Дайджест

Анахіт Паж’ян (Anahit Parzyan)

отримала PhD з міжнародних відносин в університеті Nanjing, Школа міжнародних відносин (Китайська Народна Республіка).

Анахіт спеціалізується на питаннях міжнародної безпеки, зокрема в сфері кібербезпеки, діджиталізації, електронного врядування. У 2017 році вона була обрана членом програми молодих експертів ЄС " YES Armenia". Як експерт з розробки та функціонування цифрової стратегії Фонду "Digital Armenia" та Уряду Республіки Вірменія, Анахіт працювала над розробкою Національної стратегії кібербезпеки. Основний фокус діяльності полягав на механізмах та законодавчій сфері щодо захисту критичної

Кібербезпека, технології та демократія

Як знайти баланс між демократією та технологіями?

Я думаю, що технології є основним інструментом для впровадження демократії. Коли ми використовуємо такі механізми як електронне врядування, то демонструємо, що можемо бути дуже прозорими. А прозорість – це пряме впровадження демократії. Механізм електронного врядування також може допомогти впроваджувати демократію більш ефективною, оскільки в цьому випадку всі процеси можуть здійснюватися без підходу «людина – людина», натомість використовувати підхід «система - людина».

Державні послуги можуть також надаватися без корупційної складової чи втручання інших осіб. Саме тому, я вважаю, що демократію можна реалізовувати безпосередньо за допомогою технологій. Існує багато держав, які проводять публічні консультації стосовно того, чи приймати певний законопроект. Це може бути форум та голосування за проект закону, таким чином технології можуть вирішувати питання прямого голосування, що допоможе проводити референдум за допомогою технологій чи без них. Це означає, що багато законопроектів ще до етапу їх прийняття зможуть стати питанням до обговорення і значна частина населення матимуть змогу висловити свої ідеї за допомогою технологій. Такий спосіб є економічно вигідним, швидким та прозорим. Це бажання нації, виражене за допомогою технологій.

Інший аспект полягає в тому, що через те, що люди дуже сильно покладаються на технології та електронне врядування, це означає, що наше життя і система управління державою безпосередньо залежать від технологій. Саме тому, підхід, з яким ми захищаємо свою територію, свій морський та повітряний простір від різних видів загроз, повинен використовуватись і для захисту кіберпростору. Тобто, на офіційному рівні кіберпростір теж повинен стати ще однією сферою захисту держави.

CHARLES STEWART MOTT FOUNDATION
Лабораторія Електронної Демократії
Подільська Агенція Регіонального Розвитку

інфраструктури, розробці національної кампанії з підвищення рівня обізнаності у сфері кібербезпеки, а також інших стратегічних ініціативах, пов'язаних з цифровою трансформацією Вірменії.

Анахіт стала членом спеціальної робочої групи експертів з розробки національної стратегії кібербезпеки та підтримувала Національну кампанію з підвищення обізнаності з питань кібербезпеки для шкіл. У 2016 році вона приєдналася до Ради з політичних та стратегічних досліджень «Китай-Євразія» як керівник групи з кібербезпеки.

Доктор Паж'ян - випускниця Варшавської Євроатлантичної літньої академії (WEASA). Вона періодично представляє свої дослідження з питань кібербезпеки та цифровізації у Вірменії, Китаї, Європі та є в журі різних національних та регіональних ініціатив. Вона є авторкою кількох наукових публікацій, за одну з яких була нагороджена Почесною грамотою від університету Nanjing (Китайська Народна Республіка).

З цієї причини важливо мати чітке законодавчу базу у сфері кібербезпеки та його імплементація. Відповідно, країни можуть покладатися лише на цей механізм захисту, щоб мати можливість захищати всі дані, які потім можуть збиратись за допомогою механізмів державної служби, а також сформувати такі механізми.

Що ж таке кібербезпека та чому вона важлива?

