DOI: https://doi.org/10.36486/978-966-2310-66-5-26

Жорстоке вторгнення Росії в Україну змінило контекст кібербезпеки.

Голова британського національного центру кібербезпеки (NCSC) Лінді Кемерон

РОЗДІЛ 26
Кібервійна та форсайт кіберстійкості

Сергій Демедюк

КІБЕРВІЙНА І КІБЕРСТІЙКІСТЬ

Кібервійна не є новим явищем. Перше електронне повідомлення було надіслано в 1971 році; через п'ять років групи, відомі як Тигрові команди, спробували атакувати комп'ютери ICL і IBM у рамках експериментальної програми інформаційної безпеки Міністерства оборони Великої Британії [1]. Хоча значна частина цієї теми захищена державною таємницею, стає все більш очевидним, що ми маємо досвід чотирьох десятиліть кібервійни, з якої можна отримати політичні уроки та знання, незважаючи на те, що це часто називають застарілими термінами, такими як «інформаційна безпека» або «комп'ютерна безпека» [2; 3].

Термін «кібервійна», запроваджений Пентагоном на початку 1990-х років, спочатку став об'єктом значного скептицизму. Після закінчення холодної війни бюджети на оборону раптово зменшилися. Багато експертів з питань кібербезпеки вважали обговорення про «кібервійну» дещо безнадійною спробою оборонних відомств захистити виснажені бюджети. Ця нова загроза вимагала значних витрат на дослідження та розробки, які не були достатньо зрозумілі для парламентів. Скептицизм щодо реальності справжньої «кіберзагрози» значно зріс внаслідок очевидно обмеженого впливу, спричиненого помилкою тисячоліття Y2K, і зберігся у двадцять першому столітті [4; 5].

Вважається, що перша кібервійна відбулася в Естонії в 2007 році, а друга - в Грузії в 2008-2009 роках [6]. Коли у 2010 році Stuxnet успішно використали для паралізування ядерних центрифуг Ірану, він ще більше збудив кіберскептиків. Кібератака, спрямована на Іран, була здійснена за допомогою надзвичайно складного комп'ютерного хробака, спрямованого на певну конфігурацію промислового обладнання Siemens. Хоча ніхто офіційно не знав, хто створив Stuxnet, кілька ключових компонентів було виявлено. По-перше, він продемонстрував надзвичайний інтелект, вибірково заразивши кілька комп'ютерів за межами Ірану. По-друге, він продемонстрував здатність долати складні розриви та інші засоби захисту, що застосовуються іранською владою. По-третє, хробак Stuxnet використав не один, а кілька експлойтів «нульового дня» [7, с. 23].

У лютому 2014 року розпочалась російська збройна агресія проти України, яка велась також і в кіберпросторі. Майбутній директор американського Агентства національної безпеки Майкл Роджерс з цього приводу зазначав, що разом з військовою операцією із захоплення Криму, Росія розпочала проти України кібервійну[8]. Кібервійною називають російські атаки й українські експерти[9].

Після початку збройної агресії Російської Федерації проти України, компанії, що спеціалізувалися на наданні послуг кібербезпеки, стали реєструвати зростання кількості кібератак на інформаційні системи в країні. Зазвичай кібератаки були націлені на приховане викрадення важливої інформації, ймовірніше для надання Росії стратегічної переваги на фронті. Жертвами російських кібератак ставали урядові установи України, країн ЄС, Сполучених Штатів, оборонні відомства, міжнародні та регіональні оборонні та політичні організації, аналітичні центри, засоби масової інформації, дисиденти[10].

Лише щодо деяких з них:

> *на думку Адміністрації Президента США хакерська атака на Україну з боку Росії в червні 2017 року із використанням вірусу NotPetya стала найбільшою відомою хакерською атакою [11].*
>
> *12 грудня 2023 року у роботі найбільшого в Україні оператора зв'язку «Київстар» стався масштабний збій. По всій країні у абонентів «Київстар» зник мобільний зв'язок та інтернет, при цьому користувачі не могли і приєднатися до мереж інших операторів у рамках внутрішньо українського роумінгу [12]. Також припинили роботу сайт та застосунок «Київстару». Зв'язок зник у 24 мільйонів абонентів [13]. Збої виникли у всьому обладнанні, яке використовувало зв'язок «Київстар», що призвело до серйозних інфраструктурних проблем по всій Україні [14].*

Загалом, згідно з аналітичним звітом Держспецзв'язку України за I півріччя 2023 року, лише упродовж січня-червня 2023 року кількість кібератак проти України зросла до 762 зареєстрованих інцидентів, що більше ніж удвічі за показники II половини минулого року [10].

Водночас більшість статистичних даних про кіберзлочинність піддаються сумніву.

Наприклад, професор Пітер Зоммер, професор Лондонської школи економіки, стверджує, що деякі недавні державні звіти про кіберзлочинність фактично виступають лише «інструментом для спонукання до продажу» для спеціалізованих компаній, які займаються безпекою. Він назвав звіт Detica «прикрим надуванням» [15]. Зоммер стверджує, що до цього часу ще не досягнуто згоди щодо конкретного вмісту розрахунку збитків.

Тайлер Мур, експерт з кібербезпеки Гарвардського університету, пояснює, що причина складності отримання точних оцінок полягає у тому, що не завжди повідомляють про всі випадки. Жертви не охоче зізнаються в порушенні безпеки, а в деяких випадках навіть не знають, що на них було скоєно напад [16].

На цей час одна з ключових проблем у кіберстійкості пов'язана з недостатнім розвитком освіти у сфері безпеки IT. Також потрібні культурні зміни, оскільки менше IT-експертів просуваються до найвищих посад компаній, які не входять до технологічного сектору, і їх недостатньо в урядовому багатті.

Кібервійна містить хвилюючий феномен. Передові суспільства, які розвинули ці можливості, якраз і є найбільш вразливими до електронної війни. На противагу цьому, кібератака на Кубу, яка має один з найнижчих показників використання комп'ютерів у світі (17 користувачів на 1000 осіб) і нерозвинену цифрову інфраструктуру, матиме відносно невеликий вплив [1]. Країни Організації економічного співробітництва та розвитку (OECD) дедалі більше залежать від цифрових систем в управлінні своєю життєво важливою інфраструктурою [17]. SCADA-системи, спеціально розроблені для контролю промислових процесів, можуть дистанційно керувати компонентами водопостачання, енергетики, транспорту та зв'язку. Stuxnet був створений з метою нападу на SCADA-системи і недвозначно показав, що деякі з таких систем можуть бути пошкоджені, що може призвести до значних наслідків. Більше того, точний масштаб загрози і необхідний захист залишаються непрозорими [1].

До цього часу, урядовці вважали, що критична інфраструктура розвинених країн може бути захищена шляхом використання все більш вдосконалених технічних рішень. Тим не менш, Stuxnet підтвердив, що більшість цифрових систем, незалежно від їхнього високого рівня захисту, все одно є вразливими.

Отже, щоб запобігти кібератакам, можливо, потрібно використовувати аналогові системи для моніторингу запасу електроенергії, води та інших важливих комунальних послуг. Наразі, занепокоєння можливістю кібератак на атомні електростанції вже призвело до свідомого урізноманітнення систем з поєднанням цифрових, аналогових і ручних [1]. Однак у двадцять першому столітті зробити це в основній інфраструктурі надзвичайно складно, оскільки інженери звернулися до цифрових рішень для підвищення операційної ефективності [18].

Наприклад, інфраструктуру Великої Британії не можна вимкнути, як вимикач, частково тому, що вона все ще має певну «системну різноманітність». Частково це результат застарілих систем, а частково - результат випадковості. Небезпека полягає в тому, що це ненавмисне, але цінне джерело стійкості буде знищене в ім'я скорочення витрат і підвищення ефективності. Широке впровадження інтелектуального обліку є прикладом універсальної системи, яка містить вразливість, зумовлену прагненням до більшої ефективності та результативності [1].

Отже, різноманітність систем стала новим улюбленим словом у сфері кібербезпеки.

> *Стійкість вимагає дедалі складнішого поєднання фізичної безпеки, безпеки персоналу, контролю закупівель і зміцнення систем разом з подальшими заходами для запобігання несанкціонованим або ненавмисним модифікаціям дизайну системи безпеки.*

Крім того, впровадження злагоджених аналогових і людських систем безпеки суттєво змінило уявлення про інформаційну безпеку. До цього моменту спеціалісти з інформаційної безпеки головним чином займалися кіберзлочинністю, зазвичай проводили складні спроби проникнення в системи безпеки банків і великих компаній. За більш ніж 10 років роботи в цій сфері було зроблено висновок, що більшість збоїв у системі безпеки є наслідком поєднання людської некомпетентності та зловмисності [19, с. 1]. Однак, зважаючи на загрозу серйозної кібервійни на державному рівні, експерти розглядають людей разом із системами як останню лінію захисту від витончених кібератак [1].

