ГЛАВА 7

ДАРКНЕТ: МЕТАФОРИЧНІ Й ФАКТОЛОГІЧНІ НАРАТИВИ ЕЛЕКТРОННОГО ФРОНТИРУ

Марія Бутиріна

Метафорична концептуалізація комунікаційного простору повсякчас виступала евристично цінним дослідницьким інструментом для комунікативістики. Завдяки метафорам він набував виразних структурних абрисів, функціональних характеристик, процесуальних маніфестацій. Згадаємо у цьому зв'язку низку метафор на позначення інтернет-середовища та пов'язаних з ним феноменів: всесвітня павутина, електронний котедж, глобальне село, агора, форум. Усі вони організують наші уявлення, структурують відповідний досвід, упорядковують понятійну сферу. Варто звернути увагу і на те, що історія людства також продуктивно концептуалізувалася у просторових категоріях. Сакральні/світські місця, материкова/діаспорна земля, метрополія/колонія, мирна територія/територія конфлікту. Просторові опозиції зазвичай окреслювали коло проблем, спричинених конкретикою часу, вказували на ціннісні, ідейні, функціональні та інші конфронтації в суспільстві.

У фундаментальній праці «Метафори, якими ми живемо» Дж. Лакофф та М. Джонсон характеризують цей дослідницький процес як метафоричне проєктування, під час якого взаємодіють когнітивна структура «джерела» (source domain) та когнітивна структура «мети» (target domain) (Лакофф, Джонсон, 2004). В результаті з'являються фрейми і сценарії, що дозволяють осягнути доволі абстрактні сутності за допомогою емпіричних інструментальних знань.

Традиції моделювання комунікаційного акту як процесу, що має певну просторову представленість і контекстуальність, обумовлюють домінування саме просторової метафорики у потрактуванні комунікаційних явищ. За Дж. Лакоффом та М. Джонсоном, організувати просторові уявлення здатні структурні та орієнтаційні метафори (Лакофф, Джонсон, 2004). Якщо перші відтворюють структуру одного явища відносно іншого, то другий тип метафор репрезентує місцезнаходження людини в координатах інших явищ чи систем.

Останнім часом у дискурсі комунікативістики з'являються професійно марковані просторові метафори. Зокрема, в роботі Х. Дерахшана «Знищення гіперпосилань, знищення інтернету» демонструється протистояння бібліотеки-інтернету — простору, де реалізується ключова для мережі ідея гіперпосилань, і телебачення-інтернету — системи численних замкнених ком'юніті, де потенціал інформаційної розгалуженості нівелюється лінійністю, однорідністю й пасивністю інформаційного споживання (Derakhshan, 2016).

Просторову метафору репрезентує і поширена візуалізація структури Інтернету. Тут застосовується протиставлення двох різновеликих сегментів мережі, що унаочнюються зображенням айсбергу (див. рис. 1). Видима частина Інтернету є кратною розміру сегменту, що залишився під водою. Вважається, що його розмір неможливо визначити остаточно, оскільки він

М. Бутиріна
Дніпровський національний університет імені Олеся Гончара,
Дніпро, Україна
butyrinam@gmail.com

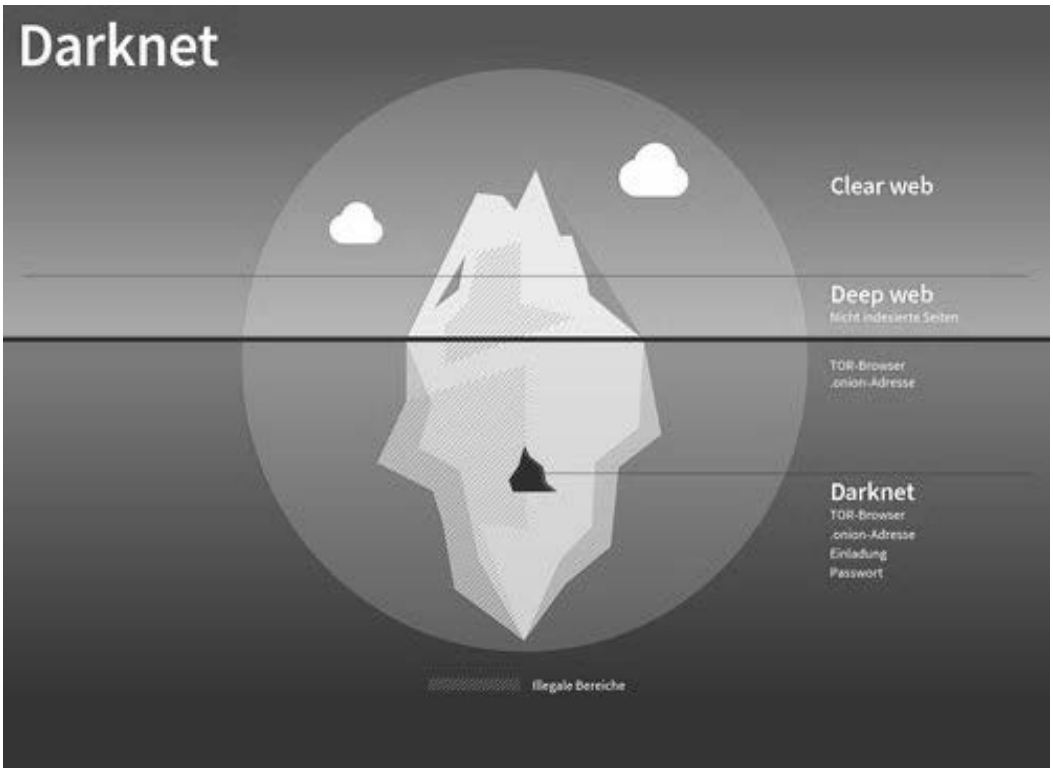

Рисунок 1. «Айсбергова» метафора Інтернету
Джерело: https://www.gdata.de/ratgeber/was-ist-eigentlich-das-darknet

постійно зростає в геометричній прогресії (Tzanetakis, 2017). Є, однак, і інші погляди на айсбергову структуру Інтернету. Експерти Recorded Future вважають, що картинка, яка унаочнює місцезнаходження та пропорції поверхневої і темної павутини, насправді є перевернутою. Вони засвідчують, що кількість доступних онлайн-доменів становить менше 0,005 % від кількості доменів поверхневих вебсайтів, а з приблизно 55 000 цибулевих доменів, які були ними віднайдені, лише 8 400 є активними[1] (Sanchez & Griffin, 2021).

Метафорична концептуалізація Даркнету спирається на бінарну логіку архетипного характеру: білий Інтернет як середовище протиставляється темному Інтернету. Метафорика кольору має цілком впізнавану аксіологію: білий Інтернет позиціонується як легітимний, соціально схвалений, інтенціонально позитивний, а темний Інтернет відповідно постає як нелегітимний, пов'язаний зі злочинними намірами та соціально засудженими способами використання. Вказане протиставлення є стереотипним і певною мірою не відповідає дійсності. У медіа педалюється тема злочинного характеру використання Даркнету, що сприяє виникненню відповідних викривлених уявлень.

