КІБЕРБЕЗПЕКА ЕРИ ГЛОБАЛЬНОЇ КОМУНІКАЦІЇ

5.1. ЕВОЛЮЦІЯ СТРАТЕГІЙ КІБЕРБЕЗПЕКИ США

Розглядаючи та аналізуючи еволюцію стратегій кібербезпеки Сполучених Штатів Америки, передусім визначимо основні поняття, які застосовуються при аналізі цих стратегій. Досліджуючи у першому розділі нашої монографії рух смислів у глобальному Інтернет-середовищі, ми приділили чималу увагу аналізу терміна «Cyberspace» і зробили наголос на надзвичайній плідності та продуктивності префікса «cyber» у продукуванні нових смислів, пов'язаних із розвитком Інтернет-сфери та соціальною активністю різних страт суспільства, так чи інакше наближених до Інтернет-середовища. Проте, оскільки в цьому підрозділі йдеться про еволюцію саме американських стратегій кібербезпеки, ми будемо використовувати дефініції, які застосовуються американськими стратегами — вченими та військовими — для визначення основних понять у цьому напрямі. Вони надаються у доповіді під назвою «Кібермайбутнє Америки: безпека і процвітання в інформаційну добу»[1].

Передусім префікс *кібер* (від. англ. cyber) широко вживається у значенні всього, що стосується комп'ютерів, електронної інформації та/чи цифрових мереж.

Кібербезпека — це захист комп'ютерів, електронної інформації та/або цифрових мереж від їх випадкового або навмисного недозволеного відкриття, передачі, переривання, модифікації чи знищення.

Кіберпростір — поняття, яке означає уявлення про простір і спільноти, сформовані комп'ютерами, електронною інформацією та пристроями, цифровими мережами та їхніми користувачами.

Кібератака — ворожий акт використання комп'ютерів, електронної інформації та/або цифрових мереж, який має на меті маніпулювання, викрадання, руйнування критично важливих систем, функцій або інформації.

Кібероперації — використання кіберможливостей із метою досягнення цілей у кіберпросторі або через кіберпростір.

Кібервторгнення — недозволений акт обхідних маневрів щодо механізмів безпеки комп'ютерів, електронної інформації та/чи цифрових мереж.

Мережа — розподілена система взаємопов'язаних комунікаційних зв'язків.

Інтернет — глобальна інформаційна система, яка базується на використанні Протоколів Інтернету, що дає змогу взаємодіяти різноманітним компонентам, таким як мережі, обчислювальне обладнання та пристрої. Його індивідуальні компоненти керуються урядами, індустрією, академічною спільнотою та приватними особами.

Інформаційно-комунікаційна революція породила нову сферу людського спілкування, роботи, досліджень і використання — кіберпростір. На відміну від інших сфер, в яких протягом століть і тисячоліть ведуться, наприклад, воєнні дії, — таких як земля, повітря, моря та океани, а нещодавно й космічний простір, — вона — творіння розуму і рук людських. Ця сфера реальна і великою мірою віртуальна. Вона не має чітко окреслених меж. Більше того, її границі щосекундно змінюються. Вона багатокомпонентна, адже Інтернет, який становить її серцевину, й сам багатокомпонентний. До того ж він пов'язаний міріадами зв'язків із супутниковими та кабельними телекомунікаціями, мобільною та стільниковою телефонією, радіо та телебаченням, новими гаджетами тощо. Кіберпростір як новітня сфера діяльності людини, спільнот, індустрії, фінансів, урядів, держав не має аналогів у минулому щодо стратегій та механізмів свого захисту. Труднощі полягають і у його відкритості, попри окремі конфіденційні захищені мережі (але навіть вони постійно є цілями несанкціонованих кібератак, які призводять до руйнування інформаційно-комунікаційних мереж, комп'ютерів, їхнього контенту). Про це, зокрема, йшлося у доповіді Конгресу США[2].

До давно відомих типів кібератак, таких як «інструменти зламу системи» («відмички»), «розподілена відмова обслуговування», «логічні бомби», «трояни», «віруси», «хробаки», постійно додаються все нові й нові. Це ціла низка кібератак, метою яких є несанкціоноване полювання на персональні дані користувачів: «фішинг», «вішинг», «сніффер», а також такий метод отримання несанкціонованого доступу до ноутбуків, як «воєнне катання», та кібератака під назвою «атака нульового дня», коли робиться все для того,

щоб кіберзахист був не в змозі вчасно спрацювати. Загроза обертається на реальність одразу ж, як тільки спільноті стає відомо, що в системі кіберзахисту є незахищені ділянки, й удари завдаються саме по них.