Кібербезпека вже давно стала питанням міжнародних відносин. Просто невеликі та середні держави не так сильно зосереджені над цим питанням. Проте, великі держави вже докладають величезних зусиль для розширення лідерства в кіберпросторі та механізмів захисту кібербезпеки для своїх держав. У 2011 році Сполучені Штати Америки заявили, що готові розглядати кіберпростір як іншу сферу війни, а також використовувати непрямий, несиметричний спосіб оборони або механізм захисту. Це означає, що якщо відбудеться напад на кіберпростір Сполучених Штатів Америки, держава може застосувати санкції чи використовувати інші форми оборонних механізмів. Це приводить нас до асиметричних воєнних дій і означає, що держави повинні захищати себе, розвиваючи і цей напрямок.

Для демократичних держав це є невід'ємною складовою, тому що вся державна інфраструктура залежить від операцій в кіберпросторі. Так зазвичай люди розрізняють кіберпростір, кібербезпеку в розумінні лише технологій. Мається на увазі IT-сфера, коли вони включаються, або вимикаються, або механізм вимикається, або механізм не вимикається. Власне, кібербезпека - більш масштабне явище. Наприклад, уся критична інфраструктура держави здебільшого залежить від технологій.

А що таке критична інфраструктура?

Критична інфраструктура - це ті важливі інституції чи шляхи, від яких залежить держава для захисту своєї життєдіяльності. Наприклад, електромережі, водопостачання, телекомунікаційна інфраструктура, транспортна інфраструктура, лікарні та ін.

До прикладу 100 років тому, завоювати державу означало завоювати її критичну інфраструктуру. Те саме зараз і зараз, відрізняються лише засоби. Завоювати державу без критичної інфраструктури - це означає провести атаку. Переважно це кібератака на критичну інфраструктуру, оскільки в основному критична інфраструктура контролюється та управляється технологіями.

До прикладу тотальне вимкнення (blackout), яке зупиняє всю діяльність.

Саме так. У вас довгий час не буде електрики. Але в той же час складність кібератаки полягає в наступному. Коли ви стикаєтесь із фізичним знищенням, ви можете його виявити та знаєте, як його виправити. У разі кібератаки ви стикаєтесь із атакою з нульового дня (zero day). Вразливість нульового дня означає, що немає розуміння звідки атака береться, де трапиться і чи атака відбулась. Отже, нульовий день - це приховане обличчя кібератаки. Тоді, коли кібератака вже відбувається, важливо зрозуміти як її виявити. З цієї причини вам потрібні і технології, і спеціаліст, який може зрозуміти це і виявити. А виявивши її, вам доведеться призупинити роботу критичної інфраструктури. А, отже, вам знову потрібні спеціаліст, техніка та час. Потім вам потрібен час, щоб відновити інфраструктуру, а процедури відновлення також є різні. Багато країн, особливо

Потужних, реалізують національні стратегії кібербезпеки, а також створюють спеціальні центри, які будуть першими центрами, до яких будуть звертатись у випадку якщо подібні операції траплятимуться.

Тому що не кожна організація точно знає, як це відбувається, чому це відбувається і хто є нападником. Тож у такому випадку буде простіше зателефонувати до цього центру і сказати: «У нас виникла така проблема і ми розглядаємо її як кібератаку». Такі центри, здебільшого, називаються Отже, це, здебільшого, називаються центри із надзвичайних ситуації кібербезпеки, і вони функціонують у багатьох країнах.

До прикладу, у Великобританії, в США, в Німеччині, в Китаї, Естонії, Грузії, а також в Україні. Питання полягає в тому, наскільки ефективно вони функціонують і як швидко реагують, і який їхній операційний механізм. Чи вони насправді є ефективними чи ні. Насправді, враховуючи кібератаки, які можуть трапитися в країні, і дисфункціонуючі кібератаки, це може бути важко.

Важливо розрізняти ці речі. Коли ви стикаєтесь із кібератаками з інших куточків світу, це національне питання. Якщо кібератака відбувається всередині, це теж національне питання, але спосіб вирішення цих питань зовсім інший. Отже, якщо кібератака відбувається із зовнішніх джерел, то яка кінцева мета цього нападу?