Серед фахівців з інформаційної безпеки була поширена ортодоксальна думка, що головною перешкодою для безпеки системи є люди, а не самі системи [20]. Вірогідною була думка, що більшість серйозних порушень безпеки виникають через недостатній рівень знань персоналу, а не через технічні неполадки. Проте поява комп'ютерного хробака Stuxnet, який був використаний для нападу

на ядерні центрифуги в Ірані, вказує на те, що такий підхід має бути переглянутий. Велика кількість людей почала вивчати майбутню кібербезпеку після виявлення складного шкідливого програмного забезпечення, яке шпигує за промисловими системами та підриває їх.

Відповідь на питання кіберстійкості, як у випадку Stuxnet, полягає в поєднанні різноманітних або гібридних систем, які керують певною частиною національної інфраструктури. У той час навіть найбільш захищені системи могли бути піддані технічним атакам іззовні. У наступні десятиліття основним каталізатором інформаційно-комунікаційних технологій стане все ближчий зв'язок між інтернетом і людьми. Головною ціллю комерційних технологічних підприємств є безперешкодне об'єднання людини та інтернету. На сьогодні це виявляється в потужніших портативних пристроях, сполучених з хмарними технологіями.

Однак, майбутнє просунутого зв'язку між людиною та інтернетом – це прямий інтерфейс між комп'ютером і мозком, сфера, в якій медичні технології вже розширюють межі [21]. Вплив цього розвитку на кіберстійкість має певну вагу. Коли людина буде відправляти електронне повідомлення, «після роздумів і короткого кліпання очима» [1], кібербезпека стане ще важливішою, ніж на сьогодні. Щоб захистити нашу інфраструктуру, ми повинні докладати рішучих зусиль, щоб впоратися з комерційними та культурними перешкодами, спрямованими на надмірну залежність від електронних систем.

Витрати на інтернет-безпеку також створюють серйозні труднощі, але в значно більшому розмірі. Це надзвичайно дорога і ризикована сфера, ніхто по-справжньому не хоче нею володіти [1]. Однак більшість людей погоджується, що інтернет має вирішальне значення, і що його потрібно захистити.

Управління кібербезпекою є типовим прикладом міжурядової сфери, яка працює на регіональному рівні значно краще. У Європі існує власна кібер-організація, Європейське агентство з мережевої та інформаційної безпеки (European Network and Information Security Agency - ENISA), розташована на острові Кіпр. У практичній сфері ENISA виконує функцію координації регулювання та сприяє зближенню, але має обмежені можливості оперативних дій. Тим не менш, більшість ІКТ-бізнесу позитивно ставиться до ENISA, стверджуючи, що один набір регуляторних практик для Європи є кращим, ніж 26 [22]. Масштаби телекомунікаційної галузі означають, що саме Європейське агентство, а не уряд, має більший операційний потенціал і, власне, досвід для забезпечення значущої кіберстійкості [1].

Будучи за своєю природою транснаціональними і часто використовуваними у контексті глобалізації, агентства Європейського Союзу, такі як ENISA, також мають схожі проблеми складності і невизначеності, які ставлять у скрутне становище національні уряди. Кіберстійкість може бути найбільш привабливою через те, що вона може використовуватися як рухома ціль. У тривалий період часу урядові програми та проекти не досягали успіху. Це було пов'язано з тим, що вони були надто вибуховими та не мали потенціалу для впровадження нових технологій, а також тому, що приватний сектор розвивався швидше, ніж уряд. Що ми знаємо напевно, так це те, що світ інформаційно-комунікаційних технологій прискорюється, а проблеми, які стоять перед урядом, зростають у своїх розмірах і складності [1].

Отже, в майбутньому враховуватиметься гібридизація процесів розвідки, безпеки, ризиків і стійкості для досягнення кіберстійкості ландшафту. Однак, короткостроково, це стає проблемою для управління, як з точки зору власності, так і з точки зору співпраці між державними й приватним секторами.

МЕТОДИ ТА СИСТЕМИ ФОРСАЙТУ КІБЕРСТІЙКОСТІ

Форсайт – це складний, багатоетапний та безперервний процес, кінцевою метою якого є прийняття обґрунтованих рішень щодо забезпечення стратегічних планів для можливого різноманітного розвитку подій у майбутньому. Він дає змогу осмислити різні можливі варіанти майбутнього та стратегічно підготуватися до ймовірних сценаріїв. З середини 1950-х – початку 1960-х років форсайт як дисципліна перетворився на основний інструмент стратегічного планування як для приватних корпорацій, так і для державного сектору [1].

Форсайт продовжує розвиватися й змінюватися і сьогодні. Це значною мірою пов'язано з тим, що

він орієнтований на дії, а отже, має відчутні результати;

він є відкритим, тобто в рамках форсайту існує свобода мислити нестандартно або переосмислювати попередні уявлення;

нарешті, він є міждисциплінарним, він об'єднує різні групи, які мають досвід у широкому діапазоні тем, таким чином забезпечуючи більш реалістичне і продумане можливе майбутнє.

У виданні ЄС «Що таке форсайт» зазначається:

> *«Форсайт – це не пророцтво і не передбачення. Він не має на меті передбачити майбутнє – розкрити його так, ніби воно визначене наперед, – а допомогти нам його побудувати» [23].*

Виділяють три основні переваги форсайту [24, 25]:
- *генерація знань,*
- *сприяння відносинам із зацікавленими сторонами,*
- *посилення спроможності.*

Знання допомагають окремим зацікавленим сторонам найкращим чином позиціонувати себе для майбутнього розвитку; маючи знання, вони можуть бачити поза оманою, що майбутнє буде схожим на теперішнє, і уявляти собі передове майбутнє [24]. Розвиток таких знань і розуміння сприяє підвищенню зв'язків між зацікавленими сторонами, що у свою чергу посилює мережі, особливо у випадку кібербезпеки.

Форсайт сприяє посиленню спроможностей; результати форсайту дозволяють визначити, що є важливішим для організаційних спроможностей і спроможностей зацікавлених сторін. Визначення та підтримка цієї інформації є життєво важливими для розвитку та отримання ключових навичок, технологій та політики.

Застосування форсайту у сфері кібербезпеки наразі не є широко розповсюдженим [26]. Проте, запровадження зазначених методів в галузь кібербезпеки сприятиме набуттю ще більш глибокого, розумного та взаємодіючого усвідомлення ризиків, а також стратегічних наслідків заходів забезпечення безпеки.

> *Щоб адекватно реагувати на майбутні загрози кібербезпеці та формувати більш безпечне суспільство, необхідно спиратися на висновки та дослідження спільноти фахівців з питань майбутнього та форсайту, щоб розробити процес застосування форсайту до кіберстійкості.*

Для досягнення здатності розуміти можливості майбутнього, важливо належним чином розвивати кібербезпекову екосистему з метою вирішення та управління новими та майбутніми викликами.

Як кіберстійкість, так і форсайт отримують вигоду від багатогранного і міждисциплінарного середовища. Часто розумно об'єднувати системи з інших галузей з цієї самої причини. Вважається [24], що керівні принципи, практики, підходи, методи та інструменти як системного мислення, так і розробок, орієнтованих на користувача, можуть бути ключовими для формування правильного мислення [27] при підході до форсайту у сфері кібербезпеки.

Для того, щоб краще проілюструвати спектр методів, відповідні методи, системи та інструменти, як правило, групуються в шість категорій [28]. Тим не менш, не всі прийоми можна визнати характерними для передбачення майбутнього. Також використовуються стратегічні методи планування та методи вирішення проблем, які часто включаються у діяльність форсайту.

Загалом, виділяються такі групи методів [23]:
- *системи аналізу середовища*
- *аналіз тенденцій*
- *форсайт експертні групи*
- *сценарний метод*
- *морфологічний аналіз та ретроспективний аналіз*
- *методи аналізу кібербезпеки.*

Системи аналізу середовища дають користувачам можливість ретельно вивчати обране середовище для виявлення слабких сигналів вхідних змін, які можуть мати значний вплив на майбутнє. Ці методи сприяють структурованому та аналітичному сприйняттю поточної ситуації з метою досягнення взаєморозуміння. Зазвичай, ці методи базуються на засадах діагностики.

Існують різні методи для сканування середовища, серед яких, наприклад, такі:

> ***STEEP*** *– система аналізу соціокультурних, технологічних, економічних, екологічних та політичних факторів певної сфери;*
>
> ***PESTLE*** *– система аналізу політичних, економічних, соціокультурних, технологічних, правових та екологічних факторів певної сфери.*
>
> ***SWOT*** *– система визначення та аналізу сильних і слабких сторін, можливостей і загроз для певного напряму або організації.*

Кожна з перерахованих систем дозволяє проводити систематичну оцінку характеристик, змін і впливів у зазначених областях, щоб отримати уявлення про навколишнє середовище.

Крім того, існують інші відмінності цих ідей, які враховують інші сфери - вибір методу або сфери має ґрунтуватися на початковому аналізі цієї теми.

Аналіз тенденцій. Тенденція визначається певним трендом змін в часовому вимірі або появою нової моделі змін, яка зазвичай впливає на великі соціальні групи [29]. Методи аналізу тенденцій зазвичай слугують прогностичним або діагностичним цілям.

