злочинів тощо. Цей інструмент почали використовувати, наприклад, правозахисні організації.

Прикладом застосування OSINT в рамках російсько-українського конфлікту можуть слугувати розслідування Bellingcat щодо катастрофи з літаком Boeing MH17 (Cochrane, 2022). Нідерландська команда Bellingcat ідентифікувала причетних до катастрофи осіб. На сайті згаданої спільноти можна знайти й низьку інших матеріалів, присвячених російсько-українській війні. Серед них можна знайти матеріали, присвячені встановленню місць дислокації сил російської армії, розслідування щодо воєнних злочинів, матеріали зі спробами довести факти цих злочинів тощо.

Згадана раніше організація InformNapalm спеціалізується на відстежуванні російської агресії та її наслідків в Україні та інших країнах (Horska, 2023). На своєму сайті InformNapalm заявляє, що спільнота є волонтерською ініціативою, що була створена у 2014 році як відповідь на російську агресію. Там само публікуються матеріали на різні теми, що об’єднані своєю приналежністю до російського вторгнення 2014-2022 та 2022-2023 років.

Проєкт DeepState являє собою програмне забезпечення, яке демонструє мапу з детальним відображення положення збройних сил. Крім цього, це детальна мапа військових операцій, стану та положення лінії фронту (Horska, 2023). DeepState, крім цього, мають Telegram-канал та інші ресурси у різноманітних соціальних мережах. Там публікуються звіти про їхню діяльність, новини та аналітика.

Наведений список OSINT-спільнот не є вичерпним. Він слугує лише як підтвердження наявності контексту, його стислий опис. Крім згаданих існують і інші українські організації, що присвячують свою діяльність тому чи іншому різновиду протистояння Росії під час її повномасштабного вторгнення. Варто додати, що крім українських хакерських та OSINT спільнот існують також закордонні групи, які також присвячують свою роботу зазначеному конфлікту.

Загалом, деякі автори називають хактивізм різновидом кіберактивізму. Проте, необхідно пам’ятати про те, що “хактивізм” - загальний термін, який іноді потребує уточнення. Саме для цього можуть бути використані запропоновані дослідниками терміни як “кібертероризм”, “патріотичний хакінг” тощо. До уваги дослідників потрапляла й російсько-українська війна, проте наразі оцінити вплив хакінгу на положення сил сторін важко, адже конфлікт досі триває, а оцінка потребує надійних даних, які не завжди можливо зібрати.

Ми будемо використовувати терміни **“хактивізм”** та **“патріотичний хакінг”** у значеннях, що їх запропонував згаданий авторський колектив (George & Leidner, 2019). Крім цього, **наше розуміння ширшого терміну “кіберактивізм”** описується через визначення, що його надав Sandor Vegh (Ayers et al., 2003). Ми також переважно погоджуємося з його класифікацією. Проте, ми не згодні з визначенням Vegh (Ayers, 2003) типу, що він називає дія/реакція. Автор розуміє під цією категорією переважно хактивізм, проте подібне обмеження ми вважаємо надлишковим. Під дією/реакцією ми розуміємо,

переважно, акти прямої дії, які можуть мати будь-який прояв. Щоб потрапити у цю категорію (як ми її розуміємо), діяльність має бути актом, дією, спрямованою на досягнення мети будь-якої, крім безпосередньо інформування, пропаганди, мобілізації чи організації. У контексті російсько-української війни, прикладами діяльності, що може потрапити до цієї категорії й, зокрема, хактивізм (в тому числі й патріотичний хакінг), пошук інформації про дислокацію ворога, який здійснюється на основі відкритих джерел, такий само пошук інформації про військових, злочинців, характеристики та кількість сил ворога тощо. При цьому ці категорії не є несумісними. Одна й та сама діяльність, на нашу думку, може розглядатися як декілька видів. Той саме пошук інформації про військових може бути згодом оформлений у заклик, інформаційний текст тощо. В такому випадку це буде поєднання дії та інформування чи мобілізації. В рамках діяльності-як-процесу ці категорії дії також можуть поєднуватися. Тобто одна спільнота може не зосереджуватися на конкретному типі, натомість використовуючи декілька з них.

Метод OSINT важко назвати суто військовим інструментом. Крім державних служб (як то розвідка, внутрішня армія, поліція тощо), його можуть застосовувати й журналісти, активістки, волонтери. Інструмент має як переваги, так і недоліки. Не дивлячись на те, що він не має суттєвих обмежень для застосування, варто пам’ятати про специфіку конкретних задач, адже інструмент не є абсолютно універсальним.

Наше розуміння OSINT загалом збігається зі згаданими трактуваннями. Ми визначаємо OSINT-діяльність як процес пошуку, обробки та компіляції даних з відкритих джерел. Метою такого пошуку є отримання певного insight’у, інформації, яка не передбачалася як така, що має бути розкрита. Подібна мета вводиться нами для того, щоб мати змогу розрізняти OSINT та інший пошук інформації, адже OSINT є саме “розвідкою”. Таким чином, пошук джерел для, наприклад, наукової роботи не є OSINT-діяльністю, адже наукові статті

передбачаються як такі, що будуть прочитані, написане в них supposed to be read. Проте, пошук таких джерел може слугувати і як приклад OSINT у випадку, коли наукова публікація виступає як джерело інформації, яке (саме по собі або у компіляції з іншими джерелами) призводить до розкриття того, що не мало стати відомим широкому загалу. Натомість, наприклад, встановлення місця дислокації військових через такий пошук може бути визначений нами як OSINT, адже подібна інформація першопочатково приховується.

Варто сказати, що сучасні принципи існування політики можуть розглядатися через призму індивідуальної дії. Ймовірно, воєнну мобілізацію також можна вважати субполітикою, як її розумів Ульріх Бек (Beck, 2005). Механізми такої мобілізації можуть лежати скоріше в полі культурного, ніж раціонального. Українське волонтерство заслужило увагу з боку вчених: воно досліджувалося та продовжує розглядатися вченими з соціальних (і не тільки) наук.

Волонтерство ми визначаємо як надання певних послуг без очікування винагороди. Таким чином, в нашому розумінні волонтерство та активізм є вельми споріднені. Кіберволонтерство (або онлайн волонтерство) у нашому розумінні є тотожним поняттю кіберактивізму. При цьому, в обох випадках винагорода може бути присутня, тому волонтерство та активізм визначаються нами саме через позицію актора, через його мотивацію. Таким чином, винагорода не має бути єдиним або головним чинником мотивації до такої діяльності. Натомість мотивація має лежати у полі емоційного, ідеологічного або соціального (Karagiannis, 2016).

РОЗДІЛ 2
СТРУКТУРА ТА ДІЯЛЬНІСТЬ ДЕЯКИХ ХАКЕРСЬКИХ ТА OSINT СПІЛЬНОТ

2.1. Дизайн та методологія дослідження

Для досягнення нашої мети, ми обрали метод напівструктурованих інтерв'ю. Саме цей метод дозволяє глибше зрозуміти принципи, на яких будується діяльність спільнот, які виступають нашим об'єктом. Такі інтерв'ю дозволяють відстежувати не лише самі відповіді, що надає респондент, але і їхнє емоційне забарвлення, дозволяє почути терміни, якими користуються люди для опису власної діяльності, структури, мотивації, як вони ставляться до людей, яких вважають ворогами тощо. Крім того, ми вважаємо, що цей метод є більш доречним для спілкування з категоріями людей, доступ до яких ускладнений. Використання ж кількісних методів ускладнюється браком даних про генеральну сукупність та її агентів. Адже, як зазначалося, доступ до нашого об'єкта обмежений. Важко оцінити їхню кількість та будь-які інші дані. До того ж такі люди можуть пильнувати про власну безпеку, зберігати анонімність тощо. Доречним було б провести етнографічне дослідження методом включеного спостереження. Проте, такий метод потребує наявності певного рівня довіри до дослідника. Під час роботи респонденти можуть працювати в тому числі з цінними для них даними, які вони не хочуть робити відомими загалу.

Нашими респондентами стало шість людей. Четверо з них належать до хакерських спільнот і двоє до OSINT. Вік респондентів - від 20 до 40 років. Два інтерв'ю проходили під час особистої зустрічі, ще 4 в онлайн-форматі, кожне інтерв'ю тривало близько години. П'ятеро респондентів дали свою згоду на запис, проте одна людина заборонила це робити тому, відповідно, аудіозапис відсутній, натомість її слова нотувалися на папері. Деякі наші респонденти піклувалися про власну безпеку та анонімність. Наприклад, один з респондентів використовував програмне забезпечення для зміни голосу, щоб інтерв'юер не

чув справжнього голосу респондента. Крім цього, інтерв'юер міг зустрітися з уточненням даних про нього. Для цього респонденти використовували певне програмне забезпечення, яке дозволяє дізнатися місце реєстрації, ім'я, номер телефону людини та інші дані про неї.

Відбір респондентів відбувався за критеріальним принципом. В першу чергу ми запрошували на інтерв'ю представників тих спільнот, які ведуть будь-яку публічну діяльність (наприклад, мають власні медіаресурси). Таким чином, ми могли провести огляд публічних даних та тверджень, які респонденти самі надають. Відповідно, критерієм відбору була наявність декларованої хакерської чи OSINT діяльності, яку ми визначаємо формулюваннями, що були надані у попередньому розділі. Така діяльність мала подаватися спільнотами як "проукраїнська", мала декларуватися спрямованість проти Російської Федерації або її представників. "Проукраїнськість" могла бути суб'єктивною самооцінкою спільноти, ми не оцінювали та не намагалися оцінити її рівень або будь-яким чином обмежити її можливі прояви. Після відбору, ми зверталися до потенційних респондентів через різноманітні комунікаційні системи: email, Telegram, Signal тощо. У випадку, якщо розмова відбулася, ми просили в респондентів порадити нам інших співрозмовників і, відповідно, зверталися до рекомендованих ними людей у випадку, якщо ті відповідали зазначеним критеріям, тобто використовували елементи методу снігової кулі. Відповідно, в нас було дві точки входу: по одній для хакерських та OSINT спільнот. Першочергове звертання саме до спільнот, які ведуть публічну діяльність обумовлено тим, що в іншому випадку доступ до людей має суттєві обмеження, адже такі люди не зазначають ніякої інформації про себе. Це ускладнює як визначення відповідності критеріям, так і безпосередньо доступ до таких людей, адже відсутній доступ до контактних даних, які зробили б можливим сам факт звернення.