Водночас кіберпростір є нагально важливим для життя і розвитку США. Можна з упевненістю констатувати, що він справді став центральною нервовою системою американського суспільства. За останні 20 років Інтернет використовують близько 80 % американських дорослих (що вже й казати про дітей і підлітків, які у переважній більшості розвинених країн світу ведуть перед у використанні Інтернету у порівнянні з дорослими). З них 94 % користуються електронною поштою, 75 % шукають новини і 67 % відвідують урядовий веб-сайт. Останнє свідчить про громадянську активність і зв'язок між громадянами й урядом. Невпинно зростає і глобальне значення Інтернету. На грудень 2010 р. число його користувачів у всьому світі перевищило 2 млрд осіб[3]. Відкритість Інтернету має і зворотний бік: кіберпростір США залишається недостатньо захищеним і тому потерпає від кібератак. Більше того, кіберпростір стає важливою, і з часом — центральною сферою військових інтересів цієї країни. Адже всі інші складові її збройних сил найтіснішим чином залежать від безперешкодного функціонування комп'ютерів, телекомунікаційних мереж та неушкодженої інформації, тобто усього того, що наповнює кіберпростір.

Отже, для висвітлення того, як виробляється сильна, дієва національна політика США в галузі безпеки, зупинимося на головних питаннях, які становлять національні інтереси цієї держави у кіберпросторі. Відомі американські дослідники — віце-президент і директор з наукових досліджень «Центру нової американської безпеки» Крістін М. Лорд та її колега по центру Тревіс Шарп, які присвятили цій проблемі перший том роботи «Американське кібермайбутнє: безпека та процвітання в інформаційну еру» (2011 р.), вважають, що такими трьома головними національними інтересами нині є безпека, економічне процвітання та просування американських цінностей[4].

Не можна не зазначити, що інформаційні технології — це величезна сила, якою володіють США, хоча не всі дослідники погоджуються із положенням, що кібербезпека є панацеєю від усіх військових загроз для США[5]. Для того, щоб це було так, міністерство оборони, за даними на 2011 р., мало у своєму розпорядженні 15 тис. телекомунікаційних мереж та 7 млн комп'ютерних

пристроїв і 4 тис. інсталяцій у восьмидесяти восьми країнах світу[6]. Така передова інформаційно-комунікаційна інфраструктура допомагає США передбачати, відстежувати та відповідати на загрози національній безпеці з надзвичайною точністю й ефективністю та значно збільшує американські військові й розвідувальні можливості у всьому світі.

Науковці констатують, що за останні двадцять років мережа Інтернет стала інтегральною частиною життя Сполучених Штатів. Вони зазначають, що доступ до кіберпростору створив нові можливості для процвітання американців[7]. Вчені підтверджують свою думку даними «Фундації інформаційних технологій та інновацій». Відповідно до них інформаційна технологічна революція дала змогу збільшувати валовий річний продукт США на 2 млрд дол. США — більше, ніж це було би без внеску інформаційної революції. Наводяться також численні свідчення американських науковців про те, що мережа Інтернет посилює ефективність, занижує ціни, розширює вибір користувачів, допомагає зростанню продуктивності, дає малому бізнесу більше можливостей для проникнення на ринок, стимулює інновації та посилює ріст заробітної платні[8].

Американські дослідники стверджують, що доступ до мережі Інтернет сприяє поширенню універсальних цінностей, які для американців є надзвичайно важливими. Це такі цінності, як свобода висловлювання та свобода зборів. Інтернет допомагає захисникам своїх цінностей втілювати їхні цілі у життя. Він надає дисидентам права голосу, а для публіки, яка потерпає від утисків, Інтернет — це засіб для того, щоб організуватися. Так само, як іншим безправним мережа Інтернет надає можливість мати новий інструментарій для свого висловлення і використання цієї мережі як глобальної платформи. Крім цих центральних американських інтересів — безпеки економічного зростання та просування універсальних цінностей, відкритий та безпечний доступ до кіберпростору полегшує міріади інтеракцій, які йдуть на користь американцям і людству в самому широкому сенсі. Він допомагає кращому функціонуванню охорони здоров'я, освіти, філантропії та управління. Він посилює інновації, науковий прогрес і спілкування між різними народами. Всі переваги мережі Інтернет не завжди можуть бути оцінені повною мірою, проте вони дуже важливі для просування як американських цінностей, так і глобального блага[9].

У США добре розуміють, що військові переваги у кіберпросторі роблять Сполучені Штати Америки найпотужнішою глобальною державою світу. Але разом із перевагами розростаються численні загрози кіберпростору. Саме тому в XXI ст. кіберпростір стає чи не найважливішою сферою державних і глобальних інтересів США. Ось чому, починаючи з 2003 р., у цій державі йдуть цілеспрямовані розробки стратегії захисту її кіберпростору. В лютому 2003 р., коли при владі були республіканці, президент Джордж Буш-молодший схвалив важливий документ «Національна стратегія безпеки кіберпростору» (The National Strategy to Secure Cyberspace)[10]. У ньому виділені три стратегічних пріоритети.

По-перше, запобігти кібератакам, скерованим проти критичної інфраструктури США.

По-друге, зменшити національну вразливість до кібератак.

По-третє, мінімізувати наслідки кібератак і час на відновлення структур, яким була завдана шкода.