Ще одна лінія протиставлення: поверхневий Веб/видимий Веб (Surface Web, Visible Web) і глибинний Веб (Deep Web) — репрезентує просторову метафору, яка концептуалізує різні рівні доступності мережі.

Маємо зважати на те, що просторові характеристики феномену мережі деформуються у сприйнятті індивідів, а отже метафорика здобуває переважно перцептуального навантаження. Вона не стільки відображає реальний часопростір певного процесу чи явища, скільки акумулює соціально-психологічний досвід переживань об'єктів метафоризації.

Метафора Е-фронтиру

Доволі частотною метафорою на позначення генези інтернет-простору є фронтир. Цей концепт, уперше застосований дослідником американської історії Ф. Дж. Тернером, сьогодні активно експлуатується дослідниками Web-простору.

[1] Цікавим є розподіл мережевих сегментів за мовною ознакою. Як засвідчують експерти *Recorded Future*, 86 % цибулевих сайтів представлені англійською мовою, а наступними двома найпоширенішими мовами є російська (2,8 %) і німецька (1,6 %). Дослідники також звертають увагу на те, що на поверхневому сайті англійська мова посідає перше місце лише з 54 % (Sanchez & Griffin, 2019).

Рисунок 2. Перевернута «айсбергова» метафора Інтернету
Джерело: https://www.recordedfuture.com/dark-web-reality/

Фронтир, окреслений, перш за все, географічно, набуває в роботі Ф. Дж. Тернера символічний сенс, оприявнює архетип розвитку, постає одночасно і як «рухомий кордон», і як «цивілізаційне перехрестя» (Тернер, 2009). Сучасні наративи концептуалізують фронтир як еластичну й проникну межу, що відділяє онлайновий світ від оффлайнового. В роботі Н. В. Плотичкіної та Є. Г. Довбиша конструкт фронтиру використовується для унаочнення експансії держав і окремих індивідів у цифровий простір, розширення завдяки технологіям їх просторових координат і можливостей впливу (Плотичкина, Довбыш, 2017).

Розробник концепції фронтиру, історик Ф. Дж. Тернер уважав, що уявлення про межовий кордон є цінними для концептуалізації історії США. Фронтирна тематика виявилася плідною для розуміння історико-ментальних процесів у Сполучених Штатах Америки, адже тут просторові характеристики відіграли значну роль у становленні держави. Подібним чином просторова представленість мережі сьогодні унаочнює розвиток суспільства цифрової доби.

Метафора Е-фронтиру дозволила концептуалізувати Інтернет як простір з особливими властивостями. Як зазначає Б. Мейсон, «гіпотеза фронтиру Тернера була повністю розграбована, щоб представити Інтернет як новий кордон із відважними першопрохідцями, що вирушають на її освоєння» (Mason, 2017).

Метафора рухливого прикордоння вплинула на навколомережеві наукові наративи. Так, наприклад, книга «Віртуальні спільноти» Ховарда Рейнгольда, якого називають першим громадянином Інтернету, має підзаголовок «Садиба на електронному кордоні». Розвідка Джеймса Піткова і Пітера Піроллі має назву «Життя, смерть і законність на електронному фронтирі» (Pitkow &Pirolli, 1997). Хелен Маклюр у розвідці «Дика, дика мережа: міфічний американський захід і електронний фронтир» демонструє, як уміст архетипу західного фронтиру, що інтегрує економічні можливості, безпекові питання та психологію «переселенців», екстраполюється на Е-фронтир (McLure, 2000). Дейв Хілі стверджує, що «комп'ютерний хакер є духовним нащадком» американських літературних героїв: «Як і Гек Фінн, прототип хакера — молодий чоловік, який знаходить порятунок від «цивілізуючого» впливу авторитетних постатей. Його пліт — комп'ютерний термінал, за допомогою якого він прокладає курс у нові та іноді небезпечні сфери» (Healy, 1997).

Які ще ремінісценції з теорії Ф. Дж. Тернера ми можемо впізнати в сучасному інтернет-просторі?

Західний фронтир відображає складний і неоднозначний процес просування переселенців на неосвоєні території. Е-фронтир репрезентує процес поступового підкорення віртуальної реальності користувачам. Якщо згадати дифузну теорію Е. Роджерса, можна визначитися і зі стратифікаційною

диференціацією такої експансії: спочатку нові «території» освоюють інноватори (2,5 %), потім йдуть ранні приймаючі (13,5 %), за ними — рання більшість (34 %), яка опановує нові ідеї до того, як вони будуть поширені серед пересічних громадян. За ранньою більшістю інновації приймає пізня більшість (34 %) і, зрештою, на сприйняття нового погоджуються консерватори (6 %).

У своїй теорії Ф. Дж. Тернер позиціонує фронтир як «запобіжний клапан», який давав США можливість пом'якшити соціальну напруженість у суспільстві: на «кордоні» формувалися і постійно відтворювалися ідеали свободи та демократії (Тернер, 2009). Вочевидь, інтернет-простір попри тенденції інституціональної медіатизації також виконує роль притулку для девіантних рухів та маргінальних персон.

Поступово термін інтегрує і додаткові значення: фронтир сприймається як територія можливостей, що безумовно корелює із сьогоднішніми уявленнями про онлайновий світ. Електронний фронтир приваблює користувачів можливостями, що охоплюють усі сфери життєдіяльності людини, — від роботи до дозвілля.

У процесі віртуалізації глобального суспільства, медіатизації всіх сфер життєдіяльності людей електронний фронтир, представлений сегментом Clearnet, здобуває статус легітимного простору. З'являється нове прикордоння, нова маргінальна царина — Darknet, який ми також можемо розглянути в категоріях теорії фронтира.

Deep Web

Концептом «Глибока павутина» позначається той контент мережі, котрий не реєструється пошуковими системами, оскільки він не інтегрований до їхньої бази даних. Причин уникнення мережевої прозорості може бути кілька. Зокрема, у глибинному вебі можуть функціонувати інтрамережі, тобто мережі компаній та організацій, навмисно відгороджені від загальнодоступного Інтернету. Це також можуть бути сторінки, жодним чином не пов'язані зі змістом білої мережі. Індексації пошуковими системами можуть також перешкоджати платіжні бар'єри та облікові записи користувачів. Такі сторінки можуть бути знайдені користувачами за умов знання конкретної адреси. Види глибинної павутини представлені у табл. 1.