Анкета містила в собі три блоки питань. Перший блок стосувався безпосередньо діяльності респондентів. У другому ми розпитували про

внутрішню структуру, взаємодію з державою та іншими подібними групами. У третьому блоці ми розкривали мотивацію людей, їхні погляди.

Перший блок слугує цілям розкриття контексту діяльності респондента, її особливостей. Другий блок дозволяє ширше зрозуміти принципи, за якими працює спільнота, яким чином вона організована тощо. Блок з питаннями щодо мотивації слугує цілям, які ми описали під час надання визначення термінам “волонтерства” та “активізму”. Оскільки ми визначаємо згадані явища через позицію людини, її мотиви тощо, ми спитали про це в респондентів. Це дозволить нам точніше описати їхню діяльність.

В цьому розділі ми подивимося детальніше на відповіді респондентів та спробуємо ширше розкрити зміст їхньої діяльності, організаційну структуру тощо. Для цього ми будемо використовувати описані у першому розділі концепції: кіберактивізм, хактивізм, патріотичний хакінг, волонтерство та інші. Крім цього, ми робимо спробу описати мотиваційний та мобілізаційний механізми. З метою збереження анонімності, ми не будемо використовувати справжні назви, імена, конкретні події. Виключенням є випадки, коли нам прямо дозволили вказувати зазначену інформацію.

2.2. Діяльність українських хакерських та OSINT спільнот як прояв кіберактивізму

Для визначення кіберактивізму ми будемо керуватися формулювання Sandor Vegh (Ayers, 2003), а саме: “...politically motivated movement relying on the internet”. Таким чином, щоб назвати певну діяльність кіберактивізмом, необхідно щоб було збережено дві умови: політична вмотивованість та централізація на інтернеті. На нашу думку, в опитаних респондентів збережено обидві умови.

Респондент 1 у відповіді на питання про те, як він сам називає свою діяльність, використав корінь “-кібер”. Назва, яку він пропонує - “кіберджихад”.

Імовірно, це свідчить про той самий фокус на кіберпросторі, інтернеті. Сама назва вже дає інформацію про те, в якому полі знаходиться респондент під час своєї діяльності. Крім того, слово “джихад” натякає на певну боротьбу. З арабської мови це слово перекладається як “зусилля” та, зазвичай, описує будь-які дії, що спрямовані на посилення ісламуб проте у Західній традиції це слово часто трактується як “священа війна” (Streusand, 1994). Проте його можна читати в переносному значенні. Таким чином, “кіберджихад” означає певні зусилля на користь чогось, у чого вірить респондент. У його описі діяльності можна побачити політичний контекст. Наприклад, серед своїх цілей він називав “*разбомбить в каменный век*”, “*чтобы Россия стала сырьевым придатком до Украины*”. Пріоритезація цілей у їхній спільноті, за словами респондента, відбувається за принципом “*как можно больше дохлых русских*”. Ми питали, чи є в респондентів інша діяльність, така, що не пов’язана з інтернетом. Наш співрозмовник відповів, що такої діяльності вони не ведуть. Тільки іноді можуть збирати кошти для тих, кого знають особисто: "*Ты не можешь всем помочь, не можешь всех накормить. Если у вас есть кент, который воюет - помогайте ему*". Проте, до зборів коштів він ставить негативно. Це підкреслює значну виключеність діяльності, яка не була б пов’язана з інтернетом.

Термін “хактивізм” та похідні від нього можна вважати загальноприйнятими. Проте таке слово не подобається Респонденту 2. На його думку, активізм це “*спроба зміни ставлення суспільства до певного питання*”, що, вочевидь, не описує те, що намагається зробити він. Натомість респондент пропонує слово “хакер”, а діяльність називає “хакерством”. Слово “хакінг” (або “хакерство” та інші варіанти) у своєму прямому значенні описує інтернет-діяльність. Коли респонденту пропонувалося обрати з деяких видів діяльності (а саме, робота з софтом, робота з громадською думкою, робота з інформацією та знанням), респондент підкреслив усі три: “*...взломали почту, до этого написали софт, потом прочитать, что там есть полезного. А потом информационная кампания…*”. Його організація є членом ширшої коаліції, в якій крім хакерів

також є й люди з OSINT. Тому злам, аналіз і публікація “всегда идут вместе”. Серед своїх цілей респондент називає російських спецпризначенців, військових, політиків та інші російські або проросійські установи та людей. Іншої діяльності респондент не вів. Він зазначає, що відбувався збір коштів на діяльність його спільноти, але додає: “...а так, только кибер”.

На відміну від співрозмовника, про якого йшла мова у попередньому абзаці, Респондент 3 називає свою діяльність кіберволонтерством, а не хакінгом. Він використовує це слово, бо, на його думку, соціальна складова його діяльності важливіша, саме тому використовується слово “волонтерство”. За аналогією з тим, що було сказано перед цим, трактуємо корінь “кібер” як фокус на інтернеті. Крім того, респондент додає, що його діяльність пов’язана з хакінгом, не дивлячись на те, що він воліє не використовувати це слово. Співрозмовник вважає важливими усі запропоновані види роботи, “*...важко виділити щось одне… Якщо викинути один з цих типів, то вже не получиться [організація]*”. Пояснюючи зміст акценту на соціальному ефекті, людина каже, що однією з їхніх цілей це давати “проукраїнськи” налаштованим людям альтернативний спосіб боротьби. Офлайн діяльності його спільнота не веде і “*скоріше за все не буде*”. Пояснюється це тим, що така діяльність більше контролюється державою, що створює певні труднощі. Саме тому вони уникають діяльності поза інтернетом.

У терміні “волонтерство” з попередньою людиною “погоджується” й Респондент 4. Проте, слово волонтерство він використовує, щоб підкреслити відсутність оплати їхньої діяльності. Його спільнота почала роботу з фокусом на DDoS-атаках. Проте наразі, на думку респондента, така діяльність стала достатньо популярною, “*з’явилася конкуренція*”, тому фокус було перенесено на інші види атак. Їхніми цілями ставали об’єкти військової та критичної інфраструктури Російської Федерації. Іншими видами діяльності, відповідно, спільнота не займається: “*збори грошей менш ефективні, бо всі збирають*”. На

його думку "*треба робити що вмієш робити*". Волонтерство поза інтернетом він вважає таким, що може виявлятися корумпованим.

Серед результатів своєї роботи респонденти згадували різні випадки. Називалися як конкретні кейси, так і загальні результати. До загальних результатів відноситься, наприклад, наступне висловлювання: *"Мы и сейчас качаем [ресурсы], только без их... разрешения, без их ведома"*. Інший респондент зазначав посилення обізнаності щодо принципів роботи російських служб: *"Понимание, как работают российские спецслужбы, какие цели они ставят, как российский истеблишмент воспринимает события в Украине. Иногда даже что они собираются делать и как"*. Деякі респонденти підкреслювали економічну шкоду:

"Любой взлом он сам по себе уже несет ущерб... Они должны выяснить что произошло, должны восстановить систему... Это все человекочасы, это collateral damage... Это даст потом отложенный вторичный ущерб…",

або *"Для Росії ми є певним подразником. Ми наносимо певну економічну шкоду"*.

В описаних випадках розповіді людей про їхню діяльність зосереджені на роботі в інтернеті. Респонденти могли додавати корінь "кібер" до свого визначення власної роботи. Робився акцент на хакерстві як основній діяльності. Серед описаних цілей були об'єкти пов'язані або з Росією загалом, або з її армією зокрема. Могло бути використаним слово "проукраїнський", зневажливе ставлення до росіян. Це все, на нашу думку, дозволяє припустити, що діяльність описаних вище респондентів може бути визначена як конкретний різновид кіберактивізму, патріотичний хакінг. Або, використовуючи класифікацію Sandor Vegh, дія/реакція, пропаганда/інформування та мобілізація. Дія/реакція за своєю мотивацією є "частиною традиційної війни". Можна було почути думки про "надання альтернативи", тобто спроби залучити більше людей до онлайн-активності. Було згадано й інформування/пропаганда, що полягає у веденні медіасторінок або висвітленні певної інформації.

Частина наших респондентів не була залучена до хакерських атак. Натомість вони працювали з OSINT. Така діяльність не пов'язана з прямими атаками. Натомість вона зосереджена на пошуці інформації у відкритих онлайн-джерелах. Мета у збору інформації може бути різною.