Тренди можна аналізувати різними способами – наприклад, за допомогою оглядів літератури, бібліометрії, текстового аналізу, патентного аналізу та аналізу впливу трендів. Ці методи виявляють поточні або нові тенденції і, як правило, досліджують причину, потенційний вплив, ймовірність і швидкість виникнення цих тенденцій [30].

Інші методи, що використовуються для аналізу тенденцій, включають [23]:

- ✓ *причинно-наслідковий багаторівневий аналіз – сприяє визначенню рушійних сил шляхом отримання розуміння сприйняття учасників, таких як світогляд, цінності та культурні норми;*
- ✓ *тренд-радар – надає міжгалузевий погляд на нові та вже існуючі тенденції в цільовому середовищі;*
- ✓ *аналіз впливу трендів – аналіз впливу однієї або декількох можливих подій на екстраполяцію тренду в майбутнє;*
- ✓ *сканування горизонту – систематичний моніторинг поточних тенденцій, а також виявлення нових, актуальних подій у певній сфері за допомогою творчого процесу колективного осмислення.*

Форсайт-експертні групи охоплюють широкий спектр методів і підходів. Експертні панелі та метод Дельфі є одними з найвідоміших складових сімейства форсайт-експертних груп. У обох випадках експерти висловлюють свою думку про майбутнє. Проте метод Дельфі полягає в більш структурованому підході до спілкування, щоб отримати відповіді від фахівців. Експерти зазвичай запрошуються для підтримки проекту з форсайту з прогнозними або рекомендаційними цілями.

> ***Дельфі*** *– це дослідницький метод, заснований на структурованому та ітеративному груповому спілкуванні між експертами, які висловлюють судження з обраної теми. У першій послідовності різні експерти в певній галузі опитуються окремо щодо конкретної теми або питання. Потім збираються їхні анонімні відповіді, і експертів просять прокоментувати зібрані думки. Для досягнення консенсусу цей процес повторюється кілька разів. Такий підхід допомагає уникнути групового мислення, а отже генерує більше креативних ідей з різних точок зору. Весь процес можна проводити дистанційно, що полегшує залучення більш різноманітної групи експертів з усього світу. Цей метод може забирати багато часу, особливо коли є кілька ітерацій [23].*

Японський національний інститут науково-технічної політики (NISTEP) проводить форсайт приблизно кожні п'ять років, більшість з яких ґрунтується на великому дослідженні за методом Дельфі, в якому беруть участь близько 2000 учасників [31].

Інші приклади методів, заснованих на експертних групах, включають [23]:

- ✓ *зведені судження / груповий прогноз – логічно поєднує декілька індивідуальних суджень в узгоджені та колективні судження;*
- ✓ *дослідження ключових технологій (технологічне прогнозування) – застосовує набори критеріїв до критичних технологічних розробок з метою надання обґрунтованої оцінки.*

Водночас існують також методи колективного форсайту, за яких інформація збирається у не експертному середовищі.

Сценарні методи. Серед найбільш поширених і відомих методів передбачення у форсайті є сценарні методи. Вони використовуються як інструменти дослідження для розмірковування про можливе, бажане або небажане майбутнє, але не для точного передбачення конкретного майбутнього. Крім того, ці методи можуть бути використані для створення та оцінки різних варіантів, щоб знайти найкращий підхід. Зазвичай вивчається кілька можливих сценаріїв майбутнього, щоб прийняти рішення, які можуть допомогти запобігти потенційним проблемам і пасткам.

Зазвичай на початку розробки сценаріїв проводиться діагностика, яка дозволяє об'єктивно розглянути основні фактори, що можуть вплинути на майбутнє питання, яке вивчається. Розгляд кількох потенційних варіантів майбутнього підвищує розуміння різних факторів, що можуть впливати на майбутнє. Ці знання дозволяють створити більш гнучкі, перспективні та адаптивні рішення.

Наприклад, сценарії можна розробляти різними методами [23]:

- ✓ *ігри – розробка ігор або рольових сценаріїв для тестування можливих стратегій або рішень шляхом визначення можливих реакцій та наслідків їх реалізації;*
- ✓ *візія – погляд в ідеальне майбутнє для створення стратегії досягнення конкретних цілей;*
- ✓ *аналіз перехресного впливу – оцінює ймовірність настання певних подій у майбутньому шляхом оцінки ймовірності настання інших подій, а потім досліджує їхній взаємний зв'язок.*

Морфологічний та ретроспективний аналіз. Ця група включає в себе різноманітні методи, які зазвичай не мають взаємозв'язку, але мають однакові дві характеристики – намір передбачення та акцент на регресію подій і декомпозицію системи. Регресійний аналіз у форсайті дотримується

підходу, подібного до статистичного регресійного аналізу. Однак регресійний аналіз у форсайті працює з якісними даними й суб'єктивною думкою, на відміну від кількісних методів визначення подій і тригерів подій, які можуть призвести до передбачуваної майбутньої події [32]. Однак декомпозиція ставить за мету розділення складних систем на менші компоненти для полегшення аналізу їх структури, динаміки взаємодії та впливу на систему в цілому.

> ***Морфологічний аналіз*** *– це творчий, евристичний, нормативний метод, який підтримує дослідження складних проблем і можливих рішень за допомогою багатовимірної матриці [23].*

Це трудомістка групова вправа, яка потребує фасилітації [33].

> ***Бек-кастинг*** *– ще один нормативний метод, який фокусується на обраному сценарії бажаного (або небажаного) майбутнього. Потім учасники рухаються назад у часі, щоб визначити рішення або події, які мають відбутися, щоб перетворити обраний сценарій на реальність [23].*

За допомогою беккастингу організації можуть планувати, дії що їм слід вжити, та оцінювати потенційні наслідки. Це підвищує обізнаність про те, що майбутнє визначається багатьма факторами і що різні дії призводять до різних альтернативних результатів [33].

> ***Прогнозування загроз*** *– це багатоетапний метод, який передбачає уявлення небажаного майбутнього, а потім реконструкцію кроків і рішень, які необхідно вжити, щоб запобігти цьому майбутньому [23].*

Він був розроблений, перш за все, для аналізу військового майбутнього. Прогнозування загроз поєднує в собі багато методів передбачення, включаючи Дельфі, науково-фантастичне прототипування, беккастинг і моделювання сценаріїв. Цей метод має визначений часовий горизонт – кожна діяльність спрямована на 10 років вперед [34].

Інші методи, що входять до цієї групи [23]:

- ✓ *аналіз технологічної послідовності – генерує імовірні часові рамки для технологічних послідовностей шляхом аналізу оцінок часу, необхідного для проміжних технічних кроків;*
- ✓ *розробка дорожньої карти – розробляється документ, який визначає кроки та етапи, необхідні для досягнення бажаного майбутнього;*
- ✓ *багатокритеріальний аналіз – порівнює можливі ідентифіковані рішення із зваженим набором критеріїв оцінки;*
- ✓ *синектика – сприяє новому і творчому мисленню, наприклад, уявляючи обрану проблему в незвичному, не пов'язаному з нею середовищі.*

Методи аналізу кібербезпеки. Кібербезпека є складовою системи, яка включає розгляд інцидентів і криз, а також ретельний аналіз майбутніх ризиків і загроз. Усі ці способи є різновидами способів оцінювання ризиків. Хоча фокус кожного з них трохи відрізняється (наприклад, на суб'єкті загрози або на візуалізації), загальна мета кожного з них полягає в тому, щоб знайти та визначити пріоритети ризику, а потім прийняти відповідні заходи. Цей підхід може бути використаний для постановки діагнозу, прогнозування або надання рекомендацій.

Найвідомішими методами, які добре себе зарекомендували в аналізі ризиків і моделюванні загроз є такі:

- ✓ *оцінка ризику агента загрози (Threat Agent Risk Assessment (TARA) [35] – метод оцінки ризиків на основі загроз, який використовується для виявлення, оцінки та визначення пріоритетності ризиків. Він зосереджує увагу на суб'єктах загроз, їх мотивації та можливих методах;*
- ✓ *оперативно критична оцінка загрози, активу і вразливості (Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) [36] – комплексний метод оцінки для виявлення, ранжування та управління ризиками кібербезпеки;*
- ✓ *моделювання загроз [37] – метод концептуального аналізу, що використовується для виявлення потенційних вразливостей і розробки заходів на ранніх стадіях розробки додатків або послуг. Існує багато систем і методів для моделювання загроз, одним з таких методів є Дерево атак. Дерева атак базуються на визначенні дерев можливих методів, які можуть допомогти зловмиснику досягти своїх цілей.*

Інструменти. Незважаючи на те, що вони не повністю ідентичні, інструменти є платформами або допоміжними системами, які допомагають у застосуванні методів прогнозування. Незважаючи на те, що деякі з них спрямовані на оцифрування форсайту, інші лише мають на меті покращити ваш досвід форсайту на індивідуальному рівні. Під час вибору інструментів форсайту для конкретної діяльності слід розглянути інші потенційні джерела, оскільки деякі з них спеціально розроблені для певної аудиторії або ситуації.