Таблиця 1. Типи глибокої павутини

Джерело: (Sherman et al., 2001). https://www.ideals.illinois.edu/bitstream/handle/2142/8528/librarytrendsv52i2h_opt.pdf

Тип Deep Web	Переклад	Пояснення
Opaque Web	Undurchsichtiges Netz Непрозора мережа	Може бути проіндексовано, але технічні характеристики та співвідношення витрат та вигод не дозволяють цього зробити.
Private Web	Privates Netz Приватна мережа	Може бути проіндексовано, однак це заборонено обмеженнями доступу. Наприклад, йдеться про інтранет (внутрішні приватні мережі організацій чи відомств) або сторінки, захищені паролем.
Proprietary Web	Gesetzlich geschütztes Netz Юридично захищена мережа	Пошукові системи в більшості випадків не можуть отримати доступ до сторінок у пропрієтарному Інтернеті, оскільки вони доступні лише людям, які погодилися на особливі умови в обмін на перегляд вмісту. У багатьох випадках реєстрація є безкоштовною, але пошукова машина не може задовольнити вимоги навіть найпростішого процесу реєстрації.
Invisible Web	Unsichtbares Netz Невидима мережа	З технічного погляду ці сторінки можна проіндексувати. Однак цього уникають з комерційних чи стратегічних причин. Наприклад, йдеться про бази даних із веб-формою
Truly Invisible Web	Tatsächlich unsichtbares Netz Справді невидима мережа	Веб-сайти, які (поки що) не можуть бути проіндексовані з технічних причин

На рис. 3 ми можемо побачити функціональну структуру Інтернету:

A) поверхнева мережа з загальнодоступними веб-сайтами (блоги, електронні магазини, журналістські матеріали).

B) глибока мережа, що складається з веб-сайтів, які вимагають входу в систему (електронна пошта, банкінг, послуги передплати).

C) темна мережа (частина глибокої мережі), до якої можна отримати доступ лише за допомогою спеціальних інструментів і яка не індексується пошуковими системами (Nelson, 2020).

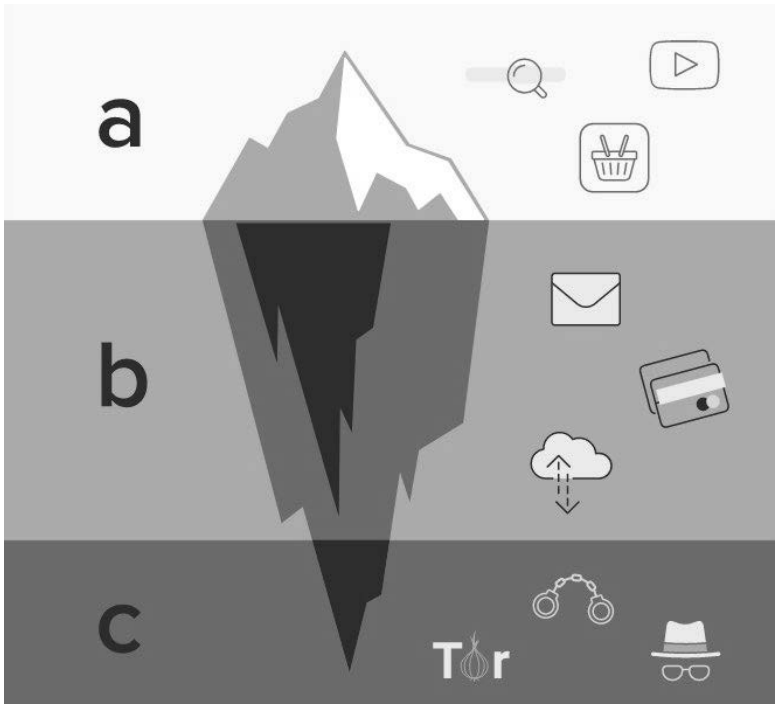

Рисунок 3. Функціональна структура Інтернету
Джерело: https://www.avast.com/de-de/c-dark-web#gref

У медіадискурсі Darknet помилково ототожнюють з Deepweb. Насправді ж, як можна побачити на рис.1, 2, 3, Даркнет є лише частиною глибинного вебу.

Даркнет — це підмножина мережі, що прихована у зашифрованому шарі під звичайним павутинням. Доступ до неї уможливлюють спеціальні інструменти, зокрема, браузер Tor (The Onion Routing), що є найпоширенішим засобом потрапляння до Даркнету. Tor використовує техніку так званої «цибулевої маршрутизації», яка передбачає, що між клієнтом і сервером для зв'язку встановлюється ланцюг з трьох вузлів. «Цибулева» маршрутизація належить до технологій, які уможливлюють анонімне спілкування через комп'ютерну мережу за допомогою шарів шифрування. Дані шифруються на кожному вузлі під час проходження через ланцюг. Така процедура приховує фактичну IP-адресу клієнта і дозволяє користувачеві переглядати вебсторінки без стеження.

Даркнет як е-фронтир

Становлення темної мережі долає ті ж самі етапи, які численні дослідники визначили нормативними для білого електронного фронтиру, послуговуючись аналогією з періодизацією Ф.Дж.Тернера. Даркнет виник унаслідок усвідомлення потреби особистої безпеки в Інтернеті. Розробники ідеї «цибулевої маршрутизації», яка згодом уможливила безпечні комунікації в мережі, керувалися ідеями децентралізації, свободи, відкритості. Йдеться, власне, про ті базові цінності, якими опікувалися «піонери» західного фронтиру. У своїй фундаментальній праці Ф. Дж. Тернер неодноразово підкреслював, що на «кордоні» формувалися і постійно відтворювалися ідеали свободи та демократії (Тернер, 2009). Показово, що у 2004 р. організація Electronic Frontier Foundation, яка поділяє цінність цифрових прав, почала фінансувати розробки проєкту Tor. Первісно можливостями нової технології опікувалися категорії активістів і технічних інноваторів, зацікавлені в забезпеченні приватності при роботі в інтернет-середовищі (Moßbrucker, 2019).

На початкових етапах (перший, другий етап, за Ф. Дж. Тернером) освоєння західного фронтиру його населення було однорідним, лише згодом воно поступово набуло різнорідності і, відповідно, стало більш численним. Подібні закономірності спостерігаються і у генезі темного е-фронтиру: поступове збільшення кількості користувачів супроводжувалося їх урізноманітненням, розширенням спектру інтересів тих, хто «заглиблювався» у темне павутиння. Важливою є заувага розробників Tor: чим вищий рівень різноманітності користувачів, тим надійніше їхня безпека.

На третьому етапі становлення західного фронтиру набули ваги самоорганізаційні процеси, сформувалися чинники порядку. За умов відсутності інституційного управління переселенці вміли зберігати лад на своїй території. В аналогічний спосіб самоорганізація відбувалася і в Даркнеті.