Один з OSINT-респондентів (Респондент 5) називає себе розслідувачем. На його думку, 70% його праці це робота з софтом, інформацією, знанням. Їхня спільнота займається, переважно, обґрунтуванням та пошуком доказів вчинення російськими військовими злочинів. Збір інформації відбувається різним чином. Наш респондент каже, що іноді йому доводиться виїжджати до інших міст, щоб особисто поспілкуватися зі свідками. Проте відбувається це, на його думку, не часто, він оцінює їхню частоту як *"3 рази на рік*" або "*5% від роботи*". Таким чином, основна його діяльність лежить відбувається саме в інтернеті. Іншими типами їхня спільнота не займається. Проте ставлення до неї таке:

"*ЗСУ це святе для нас. Ми розуміємо, що вони воюють за нас, а ми воюємо для того, щоб притягувати тих, хто скоїв злочин". "Нічого не може бути вище за те, що робить ЗСУ. Але те, що робимо ми це теж важливо... Правосуддя роблять і ЗСУ і ми одночасно, просто хтось в більшій, а хтось в меншій мірі*"

Вся діяльність зосереджена на злочинах з російської сторони. Респондент розповів, що було зібрано певну кількість інформації, відкриті справи як в українських інстанціях, так і у міжнародних. Крім цього, респондент зазначив, що його "*спеціалізація це обстріли*". Був описаний кейс, коли по фото з медіа та супутників ним було встановлено координати з яких вівся вогонь по українському місту: "*...у Чернігові, там потрібно було геолокувати де пролетіли снаряди по фотках з інтернету. У нас не було точних координат… І щось схоже мали по Миколаєву, але про це потім написали Bellingcat*"

Інша людина з OSINT-середовища, з якою ми поспілкувалися воліє назвати свою діяльність "*правозахистом*". Їхня діяльність зосереджена на обґрунтуванні

геноциду. Він сам описує це так: "*документування воєнних злочинів Росії. Насправді їх і у нас вчиняють, але переважно Росія*". Його функції в спільноті полягають у пошуці інформації та оформленні її у медіапродукт. В їхньої спільноти присутній і гуманітарний напрямок: *"наші прихильники якісь в Штатах, там знайомі, вони почали просто краудфандити якісь кошти. Величезні кошти. Ми почали розподіляти серед тих, хто потребує*". Також вони адмініструють складське приміщення, до якого надходить допомога від російських мігрантів у Європейському Союзі, "*ми намагаємося допомогу зробити комплексною…*".

Загалом OSINT-діяльність наших респондентів можна поділити на два різновиди: правозахист та розвідка. Правозахистом ми називаємо, зокрема, зусилля щодо пошуку даних про підозрюваних, або даних, що допомагають винести підозру, відкрити справу тощо. Словом "розвідка" в такому випадку ми називаємо роботу, яка допомагає встановити координати розміщення військових об'єктів: баз, техніки, іншої зброї, живої сили тощо. Крім цього, наші респонденти могли згадувати й про іншу діяльність, таку, що не відносить до OSINT та відбувається поза інтернетом - офлайн.

Таким чином, у цих випадках ми також вважаємо діяльність кіберактивізмом. Респонденти можуть доповнювати її й іншими видами роботи, такими, що проходять поза інтернетом. Наприклад збір коштів, іншої матеріальної допомоги, або особисте спілкування з інформантами. Проте, вони зазначали, що особисто вони надають перевагу саме кіберактивізму, який вже відбувається в інтернеті. Використання категоризації Vegh ускладнюється там, що під дією/реакцією автор розумів переважно хактивізм. Ми не можемо назвати роботу Респондентів 5 та 6 хактивізмом. Проте, їхня діяльність не завжди може бути описана й двома іншими категоріями, що пропонував Vegh. Наша власна думка полягає у тому, що збір даних є актом прямої дії. Подібна розвідка може бути складовою традиційної війни, адже збір доказів відбувається саме стосовно

воєнних злочинів, може відбуватися пошук місць дислокації ворога, що може призводити до посилення позицій на фронті. Пошук доказів щодо воєнних злочинів, крім того, може слугувати й актом міжнародної політики. Наші респонденти розповідали про те, що здобута ними інформація використовувалася зокрема й у міжнародних інстанціях.

В нашому випадку виявляється, що кіберактивізм може слугувати як повноцінний і єдиний вид активності. Він може не бути доповненням офлайн-активності, він може не бути перенесенням діяльності, що традиційно виконується офлайн до інтернету. Проте, Vegh зазначав, що інтернет є лише ще одним майданчиком, де активісти намагаються досягти традиційних цілей (Ayers, 2003). Загалом ми можемо погодитися, адже цілі, наприклад, патріотичних хакерів, ймовірно, в суті збігатися з такими у військовослужбовців або волонтерів, що збирають кошти на обладнання: ті й інші, припускаємо, хочуть завдати шкоди Росії, хочуть досягти перемоги України, “покарати” винних у злочинах. Різниця полягає, імовірно, переважно у деталях, не у самій меті, а у “кроках” до неї. Можна стверджувати, що інтернет-шлях, яким реалізується подібна мета є унікальним і його реалізація поза інтернетом неможлива. Він не має прямих офлайн-аналогів. На нашу думку, як OSINT, так і патріотичний хакінг є особливими видами людської діяльності, особливим видом субполітики, участі у війні тощо.

2.3. Структура організації українських хакерських та OSINT спільнот

В рамках інтерв’ю ми, крім іншого, розпитували в респондентів структурні принципи функціонування їхніх спільнот. Ми питали яким чином ставляться цілі, як відбувається обговорення. Іншим важливим для нас питання був елемент лідерства, а точніше, його наявність або відсутність. До того ж нас цікавила ступінь включеності держави у подібні групи та інші питання, пов’язані з організацією робочого процесу. Чи можна описати визначити таку діяльність як певний різновид соціального руху?

Щоб дізнатися про ступінь включеності конкретних респондентів у певне тематичне коло спілкування, ми запитували про їхнє спілкування з іншими подібними групами. Респондент 1 серед груп, з якими він спілкується назвав “Золотухін (OSINT Flow), Cyber Legion, Cyber.Anarchy.Squad, Ukrainian Cyber Alliance (RUH8, ІнформНапалм, FalconFlame)” та додав “...их больше 100, наверное”. Наш співрозмовник працює у сфері кіберзахисту. На жаль, Респондент 1 не захотів розповідати про співпрацю з державою. Проте особисто Респондент 1 працював у спецслужбах, описував своє спілкування з ексколегами, про своє ставлення до них тощо. Судячи з тверджень респондента, його можна вважати лідером спільноти, до якої він належить. Він розповідав про те, яким чином визначає ефективність, “надійність” та лояльність інших людей з організації. Говорячи про свою позицію, респондент описав її як “как в Civilization”. Civilization - серія стратегічних відеоігор, в яких гравець бере на себе роль лідера певно фракції, керує життям, політикою, економікою, військовою справою та іншими аспектами життя держави або суспільства.

Проте, ми сумніваємося, що структуру спільноти можна описати як бюрократичну. Задачі розподілені завчасно. Респондент зазначав, що у команді є люди з різними компетенціями. Тому, коли справа доходить до роботи, задачі ніби вже розподілені за замовчанням. Прийняття рішень про цілі Респондент 1 описував так: “шо есть, то берём”. Вибору цілей не передує ані дослідження, ані обговорення. Імовірно, це пов’язано зі специфікою роботи. Респондент 1 описував малу кількість доступних одночасно цілей, тому питання вибору та прийняттю рішень для нього стоїть не часто. Спільнота респондента є неформальною, тобто не зареєстрована я громадська організація або інший тип юридичної особи.

Про свою включеність у ширше тематичне коло розповів і Респондент 2. На його думку, “...мирок кибербезопасности он не очень большой”. Наш

співрозмовник працював у сфері кібербезпеки ще до повномасштабного вторгнення та до війни на Донбасі. Відповідно й про інших подібних спеціалістів, частина з яких також є патріотичними хакерами знає вже певний час. Співпраця ж відбувається, проте “...не дуже активно”. Співпрацю з державою ж цей співрозмовник описував як опосередковану: “...вся эта информация так или иначе попадёт либо к военным, либо к спецслужбам. Потому что они могут на её основе действовать…”. Проте Респондент 2 не розповів про те, чи можуть державні інститути ставити цілі або контролювати їхнє виконання. Цілі обираються спонтанно. Якщо стане відомо про існування певної вразливості якогось програмного забезпечення, організація респондента може “просканировать всю Россию” для того, щоб виявити там цілі, які використовують цей вразливий софт. Також респондент розповідав про складність роботи з цілями, адже використання набутого доступу, за його словами, зазвичай призводить до компрометації нападника і доступ втрачається. Тому його спільноті необхідно оцінювати: варто вдаватися до активних дії чи продовжити спостереження. Крім цього, може бути використана “supply chain attack”. Такий вид атак схожий за соціологічний метод побудови вибірки “снігова куля”, через одну успішно атаковану ціль отримується доступ до інших. Таргетовані атаки також називалися серед можливих методів вибору цілі. Відповідно, для того, щоб вирішити, чи варто використати ціль, проходить обговорення. Є й конкретна людина, що ухвалює подібні рішення (Респондент 2 сказав, що він не є цією людиною). Розподіл задач відбувається також на основі компетенцій, ролі є сталими, задачі розподіляються на їхній основі. Крім цього, респондент описував певний елемент менеджменту, органайзингу та обліку: “...без управления и записей даже невозможно такое количество целей вести”. Перехід від однієї цілі до іншої відбувається, відповідно, “природно”, адже використання цілі призводить до її втрати, а значить до необхідності переходити до іншої роботи. Спільно респондента є формалізованою. Їхнє об’єднання має юридичну особу у вигляді громадської організації.