Інструменти для фасилітації семінарів часто використовуються фасилітаторами воркшопів для полегшення комунікації під час воркшопів або для генерування креативних ідей від учасників. Ось кілька відомих прикладів [23]:

- ✓ *мозковий штурм, коли учасників заохочують генерувати велику кількість сирих, спонтанних ідей, надихаючись ідеями інших учасників, без негайного оцінювання;*
- ✓ *світове кафе, де велика група учасників може обговорити різні питання в структурований спосіб, по колу, в менших групах, і записати свої ідеї на великих аркушах паперу, щоб інші групи могли бачити й використовувати їх як довідник;*
- ✓ *Mind mapping – метод графічної фасилітації, який допомагає візуально організувати зібрану інформацію.*

Існує кілька *цифрових баз даних*, які надають інформацію про інструменти, що стосуються форсайту. Одним із джерел для визначення додаткових інструментів для форсайту є веб-сайт Service Design Tools [38], який описує та впорядковує інструменти на основі етапу процесу проектування, зацікавлених сторін та учасників, мети діяльності та бажаних методів візуалізації. Інші ресурси включають Платформу майбутнього (Futures Platform) [39], Інструментарій майбутнього врядування (Governance Futures Toolkit) [40] та Teach the Future [41], який має на меті надати викладачам інструменти для інтеграції форсайту в їхні навчальні програми.

Інструменти на основі штучного інтелекту (ШІ) можуть допомогти в таких видах форсайту, як оцінка поточного середовища, аналіз тенденцій або екстраполяція тенденцій. Хоча ці інструменти не є повсюдними, вони часто інтегровані в процес форсайту [42]. Особливо корисним є використання ШІ для пошуку текстів й аналізу великих обсягів даних, таких як виявлення термінів і фраз, які вказують на нові або майбутні тенденції, або для підтримки огляду літератури. У більшості випадків для цього застосовується обробка реальної мови. Також інструменти, що базуються на штучному інтелекті, можуть допомогти у виборі сценаріїв.

Інструменти співпраці та форсайту / бази даних трендів. Для кращого полегшення форсайту багато експертів рекомендують використовувати інструменти для спільної роботи (наприклад, цифрові дошки і додатки для нотаток), а також дослідницькі бази даних для камеральних досліджень і розпізнавання тенденцій. Важливо зазначити, що в експертному середовищі не завжди довіряють існуючим радарним базам даних та джерелам інформації для форсайту. Ці джерела рідко публікують деталі процесу збору та підготовки інформації, тому опитані експерти, як правило, покладаються на власні дослідження або першоджерела для визначення інформації, пов'язаної з трендами.

Інструменти для проведення конференцій часто використовуються для залучення учасників з різних географічних регіонів. Вони надзвичайно корисні для об'єднання різноманітних груп учасників. Однак, використання цих інструментів має і зворотний бік. Учасники можуть бути менш здатними повністю присвятити свою увагу онлайн-зустрічам (на відміну від особистих семінарів) через меншу інтерактивність віддалених семінарів і той факт, що деякі учасники можуть піддаватися спокусі робити кілька справ одночасно або приєднуватися до інших зустрічей. Крім того, рівень цифрової грамотності в групі може бути різним – через брак технічних навичок та обізнаності деякі учасники можуть бути не в змозі повноцінно та впевнено брати участь під час використання інструментів для проведення конференцій.

ФОРСАЙТ КІБЕРСТІЙКОСТІ

Поява нових загроз є складною, швидкоплинною та іноді непередбачуваною подією, особливо з урахуванням стрімкого приросту кіберінцидентів. Отже, часто може статися, що ймовірність та актуальність окремих загроз у багатьох випадках може раптово змінитися через непередбачувані інциденти, суспільні зміни або спонтанні інновації. Різнобічні глобальні ініціативи охоплюють широкий спектр тем, включаючи визначення кіберзагроз та класифікацію їх за рівнем небезпеки. Багато загроз, відомих сьогодні, залишаться актуальними в майбутньому, але їх характер зміниться через зростання залежності, демократизацію та розвиток нових технологій.

Прикладом системної роботи з визначення майбутнього (форсайту) у сфері кібербезпеки є проведений аналіз за ініціативою ENISA у період з березня по серпень 2022 року [43], яким було визначено та ранжовано 21 загрозу, поширеність яких зростатиме до 2030 року. Було проведено серії семінарів та інтерв'ю з відповідними експертами за методом PESTLE та застосовано різноманітні підходи до методології.

Використана методологія ENISA складається з чотирьох етапів [24].

> Перший, «*спільне дослідження*», – це фаза дослідження тенденцій та збору інформації, яка інтегрувала знання експертів, зворотний зв'язок та перевірку.
>
> На другому етапі, «*групові семінари з прогнозування*», збиралися групи експертів з досвідом роботи в одному з вимірів PESTLE для подальшого обговорення, вивчення, оцінки та визначення пріоритетів виявлених тенденцій.

Третій етап, «*ідентифікація загроз*», ґрунтувався на методології «кастингу загроз» для визначення нових викликів, які можуть виникнути впродовж наступних 10 років. Для цього невеликим групам експертів з кібербезпеки надавався сценарій, який поєднував пріоритетні тенденції.

На наступному етапі, визначені учасниками-експертами, *загрози були оцінені* за такими показниками, як імовірність, вплив, новизна і те, чи була ця загроза раніше визначена. Новизна розглядалася для того, щоб визначити пріоритетність менш відомих загроз.

Акцент було зроблено на 10 кіберзагрозах з найвищим рейтингом, при цьому, суб'єктами загроз визначено чотири основні групи: держава-спонсор, кіберзлочинці, хакери-найманці та хактивісти [44].

Методологічно прогноз побудовано на основі поточної таксономії загроз ENISA [45], яка поділяє їх на такі категорії високого рівня:

- *фізична атака (навмисна),*
- *ненавмисне пошкодження / втрата інформації або ІТ-активів,*
- *стихійні лиха (природні),*
- *збої / несправності,*
- *перебої в роботі,*
- *підслуховування / перехоплення / викрадення,*
- *недобросовісна діяльність / зловживання, а також правові аспекти.*

Важливо зазначити, що ненавмисні загрози розглядаються як вразливості, які можуть бути використані суб'єктом загрози, а тому основний акцент зроблено на навмисних загрозах [24]:

- ✓ *компрометація ланцюжка поставок програмних засобів;*
- ✓ *просунуті кампанії з дезінформації / операцій впливу;*
- ✓ *зростання авторитаризму цифрового нагляду / втрата приватності;*
- ✓ *людські помилки та застарілі системи в кіберфізичних екосистемах;*
- ✓ *цілеспрямовані атаки (наприклад, програми-вимагачі), посилені даними зі смарт-пристроїв;*
- ✓ *брак аналізу та контролю космічної інфраструктури та об'єктів;*
- ✓ *зростання сучасних гібридних загроз;*
- ✓ *дефіцит навичок;*
- ✓ *транскордонні постачальники послуг ІКТ як єдина точка відмови*
- ✓ *зловживання штучним інтелектом.*

Надамо коротку характеристику цим ключовим загрозам у кіберпросторі.

Компрометація ланцюжка поставок програмних засобів. До 2030 року все більшою буде інтеграція компонентів і сервісів, об'єднаних у нові продукти. Оскільки ринок вимагає швидких циклів випуску продуктів, програмування на основі компонентів значно зросте [46], що призведе до повторного використання коду та використання бібліотек коду з відкритим вихідним кодом.

Незважаючи на регулярну перевірку деяких з цих компонентів на вразливості, поєднання програмного, апаратного та компонентного коду створюватиме неконтрольовані взаємодії та інтерфейси [47]. З'являться нові та непередбачувані вразливості, що дасть кіберзлочинцям більше шансів порушити ланцюг постачання як з боку постачальника, так і з боку клієнта.

Потенціал використання вразливостей програмного забезпечення, атак на конфігурацію програмного забезпечення та апаратного забезпечення, фішингових атак й ін'єкцій шкідливого програмного забезпечення в бібліотеки коду є політичними та фінансовими мотивами цих суб'єктів. Це може призвести до серйозних проблем у ланцюгах постачання й використовується зловмисниками для здійснення політичних дестабілізацій, фінансового маніпулювання або шпигунської діяльності.

Злочинці можуть керувати інструментами розробки та програмними залежностями, вставляючи бекдори до складових коду. Бібліотеки з відкритим кодом є одним із найпростіших способів, якими злочинці можуть користуватися. Зловмисники можуть отримати початковий доступ до комерційних застосунків за допомогою різних методів, наприклад, компрометації «drive-by» або атаки, які використовують соціальну інженерію. Запуск троянських програм, дроперів або руткітів у програмні компоненти, які надаються, дозволяє зловмисникам отримати доступ до мережі їхньої кінцевої цілі, що залежить від апаратних або програмних компонентів організації [24].

Також можливий фізичний вплив на апаратне забезпечення на виробничих потужностях. Для того, щоб такі злочинці могли втілити свій замисел, вони мають отримати фізичний доступ (або, принаймні, бути в безпосередній близькості) до приміщень виробництва апаратних компонентів. Злочинці могли б потрапити на законні об'єкти шляхом використання особи зсередини, яка б працювала там і мала б ідеальний доступ до апаратного забезпечення для компрометації даних або системи.