У цьому доктринальному стратегічному документі були ідентифіковані п'ять критично важливих національних пріоритетів:

- імплементувати національну систему безпеки в національний кіберпростір і створити систему відповідей;
- зменшити загрози кіберпростору;
- посилити національну поінформованість і навчання щодо кіберпростору;
- захистити урядовий кіберпростір;
- посилити національну та міжнародну безпеку і кооперацію у сфері кіберпростору.

Головною метою цієї стратегії було виправити ситуацію з кібербезпекою в усій країні. І не тільки в системі уряду, а й у системі критичних інфраструктур, які перебувають у приватному секторі[11]. Значущість «Національної стратегії безпеки кіберпростору» полягає й у самому факті своєчасного її впровадження, й у тому, що основні її положення повторюватимуться у тому чи іншому варіантах або глибше розкриватимуться у подальших документах США, що стосуватимуться стратегії безпеки кіберпростору держави.

Республіканський уряд Дж. Буша-молодшого тримав проблему захисту національного кіберпростору під пильним контролем, оскільки кіберпростір став інтегральною частиною американської могутності, забезпечує США глобальні переваги, робить їхню економіку конкурентоспроможною, дає змогу справляти політичний вплив на інші країни світу та наочно демонструє новітні приваб-

ливі риси американського способу життя, втілені тепер не лише у нестримному консюмеризмі, а й у найширшому доступі до послуг та інновацій, пов'язаних із користуванням мережею Інтернет у бізнесових, соціальних і приватних цілях.

Об'єднаний Комітет голів штабів 2004 р. оприлюднив «Національну військову стратегію Сполучених Штатів Америки» (The National Military Strategy of the United States of America)[12], яка по суті становила план дій американських збройних сил для підтримки національної стратегії безпеки й національної стратегії оборони. У цьому документі наскрізно простежуються три головні ідеї: це боротьба з тероризмом; посилення об'єднаної міцності збройних сил США та трансформація об'єднаних сил для протистояння воєнним ситуаціям у близькому або віддаленому майбутньому.

2006 р. Об'єднаний Комітет голів штабів опублікував «Національну військову стратегію операцій у кіберпросторі» (The National Military Strategy for Cyberspace Operations — NMS-CO). Вона була зосереджена саме на кібербезпеці. Причому з документа випливало, що захист кіберпростору США мав п'ять головних аспектів: 1) радіоелектронну боротьбу; 2) психологічні операції; 3) операції в інформаційно-комунікаційних мережах; 4) військову дезінформацію та 5) оперативну безпеку[13]. Можна зробити висновки, що йдеться не тільки про захист національного кіберпростору, а й про відповідні дії, скеровані проти супротивника.

Слід зазначити, що документи стосовно стратегії захисту національного кіберпростору США, якими ми користуємось у цьому дослідженні, — це, природно, матеріали, які перебувають у відкритому доступі, проте окремі частини цих документів засекречені, тобто нам недоступні. Саме через такі обставини ми можемо спиратися тільки на ті положення, дані та інформацію, які містяться у відкритих частинах цих документів. Наприклад, як стверджує відомий науковець і експерт із протидії кібертероризму Томас М. Чен, який працював не лише в різних університетах США, а й співробітничав з дослідниками провідних компаній, пов'язаних із проблемами безпеки, йому відомо, що NMS-CO «ідентифікує *шість* шляхів, які дають змогу підтримувати перевагу в кіберпросторі, включаючи ці *три* (курсив мій. — *Авт.*):

1. Інвестиції в науку і технології;
2. Партнерство з індустрією, урядовими агентствами та іншими державами та
3. Інвестиції у навчання та підготовку робочої сили»[14].

Директива міністерства оборони D 3600.1 під назвою «Інформаційні операції» (Information Operations) була видана 14 серпня 2006 р.[15] В ній, зокрема, вводився принцип розподілення інформаційних операцій у кіберпросторі на такі три категорії:

- атака на комп'ютерні мережі;
- захист комп'ютерних мереж;
- забезпечення доступу до комп'ютерних мереж супротивника та їх використання у своїх інтересах.

Ця директива демонструє дедалі зростаючу структурованість військових операцій, запропоновану міністерством оборони США. Зокрема, чітко прописана контрнаступальна складова.

З метою поліпшення стану справ у галузі кібербезпеки США Дж. Буш-молодший створив у липні 2007 р. «Комісію з кібербезпеки на строк 44-го президентства» (Securing Cyberspace for the 44th Presidency). Головним висновком роботи комісії було те, що кіберпростір входить до найгостріших проблем безпеки США.

Практично у той самий час президент Буш-молодший видав «Вичерпну національну ініціативу з кібербезпеки» (The Comprehensive National Cybersecurity Initiative — CNCI) США[16].