Проте спілкування з іншими тематичними об’єднаннями може відбуватися обмежено. Про це нам розповів Респондент 3, спільнота якого спеціалізується на DDoS-атаках. Він мало знає про інші групи. Іноді вони можуть об’єднувати зусилля, адже DDoS-атаки потребують значних потужностей для їхнього успішного впровадження. Респондент 3 вважає таку самостійність і автономність перевагою, тому не дуже хоче об’єднуватися з іншими. До початку повномасштабного вторгнення він мало цікавився сферою хакінгу. З державою ж натомість співпраця відбувається прямо, адже спільнота респондента була започаткована державним органом. Проте, він підкреслював автономність: “...Ми абсолютно не залежимо від них ані в стратегії, ані в прийнятті якихось повсякденних рішень”. Співпраця з державними органами відбувається, переважно, через інформаційну підтримку з їхнього боку. В спільноті, до якої належить Респондент 3 є окрема команда людей, які відповідають за прийняття рішень про конкретні цілі, він назвав її “команда розвідки”. Відбувається це на основі завчасно сформованої місії, системи пріоритетів: “...ми не атакуємо, наприклад лікарні… Хочемо максимізувати збитки... Це фінансовий сектор, інфраструктурні цілі… Є пріоритети”. Атакам передує дослідження. Як вже зазначалося, DDoS потребує обладнання. Тому у моменти, коли більш пріоритетні цілі недоступні, можуть відбуватися атаки на “менш важливі” цілі, щоб обладнання весь час знаходилося в роботі. Респондент 3 також розповідав про необхідність пошуку вразливостей: “...мають бути певні вразливості. Таких вразливостей не багато”. Спільнота, про яку йшла мова певною мірою може вважатися формалізованою, адже була заснована державним органом.

Про обмеженість спілкування з колегами розповідав й Респондент 4, який фокусувався на DDoS-атаках, проте наразі перейшов до інших типів. Про інші хакерські спільноти він дізнався вже під час повномасштабного вторгнення, його робота до цього не була пов’язана з кібербезпекою. За його словами, може відбуватися обмін інформацією з OSINT-спільнотами, проте загалом вони працюють окремо. Про своє скептичне ставлення до співпраці з державними

органами респондент зазначив ще до початку інтерв'ю. Його спільнота не зареєстрована офіційно. Він вважає, що організації, які мають юридичну реєстрацію (він навів приклад Ukrainian Cyber Alliance) можуть "отримувати поблажки" з боку держави, проте проявляються вони, на його думку, у вигляді "офіційних подяк". Проте, представники держави все ж таки можуть ставити цілі його спільності. Респондент 4 розповів про спільний чат, до якого належать представники інших подібних груп. В цьому чаті знаходиться представник Служби Безпеки України (СБУ), який надсилає цілі. Проте, за словами співрозмовника, ці повідомлення часто ігноруються іншими учасниками чату. До його спільноти належить, зокрема, людина з СБУ. За словами респондента, ця людина "дуже допомагає". Цілі ж з'являються раптово, відбувається перевірка на вразливості, про яку зазначали й інші респонденти. Спільнота респондента налічує наразі три людини. Прийняття рішень відбувається шляхом обговорення, проте був досвід "лідерства", який респонденту не подобається, він "...за демократичний підхід". За розподіл задач всередині спільноти відповідає сам респондент. Органайзинг, менеджмент та контроль наш співрозмовник вважає недоречними для їхньої спільноти, бо зараз в ній "...майже нікого не залишилося". Перехід до іншої задачі відбувається через певний проміжок часу (респондент казав про п'ять годин), адже якщо подібна атака не спрацювала за певний проміжок часу, це означає, що відсутня необхідна вразливість. Проте наразі цей вид атак використовується спільнотою рідше, адже "...з'явилася конкуренція" в обличчі IT Army. Дана спільнота, не дивлячись на членство людини з державного органу в ній, не є формалізованою, тобто не є юридичної особи.

Таким чином, структура спільноти може бути різною. В ній може як бути, так і не бути присутнім лідер, відповідальна особа або голова. Таке ж різноманіття спостерігається й у питаннях формалізації, адже спільноти можуть як мати юридичну особу, так і не мати такої. Цілі наші респонденти обирають переважно спонтанно, це залежить від контексту, обізнаності та доступу до

інформації про вразливості. Ймовірно, це обумовлено специфікою сфери кібербезпеки. Були згадки про необхідність вибору між використанням цілей, що призводить до їх втрати та продовженням спостереження. Присутнє різноманіття й у питаннях належності до ширшого кола. Можна було почути про включеність до “мирка кибербезопасности”, проте зустрічалися й думки про необхідність працювати окремо, відсутність інтересу, спілкування та співпраці з іншими групами. Робота з державою також може мати різний характер. Це може бути пряме ставлення цілей, проте наші респонденти зазначили про свою незалежність, відсутність контролю за виконанням з боку державних органів. Співпраця може відбуватися й опосередковано. Варіюється й саме ставлення до такої співпраці. Можуть бути присутні елементи менеджменту, органайзингу та бюрократії, зокрема у вигляді обліку, про який згадував один з респондентів.

Вже під час повномасштабного вторгнення долучився до роботи й Респондент 5. Він потрапив до своєї OSINT-спільноти через те, що там працювали його знайомі. Про інші подібні групи він дізнався також після початку вторгнення. Співрозмовник розповідав, що може вестися спільна робота: писатися розслідування, відбуватися обмін інформацією. На його думку, після Майдану кількість таких спільнот збільшилася: “*...таких організацій дуже багато. Вони завжди з'являються, як тільки відбувається конфлікт*”. Стосунки спільноти з державою описувалися у скоріше позитивному ключі: “*Хороші. Ну, з ким як… В основному прокуратура... СБУ, Поліція, Прокуратура. Це три гілки влади, з якими у нас хороші плідні відносини. В одному регіоні можуть бути нормальні стосунки, а в іншому - інші*”. Таку співпрацю респондент скоріше вітає: “*Загалом це ідеальний варіант: коли вони приходять до нас з якимось запитом і ми на нього відповідаємо... І таке відбувається довольно часто*”. Крім цього, респондент займається й георозвідкою, про що згадувалося в одному з попередніх розділів (кейс з пошуком позицій, з яких вівся вогонь по Чернігову). Таким чином, відбувається пряма чи опосередкована співпраця й з військовими, які, припускаємо, потім можуть використати отримані дані для нанесення

ураження. На відміну від наших співрозмовників з хакерських спільнот, Респондент 5 розповів, що браку доступних цілей його спільнота не відчуває: "...у нас дуже багато інформації, є з чого обирати". Відповідно, виникає необхідність приймати рішення щодо того, яка з отриманої інформація буде оброблятися далі. Вирішується це під час обговорення: "*...або запит, або ми самі знайшли цікаві матеріали… Ми це все аналізуємо, сідаємо, у нас є декілька варіантів і з цих варіантів ми обираємо… Ми доходимо до спільної згоди. Не можу одна людина вирішувати*". Респондент 5 негативно ставиться до стратегії управління спільнотою, коли рішення приймає одна людина: "*...по іншому було б якось дико*". Розподіл задач відбувається шляхом пошуку добровольців. Людині можуть запропонувати кейс, проте вона може відмовитися. Проте присутній й елемент профілю. Різні люди у спільноті спеціалізуються на різних типах пошуку. Тому в процесі роботи може відбуватися обмін порадами. Респондент також зазначав на відсутності контролю: "*Не те щоб контроль... Голова відділу читає і пише коментарі... Не можна це назвати контролем*". Дедлайн можуть ставитися у випадках, коли інформація необхідна терміново (наприклад, по запиту з державних органів). Рішення про те, чи буде взята в роботу подібна термінова задача приймає голова. Перехід до інших задач відбувається у випадках, коли попередні вже оброблені або якщо надходить та сама термінова робота. Спільнота Респондента 5 є формалізованою, має юридичну особу.

Респондент (6) з правозахисної спільноти розповів, що співпраця у нього відбувається переважно з правозахисними групами та менше з OSINT-спільнотами. Він це пояснив тим, що "наш OSINT - це не рівень Bellingcat". Не дивлячись на те, що спільнота Респондента 6 співпрацює з державою ("[можуть] проводити допити у нас в кабінетах… Нещодавно почали працювати з СБУ"), його ставлення до таких органів неоднозначне: "...це для нас був дивний симбіоз, бо ми завжди були опонентами з цими структурами... Спадкоємцями КГБ". Проте, співпраця ця, за словами співрозмовника, працює переважно в один бік:

“*...Ми купили їм дрон, спільно їздили документувати злочини… Сказати, щоб вони нам щось дали - такого не було. Бо це держслужбовці, а вони не дуже охоче роблять те, чого від них не вимагає інструкція... І вони не зобов'язані з нами ділитися... Доступу до справ, у яких ми не беремо участь, ми не маємо*”.

Цілі ставляться як похідні від завчасно сформованої місії: “...ціль завжди одна: виявити склад воєнних злочинів”. До прикладу розслідування злочинів у Маріуполі було взяте у роботу через те, що той випадок респондент вважає “надзвичайним”. Подібні рішення про початок роботи приймаються колегіально, проте голова спільноти також бере участь у цьому обговоренні. Присутній і розподіл ролей в залежності від компетенції, а отже є сталі ролі, відповідальні особи. Перехід від задачі відбувається у випадку зникнення контексту, як то було з Маріуполем, коли місто було окуповано і працювати далі в ньому стало неможливо. Дана спільнота є формалізованою, має юридичну реєстрацію.

Таким чином, наші респонденти могли як бути, так і не бути включеними у спілкування з іншими подібними групами. Наприклад, респонденти з хакерських спільнот згадували про те, що вони вже певний час працюють у сфері кібербезпеки. Через це їхнє коло спілкування включає до себе інших професіоналів: колег, товаришів по форумах тощо. Проте респонденти з інших хакерських спільнот не працювали у цій сфері до початку повномасштабного вторгнення. Відповідно, про існування інших подібних груп вони дізналися вже після 24 лютого 2022 року. Ті самі респонденти не співпрацюють, або співпрацюють обмежено зі своїми колегами по справі. Подібне різноманіття можна спостерігати й у респондентів з OSINT-спільнот. Вони можуть співпрацювати з іншими групами, а можуть цього не робити чи робити обмежено. Проте співпраця з державою в нашому випадку відбувається в обох категорій респондентів. Вона може бути як прямою, так і опосередкованою. Проте подекуди державні органи можуть напряму ставити задачі деяким з наших респондентів. Ставлення до держави варіювалося в обох категорій респондентів.