Іншим випадком може бути компрометація широко використовуваної приватної компанії з доступом до конфіденційних даних [48].

Просунуті кампанії з дезінформації / операцій впливу. У 2030 році окремі суб'єкти, такі як злочинні угруповання, наймані хакери, а також держави-спонсори, імовірно, матимуть доступ до нових технологій, таких як діпфейки, для розширення своїх зловживань і маніпуляцій суспільством шляхом поширення дезінформації. Незважаючи на те, що використання технології діпфейк може призвести до незаконного збагачення окремих осіб або злочинних угруповань, основна мета дезінформаційних кампаній з використанням підроблених ідентичностей зазвичай є геополітичною, і, швидше за все, їх ініціаторами є окремі держави та інші політично мотивовані групи [24].

Джерел даних зараз незліченна кількість; противники можуть тренувати свій ШІ для глибоких фейкових атак [49], використовуючи широкий спектр загальнодоступних відео, фотографій і записів голосу людей (навіть тих, хто не є публічною особою). Біометричні зображення обличчя особливо вразливі до морфінг-атак (morphing attacks), в яких зловмисник може з високим ступенем точності видавати себе за свою ціль. Технологія глибокої підробки також може створювати нереальні обличчя [50], які людське око не в змозі відрізнити від справжніх. Тобто виникає можливість створення реалістичних аватарок, які відрізняються від уже складних ботів у соціальних мережах. Крім того, майбутні боти, які мають здатність впливати на вибори та формувати довіру громадськості, будуть публікувати свої відео в соціальних мережах та активно брати участь у дебатах. За допомогою штучного інтелекту, аналізу тексту або голосу можна ще більше посилити дезінформаційні кампанії, щоб забезпечити індивідуалізовані відповіді окремим особам.

Зростання авторитаризму цифрового нагляду / втрата приватності. Злочинців все частіше ідентифікують за допомогою таких технологій, як відстеження місцезнаходження, громадські камери та розпізнавання обличчя [51]. У майбутньому це може спонукати держави, а також приватних суб'єктів, значно розширити використання цих технологій. Через такі технології, як розпізнавання обличчя у публічній сфері, посилення цифрового нагляду на інтернет-платформах або запровадження цифрової ідентичності, індивідуальні свободи можуть бути обмежені заради безпеки та захисту. Доступ до цих даних дозволить правоохоронним органам та іншим державним установам відстежувати потенційних підозрюваних і заохочуватиме їх до цього. Ці сховища даних також можуть стати величезною мішенню для злочинних угруповань, які зможуть продавати в інтернеті дані про особу на основі однієї лише фотографії [24]. Приватний сектор також відіграє важливу роль, особливо коли основні технології розпізнавання обличчя або контент-платформи знаходяться під контролем одного лідера ринку. Провайдери, які надають технології розпізнавання обличчя або контент-платформи, стануть мішенню для величезних масивів консолідованих даних голосу та зображень. Крім того, дії приватних корпорацій не завжди можуть відповідати вимогам захисту даних і безпеки.

Уряди (в тому числі правоохоронні органи) й приватні підприємства в рамках державно-приватного партнерства можуть в межах своїх правових норм законно збирати персональні дані, в тому числі біометричні дані. Це створює виклики [52] для регуляторних органів і громадськості, щоб забезпечити дотримання законів, які захищають їхнє приватне життя. Крім того, це вимагає від усіх суб'єктів, які збирають ці дані, мати необхідні механізми захисту. Як тільки зловмисники отримують доступ до мережі, вони можуть почати автоматизований збір даних, потенційно використовуючи інтерпретатор команд і сценаріїв, а також API, інтерфейси командного рядка або сервіси вилучення, перетворення й завантаження (ETL) в хмарних середовищах. Одним із варіантів використання може бути зловживання зібраними даними правоохоронними органами або онлайн-спільнотами для відстеження потенційних злочинців [24].

Поява інтерфейсу між комп'ютером і мозком також ознаменує остаточне зникнення розриву між кібербезпекою і розвідкою. Ми добровільно розміщуємо величезні обсяги даних в Інтернеті, і багато з наших повсякденних дій залишають за собою електронний слід. Наш набір публічних і приватних даних містить широкий спектр інформації та включає в себе все – від покупок за кредитними картками й бібліотечних книг до «оновлень статусу», які ми охоче публікуємо на платформах соціальних мереж. За останні 10 років одним з найважливіших досягнень у сфері спостереження стала можливість видобувати дані з цих величезних пилових пагорбів тривіальних, на перший погляд, даних для отримання розвідувальної інформації, яка має все більшу цінність. Показово, що служби технічної розвідки зараз інвестують менше грошей в криптографію і більше – в зберігання даних і великомасштабну обробку даних [1].

Водночас існує і альтернативна точка зору щодо поглинання приватності. У 1998 році Девід Брін опублікував інтригуючу книгу під назвою «Прозоре суспільство». Недооцінена під час першої публікації, ця маленька класика є однією з найбільш інтригуючих дискусій про наше цифрове майбутнє. Він стверджує, що, хоча приватність добігає кінця, ми не повинні надмірно перейматися цим питанням. Він наполягає на тому, що насправді важливо, хто володіє даними і як ними керує. Універсальні дані потенційно притягують до відповідальності як уряди, так і громадян. Коротше кажучи, Брін був оптимістом і наполягав на тому, що ми не так вже й далеко від радикально покращеного суспільства. Він наполягав на тому, що більше інформації звідусіль може сприяти більшій цивілі-

зованості й навіть перерозподілу влади. У такому майбутньому не матиме значення, що держава вимагає прозорості від своїх громадян, доки держава пропонує прозорість у відповідь [53]. Чи стане Прозоре суспільство Бріна врешті-решт реальністю, чи ми зіткнемося з чимось більш похмурим? Брюс Шнайєер, авторитетний експерт з кібербезпеки, який свого часу очолював службу безпеки British Telecom, скептично відповів на це запитання, наполягаючи на тому, що право власності на ці дані навряд чи буде достатнім для того, щоб сприяти колективній людській підзвітності, яку передбачає Брін [54; 55]. Який би оракул не виявився правим, майбутнє стрімко наближається, і коли воно настане, наші нинішні системи управління інтернетом і кіберстійкості навряд чи зможуть з ним впоратися.

Людські помилки та застарілі системи в кіберфізичних екосистемах. У 2030 році інтернет речей проникне у значну частину транспортної, енергетичної, водопровідної та промислової інфраструктури, щоб підвищити ефективність та покращити прийняття інтелектуальних рішень. Крім того, відбудеться значне збільшення кількості розумних пристроїв, які пересічний користувач пов'язує з собою (станом на 2021 рік середньостатистична людина мала сім розумних пристроїв) [56]. Через це може стати надзвичайно складно обслуговувати всі пристрої та керувати ними, особливо з точки зору безпеки. Крім того, виробники смарт-пристроїв, ймовірно, не зможуть навчити кінцевих користувачів необхідності обслуговування пристроїв. Швидке впровадження IoT і постійний дефіцит навичок призведе до того, що до 2030 року бракуватиме знань, підготовки й розуміння кіберфізичної екосистеми, що призведе до проблем з підтримкою безпеки IT, пов'язаних з неправильною конфігурацією, несвоєчасним обслуговуванням і неадекватною підтримкою в кінці терміну служби застарілого програмного забезпечення IoT [24]. На додаток до цих проблем, зловмисники можуть розгортати інтелектуальні атаки з використанням таких методів, як генеративні ворожі мережі (Generative Adversarial Networks, GAN), які можуть різко знизити рівень виявлення кібератак. Одним із прикладів використання GAN може бути атака на сервери, що розповсюджують патчі, з метою зриву запланованих оновлень [57]. Через критичність пристроїв, це може створити системний ризик, що призводить до перебоїв у роботі, пошкоджень, а також перехоплення даних між пристроями.

На стороні кінцевого користувача пристроями «інтернету речей» часто керують мобільні пристрої, що працюють на iOS або Android. Кінцеві користувачі спілкуються через свої мобільні додатки з розумними пристроями, які є частиною їхнього будинку, транспорту або іншого оточення. Зловмисники можуть спробувати отримати початковий доступ до мобільних пристроїв за допомогою підробки біометричних даних, атак грубої сили або використання вразливостей на пристрої. Отримавши доступ до телефона й законних каналів зв'язку між телефоном кінцевого користувача та інфраструктурою, вони можуть втручатися в роботу смарт-пристроїв, проникати в мережу або отримати доступ до облікового запису, який керує смарт-пристроями [58]. У промисловій екосистемі зловмисники можуть отримати початковий доступ через співробітників за допомогою атаки соціальної інженерії або через їхні кінцеві точки, переміститися вглиб корпоративної мережі й шукати пристрої з доступом до інтернету, які підключені до промислових систем управління. Крім того, атаки можуть бути успішними через тимчасові кібер-активи, які розгортаються з незахищеною конфігурацією, в тому числі від сторонніх постачальників і партнерів

Цілеспрямовані атаки (наприклад, програми-вимагачі), посилені даними зі смарт-пристроїв. У 2030 році збір поведінкових даних збільшиться в геометричній прогресії. Використання смарт-пристроїв у нашому повсякденному житті значно зросте; будуть збиратися дані з усіх аспектів життя, що призведе до створення точного та унікального поведінкового профілю кожного користувача. Зібрані дані можуть включати (серед інших джерел) дані про стан здоров'я з натільних пристроїв і медичного обладнання або з пристроїв інтернету речей в «розумних будинках», які збирають інформацію про поведінку вдома, дані про пересування або поведінку на онлайн-платформах. Оскільки смарт-пристрої часто будуть незахищеними через громіздкість пристроїв і недостатню обізнаність кінцевих користувачів ці дані можуть бути використані [50]. Інтелектуальні периферійні пристрої вже зараз важко захистити від маніпуляцій та прослуховування.