Її метою було посилення заходів міністерства внутрішньої безпеки, так само, як і ряду інших урядових установ, задля захисту від існуючих та майбутніх втручань у національний кіберпростір. Головним завданням CNCI було покращення кібербезпеки США. У цій ініціативі були чітко окреслені взаємопов'язані між собою цілі. Серед них:

- установити фронтальну лінію оборони проти наявних загроз, використовуючи об'єднане розуміння ситуації, та запобігти майбутнім утручанням, зменшуючи можливі ураження;
- забезпечити захист плат від цілого спектра загроз, посиливши контррозвідувальну діяльність та безпеку всієї мережі постачання для ключових інформаційних технологій;
- розширити кіберосвіту, за допомогою федерального уряду скоординувати галузі досліджень і розвитку та розвинути стратегії відстеження шкідливої діяльності у кіберпросторі США[17].

Коли республіканську адміністрацію Буша-молодшого змінила демократична адміністрація президента Барака Обами, останній вже на початку 2009 р. приділив велику увагу питанню кібербезпеки США. По-перше, він обіцяв, що інформаційний простір США буде відкритим і транспарентним. Відповідно до своєї обіцянки президент Обама, по-перше, розсекретив частину документів із питань безпеки, прийнятих адміністрацію Джорджа Буша,

зокрема документи, що стосуються захисту кіберпростору Сполучених Штатів. По-друге, за його наказом проводився широкий огляд національної стратегії кібербезпеки, включаючи CNCI. В результаті цього огляду в березні 2009 р. від імені Білого дому були зроблені наступні висновки: вказувалося, що заходи задля забезпечення безпеки кіберпростору США не є задовільними, що багато урядових міністерств і відомств забюрократизували цю роботу, що потрібні ключові покращення у цій сфері, що не існує керівного державного органу, який би централізовано керував утіленням стратегії захисту кіберпростору США[18].

У травні 2011 р. Білий дім оприлюднив документ під назвою «Міжнародна стратегія для кіберпростору» (International Strategy For Cyberspace: Prosperity, Security and Openness in a Networked World)[19], в якому зазначалося, що мета цього документа — уможливити, щоби глобальне кіберсередовище стало більш відкритим, інтероперабельним, безпечним і надійним. Оскільки цей документ має зовнішньополітичний характер, він поділений на три відповідні частини. Це — дипломатія, оборона, розвиток. У ньому також визначені 8 пріоритетів. До них належать:

- розвиток національної інформаційної інфраструктури;
- розвиток національної економіки;
- захист інформаційно-комунікаційних мереж;
- посилення військового компонента;
- модернізація законодавства в інформаційній сфері;
- розвиток міжнародного співробітництва;
- створення ефективної структури для керування Інтернетом;
- забезпечення фундаментальних принципів свободи в Інтернеті.

В документі йдеться також про завдання створити необхідні норми міжнародного права у сфері кібербезпеки. Окреслюється ідея стратегії кіберстримування стосовно до потенційних супротивників (це можуть бути держави, недержавні структури, терористичні угруповання тощо)[20].

Через два місяці, у липні 2011 р., міноборони випустило «Стратегію міністерства оборони для операцій у кіберпросторі» (Department of Defense Strategy for Operating in Cyberspace)[21]. Вона має 2 версії — відкриту і засекречену. Та, що відкрита для громадськості, — це документ на 13 сторінках, і саме його ми маємо змогу аналізувати. Довша — засекречена — версія вживається для закритого користування. Відкриту версію оприлюднив тодішній заступник міністра оборони Вільям Дж. Лінн[22]. У цьому важливому документі окреслені п’ять стратегічних ініціатив, що стосуються кібербезпеки:

1. Визнати кіберпростір сферою оперативної діяльності, яка потребує організації, підготовки та екіпірування у такий спосіб, аби міністерство оборони могло мати всі переваги потенціалу кіберпростору.

2. Застосовувати нові операційні комплекси оборони для захисту інформаційно-комунікаційних мереж і комп'ютерних систем міністерства оборони.

3. Міністерству оборони взаємодіяти з іншими урядовими міністерствами та агентствами і приватним сектором, аби виробити стратегію кібербезпеки усього уряду.

4. Досягти надійного співробітництва із союзниками та міжнародними партнерами США, щоби посилити колективну кібербезпеку.

5. Збільшити інтелектуальний потенціал держави через підготовку висококваліфікованих профільних спеціалістів із кібербезпеки та швидкі технологічні інновації.

Та перш, аніж перейти до аналізу п'яти стратегічних ініціатив, зупинимося на «Вступі» та двох розділах, що їм передують.

У «Вступі» кіберпростір називається «визначальною рисою сучасного життя». Підкреслюється, що «окремі люди та суспільства у всьому світі зв'язуються, спілкуються та організовують себе в кіберпросторі та через кіберпростір. З 2000-го до 2010 р. використання Інтернету глобально зросло з 360 млн користувачів до більше ніж 2 млрд користувачів»[23]. Оскільки використання мережі Інтернет продовжує зростати, кіберпростір стає все більше інтегрованим у щоденне життя людства на всій земній кулі.