Елементи управління, органайзингу чи менеджменту також зустрічаються у наших респондентів. Проте спостерігається певна демократичність, відсутність голови за яким залишається кінцеве право рішення.

Ми можемо виділити декілька особливостей структури та організації, які нам вдалося спостерігати під час спілкування. Не дивлячись на те, що терміном “хакінг” називається по суті незаконна діяльність, такі організації все одно можуть бути зареєстрованими офіційно. Офіційна реєстрація потребує створення низки документів. На нашу думку, створення юридичної особи каже про наявність певного політичного чи (та) ідеологічного підґрунтя. Таким чином, це каже про те, що подібний хакінг є інструментом досягнення, відповідно, політичних та/чи ідеологічних цілей. В певному сенсі він схожий на роботу pro bono publico - надання професійних послуг “на благо суспільства”, без очікування на винагороду у будь-якій формі.

Таким чином, відбувається не просто співпраця з, а й включення до формального поля. Принаймні під час повномасштабного вторгнення хакери, які зазвичай можуть переслідуватися державою, наразі або співпрацюють з нею або, принаймні, не зазнають такого переслідування. Певну цікавість для нас становить подібний перехід, коли зазвичай незаконна діяльність переходить у категорію такої, що вітається. Ми вважаємо за доцільне згадати про мертонівську класифікацію девіантної поведінки (Merton, 1968). Ми вважаємо, що діяльність хакерських спільнот може бути описана як “інновація” у значенні, що його використовував Мертон та яка, на його думку, свідчить про наявність стану аномії у суспільстві. Тобто цілі такої поведінки є такими, що (принаймні на думку респондентів, про що кажуть їхні цитати наведені перед цим) схвалюються суспільством, проте методи досягнення таких цілей з першого погляду здаються неприйнятними, адже вони є незаконними.

Проте, війна, імовірно, є особливим часом, який, припускаємо, суттєво впливає на суспільство. Ми вважаємо, що відбувся певний перехід хакерської діяльності з категорії неприйнятних до категорії суспільно схвалюваних через прив'язку їх до "правильної" мети. Можливо, подібний перехід можна пояснити станом аномії, що викликаний цією війною. Чинити шкоду ворогу ніби стає важливішим за дотримання законів. Деякі цілі (користь для України, шкода для Росії) починають слугувати виправданням для деяких методів. В такому випадку певні дії, що несуть однозначну шкоду ворогу або таку ж однозначну користь Україні можуть бути протрактовані як позитивні, навіть якщо вони можуть бути описані через статті Кримінального кодексу України. Аргументом на користь самого факту такого переходу може слугувати відсутність переслідувань з боку держави (принаймні до тих пір, поки сама держава не стає об'єктом атак). Один з державних органів створив організацію, яка займається хакінгом, проводить DDoS атаки. Тобто держава визнає подібні методи у комбінації з відповідними цілями за прийнятні. Таким чином, подібна діяльність ніби робить перехід з категорії інновації (прийняття цілей, відкидання методів) до категорії конформного (прийняття цілей, прийняття методів) і більше не може вважатися нами девіантною. Проте, ми не вважаємо, що "проукраїнські" цілі можуть слугувати виправданням для взагалі будь-яких методів, адже ми не володіємо відповідними даними, які дозволили б зробити такий висновок. Але, на нашу думку, наявність таких цілей дещо розширює категорію прийнятних методів. Імовірно, це особливості подібних визначних подій.

Вважаємо за потрібне додати інший приклад подібного зсуву певної діяльності з категорії "неприйнятних" до категорії суспільно схвалюваних. Це шахрайство, яке спрямовано на жителів Росії. Наразі у ЗМІ можуть публікуватися матеріали про подібне шахрайство, в яких воно оцінюється журналістами чи журналістками як щось "позитивне". У своєму репортажі на ресурсі Економічна Правда, журналіст Семен Троянов пише про свій досвід роботи в подібній шахрайській групі (Троянов, 2023). Не дивлячись на те, що він

оцінює їхню діяльність загалом негативно, він пише й таке: "*...добре, що ці гроші частково потрапляють в економіку України*". Можна зустріти й згадки про шахрайство, здійснене проти росіян з прив'язкою до хакінгу. Про це писали такі медіаресурси як "24 канал" (Мінджоса, 2022), "Факти" (Степанюк, 2023), "Фокус" (ФОКУС, 2023). У згаданих матеріалах журналісти використовували такі слова як "хактивіст", "кіберактивіст", "ІТ-фахівець". При цьому такі слова як "шахраї", "злочинці" та інші подібні уникалися. На нашу думку, поява позитивних згадок про шахрайство, яке описується статтею 190 Кримінального кодексу України, слугує аргументом факту "зсуву", "переходу", "наближення" певної діяльності до категорії прийнятного. При цьому відбувається це у випадку, коли діяльність поєднується з певною метою. І рівень схвалюваності такої мети, імовірно, достатній для того, щоб виправдати дії, які зазвичай трактуються як злочинні.

Слід додати, що мета на кшталт "шкодити Росії" стала суспільно прийнятної, імовірно, після окупації Криму, початку війни на Донбасі тощо. Адже до цього контекст протистояння Росії був іншим. Тому наразі важко сказати, наскільки хакерство є суспільно прийнятним методом досягнення цієї мети. На користь прийнятності говорять згадані державні дії (створення хакерської організації) та бездіяльність (стосовно "проукраїнських" хакерів). Проте, Закони досі не змінювалися та у них відсутні виключення для "проукраїнських" хакерських дій. Такий, на нашу думку неоднозначний статус подібної діяльності ускладнює можливість робити однозначні висновки. Можемо припустити, що відбувається й зворотна тенденція. Тобто піднесення інституційних шляхів (слідування законодавству) над метою ("поразка для Росії", "перемога для України") може вважатися чимось з категорії неприйнятного. Така ситуація могла б бути названа ритуалізмом, який також належить до категорії девіантної поведінки за класифікацією Мертона (Merton, 1968). Розгляд такої зворотної тенденції лежить поза метою дослідження, тому робити однозначних висновків з цього приводу ми не можемо.

Проте, не всі хакерські спільноти, з представниками яких нам вдалося поспілкуватися мають формалізацію. На нашу думку, це не заперечує наявності в них певних ідеологічних чи політичних переконань та цілей. Респонденти з таких неформальних спільнот також могли згадувати про свої намагання приносити суспільну користь. На нашу думку, відсутність формалізації не унеможливлює класифікації таких спільнот як суб'єктів субполітики. Існування хакерських спільнот, які при цьому мають юридичну особу у нашому тексті слугує, скоріше, як аргумент на користь факту переходу певної діяльності з категорії девіантної до категорії конформної у разі, якщо вона комбінується з відповідними цілями.

Для деяких респондентів патріотичний хакінг став новим видом діяльності під час повномасштабного вторгнення. Вони не проявляли зацікавленості у ньому до 24 лютого 2022 року. Також ці люди розповідали про небажання продовжувати таку діяльність після закінчення війни. Це може сказати про відсутність суттєвої зацікавленості у цьому виді діяльності. Проте, для них подібна робота стала більш доступною альтернативою службі в армії. Виходячи з цього, можна припустити, що в умовній комбінації "цілі-методи", важливішими є саме "цілі", а методи можуть не бути принциповими для цих респондентів. Таким чином, це може свідчити про певну "епізодичність" їхнього кіберактивізму, патріотичного хакінгу. Цілком імовірно, що сфера їхньої роботи може бути змінена, якщо більш приваблива ініціатива стане доступнішою. На нашу думку, це слугує аргументом на користь описаного перед цим явища. Може простежуватися певний примат, перевага цілей над методами. Тобто така ціль є достатньо вагомою для респондентів для того, щоб вони могли вдатися до мало цікавої для них діяльності. Але ми вважаємо, що не варто казати про повну відсутність уваги до методів з їхнього боку. Адже наприкінці ними був обраний саме патріотичний хакінг.

Проте, OSINT-спільноти мають свої особливості. Сама OSINT-діяльність не може бути прямо описана будь-якою зі статей Законів України. Тому така діяльність першопочатково належить до, скоріше конформної, крім випадків, коли загалом прийнятні методи (пошук інформації у відкритих джерелах) використовується з неприйнятною у суспільстві метою. Представники спільнот, які стали нашими респондентами належать до формалізованих організацій.

2.4. Мотиваційна складова діяльності українських хакерських і OSINT спільнот

Мотивація до OSINT-діяльності, патріотичного хакінгу та інших форм кіберактивізму може бути різною. Мобілізаційними чинниками може виступати безліч явищ. На мобілізаційні механізми впливає, зокрема, суспільство, особисті риси тощо. Ми спробували простежити мобілізацію наших респондентів та описати її термінами Emmanuel Karagiannis та доповнити їх власними за потреби (Karagiannis, 2016). У попередньо згаданій його роботі (про мотивацію добровольців під час війни на Донбасі) він заочно дискутує з позицією, яка пояснює особисті рішення людей виключно раціональним вибором. Натомість він пропонує, крім іншого, розглядати ідеологічні, соціальні та емоційні чинники.

Проте, в нашому випадку мобілізація може бути пояснена і через раціональне. Принаймні сам так пояснював свою залученість до проукраїнського хакерського руху Респондент 1. На питання про те, чому він вирішив цим займатися, він відповідав так:

“*Это выгодно… Если бы война не началась - я бы не жил здесь. А вот когда война началась, я говорю: наоборот! Наконец-то! Прекрасно! Слава богу! Потому что теперь патриотом быть выгодно*”.