З’явилися неписані правила поведінки в ком’юніті. Спосіб, яким використовується інтернет на віртуальному темному фронтирі, передбачає сувору анонімність. Режим «інкогніто» провокує інтерес користувачів до протиправної діяльності, хоча первісно інструменти анонімізації розроблялися із цілком гуманними цілями. Серед різновидів злочинної діяльності у Даркнеті можна назвати: збут наркотиків та психотропних речовин; продаж зброї та боєприпасів; торгівлю фальшивими документами, людьми; надання послуг убивць-найманців; продаж даних, отриманих хакерським шляхом. Незаконні сервіси, злочинні ком’юніті — все це кореспондується із такою тенденцією, як зростання беззаконня на ранньому фронтирі.

На подальших етапах розвитку західного фронтиру, за Ф. Дж. Тернером, з’являються нові стилі поведінки, формується фронтирна ідентичність. Подібні процеси спостерігаються й у середовищі Даркнету. Абсолютизація анонімності спричиняє формування мережевих ідентичностей і культ статусності користувача, реальні дані якого у темній павутині повністю знівельовані. У вимірі Даркнету ідентичності не стільки оприявнюються, скільки конституюються.

Медійні наративи і демістифікація Даркнету

Даркнет має усталений медійний образ території зла, такої собі тінистої ділянки вулиці, де відбуваються темні справи. Заголовки публікацій, присвячених Даркнету, рясніють усіма категоріями найтяжчих злочинів — педофілія, вбивства, продаж органів, наркоторгівля, торгівля зброєю та вибухонебезпечними речовинами, тероризм.

СБУ викрила схему, на якій «відмили» десятки мільйонів доларів у Darknet. *Укрінформ.* 25.10.2021

Найбільший злив даних в історії: у Даркнеті продають дані 1,5 млрд користувачів Facebook. *Фокус.* 04.10. 2021

Хакери у даркнеті опублікували конфіденційну інформацію про вакцини проти COVID-19. *Дзеркало тижня.* 13.01.2021

Поліція встановила причетних до зливу даних мільйонів користувачів Telegram в даркнет. *Укрінформ.* 25.06.2020.

Даркнет: там, де злочинці почуваються у безпеці. *Obozrevatel.* 14.08.2018

Представлений на рис. 3 візуальний образ темної павутини є колажем з медійних ілюстрацій даркнетівської тематики. Синьо-чорна кольорова гама є типовою для медіапрезентацій цього сегменту Інтернету. Так само і образний ряд, що конотує смертельну небезпеку і криміналітет, закріплює у свідомості реципієнтів суто негативні настанови на сприйняття темного павутиння.

Рисунок 4. Колаж з ілюстрацій на теми Даркнету в українських медіа

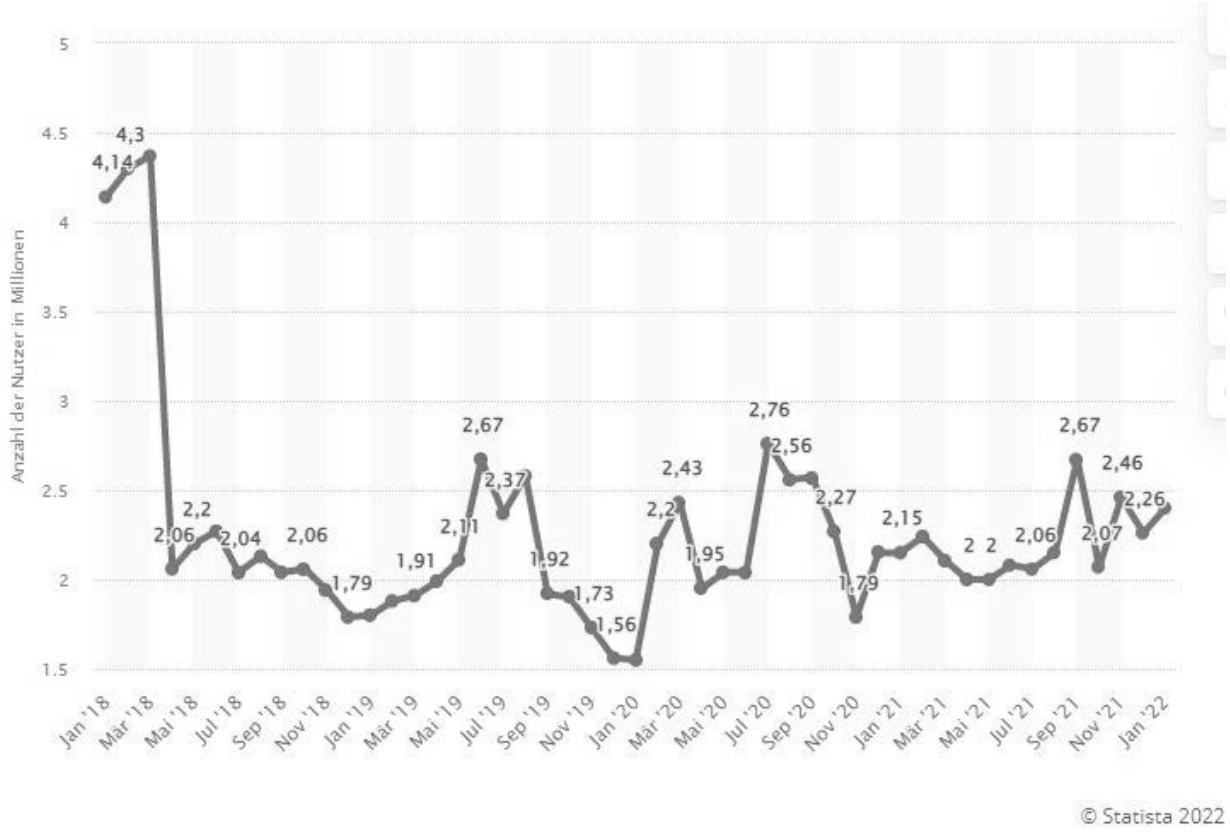

Рисунок 5. Кількість користувачів Tor у світі (січень 2018 — січень 2022 рр.) в мільйонах осіб.
Джерело:https://de.statista.com/statistik/daten/studie/1024020/umfrage/anzahl-der-taeglichen-nutzer-des-tor-netzwerkes-weltweit/

З одного боку, від'ємні конотації є цілком справедливими для цього інтернет-сегменту, адже він, дійсно, є майданчиком для криміналітету завдяки непрозорості, анонімності, прихованості від спостерігачів. Водночас анонімність як ключова характеристика комунікаційних зв'язків Даркнету сприяє також практикам, мотивованим загальновизнаними цінностями — свободи, справедливості, прав людини тощо.

Риторика проєкту Tor оприявнює високі гуманістичні ідеали і, що цілком закономірно, жодним чином не заторкує тіньовий бік його використання. На сайті проєкту зазначається, що його команда працює заради просування громадських прав і свобод та захисту конфіденційності користувачів, що Tor — це більше, ніж програма, адже у неї заклали душі волонтери з усього світу, що вірять у цінність прав людини (https://www.torproject.org/). На рис. 4 можемо побачити динаміку кількості користувачів Tor у світі за останні чотири роки. Після вибухоподібного сплеску інтересу до цієї програми у березні 2018 року бачимо спад і стабілізацію на рівні 2–2,5 млн осіб.