Американський і міжнародні бізнеси продають товари та послуги у кіберпросторі, переміщують авуари по планеті за секунди. На додаток до того, що кіберпростір полегшує торгівлю в інших секторах, він сам по собі є ключовим сектором глобальної економіки. Кіберпростір став інкубатором нових форм підприємництва, нових прогресивних форм технологій, поширення свободи слова і нових соціальних мереж, які розвивають нашу економіку та відображають наші принципи. Безпека та ефективні операції американської критичної інфраструктури, включаючи енергетику, банкінг та фінанси, транспорт, комунікації та індустріальну базу сектору оборони, залежать від кіберпростору, систем, які контролюють індустрію, та інформаційних технологій, які можуть бути вражені або зруйновані чи використані. Ось чому визнається, що міністерство оборони, як і весь американський уряд, залежить від кіберпростору.

Міністерство оборони використовує кіберпростір, щоб «уможливити свої військові розвідувальні та бізнесові операції, включаючи рух персоналу, матеріальної частини, командування і контроль повним спектром»[24].

Розділ «Стратегічний контекст» складається з двох частин. У першій — «Сильні сторони та можливості міністерства оборони в кіберпросторі» — наголошується, що «військові можливості Сполучених Штатів щодо використання кіберпростору для швидкої комунікації та постачання інформації на підтримку операцій мають критичний характер для місій міністерства оборони. Радше можна стверджувати, що глибина знання міністерством оборони сектору глобальних інформаційних і комунікаційних технологій, включаючи експертизу кібербезпеки, надає міністерству стратегічні переваги у кіберпросторі»[25].

Якість людського капіталу та знань у США базується як на публічному, так і на приватному секторах, які надають міністерству оборони надійну основу, на якій побудовані сучасні та майбутні можливості.

Наприкінці першого розділу розвивається думка про те, що всі держави мають працювати разом для відвернення небезпеки у кіберпросторі; що має продовжуватися залучення країн для встановлення міжнародних норм у ньому, що також сприятиме посиленню кіберпростору для процвітання всіх.

У другому підрозділі під назвою «Кіберзагрози» увага звертається на те, що, коли розвивався Інтернет, його дизайнери не могли навіть уявити зростаючої та важливої ролі цієї системи в операціях міністерства оборони. Глобальна кількість мереж і систем міністерства оборони надає супротивникам широкі можливості для їх використання та атак на них.

Підкреслюється, що існуючі низькі бар'єри входу до мереж із метою шкідливої кіберактивності, включаючи хакерські знаряддя, означають, що окремий індивід або чимала група акторів можуть потенційно завдати чималих збитків як міністерству оборони, так і національній та економічній безпеці. Мається на увазі, що невеликі за обсягом технології можуть мати диспропорційно великі шкідливі наслідки. Роз'яснюється, що потенційні супротивники не мають створювати дуже затратні системи озброєнь, аби стати значною загрозою для національної безпеки Сполучених Штатів.

Між тим зазначається, що проти публічного та приватного секторів США такі операції збільшуються як за чисельністю, так і за складністю. Намагання порушити системи міністерства обо-

рони здійснюються мільйони разів кожного дня, й успішні проникнення призводять до втрати тисяч файлів із мереж Сполучених Штатів, а також із мереж їхніх колег і партнерів по індустрії. Такий потенціал малих протиправних груп, який можна назвати асиметричним впливом у кіберпросторі, створює реальні можливості для шкідливої діяльності у ньому[26].

Кіберзлодії нарощують свої потенціали у різних ділянках мереж. Їхні інтереси можуть бути зосереджені й на фінансових потоках, й на доступі до інтелектуальної власності, й на руйнуванні критичних систем міністерства оборони. Підкреслюється також, що деякі з кіберзагроз надходять від інсайдерів. Вони можуть працювати й на зарубіжні уряди, й на терористичні групи, й на кримінальні елементи, й за власною ініціативою. Наслідки від цієї діяльності можуть бути руйнівними.

Загрози національній кібербезпеці можуть випливати з того, що софтвер і хардвер можуть бути пошкоджені навіть до того, як вони інтегруються в операційні системи Сполучених Штатів. Адже їх виробляють або збирають за кордоном. Тут слід зазначити: міністерство оборони усвідомлює, що через широко розвинений економічний тренд аутсорсингу більшість продуктів інформаційних технологій, які використовуються у США, виробляється в інших країнах. Таке виробництво значно дешевше для американських компаній — оригінальних виробників цих продуктів. Тож залежність міністерства оборони від зарубіжного виробництва та розвитку породжує виклики та посилює ризики на етапах дизайну, виробництва, послуг, дистрибуції та використання інформаційно-комунікаційних продуктів та їхніх окремих компонентів.

Міністерство оборони висловлює занепокоєність щодо трьох потенційних загроз ворожої діяльності: «По-перше, крадіжка чи експлуатація даних, по-друге, відмова у доступі до послуг, яка впливає на можливості доступності до мереж інформації та пов'язаних з мережами ресурсів; по-третє, деструктивні дії, які включають корупцію, маніпуляції чи пряму діяльність, що загрожує виведенням з ладу чи руйнуванням мереж і пов'язаних з ними систем»[27].