Він також додав про те, що воєнні реалії дозволяють йому отримати доступ до практичних і теоретичних знань, які було неможливо здобути в мирні часи. На його думку, це дасть конкурентну перевагу як йому, так і іншим українським

спеціалістам з кібербезпеки. Наш респондент, розповідаючи про своє ставлення до такої діяльності використав слово фразу "...Садизм это весело". І загалом позитивно відгукувався про свій проукраїнський хакінг. Проте, враховуючи висловлювання Респондента 1, які ми наводили у попередніх підрозділах, ми можемо припустити, що емоційна складова все одно присутня. Він використовував лайливі слова щодо росіян, російських військових, згадував про них зі зневагою. Це може свідчити про те, що в нього є негативне ставлення до Росії. Проте, прямо він нам цього не говорив. Варто додати, що Респондент 1 також веде просвітницьку роботу: виступає в університетах, державних службах тощо. Там він розповідає про кіберзахист і, на нашу думку, робить це з емоційним забарвленням: бажанням змінити речі, які він вважає недосконалими. Проте це не заперечує й раціональної складової. Нажаль, виявити яка з них (або обидві) відверта - для нас було неможливо, так само як і встановити яка з них превалює.

Проте, іноді емоційна та соціальна складові можуть виступати й у ролі основних термінів раціоналізацій власної мотивації. Таким чином, Респондент 2 розповів, що він жив у місті, яке наразі є тимчасово окупованим і пояснив свою мотивацію використовуючи емоційні, на нашу думку слова:

"*Ну, во-первых, я из [окупованого міста]. Потому эта война меня касается непосредственно... Меня, мягко говоря обижает, что какой-то неадекватный сосед приперся на мою землю... Не могу появится на своей малой родине давно уже. В каком-то смысле это месть. В каком-то смысле это развлечение…*".

На нашу думку, це є прикладом емоційного механізму мобілізації, що описував зокрема й Karagiannis (Karagiannis, 2016). У раціоналізаціях Респондента 2 були присутні й слова про "соціальний обов'язок: "...Это и наша обязанность как граждан". Ми розцінюємо цей вислів як такий, що може свідчити про соціальну складову, адже респондент посилається на певні соціальні норми або ж юридичні закони. За словами нашого співрозмовника, у хакерське середовище Росії, України та інших пострадянських країн були об'єднані у загальне. Він

розповідав і про те, що до початку конфлікту у нього не було бажання якимось чином шкодити Росії у кіберпросторі:

“*Фанатом России я никогда не был. Никаких братских чувств не испытывал... Постсоветская хакерская тусовка была довольно однородна и едина, но разделение все равно постепенно происходило. Я точно знал, что вот здесь Украина, Донецкая область, а через сто километров Россия, Ростовская область. И никогда не путал где кто… Но и никаких мотивов ломать что-то внутри России у меня никогда не было. Ну, не нравится мне Россия и не нравится. Никто ж силком меня туда не гонит… Был негласный договор со спецслужбами: вы ничего не ломаете тут, а мы закрываем глаза на всё остальное. И это правило в целом, не идеально, но соблюдалось. По крайней мере в черной части андеграунда*”

Як кінцеву мету своєї діяльності він назвав повернення Росії до кордонів 1991 року. Проте, у випадку якщо війна закінчиться без збереження зазначеної умови, діяльність може продовжуватися. Це все дозволяє нам припустити, що в цьому випадку спрацювали соціальні та емоційні механізми мобілізації. Цілком можливо, що вони не єдині, проте саме вони були згадані в першу чергу і ми не змогли знайти у діяльності респондента чогось, що говорило б про помітну присутність раціонального механізму.

Соціальну складову ми помітили й в іншому випадку. Респондент 3 пояснював своє долучення до хакерської спільноти так:

“*Стріляти не вмію... Для мене це була можливість зробити свій внесок… Були люди, які "непричьом". І коли війна закінчиться, до них будуть справедливі питання. Я не хочу бути такою людиною. Це питання совісті*”.

На нашу думку, це свідчить про наявність мобілізації через соціальне середовище, його норми. Людина згадує про “питання”, які, вочевидь, можуть з’явитися з боку інших людей. Ми трактуємо це як слідування певним соціальним нормам, правилам. До того ж в Респондента 3 є бажання припинити подібну діяльність після війни. Адже він, за його словами, не має зацікавленості

у темі кібербезпеки та працює в іншій сфері - у фінтесі. Таким чином, припускаємо, для нього можливість долучитися до спільноти була можливістю реалізувати певну позицію (наприклад, патріотичну).

Подібним чином про своє долучення розповідав й інших представник хакерської спільноти. Респондент 3 розповів: "*Чую сирени, грихіт, але не можу іти служити... Просто рве, не хочу бути непричастним*". Вважаємо потрібним додати й про те, яким чином, на думку респондента, інші люди мотивуються на роботу: "...людей мотивує страх, злість". До повномасштабного вторгнення наш респондент не цікавився (патріотичним) хакінгом. Після закінчення війни планує завершити діяльність. У випадку, якщо конфлікт буде "заморожений" він продовжить свої атаки на російські об'єкти. Таким чином ми можемо спостерігати те, що респондент, говорячи про мотивацію, використовує емоційні терміни, певним чином посилається на соціальний тиск.

Ми можемо описати мотивацію наших респондентів з хакерських спільнот як різноманітну. Тут можна було спостерігати як емоційне забарвлення, так і пояснення через раціональне. Був присутнім і елемент посилання на соціальні чинники: норми, закони, приналежність.

Під час розмов з OSINT-спеціалістами, які стали нашими респондентами, можна було почути звертання до власних бажань приносити користь. Таким чином, Респондент 5 описував власну мотивацію так: "*Я розумію, що це те, що треба робити. Це принесе користь і цим можна займатися, я це вмію… Хочеться працювати на країну і допомогти країні*". Крім цього, він зазначав, що для нього така робота є альтернативою військовій службі: "*Був вибір: або працювати зараз, або вже йти в ЗСУ*". Бажання "*допомогти постраждалим від війни [на Донбасі]*" в респондента, за його словами, з'явилася під час навчання в університеті. Змінилося і його ставлення до OSINT загалом, ця діяльність стала йому цікавою. Після війни він передбачає збільшення обсягів роботи, тому

планує залишатися в цій сфері. Кінцевою метою подібної діяльності є "*притягнення всіх до відповідальності…*". Таким чином, на нашу думку, мотивація Респондента 5 раціоналізується ним через соціальні чинники. Він відчуває потребу "приносити користь", бажання "працювати на країну". Згадка про країну може бути трактована як риса, що свідчить про наявність патріотичних відчуттів, що може виступати як ідеологічний чинник мобілізації.

Подібним чином раціоналізував свою мотивацію до OSINT-діяльності й Респондент 6. Для нього така робота також є певною альтернативою військовій службі: "*Я, як і більшість українців, думав чим я можу допомогти нашій спільній перемозі. Дуже жалкував, що не пішов в армію… Постійно думаю про те, щоб піти служити*". Цікавість до правозахисної діяльності з'явилася в співрозмовника, з його слів, ще у шкільному віці. На його думку, це йому "*властиве за характером*". Також він наголошував на тому, що закінчення війни призведе до збільшення обсягів роботи. Це є однією з причин, чому він хоче продовжити вести свою діяльність. Проте, кінцевої мети його діяльність не має, адже OSINT в цьому випадку слугує, скоріше, інструментом правозахисної діяльності. Потреба ж у правозахисті, за словами респондента, є неодмінною рисою держави: "*Поки є держава - будуть порушення прав людини*". Ми можемо простежити у раціоналізаціях Респондента 6 наявність емоційного ("...**жалкував**, що не пішов в армію…"), соціального та ідеологічного механізмів мобілізації. Адже бажання "допомогти перемозі" може бути прочитано як прояв патріотизму або інших ідеологічних переконань.

Таким чином, від наших респондентів можна було почути як "раціональні" пояснення власної мотивації, так і ідеологічні, соціальні чи емоційні. Крім цього, можна було почути про те, що кіберактивізм є альтернативою службі в армії, прямій участі у війні. Можливо, що для тих респондентів, від яких це можна було почути, кіберактивізм є участі є менш цінною формою участі, адже вони прийшли до неї тільки після того, як зрозуміли неможливість служби. Існує

можливість того, що кіберактивізм виступає у ролі меншовартісного замінника. Разом з тим, що респонденти могли залучатися до подібної активності вже після повномасштабного вторгнення та не практикувати її до його початку, це каже про те, що кіберактивізм не завжди є “повноцінним” способом реалізації власної позиції. Він може виступати як епізодична активність, яка трапляється в момент, коли людина з якихось причин не може звернутися до того виду діяльності, який вважає найкращим. Про це свідчить і факт того, що респонденти могли згадувати про відсутність планів продовжувати роботу після завершення війни. На нашу думку, це свідчить про певний пошук людиною способів реалізації власних бажань. В цьому пошуці, ймовірно, відбувається певна пріоритезація видів активності.

Проте, не варто відкидати й елемент соціальних очікувань. Респонденти, спілкуючись з нами, могли припускати, що ми очікуємо від них бажання служити, адже вони можуть бути марковані як “чоловіки”. Таким чином, подібні ремарки про службу можуть слугувати бажанню переконати співрозмовника у власній маскулінності. В певному сенсі, слова про “неможливість” слугують виправданням невідповідності соціальним очікуванням (реальним чи таким, що здаються реальними респондентові) повною мірою. Враховуючи зазначене, важко робити однозначні висновки щодо меншовартості кіберактивізму, адже ми не можемо бути впевнені у тому, що саме стало причиною згадок про армію: щире бажання або спроба відповідати очікуванням (або щире бажання, викликане необхідністю відповідати ним).