Злочинні групи намагатимуться отримати доступ до величезних масивів даних, щоб адаптувати атаки соціальної інженерії на основі поведінкового профілю користувача. Рівень витонченості цих атак соціальної інженерії змусить кінцевих користувачів, правоохоронні органи та уряди шукати нові способи запобігання соціальній інженерії та покращення автентифікації.

Зловмисники можуть отримати початковий доступ через підключені до інтернету смарт-пристрої, які не мають оновлень або все ще працюють зі стандартними налаштуваннями. Злочинці та хакери-найманці [44] збиратимуть інформацію про особу жертви, облікові дані та контактну інформацію, щоб отримати початковий доступ, а потім просуватимуться далі в мережі, щоб отримати доступ до більш чутливої інформації. Зловмисники використовуватимуть автоматизований збір даних і проникнення, зіставлятимуть та інтерпретуватимуть дані для створення поведінкового профілю своєї жертви. Щоб утримати свої позиції, зловмисники використовуватимуть методи наполегливості

[24]. За допомогою поведінкового профілю вони намагатимуться отримати доступ до фінансових активів, використовуватимуть профіль для підміни високопосадових осіб у мережі жертви або продаватимуть зібрані дані на чорному ринку.

Брак аналізу та контролю космічної інфраструктури та об'єктів. Початок 2010-х і 2020-х років розпочав нову еру космічних подорожей, коли приватні компанії приєдналися до урядів у прагненні досліджувати наш всесвіт. До 2030 року космічний сектор, ймовірно, трансформується ще більше завдяки збільшенню інвестицій приватних суб'єктів, партнерствам між приватними компаніями та урядами, а також зростанню геополітичної та комерційної конкуренції в космосі [24].

Швидке зростання цього сектору уможливить надання багатьох ключових послуг. Незважаючи на прогрес, досягнутий за останні роки, цей сектор все ще залишається в центрі уваги безпекової спільноти.

З точки зору безпеки бракує розуміння, аналізу й контролю космічної інфраструктури. Без ширшого загальноєвропейського фокусу розбудова надійного захисту космічної інфраструктури може бути надто повільною (наприклад, науково-дослідні проекти, які потребують часу на планування й бюджетування). Це також означає, що може бракувати своєчасної підготовки до ідентифікації та використання невідомих вразливостей [59] (нульові дні) – якщо ресурси не розподілені належним чином. Ринки стимулюють приватні компанії швидше впроваджувати інновації та знижувати витрати за рахунок кібербезпеки. Приватні компанії можуть спробувати використати це для саботажу своїх конкурентів; уряди можуть спробувати використати вразливості для створення конкурентної геополітичної переваги в космосі; а злочинні угруповання використовуватимуть вразливості, щоб вимагати у компаній фінансову вигоду і створювати хаос [24].

Через перетин приватної та державної інфраструктури в космосі зловмисники можуть отримати початковий доступ до космічної інфраструктури, обравши своєю мішенню приватних суб'єктів, урядові установи або окремих осіб, які взаємодіють з інфраструктурою. Оскільки уряди й суспільства значною мірою залежать від супутників (наприклад, GPS), державні зловмисники й хакери-найманці намагатимуться отримати початковий доступ до апаратного забезпечення через атаки на ланцюжки поставок і використовуватимуть методи, щоб зберегти свою присутність у космічній інфраструктурі, зокрема на базових станціях [24]. Зловмисники використовуватимуть наявні технології, щоб обійти механізми захисту й виявлення, але залишатимуться бездіяльними, доки не використають їх у стратегічних цілях, наприклад, під час конфлікту як засіб гібридної війни. Впровадження зброї космічного базування може змінити геополітичну парадигму.

Зростання сучасних гібридних загроз. До 2030 року кібератаки стануть більш витонченими й будуть поєднуватися з фізичними або офлайн-атаками. Методи атак постійно розвиваються і часто комбінуються – послідовно й паралельно – для досягнення своїх цілей. Ці гібридні операції складніше виявити й захиститися від них через їхню складність і тенденцію розглядати кожну атаку окремо [24]. За нового способу дій інструменти виявлення потребують більшої кореляційної здатності, в тому числі пов'язувати, здавалося б, не пов'язані між собою події. Тому вони становлять все більший виклик як для урядів, так і для компаній та громадян. У минулому гібридні атаки здійснювалися переважно державними суб'єктами як поєднання традиційних і кібервійськ. У 2030 році гібридні загрози еволюціонували до застосування нових технологій та комбінування різних типів механізмів експлуатації для того, щоб обійти існуючі системи реагування [24].

Наприклад, зловмисники все частіше використовуватимуть штучний інтелект і глибоке навчання, щоб об'єднати свої можливості [49] для створення нових, непередбачуваних способів дій. Зловмисники використовуватимуть одночасну комбінацію методів для отримання початкового доступу, включаючи збір великих даних для адаптації своїх фішингових кампаній, машинне навчання для інтерпретації даних, розробку нових інструментів для обходу захисних механізмів і поєднання фізичного й віртуального для здійснення своїх атак. Зі збільшенням кількості смарт-пристроїв, використання хмарних технологій, збільшенням кількості онлайн-ідентифікаторів і соціальних платформ, а також цифрових посвідчень особи, виданих урядами, зловмисники отримають безліч нових сфер для використання й комбінування для створення креативних векторів атак.

Дефіцит навичок. До 2030 року проблема дефіциту навичок [60] не буде вирішена. Хоча зростання кількості незаповнених робочих місць у сфері кібербезпеки вирівнялося, дефіцит навичок і надалі становитиме значний ризик для суспільства та урядів. Одним з важливих факторів, який впливатиме на загрозу у 2030 році, є готовність (і ресурси) організацій розширювати штат і розвивати таланти. Впровадження функцій кібербезпеки також постраждає через брак навичок і загальної зрілості функцій кібербезпеки, навіть за наявності бажання.

У міру того, як технології все більше інтегруються в наше життя, пересічні громадяни можуть стати апатичними – всі їхні комунікації та дії управляються десь іззовні, і вони не мають на це жодного впливу. Цей ризик посилюватиметься взаємодією між новими технологіями та застарі-

лими технологіями, для яких робоча сила не була підготовлена – знання застарілих технологій передаються недостатньо швидко, щоб управляти цим ризиком у 2030 році [24]. На додаток до дефіциту застарілих навичок, нові технології, такі як розумні пристрої, штучний інтелект, космічна інфраструктура або квантові обчислення, створюватимуть нові виклики кібербезпеці. Злочинні групи обиратимуть організації, установи та компанії, які мають велику кількість незаповнених вакансій у сфері кібербезпеки, з метою пошуку вразливостей та використання цих вразливостей для отримання фінансової вигоди.

Зловмисники аналізують організаційні навички та недоліки, щоб отримати уявлення про слабкі місця в захисті, потенційні вразливості та можливості для використання їхніх систем і мереж. Публічні оголошення про вакансії часто містять детальну інформацію про те, яких навичок наразі бракує в компанії чи державній установі, що дає зловмисникам уявлення про можливі вектори проникнення. Крім того, зловмисники намагатимуться отримати інформацію з відкритих і закритих джерел, щоб зібрати організаційну та мережеву інформацію і виявити застарілі системи з відомими вразливостями. Наприклад, в оголошенні про вакансію на місцевій електростанції може бути вказаний постачальник і тип продукту, для якого їм потрібна підтримка – це дає зловмисникам достатньо часу для дослідження вразливостей конкретного продукту. Крім того, розробляючи нові технології, працівники, які мають кваліфікацію для впровадження безпеки, не мають достатньої пропускної здатності, щоб застосувати безпеку до виходу на ринок через брак кваліфікованих працівників.