Насамкінець ідеться про загрозу інтелектуальній власності від кібератак. Наголошується, що вона менш очевидна, ніж загроза критичній інфраструктурі, проте це може бути чи не найпоширенішою на сьогодні кіберзагрозою. Кожного року кількість інтелектуальної власності, за обсягом більша, ніж обсяг матеріалів, які зберігаються у бібліотеці Конгресу США, викрадається з мереж, які підтримуються американськими бізнесами, університетами,

урядовими департаментами та агенціями. Робиться закономірний висновок: «У зв'язку з тим, що американська міць абсолютно залежить від економічного розвитку, втрата інтелектуальної власності підриває як військову ефективність, так і національну конкурентоспроможність Сполучених Штатів у глобальній економіці».

«Перша стратегічна ініціатива». Міністерство оборони визнає кіберпростір сферою оперативної діяльності, яка потребує організації, підготовки та екіпірування у такий спосіб, щоби воно мало змогу використовувати всі переваги потенціалу кіберпростору. В ініціативі наголошується: «Хоча мережі й системи, які створюють кіберпростір, зроблені людиною, часто є приватними і, більше того, — використовуються цивільними громадянами, вважаємо кіберпростір критичною сферою для концепції національних безпекових місій міністерства. Це дає змогу міністерству оборони організовувати, тренувати та екіпірувати для кіберпростору все, що ми робимо у повітрі, на землі, морях та в космосі для підтримки інтересів національної безпеки. Більше того, ці зусилля мають включати в себе виконання основних місій в ушкодженому кіберпросторі»[28].

Дуже важливим є те, що ця стратегічна ініціатива — офіційна заява з приводу того, що кіберпростір буде розглядатися і як п'ята сфера операцій міністерства оборони на додаток до землі, повітря, морів і космічного простору. Не менш важливим є визнання міністерством оборони, що кіберпростір є взаємозалежним і взаємопов'язаним з іншими операційними сферами, де можуть відбуватися операції. Кібератаки можуть нашкодити в будь-якій операційній сфері. Тому міністерство оборони дуже зацікавлене у підготовці висококваліфікованих професійних кадрів у сфері кібербезпеки. Йдеться про підвищення кваліфікації у період підготовки, під час перепідготовки, використання спеціальних тренувальних ігор для покращення навичок у відверненні кібератак. Те, що цій сфері надається особлива увага, підтверджується створенням спеціальної структури під назвою «Кіберкомандування Сполучених Штатів». Вона підпорядкована «Стратегічному командуванню Сполучених Штатів» під керівництвом міністра оборони. «Кіберкомандування Сполучених Штатів» відповідальне за координацію всіх відповідних гілок військової структури США.

В американських дослідників «перша стратегічна ініціатива» викликає такі застереження: по-перше, щодо свободи дій міністерства оборони у кіберпросторі США, де багато мереж є приватними. Останні у такий спосіб підпадають під військові операції.

Така мілітаризація кіберпростору без відповідної юрисдикції викликає запитання. По-друге, як розрізнити кібератаки від інших ворожих дій у кіберпросторі, як-от кіберзлочинство. По-третє, чи можуть кібератаки викликати перехід до фізичних військових акцій[29].

У «другій стратегічній ініціативі» визначені чотири концепції. По-перше, йдеться про введення в обіг найкращих взірців *кібергігієни*. По-друге, відповіддю на внутрішні загрози має бути *посилення дієвості комунікацій, звітності та внутрішнього моніторингу*. По-третє, імплементується *активний кіберзахист* від зовнішніх загроз. По-четверте, стимулюється розвиток нових операційних концепцій та нової комп'ютерної архітектури, таких як *safe cloud computing* (*безпечні хмарні обчислення*). З одного боку, хмарні обчислення дають різним організаціям такі преференції, як низькі ціни на початковому етапі, оплату за схемою «заплатив стільки, скільки використав». Проте хмарні обчислення призводять до нових безпекових ризиків, пов'язаних із володінням даними, прайвесі, мобільністю даних і якістю обслуговування, та багатьох інших загроз.

Нам би хотілося звернути увагу на те, що особливо важливою не тільки для США, а й для України є концепція *безпечних* хмарних обчислень, в якій наголос робиться саме на їх безпечності. Про цей новий технологічний мегатренд, його плюси і мінуси ми писали ще 2011 р. у статті «Новий виток конкурентної боротьби в Інтернеті: Cloud Computing» і застерігали наші урядові міністерства і відомства від загроз, притаманних цьому тренду[30].

Відзначаючи роль партнерства з іншими американськими департаментами, агенціями та приватним сектором, «третя стратегічна ініціатива» підкреслює, що бажаним є широкий спектр кооперації з іншими урядовими департаментами та приватними компаніями. Такі відозви вже були оприлюднені у меморандумі 2010 року у зв'язку з угодою з міністерством внутрішніх справ про координування зусиль для захисту критичних інфраструктур і комп'ютерних мереж. Ця стратегічна ініціатива також заохочує публічне та приватне партнерство ще й тому, що наразі існує *глобальне* постачання необхідних деталей, механізмів й устаткування для усього технологічного ланцюга, що є проблематичним з боку його надійності для безпечного функціонування інформаційно-комунікаційних мереж США. Мета цього партнерства — ділитися ідеями, розвивати нові масові можливості та підтримувати колективні зусилля[31]. Звісно, спільна робота публічного і

приватного секторів не є можливою, оскільки інтереси в них різні. Проте вони можуть співпрацювати на основі, яка називається «базою індустріального захисту», для посилення захисту найуразливіших ділянок інформації. У відкритому варіанті документа нечітко прописані специфічні засоби кооперації між приватними та публічними секторами, але зрозуміло, що передусім ідеться про обмін інформацією щодо загроз і ризиків, які зачіпають інтереси кіберпростору США.