Подібна “меншовартість” (щира чи ні - не принципово) може свідчити й про наявність певних соціальних норм щодо найбільш прийнятних способів дії. В нашому випадку служба в Збройних Силах України може виступати як певний “ідеал”. Тоді інші види діяльності можуть бути дещо затьмарені, виступати як “недостатні”. Від наших респондентів можна було почути слова про “святість” військової справи в контексті повномасштабного вторгнення. Проте, навіть якщо

припустити зазначене, інша діяльність, як от патріотичний хакінг чи OSINT все одно залишає за собою певну частку значущості.

Ми згадували про недосконаліть класифікації Мертона, яка полягає у відсутності уваги до значущості цілей для конкретного суспільства. Таким чином, до класифікації можна було б додати певні “рівні” цієї значущості. Адже, як було згадано, певні цілі можуть робити певну діяльність менш “неприйнятною”, або більш конформною, нормалізувати її. Це не обов’язково означає повне “відбілювання” методів. У згаданому перед цим прикладі про шахрайство, метод оцінювався журналістами як щось скоріше неприйнятне. Проте з’явився простір для схвалювання, з’явився елемент такого схвалювання, хоча діяльність загалом і не стала повністю конформною. Проте й застосувати класифікацію Мертона в згаданому прикладі важко. Адже не до кінця зрозумілий статус методів: чи можна вважати їх відхиленням від суспільної норми? Наскільки багато ненормативності має бути в методі, щоб його можна було вважати відкиданням суспільних норм? Таким чином, класифікація розрахована скоріше на роботу з ідеальними типами. Проте, наведені приклади патріотичного хакінгу, хактивізму, шахрайства, кажуть про те, що діяльність може мати неоднозначний статус, в ній можуть бути присутні одночасно як елементи девіантної поведінки (порушення закону, “аморальність”), так і елементи нормативності (відсутність переслідувань, визнання методу державою, оцінки ЗМІ).

ВИСНОВКИ

Як кіберактивізм загалом, так і хакінг та OSINT зокрема потрапляли до уваги дослідників. Ці явища розгляладалися в різних контекстах: воєнному, громадському тощо. Хакінг як прояв кіберактивізму може мати різні прояви: кібертероризм, патріотичний хакінг та інші. OSINT можуть використовувати як державні інституції, так і громадські активісти, ЗМІ та інші актори. Обидва ці різновида діяльності знаходили застосування і в Україні, зокрема під час збройного нападу з боку РФ у 2014 та у 2022 роках. В Україні існує низка спільнот, що впроваджують таку діяльність в рамках активізму, спрямовуючи її на підтримку України або на шкоду Росії. Як хакінг, так і OSINT вважаються ефективними методами боротьби в рамках збройного конфлікту.

Цим дослідженням було виявлено певні особливості структури та діяльності хакерських та OSINT спільнот. Зокрема, було виявлено, що така діяльність може як бути інституціоналізованої, так і ні. Інституціалізація проявляється у наявності юридичної особи або у прямому включені спільноти до державного апарату. Виявлено можливе різноманіття у питаннях лідерства. Такі спільноти не обов’язково мають “формального” лідера. Натомість рішення можуть прийматися колегіально. Спостерігалася сталість функціональних ролей у деяких спільнотах, на основі якою відбувається розподіл задач. Виявлена можливість наявності елементів бюрократії, органайзингу, менеджменту.

Спостерігалися й певні особливості самої діяльності. Виявлено, що така діяльність може бути класифікована як кіберактивізм. До особливостей діяльності хакерських спільнот належить неможливість багаторазового використання одного здобутого інструменту. Натомість може бути присутня необхідність вирішувати, в який момент здобута інформація може бути використана з найбільшою вигодою. Адже використання, наприклад, здобутих доступів призводить до їхньої втрати. Виявлено можливий брак цілей, що

призводить до необхідності брати в обробку усі доступні в моменті цілі. Серед OSINT спільнот згаданих особливостей виявлено не було. Натомість респонденти наголошували на надлишок доступних цілей. Обидва згадані форми кіберактивізму можуть виступати як єдина і головна форма активності. Поєднання її з офлайн може не відбуватися взагалі, або, якщо таке поєднання таки відбувається, то офлайн діяльність отримує менше уваги з боку акторів, не вважається ними головною чи пріоритетною.

Підтверджено результати інших досліджень: хакерська та OSINT діяльність може бути зумовлена політичними, ідеологічними переконаннями людини, впливом соціального оточення. Проте, не можна виключати й "раціональний", егоїстичний елемент. Не дивлячись на те, що онлайн-активність може виступати як єдина та головна, вона при цьому може бути певним substitute до іншої, офлайн активності. Таким чином, виявлена її можлива "інструменталізація", використання без зацікавленості у самому процесі, примат цілей над методом.

Хакерську діяльність у мирний час, імовірно, може потрапляти до категорії девіантної поведінки. Такі дії заборонені законом та караються, хакери переслідуються державою. Ми виявили, що може мати місце певний зсув нормативності: діяльність, яка зазвичай є неконформною наближається до категорії схвалюваної у випадку, якщо поєднується з певною метою, нормалізується. В нашому випадку в ролі такої мети виступає "шкода для Росії" або "користь для України". Така мета може "виправдовувати" певну діяльність, роблячи її більш прийнятною. Це каже зокрема й про те, що конформність поведінки не завжди може бути встановлена однозначно. Певна поведінка в певних контекстах може мати як елемент девіації, та й елемент конформності.

Питання кіберактивізму і, зокрема, хактивізму та OSINT-активізму заслуговує на подальше дослідження. Сучасний український контекст може

робити таку діяльність більш привабливою. Вона може слугувати певним “замінником” більш “традиційним” шляхам участі у війні. При цьому така діяльність несе значну користь державі: військову та економічну. Враховуючи відносно низькі вимоги до технічних навичок з боку певних видів подібної діяльності, можна сказати, що вона ще має ресурс до зростання. Таким чином, кіберактивізм може допомогти українським державі та суспільству впоратися з новими викликами сьогодення.

ДЖЕРЕЛА

Комiссарчук Ю. OSINT ЯК ОДИН З ІНСТРУМЕНТІВ ДЛЯ ЗБИРАННЯ ІНФОРМАЦІЇ ПРО ВОЄННІ ЗЛОЧИНИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ В УКРАЇНІ // Modern science: innovations and prospects. Proceedings of the 14th International scientific and practical conference. SSPG Publish. Stockholm, Sweden. 2022. Pp. 451-454. URL: https://sci-conf.com.ua/xiv-mizhnarodna-naukovo-praktichna-konferentsiya-modernscience-innovations-and-prospects-16-18-10-2022-stokgolm-shvetsiya-arhiv/

Кримінальний кодекс України. Офіційний вебпортал парламенту України. Retrieved May 25, 2023 from: https://zakon.rada.gov.ua/laws/show/2341-14#Text

Мінджоса, С. (2022). Росіяни помилково скинулися на дрон для ЗСУ: хакери обкрутили їх навколо пальця. 24 Канал. Retrieved May 25, 2023 from: https://24tv.ua/rosiyani-pomilkovo-skinulisya-dron-dlya-zsu-yim-dopomogli-hakeri_n2131545

Офіційний сайт боротьби проти ворога на it-фронті - it Army of Ukraine. it Army of Ukraine. (n.d.). Retrieved May 25, 2023 from: https://itarmy.com.ua/

Степанюк, М. (2023). Хакери зламали акаунт “волонтера” з РФ і замовили секс-іграшки замість дронів на $25 тис. Факти. Retrieved May 25, 2023 from: https://fakty.com.ua/ua/ukraine/20230403-hakery-zlamaly-akaunt-volontera-z-rf-i-zamovyly-seks-igrashky-zamist-droniv-na-25-tys/

Троянов, С. (2023, March 23). Шахрайські “офіси” обманюють росіян і заводять в Україну мільярди. ЕП попрацювала в одному з таких. Економічна правда. Retrieved May 25, 2023 from: https://www.epravda.com.ua/publications/2023/03/23/698383/

Укрінформ. (2023). Галузь OSINT в суспільній та державній діяльності. Retrieved May 25, 2023 from: https://www.ukrinform.ua/rubric-presshall/3679281-galuz-osint-v-suspilnij-ta-derzavnij-dialnosti.html

ФОКУС, Р. (2023). Невідомий хакер зламав гаманці спецслужб РФ та відправив гроші на допомогу ЗСУ. ФОКУС. Retrieved May 25, 2023 from: https://focus.ua/uk/digital/563651-nevidomij-haker-zlamav-gamanci-specsluzhb-rf-ta-vidpraviv-groshi-na-dopomogu-zsu

Ayers, M. D., McCaughey, M., & Vegh, S. (2003). Classifying Forms of Online Activism: The Case of Cyberprotests Against the World Bank. In Cyberactivism: Online activism in theory and Practice (pp. 71–95). essay, Routledge.

Beck, U. (2005). Ways to Alternative Modernities. In The reinvention of Politics: Rethinking modernity in the global social order (pp. 94–109). essay, Polity Press.