Даркнет потребує демістифікації, розуміння того, що метафора темної мережі нічого не повідомляє нам про зміст цього інтернет-сегменту, скоріше вона вказує на особливості доступу до цього змісту і на характер міжособистісних зв'язків.

Активність журналістів-розслідувачів, застосування інсайдерської інформації, інформаційна протидія владним інституціям гостро ставить питання кібербезпеки. У редакцій виникає потреба мати канали безпроблемної анонімної передачі даних. Деякі з них поступово освоюють Даркнет саме тому, що ця цифрова мережа захищена від решти Інтернету та використовує технологічні засоби для створення анонімності для своїх користувачів. Хто пропонує контент, хто з ким і про що спілкується — все це приховується за допомогою технологій шифрування.

Ключовий мотив звернення до можливостей темного Інтернету — потреба не залишити своїх «цифрових слідів» під час пересування майданчиками Вебу. Як слушно зазначає представник «Репортерів без кордонів» Даніель Мосбрукер, «Даркнет – це інструмент, як будь-який інший. Молоток можна використовувати у корисних цілях, а можна ним покалічити людину» (цит. за Соколовська, 2017).

До соціально схвалюваних користувачів Даркнету відносяться репортери та журналісти з країн, де свобода ЗМІ не гарантується або в яких критичні репортажі караються. Це також можуть бути

фахівці, які не працюють у медіаіндустрії, утім прагнуть ділитися інформацією, не наражаючи себе на небезпеку.

Наприклад, британське видання *The Guardian*, американські видання *The New York Times* та *Heise Online* створили анонімні електронні скриньки у Tor Darknet для захисту безпеки своїх інформаторів.

Deutsche Welle також тривалий час користується власною «цибулевою службою», що полегшує користувачам у всьому світі отримувати анонімний доступ до вільних мас-медіа. Йдеться про представників аудиторії, яким доводиться побоюватися репресій за використання непідконтрольних владі ЗМІ. Tor також може бути корисним інструментом для журналістів, якщо вони не можуть здійснювати відкритий пошук інформації через те, що їх переслідують державні структури та спецслужби. Така можливість є надзвичайно важливою для журналістської діяльності, оскільки страх перед стеженням спричиняє самоцензуру і призводить до відповідних викривлень інформації.

У країнах, де заборонено користування соцмережами Фейсбук, Твіттер, Ютуб Даркнет надає інструменти, що дозволяють обійти таку заборону. У блозі Інституту Інтернету і суспільства дослідниця Меропі Цанетакіс (Institut für Internet und Gesellschaft) коментує емпіричні дослідження Даркнету, згідно з якими 52 % контенту є легальними відповідно до законодавства Великобританії та США.

Серед усіх досліджених сайтів перше місце посідають послуги обміну файлами — 29 %, за ними — витік даних (28 %) і фінансове шахрайство — 12 %. Лише 4 % перевірених вебсайтів стосуються наркотиків, а 0,3 % — зброї (Tzanetakis, 2017). Дослідниця вказує на високий рівень безпеки і конфіденційності як на ключові цінності Даркнету, якими можуть скористатися дисиденти, журналісти або правозахисники, аби проінформувати про утиски, корупцію, дискримінацію та інші зловживання. Згадує, що під час арабської весни активісти використовували Tor для обміну інформацією, аби бути поінформованими і водночас залишатися анонімними.

Вкажемо на кілька топових сайтів .onion, якими можуть скористатися відвідувачі Даркнету: *The Hidden Wiki* – каталог темної мережі, що дозволяє знайти сайти та інструменти, які можуть зацікавити користувачів; бібліотека *Genesis* — величезна колекція книг, літератури та коміксів; *Sci-Hub* — база даних, яка уможливлює безкоштовний доступ до наукових праць; *The Intercept* — онлайн-платформа, яка надає останні новини без цензури та обробляє інформацію від викривачів; *ProPublica* — платформа, що спеціалізується на матеріалах з політичної, фінансової та екологічної тематики; *Secure Drop* — невідстежувана платформа для викривачів, що надсилають інформацію у масмедіа (Schuster, 2022).

Парадоксальність застосування Даркнету полягає у тому, що відкриті темною мережею можливості рівною мірою використовуються і для захисту громадських прав і свобод, і для ведення злочинної діяльності. Найбільш відомим у царині криміналітету є створений на теренах Даркнету перший чорний онлайновий ринок *Silk Road* (Шовковий шлях), який був закритий правоохоронцями у 2013 р., а його засновника було засуджено до вічного ув'язнення.

Анонімність темної мережі також використовується у злочинних цілях і терористичними організаціями.

Даркнет приваблює багатьох акторів, що здійснюють легальну, напівлегальну і нелегальну, пов'язану із криміналом, діяльність. Відомий викривач Едвард Сноуден свого часу застосував Даркнет для того, щоб переслати отримані відомості журналістам. У Даркнеті також можна знайти анонімні біржові трейдери, вебсайти активістів, інформаційні бази для журналістів, політичні чати, сервіси миттєвих повідомлень, платформи художників, портал *WikiLeaks*, що надає можливість анонімного подання інформації (Viney, 2017).

Значна обмеженість втручання владних інституцій у функціонування Даркнету відповідає ситуації 90-х рр., характерної для білого сегменту електронного фронтиру, коли контроль був обмежений.

Серед акторів, які застосовують Даркнет у професійних цілях, можна назвати правоохоронні органи, що використовують інструментарій темної мережі для онлайн-спостереження і проведення операцій, і військові та розвідувальні служби, які вивчають ризики середовища, в якому вони діють.

Як повідомляє експерт з кібербезпеки Міністерства оборони США Кріс Коуен, Ісламська держава і угруповання, що підтримують її, використовують анонімність темної павутини не тільки для обміну інформацією, вербування та розповсюдження пропаганди, але й для збору грошей на

свої операції за допомогою біткоїну. Військові відстежують цю діяльність та застосовують різні тактики, щоб зірвати плани терористів (Cowen, 2019).

Даркнет використовують у своїх приватних цілях і особи, які прагнуть безпроблемного самовираження серед однодумців та опонентів. Як зазначає французький журналіст Жан-Марк Манах, «ми знаходимося в центрі парадоксу конфіденційності: з одного боку, користувачі Інтернету постійно висловлюються в мережі, з іншого, вони бояться наслідків, які це може мати для їхнього приватного життя» (Manach, 2010).

Даркнет як гетеротопія

У своїй роботі «Інші простори» Мішель Фуко пропонує концепт «гетеротопія», що може стати евристично цінним для концептуалізації Даркнету як «простору усередині простору» (Foucault, 1967).