«Четверта стратегічна ініціатива» відкриває перспективи зміцнення колективної кібербезпеки разом із союзниками та міжнародними партнерами задля уникнення будь-яких кіберзагроз. Це включає підготовку кадрів, постійний діалог, що має на меті обмін кращим досвідом, новими напрацюваннями у цій галузі та встановлення міжнародних норм і принципів у кіберпросторі, що уможливлює більшу інтероперабельність, безпеку та надійність[32].

«П'ята стратегічна ініціатива» має на меті підтримку американського лідерства в цій галузі через інвестиції у свої кадри та в новітні технології, щоби створити і підтримувати найкращі можливості безпеки кіберпростору США. Перша частина присвячена покращенню роботи персоналу, який забезпечує функціонування інформаційно-комунікаційних мереж. Це стосується і нових практик прийняття на роботу персоналу, і програм обмінів. Заохочується перехід професіоналів із публічних у приватні сектори й навпаки. Йдеться також про програми обмінів між представниками цих професій різних генерацій, створення резерву кадрів, про постійно діючі навчальні програми. Друга частина цієї ініціативи стосується інвестицій у технологію. Маються на увазі скорочення строків уведення в обіг нових мереж, прискорення необхідних покращень у мережах, сприяння різних рівнів нагляду за ними. На цьому базується принцип пріоритетності для міністерства оборони критичних систем і покращення ним процедури придбання для них софтвера і хардверу, з використанням безпекового підходу.

Про те, що проблеми захисту кібербезпеки займають важливе місце в оборонній політиці США, свідчать доповіді у палаті представників та у Конгресі цієї країни щодо військового бюджету на 2015 фіскальний рік. Так, у палаті представників комітет з бюджету визнає важливість підтримки ґрунтовного дослідження програми кібербезпеки у міністерстві оборони, оскільки це пов'язано з міждисциплінарною природою кіберсистем і роллю людської поведінки взаємодії з ними. Міждисциплінарні дослідження моделі кі-

бербезпеки можуть внести свій вклад у розвиток найновіших підходів до оцінки ризиків, які інколи інкорпорують у себе ризики за межами комп'ютерної науки. Такі само, як і пов'язані з ризиками розуміння фундаментальних основ динаміки кіберзагроз, розвиток розпізнавальних можливостей нових кіберзагроз та посилення резистентності систем проти кібератак. Відповідно комітет спонукає міністра оборони підвищити рівень досліджень гарантій інформаційної безпеки та захисту кіберпростору, які провадяться в агенціях безпеки, включаючи Національне агентство безпеки, у зв'язку з тим, що міністерство планує і провадить міждисциплінарні дослідження з розпізнавання, ідентифікації та закриття поривів у кібербезпеці.

Відповідно до представлених палатою представників фінансових показників цифра ресурсів, виділених на дослідження, розвиток, тестування та оцінку результатів у військовій сфері, сягає 16 766 084 тис. дол. США. Для порівняння: в рядку, що стосується дослідження кібербезпеки, всього 15 000 тис. дол. США. Декілька рядків присвячено розвитку ініціативи кібербезпеки: рядок 115 — 961 тис. дол. США — і рядок 212 — 3234 тис. дол. США. Також існують ще два рядки, що стосуються програм інформаційної безпеки (11 304 тис. дол. США та 125 854 тис. дол. США), на кіберрозвідку виділено 6748 тис. дол. США. Проте, як було зазначено вище, дослідження кібербезпеки мають інтердисциплінарний характер, на дослідження та розвиток інформаційної і телекомунікаційної технологій виділено, зокрема, 334 407 тис. дол. США; на спеціальні операції, пов'язані з розвитком розвідувальних систем, — 9490 тис. дол. США; на розвиток глобальної космічної системи нагляду і відстеження — 31 346 тис. дол. США; на діяльність глобального відеонагляду — 3788 тис. дол. США. Якщо ж додати до цього, що на закриті програми з досліджень і розвитку військової проблематики виділено 3 118 502 тис. дол. США[33], стає зрозумілим, що певна частина цих асигнувань іде на міждисциплінарні дослідження кібербезпеки США.