Транскордонні постачальники послуг ІКТ як єдина точка відмови. У 2030 році технологічна взаємопов'язаність буде посилюватися. Межа між фізичним і кіберпростором ще більше розмиватиметься, оскільки такі сектори інфраструктури, як транспорт, охорона здоров'я, електромережі та промисловість [50], все більше покладаються на постачальників послуг ІКТ для підключення до інтернету та управління всіма міжпристрійними зв'язками. Хоча їхня відповідальність за підтримку функціонування суспільства була значною ще у 2022 році, до 2030 року їхня важливість зростає ще більше. Провайдери ІКТ-послуг та їхня інфраструктура, включаючи супутникові технології, є основою суспільства і тому можуть стати єдиною точкою відмови. Розумні міста є прикладом того, що через 10 років операційні мережі стануть ще більш критично важливими. Отже, ці постачальники послуг, імовірно, стануть мішенню для урядів, терористів і злочинних угруповань. Використання вразливостей для отримання доступу до їхніх мереж, кінцевих точок, центрів обробки даних або інших фізичних компонентів ІКТ-інфраструктури може завдати шкоди містам і цілим регіонам [24].

Іноземні уряди можуть спробувати використати це для дестабілізації країн, терористи – для нагнітання страху й досягнення політичних цілей, а злочинні угруповання – для захоплення міст у заручники. ІКТ-інфраструктура [61], ймовірно, буде використана як зброя під час майбутнього конфлікту. Провайдерам ІКТ доведеться захищатися від спонсорованих державою, наполегливих і високорозвинених атак, які спираються на дані урядових розвідувальних служб і наступальні кіберпотужності. Ресурси, які будуть виділені для такої атаки, є значними – зловмисникам знадобиться час, щоб уникнути традиційних функцій реагування, і вони, імовірно, розгорнуть гібридні атаки для отримання початкового доступу й нещодавно розроблених експлойтів з можливостями командування та контролю. Оскільки сектор ІКТ з'єднує так багато критично важливих послуг, він стане мішенню для таких технологій, як бекдори, фізичні маніпуляції й відмова в обслуговуванні, через масштаб збитків, яких можна досягти.

Зловживання штучним інтелектом. ШІ можна маніпулювати з моменту його створення та протягом усього життєвого циклу за допомогою маніпуляцій з навчанням і ворожих атак [62]. Несвідома упередженість ШІ була добре відома на початку 20-х років, однак у 2030 році існує реальна загроза навмисного маніпулювання алгоритмами ШІ та навчальними даними. Так само будь-яке спотворене навчання алгоритмів ШІ може навчити їх приймати неправильні рішення щодо секторів підвищеного ризику [63].

Зловмисники намагатимуться використати можливості додатків зі штучним інтелектом для формування результатів прийняття рішень і збору інформації про потенційних жертв. Наприклад, вони можуть втручатися в навчальні набори даних для створення дисфункціональних і шкідливих програм штучного інтелекту – це може стосуватися й проектів збору даних на основі краудсорсингу (crowdsourcing). Крім того, зловмисники можуть використовувати ШІ в наступальних або злочинних цілях – наприклад, аналізувати поведінку користувачів для створення високорозвинених фішингових або гібридних кампаній [24].

ШІ може бути використаний для посилення багатьох нечесних дій, таких як створення дезінформації та фейкового контенту, використання упереджень, збір біометричних та інших конфіденційних даних, створення військових роботів, отруєння даних тощо.

Майбутнє кіберстійкості частково пов'язане з людьми як антидотом до вразливостей інтернету. Однак у той час як нова логіка безпеки систем передбачає необхідність різноманітності та навіть,

можливо, обережного відокремлення, загальна тенденція в інформаційних технологіях полягає в конвергенції людей і комп'ютерів. Мабуть, найпомітнішим проявом цього є світ ігор, де ми спостерігаємо прагнення об'єднати людину й машину в симульованій топографії [64]. Витончені ігри все частіше використовуються провайдерами військової підготовки для створення різноманітних тренувальних середовищ. Як у військових, так і в розважальних цілях, реальність і кіберпростір дедалі більше зближуються, і наступним викликом є безперешкодна взаємодія між мозком і комп'ютером.

Найпоширеніший досвід цього можна знайти в сучасних ігрових технологіях, які використовують розпізнавання зображень для перетворення людських жестів на команди. Система Microsoft Xbox Kinect дозволяє гравцям взаємодіяти з грою через фізичні рухи, зафіксовані відеокамерою. Очевидно, що Xbox вимагає фізичного руху. Однак у 2009 році компанія Mattel випустила «Mindflex» - гру, яка отримувала вхідні дані безпосередньо від мозку. Вхідні дані були відносно примітивними, оскільки гравець не міг свідомо керувати пристроєм. Замість цього гра зчитувала електромагнітні імпульси (ЕМІ). У лабораторних умовах піддослідних навчили набирати номер мобільного телефону, використовуючи лише ЕМІ. Всі ці пристрої, хоч і примітивні, тим не менш, вказують шлях до майбутнього технологій і потенціалу, який пропонує інтерфейс між комп'ютером і мозком [1].

Очевидним застосуванням зростаючого зв'язку між людьми та інтернетом є превентивна охорона здоров'я. Вчені-медики все більше цікавляться маленькими чіпами, які відстежують життєво важливі показники й можуть вказати на ранній початок проблем з серцем, інсультів та інших захворювань [65; 66]. Рання діагностика та втручання до того, як ці захворювання настануть, суттєво підвищує шанси на успішний результат. Ця технологія вже існує. Використовуючи нові технології, наприклад, смартфони з підтримкою GPS, ми можемо вимірювати ключові життєві показники, скільки часу ми спимо, куди їдемо, що їмо й п'ємо та як проводимо свій день. Зібравши ці дані, одержимі самоспостереженням люди розміщують їх у «хмарі». Останнім прикладом є «Fitbit» - крихітний пристрій, який можна прикріпити до одягу та який бездротовим способом надсилає медичні дані на веб-сайт, що створює графіки активності суб'єкта [1].

Найважливіші зміни відбулися в медичній технології, призначеній для лікування військових поранених. Вищі показники виживання на полях битв в Іраку та Афганістані в поєднанні з травмами, що змінюють життя, спричиненими саморобними вибуховими пристроями, підвищили попит на більш складні протези кінцівок. Виклик полягав у тому, щоб з'єднати сучасні протези з нервовою системою, щоб досягти чогось набагато ближчого до природного контролю з боку пацієнта. За останні п'ять років відбулися радикальні зміни у можливості підключення мікроелектроніки до нервової системи людини. Результати були вражаючими. Дрібна моторика, яку забезпечують ці пристрої, майже не відрізняється від тієї, яку забезпечують справжні кінцівки. Вчені очікують, що це дослідження призведе до створення нейронних протезів для всього тіла, спрямованих на відновлення повних, життєво важливих функцій руху паралізованих пацієнтів [1]. Коротше кажучи, проблема поєднання електронних повідомлень, що надсилаються людським мозком, і мікроелектронних систем буде вирішена в найближчі 10 років [67].

Мало хто з учених сумнівається, що прямий інтерфейс між комп'ютером і мозком не за горами. Якими можуть бути наслідки для кіберпростору? Такий розвиток матиме значні економічні, соціальні та політичні наслідки. Люди, які будуть постійно підключені до інтернету в більш фундаментальний спосіб, стануть більш здібними – але також будуть думати й діяти по-іншому. Можливість бути підключеним, а отже, бути на «постійному зв'язку» буде одним з найбільш фундаментальних рішень, які чекають на людину в середині двадцять першого століття [1].

> *Виникає запитання: як досягти кіберстійкості у світі, в якому людина все більше стає синонімом інтернету?*

Ця можливість викликає альтернативні бачення, утопічні або антиутопічні. Можливо, зростаючий зв'язок між 8 мільярдами людей та інтернетом нарешті створить кіберпростір, який дійсно представлятиме глобальне надбання – спільну віртуальну топографію, засновану на взаємній власності, повазі й довірі. З іншого боку, це нове середовище може призвести до збільшення глобальних ризиків і невизначеності [1].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Lewis, Herrington & Richard, Aldrich (2013). The Future of Cyber-Resilience in an Age of Global Complexity. POLITICS, 33 (4), 299–310. DOI: 10.1111/1467-9256.12035
2. Ministry of Defence (1976). Working Group on Testing of Computer Security, 1976/7 (D/DCCIS/56/8/5/4), DEFE68/287, TNA.
3. Warner, M. (2012). Cybersecurity: A Pre-historyю. Intelligence and National Security, 27(5), 781–799.
4. Arquilla, J. & Ronfeldt, D. (1993). Cyberwar is Coming! RAND Corporation RP-223.
5. Rid, T. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35 (1), 5–32.