Просторова парадигма наразі збагачує аналітичний інструментарій міждисциплінарних досліджень, поволі витісняє ідею історії як ключову змістотвірну категорію. Французький дослідник вказує на існування двох просторових вимірів суспільства. Це утопії — так звані місця без реальних місць, що представляють суспільство в удосконаленому вигляді, часто перевертаючи його з ніг на голову. І це антиутопії, які доводять до абсурду ганебні суспільні риси, утворюючи гротескний образ соціуму, насичений від'ємними конотаціями. Водночас Фуко вважає, що кожне суспільство генерує місця, які перебувають у зв'язку з його основним простором і водночас суперечать йому. Йдеться про гетеротопії — контрмісця, де знаходить притулок узагальнений Інший і відбувається трансгресія, де має місце «ерозія нашого буття» і знаходиться вихід за межі самих себе. Саме тому вони «дисциплінують девіантів і підтримують загальний соціальний порядок, сприяють критиці, але не вдаються до підривної діяльності» (Dreesen, 2021).

Фуко переконливо доводить, що гетеротопії є константами кожної спільноти. Вони локалізують людей з певною функціональністю (військова служба), девіацією (психіатричні заклади), деструкцією (тюрми). Вони виникають у місцях викривлення часу (театр), зберігання часу (бібліотеки, музеї), поєднання гетеротопії з гетерохронією (цвинтарі). За характером гетеротопії можуть бути кризовими, ілюзорними, привілейованими. Утім, в контексті топологічної презентації Даркнету найбільш доречно говорити про компенсаційну гетеротопію, яку Фуко пов'язував із колонізацією нових земель. Аналогію такого роду гетеротопії ми простежували у метафорі електронного фронтиру.

На прикладі гетеротопії Даркнету простежується роль системи відкриття/ закриття у такого роду просторі. Вхід до локального простору темної павутини уможливлює технологія (Tor, I2P, Freenet). Доступ до сторінок може бути лише безпосередній (peer-to-peer) за умов знання точної URL-адреси.

Даркнет-журналістика

У 2021 р. Бірмінгенська медіашкола запроваджує новий напрям — Даркнет-журналістика, яка позиціонується як природне відгалуження онлайнової журналістики. Її виникнення пов'язують з міграцією комерційних, політичних та особистісних практик до Даркнету. Цілком закономірно, що журналістика, керуючись суспільним інтересом, рухається туди, куди пересуваються інформаційні приводи й історії, факти й новини. Передбачувано, що у темній павутині вона стикається з низкою питань етичного й правового характеру, адже стандартів функціонування медіа в Даркнеті не існує. І питання «Чи можна вважати збір інформації у темному сегменті веба винятковою практикою, яку можна виправдати соціальною місією медіа?» висне у повітрі.

Серед перспективних форм застосування Даркнет-можливостей — розслідувальна журналістика, для якої темна мережа відкриває майже необмежене коло джерел для здобуття інформації і водночас надзвичайно актуалізує питання безпеки. Які професійні й безпекові орієнтири сьогодні скеровують діяльність журналістів у Даркнеті?

Організація «Репортери без кордонів» (RSF) створила платформу We Fight Censorship, де публікуються матеріали журналістів, які зазнали репресій унаслідок публікації забороненого цензурою контенту (We fight censorship — Let's shelter the news, 2012). Для захисту анонімності медійників розроблено цифровий сейф, який є захищеним майданчиком для просування резонансних матеріалів: окрім оригінальних текстів тут публікуються супроводжувальні й бекграундові дані, які дозволяють широкому загалу адекватно оцінити публікації. Щоб убезпечити своїх авторів, RSF також пропонує цифровий набір для виживання: він містить рекомендації, як

безпечно переглядати веб-сторінки, очищати PDF-документи від своїх слідів, убезпечити свою електронну пошту тощо.

Французький журналіст і тренер з журналістських розслідувань Жан-Марк Манах розробив методику, яка навчає медійників безпечно виконувати свої функції у мережі. Через 40 років після проголошення Енді Уорхолом культової фрази про те, що «у майбутньому кожен матиме право на 15 хвилин всесвітньої слави», Ж.-М. Манах іронічно переінакшив її, говорячи, що «в майбутньому кожен матиме право на 15 хвилин анонімності» (Manach, 2010).

Відома також розробка «DICE-E: структура щодо ідентифікації, збору, оцінки темної мережі з дотриманням етичних норм» (Benjamin et al., 2019).

Автор посібника «На шляху до рамкової структури Даркнет-журналістики» Д. Кесслер вбачає ключове нормативне питання означеного напряму журналістики у кореляції світових етичних кодексів масмедіа з етикою поводження в темній мережі. Структурна і функціональна специфіка Даркнету унеможливлює усталену офіційну етику як зведення нормативних приписів для всіх користувачів. Натомість певна етична унормованість комунікацій спостерігається на форумах, де модератори захищають свої майданчики від нелегітимного контенту. Зокрема, Д. Кесслер цитує модератора Даркнет-форуму Dread:

> Як платформа вільного слова, без невиправданої цензури, яку надають сайти Clearnet, такі як Reddit, ми будемо процвітати, дозволяючи обговорювати весь вміст і обслуговувати якомога більше різних спільнот. Однак, виходячи з моєї моралі та питань законності, важливо встановити деякі основні правила, щоб запобігти поширенню незаконного вмісту на платформі (Kessler, 2021).

Британський дослідник проводить унікальне опитування модераторів форумів Даркнету за категоріями: анонімність, облуда, різноманітність, шкода, юридичні дані та неповнолітні, щоб довести: на Даркнет-форумах існує не лише кодекс поведінки, а й особливий корпоративний дух.

Розглянемо ряд категорій, які засвідчують наявність у темній мережі набору поведінкових нормативів.

Категорія «анонімність» є ключовою для Даркнету.

«Анонімність є священною. Уникайте обговорень, які можуть розповісти занадто багато про вас чи іншого користувача»[1].

Абсолютизація анонімності в Даркнеті спричиняє заборону практик доксингу[2], аватарфагінгу[3], експериментів з ідентичністю та використання форуму як власного блогу.

Категорія «неповнолітні» розкриває зміст положення, яке позиціонує Даркнет-форуми як майданчики для дорослих. Тут можуть спілкуватися користувачі за умов досягнення ними повноліття. Табуйованими є теми дитячої порнографії, педофілії та дитячого аб'юзу. Забороняються навіть мальовані зображення дітей у сексуальному контексті.

Категорія «шкода» узагальнює вимоги форумів усіляко протидіяти намірам користувачів завдати шкоди іншим учасникам — від нанесення особистих образ до публікації шокуючого контенту. Будь-які повідомлення, опубліковані заради хайпу, видаляються. Окремо прописана заборона публікацій, пов'язаних зі шкідливими речовинами, тероризмом, вбивствами. Забороняється також практика спойлерингу[4].