У доповіді Сенату щодо бюджету міністерства оборони на фіскальний рік, що закінчився 30 вересня 2015 р., були вміщені, зокрема, важливі положення, які мають принципове значення для розвитку кібербезпеки Сполучених Штатів[34]. По-перше, там ідеться про федеральні дослідницькі організації, підкреслюється, що комітет залишається занепокоєним щодо повної ясності в різноманітних ролях, які відіграють урядові установи, та в їх відповідальності в сенсі національної кібербезпеки США. Міністер-

ство оборони, міністерство внутрішньої безпеки та міністерство юстиції — кожне з них має визначені ролі в забезпеченні кібербезпеки держави та місцевих урядів, академії, індустрії та інших. Комітет прагне, щоби було знайдене краще порозуміння між ними та визначені ролі, які можуть або повинні відігравати центри дослідження і розвитку, які діють на федеральному рівні, національні лабораторії та університетські афілійовані дослідницькі центри, військові дослідження, дослідницькі лабораторії та подібні організації, кожна з яких повинна провадити грунтовну експертизу кібербезпеки та чиї дії у цьому відношенні мають бути дуже чітко скоординовані, щоб ефективно впроваджувати спрямовані на цю важливу тему ресурси.

З-поміж усього іншого комітет визнає вклад міністерства оборони у роботу з Радою губернаторів щодо створення спільного плану дій і розвитку державно-федеральної єдності зусиль із кібербезпеки та підтримує міністерство у продовженні цієї спільної діяльності. Особливо наголошено на розумінні комітетом дій американського Кіберкомандування та міністерства оборони, які досягли чималого прогресу в посиленні військових планів, що інкорпоруються у тренування та у військову доктрину США. У доповіді згадується документ 2011 року міністерства оборони США щодо стратегій оперування у кіберпросторі, в якому зазначено, що безперервні освіта та підготовка спеціалістів у цій сфері мають бути головними та визначальними завданнями для працюючих у сфері кіберзахисту. Тому комітет наказав міністру оборони представити через 180 днів до комітетів оборони Конгресу доповідь про впровадження цього плану як для офіцерів, так і для всього численного персоналу. Ця доповідь мала включати дефініції військових спеціальностей або рейтинг спеціальностей для кожної посади з відповідним рівнем тренування, освіти, присвоєння кваліфікацій та отримання сертифікатів, які слугували би певними маркерами безперервної освіти в цій новій галузі щодо професіонального розвитку від першого початкового рівня навчання до вищих військових шкіл і коледжів.

Особливу увагу в доповіді приділено дослідженню і розвитку кіберпростору в університетах. Констатується, що Агентство національної безпеки у координації з міністерством внутрішньої безпеки нещодавно спонсорувало в ряді університетів національні центри наукових досягнень в інформаційній освіті та в інформаційних дослідженнях.

Згідно із Програмою безпеки інформаційних систем (Information Systems Security Program — ISSP) Агентство національної безпеки провадить закрите кібердослідження, пов'язане через програми партнерства з певними університетами. Комітет розуміє, що ці зв'язки з університетами зарекомендували себе як продуктивні. Відповідно комітет рекомендував асигнувати додаткові 7,500 тис. дол. США для підтримки цих зв'язків із наукою[35].

Отже, можна дійти висновків щодо еволюції стратегій кібербезпеки США. Протягом XXI ст. вони поставлені на державний рівень, розвиваються не тільки відповідними міністерствами та відомствами (виконавчою владою), а й палатою представників і Конгресом США (тобто законодавчою владою) та перебувають у полі їхньої постійної зростаючої уваги. Це пояснюється розумінням правлячою елітою США як важливості експонентного зростання національного кіберпростору для процвітання держави, так і зростаючих загроз кібербезпеці США. Ось чому в цій галузі чітко простежуються такі стратегічні імперативи, як нарощування наукового та людського потенціалу, які були би здатними на миттєві адекватні відповіді ворожим кібератакам, безперервність навчання та підвищення кваліфікації, тісне співробітництво (наскільки можливо) публічного та приватного секторів, вищих навчальних закладів, наукових центрів, лабораторій, персоналу різного вікового складу, тісніше взаєморозуміння та розподілення функцій між відповідними урядовими міністерствами та відомствами, підтримання дієвої співпраці із союзниками та партнерами.

Досвід США щодо розробки та втілення в життя стратегій національної кібербезпеки є надзвичайно корисним для України. Зрозуміло, що ні військовий, ні фінансовий потенціали України не можуть бути порівняні із відповідними потенціалами США. Те саме можна зазначити й відносно ефективності діяльності виконавчої та законодавчої гілок української влади.

Захист кіберпростору України при всьому тому, що потенціали США та нашої країни далеко не рівні, все ж таки має перспективи. Цей потенціал — людський капітал, неоціненні інтелектуальні здібності нашого народу, починаючи від школярів, які швидко і досить глибоко опановують комп'ютер та «ширяють» у кіберпросторі, й до студентства, викладачів, професорів і спеціалістів у цій галузі в різних академічних та галузевих інститутах України. Якщо владі вдасться припинити відтік мізків з України, створити тут відповідні умови для фахівців цих галузей, українська

відповідь кіберзагрозам як глобальним, так і регіональним буде здатна доволі швидко стати однією із пріоритетних сфер розвитку України.