Cochrane, J. (2022). Citizen OSINT Analysts : Motivations of Open-Source Intelligence Volunteers (Dissertation). Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:sh:diva-49278

Evangelista, J. R., Sassi, R. J., Romero, M., & Napolitano, D. (2020). Systematic literature review to investigate the application of Open Source Intelligence (OSINT) with Artificial Intelligence. Journal of Applied Security Research, 16(3), 345–369. https://doi.org/10.1080/19361610.2020.1761737

Fedorov. Telegram. (2022). Retrieved May 25, 2023 from: https://t.me/zedigital/1114

George, J. J., & Leidner, D. E. (2019). From clicktivism to hacktivism: Understanding digital activism. Information and Organization, 29(3). https://doi.org/10.1016/j.infoandorg.2019.04.001

Horska, K., Dosenko, A., Iuksel, G., Yuldasheva, L., & Solomatova, V. (2023). Internet platforms as alternative sources of information during the Russian-Ukrainian war. Amazonia Investiga, 12(62), 353-360. https://doi.org/10.34069/AI/2023.62.02.36

Hwang, Y.-W., Lee, I.-Y., Kim, H., Lee, H., & Kim, D. (2022). Current status and security trend of OSINT. Wireless Communications and Mobile Computing, 2022, 1–14. https://doi.org/10.1155/2022/1290129

Karagiannis, E. (2016). Ukrainian volunteer fighters in the Eastern Front: Ideas, political-social norms and emotions as mobilization mechanisms. Southeast European and Black Sea Studies, 16(1), 139–153. https://doi.org/10.1080/14683857.2016.1148413

Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications (pp. 39-48), Tallinn 2015

Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications (pp. 55-58), Tallinn 2015

Lindgren, S., & Linde, J. (2012). The subpolitics of online piracy: A Swedish case study. Convergence: The International Journal of Research into New Media Technologies, 18(2), 143–164. https://doi.org/10.1177/1354856511433681

Lokot, T. (2017). Public Networked Discourses in the Ukraine-russia conflict: ‘patriotic hackers’ and digital populism. Irish Studies in International Affairs, 28, 99. https://doi.org/10.3318/isia.2017.28.9

Mansfield-Devine, S. (2015). The growth and evolution of ddos. Network Security, 2015(10), 13–20. https://doi.org/10.1016/s1353-4858(15)30092-1

Mercado, S. C. (2004). Sailing the sea of OSINT in the information age. Studies in Intelligence, 48(3). https://doi.org/10.1037/e741272011-005

Merton, R. K. (1968). SOCIAL STRUCTURE AND ANOMIE. In Social Theory and Social Structure (pp. 194–216). essay, Free Press.

Streusand, D. E. (1994). What Does Jihad Mean? Middle East Quarterly, 7(3), 9–17. https://doi.org/10.47620/jvpm8028

NATO CCD COE Publications (pp. 39-47), Tallinn 2015

Toler, A. (2018). Crowdsourced and patriotic digital forensics in the Ukrainian conflict. Digital Investigative Journalism, 203–215. https://doi.org/10.1007/978-3-319-97283-1_19

ДОДАТКИ

Додаток А. Лист-запрошення на інтерв’ю.

Доброго дня!

Мене звати Євген Міщенко. Я студент магістратури соціології Києво-Могилянської Академії. Пишу вам, бо я проводжу дослідження на тему OSINT та хак-спільнот в Україні в контексті протистояння росії. Хочу запросити представника чи представницю [назва спільноти] на інтерв'ю.

Інтерв'ю є конфіденційним. Я також можу виключити певну інформацію надану під час інтерв'ю з тексту дослідження за вашим запитом. Мої питання стосуватимуться вашої організації, мотивації, поглядів і вашого спілкування з колегами. Розмова може бути анонімною (через аудіозв'язок) або ж якщо ви бажаєте, можемо зустрітися особисто в Києві.

Я буду дуже вдячний, якщо зможете знайти час для інтерв'ю. Будь ласка, напишіть мені на мою робочу пошту eu.mischenko@ukma.edu.ua або у Signal (+380 99 127 0924) про те, чи можете Ви взяти участь в дослідженні, і який день та час Ви бажаєте обрати для спілкування.

Додаток Б. Гайд інтерв'ю на тему "Діяльність і структура українських хакерських та OSINT спільнот під час російсько-української війни у 2022-2023 рр."

Доброго дня! Мене звати Євгеній Міщенко, я студент шостого курсу соціології в НаУКМА, дякую вам, що погодились на інтерв'ю. Отриману інформацію я буду використовувати під час написання своєї дипломної роботи.

- Хочу зазначити, що інтерв'ю є повністю конфіденційним і я гарантую, що не буду передавати інформацію про вас або про ваші відповіді іншим людям.
- В інтерв'ю немає «правильних» або «неправильних» відповідей, мені важливо дізнатися саме ваше бачення.
- Участь є добровільною і ви не зобов'язані відповідати на питання, якщо не хочете.
- У вас є право в будь-який момент перервати інтерв'ю.
- Уся інформація буде розглядатися в узагальненому вигляді й ніде не буде згадуватися ваше справжнє ім'я чи інша інформація, що дозволяє вас ідентифікувати.

Ваші відповіді допоможуть мені під час написання моєї дипломної роботи, завданням якої є глибше розуміння теми. Якщо у вас виникнуть додаткові питання, коментарі чи ви хочете отримати запис, то ви можете зв'язатися зі мною поштою: eu.mischenko@ukma.edu.ua або за телефоном: +380–98–124–5230.

1. **Почати розмову хочу зі спілкування на тему вашої діяльності в кіберпросторі. Якщо ви вважаєте, що розкриття певної інформації може зашкодити — опишіть загалом, не називаючи конкретних деталей (тобто без імен, адрес, назв).**
   1.1. Як ви самі називаєте ті дії в кіберпросторі, які спрямовані на допомогу Україні або на шкоду Росії? Наприклад, якщо мова йде про

[якщо хактивіст] атаку на сайт великого банку, оператору, міністерства тощо [якщо OSINT] пошук інформації про злочинців, місця дислокації ворога тощо?

1.2. Чи пов’язана ваша робота з [cybersecurity якщо мова про хакінг АБО OSINT/Intelligence якщо мова про OSINT]? Я маю на увазі роботу, яка приносить вам основний дохід.

1.3. У яких із наступних типів дій вам доводилося брати участь? *[тут і далі: якщо респонденту некомфортно говорити про себе — спитати про його знайомих, друзів або попросити описати дії, про які він чи вона чули] [перерахувати та спитати чи брали участь у чомусь із цього без уточнення в чому саме]* Маніпуляція із софтом (*manipulation of software),* інформацією *(data)*, знанням (*knowledge),* громадською думкою *(opinion)*. Можливо, є якісь інші типи крім тих, що я назвав? Можете навести приклад?

1.4. На вашу думку, які із цих дій застосовуються вами та іншими волонтерами найчастіше?

1.5. Розкажіть про наслідки цих дій для ворога та для України. Ви сказали, що були [такі то дії]. За вашою оцінкою, наскільки багато шкоди-для-ворога та/або користі-для-України принесли ці дії?

1.6. Чи доводилося вам протистояти ворожим інформаційним, чи іншим атакам, операціям? Що це були за операції (якого штибу, якого типу — якщо не можете сказати прямо) і як саме ви протистояли їм, наскільки успішно?

1.7. Я знаю, що деякі групи спеціалістів мають іншу діяльність крім безпосередньо протистояння в кіберпросторі. Це може бути збір коштів, купівля обладнання, робота на користь суспільства та багато інших форм. Чи займєатися ви чимось крім кібербезпеки?

1.8. *Якщо так:*

Яку із цих форм волонтерства (кібер та не-кібер) ви б назвали для

себе головною? Чим ви займаєтеся більше? Яка діяльність вам здається більш ефективною?

2. У наступному блоці я б хотів розпитати вас детальніше про організацію спільноти, до якої ви належите або з якою координуєте свої дії:
   2.1. Чи відомо вам про інші групи, які ведуть схожу на вашу діяльність? Чи співпрацюєте ви з ними задля досягнення спільних цілей?
   2.2. Як і коли ви про них дізналися?
   2.3. Як ви вважаєте, чи вплинув Майдан на кількість таких груп?
   2.4. На вашу думку, які стосунки в груп, про які ви знаєте з представниками держави (Кіберполіція, Міністерство оборони тощо)? Чи може відбуватися обмін інформацією з державними інститутами? Чи можуть представники держави ставити цим групам цілі та/або контролювати їхнє виконання?
   2.5. Прошу вас подумати про якусь конкретну операцію. Можете не називати її, просто подумайте. [Якщо вам важко згадати, уявіть типову операцію]. Наступні питання я буду ставити про цю реальну чи уявну операцію:
   З чого все почалося? Як була обрана ціль?
   Чи передувало вибору певне обговорення, дослідження, оцінка, голосування?
   Чи була конкретна людина, яка поставила цю ціль?
   Якщо відбулося обговорення/голосування, у якому форматі воно було? Переписування, дзвінок, особиста зустріч або щось інше?
   Яким чином була розділена робота? Чи була конкретна людина, яка розподіляє задачі?
   Чи присутній елемент контролю за виконанням? Органайзинг?
   Чи всіх поставлених цілей вдалося досягнути?
   В який момент вирішується, що варто відкласти цю задачу та поставити нову?

3. Далі хотілося б перейти до завершальної частини інтерв’ю. А саме до вашої мотивації та поглядів.
    3.1. Чому ви вирішили займатися цим? Як до цього прийшли?
    3.2. Як ви ставилися до подібної діяльності до 24 лютого 2022? А до 2014 року?
    3.3. Чи змінилося ваше ставлення зараз? Коли? Яке воно тепер?
    3.4. Чи займалися ви подібним до 2022 року (та до 2014)? Якщо так: Чи змінився ваш фокус після цих подій (чи ця діяльність також була пов’язана з протистоянням Росії)?
    3.5. Чи плануєте займатися після?
    3.6. Що має відбутися, щоб ви вирішили зупинити таку діяльність? [наприклад: перемога України?]

Дуже дякую вам за участь!