Категорія «облуда» безпосередньо пов'язана із імовірною шкодою, яку можуть завдати один одному фейковими повідомленнями учасники форуму. Забороняється спотворення або приховування правди. Наприклад, «*поширення кричущої дезінформації в надії обдурити тих, кому менш пощастило інтелектуально, заборонено*». Табуйовано контент, що не має фактологічної основи та достатніх доказів.

Категорія «юридичні засади»

Більшість форумів у своїй діяльності підпорядковуються законодавству тих країн, з якими вони пов'язані. Вони функціонують у конкретних правових рамках, навіть залишаючись анонімними. Наприклад: «*Жодних повідомлень, що порушують австралійський закон і можуть зганьбити форум та викликати перевірку з боку ЗМІ або державних органів*».

---

[1] Ця та інші цитати, наведені у характеристиці категорій, запозичені з дослідження Д.Кесслера. Дані авторів висловлювань, узятих в Даркнеті, зашифровані.

[2] Оприлюднення приватних даних незаконними методами.

[3] Створення ідентичності шляхом залучення певного анімованого персонажу, який супроводжує кожне повідомлення користувача Даркнету.

[4] Практика сповіщення користувачів про існування певного прихованого матеріалу і заклику до вчинення дії, яка б його оприявнила.

Категорія «інтолерантність» засвідчує, що більшість форумів виступають проти різноманіття людей і схильні до дискримінації.

Якщо підбивати підсумки щодо категоріальних оприявнень нормативної поведінки на Даркнет-форумах і говорити про імовірний спільний знаменник журналістської та Даркнет-етики, першою точкою дотику тут буде свобода слова як цінність і як імператив. Щоправда, шляхи забезпечення цього ціннісного орієнтиру у білому й темному вебі різні. Традиційна та онлайнова журналістика захищають свободу слова, вдаючись до відповідних правових гарантій, натомість Даркнет застосовує практики анонімізації та шифрування, які забезпечують свободу висловлювань у нелегальному середовищі. Позитивної синергії взаємодія журналістики із Даркнет-контентом може набувати за умов його ексклюзивності і одночасної легітимності. Негативні наслідки для розвитку Даркнету як майданчика для захисту свободи слова має його майже виключно кримінальне позиціонування у медіа. Водночас використання унікальних даних, які можна знайти в темній павутині, за умов збереження балансу між правами особистості та правами суспільства на знання, може сприяти продуктивній реалізації журналістського фаху.

Оскільки Даркнет багато в чому нагадує «анонімну анархію», отриману на теренах темного павутиння, інформацію рекомендується подавати лише у відповідному контексті, переважно як додаткову. А підтвердження ексклюзиву потрібно знаходити у «білих» джерелах.

Даркнет: кіберзлочинність vs кібербезпека

Злочинність усе впевненіше опановує інтернет-простір, адже сюди поступово пересуваються торгівля, розваги і владні інституції. Злочинна поведінка модифікується й розширюється у міру вдосконалення технологій. Префіксом кібер- охоплюються і традиційні види злочинів, що здобули цифрове розширення, і нові, що з'явилися завдяки технологіям. Darknet називають «раєм» для злочинців, адже механізми анонімізації максимально знеособлюють тих, хто вдається до незаконних практик. Злочинній діяльності сприяють гнучкі нелегальні ринки, приховані сервіси та криптовалюта.

З дискурсу правоохоронних органів стає зрозумілим, що ринки Даркнета можна знищити лише шляхом деанонімізації темного павутиння. Втім це може суттєво зашкодити тим, хто використовує його у соціально схвалених цілях. Саме тому акцент робиться не на деанонімізації темної мережі, а на регулюванні її з боку правоохоронних органів. Своєю чергою варто визнати, що можливості правоохоронців на сьогодні тут значно обмежені. Це обумовлено не лише дією механізмів шифрування, а й транскордонним характером кіберзлочинності. Нелегальна діяльність перетинає межі держав, а отже потребує спеціального потрактування у різних правових системах. Питання юрисдикції щодо темної мережі варіюються від країни до країни, що унеможливлює комплексний характер такого регулювання. Крім того, правоохоронцям не вистачає спеціальних знань з галузі кібертехнологій, а також ресурсів, які б спрямовувалися на боротьбу зі злочинами у темному павутинні. У міру того, як органи правопорядку здобувають необхідні навички з протидії кіберзлочинності, власники темних ринків удосконалюють їхній захист, впроваджують усе більш суворий і виважений менеджмент (Rose, 2020).

Згідно з даними видання *Cybercrime Magazine*, у 2021 р. кіберзлочинність завдала світові збитків на загальну суму 6 трильйонів доларів і надалі протягом наступних чотирьох років, за прогнозами, буде лише зростати — орієнтовно на 15 % на рік (Morgan, 2022). За словами головного редактора означеного видання Стіва Моргана, ця цифра співмірна з третьою у світі економікою після США та Китаю. Втрати від кіберзлочинів складають довжелезний перелік: пошкодження та знищення даних, крадіжки коштів, втрату продуктивності, крадіжку інтелектуальної власності, крадіжку особистих і фінансових даних, шахрайство, порушення нормального перебігу бізнес-процесів після атак, відновлення та видалення «зламаних» даних і систем, репутаційні втрати (Morgan, 2022).

Заходи, до яких нині вдаються правоохоронці, щоб подолати злочинність на темному фронтирі, мають переважно тактичний характер. Йдеться про сканування спільноти з метою припинення заборонених видів діяльності і впровадження прихованих вузлів у мережу Tor.

***

Метафори не лише відтворюють наше життя у впізнаваних образах, а й проєктують його у майбутнє, формують настанови на сприйняття об'єктів метафоризації, програмують поведінку людей у суспільстві. Метафори концептуалізують наративи, перекодовуючи буденне сприйняття реальності у категоріях актуальних когнітивних фреймів та моделей.

Просторові та орієнтаційні метафори традиційно уґрунтовують наше сприйняття комунікацій, функціональність яких ми не менш традиційно пов'язуємо з контекстом місця і динамікою перебігу комунікаційного процесу. Просторовий поворот початку нового тисячоліття, що відбився у наукових і художніх дискурсах, також інспірує сприйняття новітніх комунікаційних явищ у категоріях простору. Евристично цінною у цьому зв'язку може стати метафора фронтиру, яку запровадив з метою концептуалізації американської історії Ф. Дж. Тернер. Цілком закономірним є запозичення цієї просторової метафори дослідниками мережевого середовища. Інтернет у дискурсі західних досліджень позиціонується як рухливе прикордоння з атрибутами американського фронтиру: інноваторами-першопрохідцями, масовими переселенцями, маргінальними цінностями, процесами самоорганізації і злочинними практиками.