6. Deibert, R.J., Rohozinski, R. & Crete-Nishihata, M. (2012). Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War. Security Dialogue, 43 (1), 3–24.
7. Farwell, J.P. & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. Survival, 53 (1), 23–40.
8. Американский адмирал подтвердил, что Россия ведет кибервойну против Украины. URL: https://web.archive.org/web/20160429082331/http://ain.ua/2014/03/17/515999
9. Russian Electronic Warfare in Ukraine: Between Real and Imaginable - Jamestown. Jamestown. Retrieved from https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable/
10. Російські хакери у 2023 році збільшили кількість атак на Україну: що відомо. URL: unian.ua/war/rosiyski-hakeri-u-2023-roci-zbilshili-kilkist-atak-na-ukrajinu-shcho-vidomo-12426765.html?_gl=1*b62dke*_ga*NTUzMzI0Mzg3LjE2OTc0NzgxNzY.*_ga_TECJ2YKWSJ*MTY5NzQ3ODE3NS4xLjAuMTY5NzQ3ODE4MC41NS4wLjA.*_ga_DENC12J6P3*MTY5NzQ3ODE3NS4xLjAuMTY5NzQ3ODE3OS41Ni4wLjA.
11. Statement from the Press Secretary. The White House. Retrieved from https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%BE-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1%8C%D0%BA%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B0_(%D0%B7_2014)
12. Атака на «Киевстар». Прекратил работать крупнейший в Украине оператор мобильной связи, СБУ подозревает Россию. URL: https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0_%D0%BD%D0%B0_%C2%AB%D0%9A%D0%B8%D1%97%D0%B2%D1%81%D1%82%D0%B0%D1%80%C2%BB_(2023)
13. НБУ рекомендує банкам створити резервні канали зв'язку після кібератаки на «Київстар». РБК-Україна. URL: https://www.rbc.ua/rus/news/nbu-rekomendue-bankam-stvoriti-rezervni-kanali-1702538362.html
14. «Київстар» не працює. Що сталось і чи можна обійти проблему. BBC News Ukrainian (укр.). URL: https://www.bbc.com/ukrainian/articles/cz92xrkklwro
15. Espiner, T. (2011). Cybercrime Cost Estimate is «Sales Exercise». Say Experts', Znet, 18 February. Retrieved from http://www.zdnet.com/cybercrime-cost-estimate-is-sales-exercise-say-experts-3040091866/
16. Curtis, S. (2011). Government Cyber Crime Report Debunked, Tecweek Europe, 22 February.
17. Press, L. (2011). The State of the Internet in Cuba. Unpublished research paper. Retrieved from som.csudh.edu/fac/lpress/cuba/chapters/lpdraft2.docx?.
18. Zhang, D.J. (2010). Integrating Cyber Security into Nuclear Digital I&C Safety Systems. ASME Conference Proceedings 18th International Conference on Nuclear Engineering, Vol. 1/Instrumentation and Controls (ICONE18).
19. Stolfo, S.J. (ed.) (2008). Insider Attack and Cyber Security: Beyond the Hacker. Boston, MA: Springer.
20. Arce, I. (2003). The Weakest Link Revisited. IEEE Security and Privacy, 1 (2), 72–76.
21. Dornhege, G., Millan, J., Hinterberger, T., McFarland, D. & Müller, K. (2007). Toward Brain–Computer Interfacing. Cambridge, MA: MIT Press.
22. Bures, O. (2006). EU Counterterrorism Policy: A Paper Tiger? Terrorism and Political. Violence, 18 (1), 57–78.
23. European Foresight Platform (efp), What is Foresight? (2010). Retrieved from http://www.foresight-platform.eu/community/forlearn/what-is-foresight/
24. Foresight Challenges. A study to enable foresight on emerging and future cybersecurity challenges. European Union Agency for Cybersecurity (ENISA), 2021.
25. Haegeman, K., Spiesberger, M. & Könnölä, T. (2017). Evaluating foresight in transitional research programming. Technological Forecasting and Social Change, 115, 313 – 326.
26. Althonayan, Abraham & Alina Andronache (2019). Resiliency under strategic foresight: The effects of cybersecurity management and enterprise risk management alignment. 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA). IEEE.
27. Senge, Peter M. (1990). The fifth discipline: the art and practice of the learning organization. New York: Doubleday/Currency
28. Jackck, E. Smith & Saritas, Ozcan (2011). Science and technology foresight baker's dozen: A pocket primer of comparative and combined foresight methods. Foresight, 13 (2), 79-96.
29. Megatrend / Trend / Driver / Issue, 2010. Retrieved from http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/megatrend-trend-driver-issue/
30. GCPSE, Foresight (2014). The Manual, UNDP Global Centre for Public Service Excellence, Singapore.
31. NISTEP. Retrieved from https://www.nistep.go.jp/en/?page_id=56
32. A Refresher on Regression Analysis. Retrieved from https://hbr.org/2015/11/a-refresher-on-regression-analysis
33. Jackson, M. (2013). Practical Foresight Guide– Chapter 1.
34. Vanatta, N. & Johnson, B.D. (2019). Threatcasting: a framework and process to model future operating environment. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 16 (1), 79 – 88.
35. Matthew, Rosenquist & Timothy, Casey (2009). Prioritizing Information Security Risks with Threat Agent Risk Assessment. Intel Information Technology, USA, 1-8.
36. Note that Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473
37. Barber, C. (2020). Cyber Security Predicting the Future.
38. POLI.design and Oblo, Service Design Tools, Tools. Retrieved from https://servicedesigntools.org/tools

39. Futures platform. Retrieved from https://www.futuresplatform.com/product
40. IFTF - The Future Is Wide Open. Retrieved from https://www.iftf.org/uploads/media/GovFuturesLab_Toolkit.pdf
41. Teach the Future: Futures Thinking Educators. Retrieved from https://www.teachthefuture.org/
42. Kayser, Victoria & Knut Blind (2017). Extending the knowledge base of foresight: The contribution of text mining. Technological Forecasting and Social Change, 116, 208-215.
43. ENISA (2022). Identifying Emerging Cyber Security Threats and Challenges for 2030.
44. ENISA (2022). Threat Landscape Report. Retrieved from https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_de.pdf
45. ENISA (2016). Threat Taxonomy. Retrieved from https://www.enisa.europa.eu/topics/threatrisk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy
46. ENISA (2021, July). Understanding the increase in Supply Chain Security Attacks. Retrieved from https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-insupply-chain-security-attacks
47. Jubb, S. (2022, August). Escalating supply chain cyber-attacks need a strategic response. Retrieved from https://www.openaccessgovernment.org/escalating-supply-chain-cyberattacks-need-a rategicresponse/141371/#:~:text=What%20are%20supply%20chain%20attacks,and%20cause%20disruptions%20or%20outages
48. Newman, L. H. (2021, December). A Year After the SolarWinds Hack, Supply Chain Threats. Retrieved from https://glock.co.uk/blog/a-year-after-the-solarwinds-hack-supply-chain-threats-still-loom-wired/?doing_wp_cron=1706623406.9687340259552001953125
49. Shein, E. (2022, August). Deepfake attacks and cyber extortion are creating mounting risks. Retrieved from https://www.techrepublic.com/article/deepfake-attacks-and-cyberextortion-are-creating-mounting-risks/
50. ENISA (2021). Threat Landscape. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
51. ENISA (2020). Personal Data Breaches. Retrieved from https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches
52. ENISA (2021). Retrieved from Foresight Challenges: https://www.enisa.europa.eu/publications/foresight-challenges
53. Brin, D. (1998). The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom? Reading, MA: Addison-Wesley.
54. Brin, D. (2008). David Brin Rebuts Schneier in Defense of a Transparent Society. Wired News, 12 March.
55. Schneier, B. (2008). The Myth of the «Transparent Society». Wired News, 6 March. Retrieved from http://bakerinstitute.org/publications/ITP-pub-PlanksOfUSInternationalCyberPolicy-052112.pdf
56. BSI-Magazin (2021, January). Mit Sicherheit. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSIMagazin_2021_01.pdf?__blob=publicationFile&v=4
57. Shi, A. (2021, September). Cyber Attacks Detection Based on Generative Adversarial Networks. Retrieved from https://ieeexplore.ieee.org/document/9681469
58. SOCRadar (2022, May). Common IoT Attacks that Compromise Security. Retrieved from https://socradar.io/common-iot-attacks-that-compromisesecurity/#:~:text=Privilege%20escalation%3A%20Attackers%20could%20exploit,unauthorized%20access%20 to%20the%20network.
59. Erwin, S. (2022, March). Cyber warfare gets real for satellite operators. Retrieved from https://spacenews.com/cyber-warfare-gets-real-for-satellite-operators/
60. Fortinet (2022). Retrieved from fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf
61. Allianz (2016). Cyber attacks on critical infrastructure. Retrieved from https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-oncritical-infrastructure.html
62. West, T. (2017). The Future of Weaponized Artificial Intelligence. Retrieved from https://threatcasting.asu.edu/sites/default/files/2019-12/ThreatcastingWest2017.pdf
63. Commission, E. (2022). Regulatory framework proposal on artificial intelligence. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
64. Der Derian, J. (1990). The (S)pace of International Relations: Simulation, Surveillance, and Speed, International Studies Quarterly, 34 (3), 295–310.
65. Michael, K. & Michael, M.G. (2005). Microchipping People: The Rise of the Electrophorus. Quadrant, 49(3), 22–33.
66. Streitfield, D. (2002). First Humans to Receive ID Chips; Technology: Device Injected under the Skin Will Provide Identification and Medical Information. Los Angeles Times, 9 May.
67. Lebedev, M.A. & Nicolelis, M.A. (2006). Brain–Machine Interfaces: Past, Present and Future. Trends in Neuroscience, 29(9), 536–546.