З набуттям сегменту *Clearnet* легітимного статусу з'явилася можливість говорити про нове прикордоння і концептуалізувати його як нову маргінальну царину. У своєму становленні Дакнет як електронний фронтир проходить етапи розвитку, притаманні ґенезі західного фронтиру. Він акумулює маргінальні спільноти, виступає запобіжним клапаном при зростанні суспільного незадоволення, відкриває можливості для ведення діяльності, яка потребує утаємниченості й герметичності, які унеможливлюють інституціональний нагляд.

Як було з'ясовано, у Даркнеті відбуваються самоорганізаційні процеси, характерні для ранніх етапів становлення західного фронтиру. Формується корпоративна етика, стверджуються стандарти спілкування на форумах. Водночас темний електронний фронтир демонструє дилему, спричинену його базовими характеристиками. Анонімність, забезпечена технологією «цибулевого» шифрування, стимулює злочинну діяльність, не зважаючи на те, що первісно браузер Tor був розроблений з гуманістичною метою.

Функціональна настановчість Даркнету як майданчика, де панує свобода висловлювання, дискусії та самореалізації, унеможливлює скасування самої ідеї анонімності. Її побічні наслідки віддаються на відкуп правоохоронним органам, які протидіяють функціонуванню у Даркнеті чорних ринків та сервісів. Боротьба із кіберзлочинністю ускладнюється чинниками анонімності (важко встановити особу злочинця), транскордонності (неможливо вирішити питання у рамках одного правового поля), гнучкості нелегальних ринків (рівень захищеності їх постійно підвищується).

Починає функціонувати Даркнет-журналістика, яка послуговується історіями, інфоприводами й даними темного павутиння. Відкритим залишається питання стандартів роботи журналістів на новому е-фронтирі.

Література

Benjamin, V., Valacich, J. S., & Chen, H. (2019). DICE-E: A framework for conducting darknet identification, collection, evaluation with ethics. *MIS Quarterly*, *43*(1), 1-22. https://doi.org/10.25300/misq/2019/13808

Cowen, C. (2019, June 1). *Shining a light on the Dark Web.* Cyber Defense Magazine. https://www.cyberdefensemagazine.com/shining-a-light-on-the-dark-web/

Derakhshan, H. (2016). Killing the hyperlink, killing the web. *Proceedings of the 2016 Conference on User Modeling Adaptation and Personalization*. https://doi.org/10.1145/2930238.2954034

Dreesen, P. (2021). Darknet und Diskurs. Tabu eines Ortes und ort fur tabus? *Aptum, Zeitschrift für Sprachkritik und Sprachkultur*, *17*(2). https://doi.org/10.46771/9783967691689_3

Foucault, M. *Of other spaces (1967), heterotopias*. (1967, March 1). Michel, Info. https://foucault.info/documents/heterotopia/foucault.heteroTopia.en/

Healy, D. (1997). Cyberspace and Place : The Internet as Middle Landscape on the Electronic Frontier In D. Porter (ed). *Internet Culture*. London : Routledge, 1997.

Kessler, D. (2021). Towards a Darknet Journalism Framework - *https://www.academia.edu/61636613/Towards_a_Darknet_Journalism_Framework_Dror_Kessler?auto=download&email_work_card=download-paper*

Manach, J.-M. (2010, March 9). *Dans Le futur, chacun Aura droit a son quart d'heure d'anonymat*. Internet. Actu.net. https://www.internetactu.net/2010/03/09/dans-le-futur-chacun-aura-droit-a-son-quart-dheure-danonymat/

Manach, J.-M. (2014, January 2). *Le problème, CE n'est pas la transparence, mais la surveillance*. BUG BROTHER. https://bit.ly/9aIrHl

Mason, B. L. (2017). *The creation of folk cultures on the internet: a proposed methodology of investigation with case studies* [Master's thesis]. https://research.library.mun.ca/12274/1/Mason_BruceLionel.PDF

McLure, H. (2000). The wild, wild web: The mythic American West and the electronic frontier. *The Western Historical Quarterly*, *31*(4), 457. https://doi.org/10.2307/970103

Morgan, S. (2022) Report: Cyberwarfare in the C-Suite. *Cybercrime Magazine*. https://cybersecurityventures.com/wp-content/ uploads/ 2021/01/Cyberwarfare-2021-Report.pdf

Moßbrucker, D. (2019). Überwachbare welt: Wird das darknet zum mainstream digitaler Kommunikation? *Medienwandel kompakt 2017-2019*, 9-29. https://doi.org/10.1007/978-3-658-27319-4_2

Nelson, B. (2020, December 18). *Was ist das darknet?* Avast. https://www.avast.com/de-de/c-dark-web#gref

Pitkow, J., & Pirolli, P. (1997). Life, death, and lawfulness on the electronic frontier. *Proceedings of the ACM SIGCHI Conference on Human factors in computing systems*. https://doi.org/10.1145/258549.258805

Rose, M. (2020) *Law enforcement techniques in darknet markets: A case study*. ProQuest. https://www.proquest.com/openview/38024442a3a30ce4d583c89d7cf16d79/1?pq-origsite=gscholar&cbl=18750&diss=y

Sanchez, J. & Griffin, G. (2019, May 07). *Who's afraid of the dark? Hype versus reality on the Dark Web*. Recorded Future. https://www.recordedfuture.com/dark-web-reality/

Schuster, U. (2022, February 1). *14 besten Dark Web links in 2022 (und wie du .onion-seiten aufrufst)*. WizCase. https://de.wizcase.com/blog/besten-dark-web-links/

Sherman, C. B., Freekbass, Sherman, C., Sherman, R., & Price, G. (2001). *The Invisible Web: Uncovering information sources search engines can't see*. Information Today. https://www.ideals.illinois.edu/bitstream/handle/2142/8528/librarytrendsv52i2h_opt.pdf

Tzanetakis, M. (2017, March 27). *The dilemma of an Anonymous darknet — Digital society blog*. HIIG. https://www.hiig.de/en/the-dilemma-of-an-anonym-darknet

Viney, S. (2017, July *20). What is the dark net, and how will it shape the future of the digital age?* ABC (Australian Broadcasting Corporation). https://www.abc.net.au/news/2016-01-27/explainer-what-is-the-dark-net/7038878

We fight censorship - Let's shelter the news | Reporters without borders. (2012, July 23). RSF. https://rsf.org/en/news/we-fight-censorship-lets-shelter-news

Лакофф, Дж., Джонсон, М. (2004). *Метафоры, которыми мы живем*. Едиториал УРСС.

Плотичкина, Н.В., Довбыш, Е.Г. (2017). Сетевой фронтир как метафора и миф. *Вестник РУДН. Серия: Социология*, *17*(1), 51-62.

Соколовська, Н. (2017, May 01). *Темний бік анонімності — що таке Darknet і як він працює*. Na chasi. https://nachasi.com/tech/2017/05/01/what-is-darknet/

Тернер, Ф. Дж. (2009). *Фронтир в американской истории.* Издательство «Весь Мир».