Зазвичай в рамках свого дослідження я розрізняю три різні типи атак, які можуть статися з-за кордону, з-за меж країни.

Перший рівень - це основи кібербезпеки, тобто, хакери (особа чи група осіб). У цьому випадку вони хочуть заробити гроші чи вчинити якийсь деструктив. По суті, ви повинні їх виявити, заблокувати їх, і це все.

Другий рівень - це наймані групи. Їх може наймати приватний сектор чи інші країни. Ніколи не знаєш, ким вони були найняті, але проводиться розслідування, судово-медична експертиза, і, можливо, тоді можна буде здогадатись, хто за цим стоїть.

Найвищий (третій) рівень – атаки, які фінансуються державами. Це можуть бути спеціально навчені групи і багато країн зазначають, що вони мають такі типи груп і хакерські угруповання, які можуть напасти на ту чи іншу державу, особливо на політичну інфраструктуру, банківську систему, фінансову систему, гроші. Але в кіберпросторі дуже важко зрозуміти, як впоратися з цими ситуаціями. Для провідних великих держав це насправді складно. Вони завойовують владу та лідерство в кіберпросторі. Але в той же час у них є гроші, щоб вкласти кошти у свої механізми захисту, і якимось чином вони можуть передбачити напади на свою сторону. З іншого боку, у нас є маленькі держави та країни, що розвиваються, але вони не можуть дозволити собі такий дорогий арсенал у кіберпросторі. Але в той же час вони переживають кібератаки. Отже, що робити?

Це питання, яке зараз існує у кіберпросторі. Деякі країни, в основному американці та їхні союзники вважають, що кіберпростір повинен керуватися незалежним способом управління, як організації, державний сектор, приватний сектор, чи усі разом і немає необхідності створювати конкретні відомі законодавства. Китай та Росія підтримують суверенні механізми управління кіберпростором, вважаючи, що повинні бути розроблені та прийняті міжнародні чи інші норми. Але в той же час повинно бути зазначено, що є суверенним, але я маю на увазі невтручання в суверенність іншої країни. Проводилось багато дискусій та було зроблено багато пропозицій.

В 2015 році Росія, Китай, США вперше узгодили взаємні норми поведінки за принципом консенсусу, яких насправді дотримуються й досі. Я вважаю, що Рада Безпеки Організації Об'єднаних Націй повинна розглядати кіберпростір як іншу сферу воєнних дій і захищати всіх, хто не здатний захистити себе, і, можливо,

думаю, що Рада Безпеки Організації Об'єднаних Націй повинна розглядати кіберпростір як іншу сферу воєнних дій і захищати всіх, хто не здатний захистити себе, і, можливо, створити мирну організацію, яка буде підтримувати їх у разі надзвичайних ситуацій. Зараз це питання залишається на розгляді.

Коли говоримо про кібербезпеку, потрібно розуміти, що всі держави так само розуміють норми та поняття кіберпростору. Деякі держави розуміють кібербезпеку як аспект інформаційної безпеки.

Коли вони розуміють, що контент (зміст) має бути захищеним та захищеним. Хоча інші держави розуміють, що механізм комунікації може включати як зміст, так і технології та загрози. І третя група держав вважає, що кібербезпека це лише технологічна частина.

Саме тому існує потреба в Раді Безпеки Організації Об'єднаних Націй та міжнародно прийнятих механізмам захисту, оскільки нам дійсно потрібно дійти до консенсусу шляхом визначення того, що таке кібербезпека та як її забезпечити.

Які ж приклади основних атак на кібербезпеку?

У 2007 році відбувся напад на кібербезпеку Естонії, після чого вона стала однією з провідних країн, які інвестують у цю сферу.

Після цього Естонія стала однією з провідних країн, які інвестують у кібербезпеку. Вона повинна була це зробити через безперервні кібератаки, DDoS-атаки на інфраструктуру. Насправді було вирішено вимкнути всю електроенергію та Інтернет через те, що не було іншого вибору. Після чого країна почала розвивати цю сферу.

Україна також зазнала кібератаки на електромережі в 2008 році. Після цього Україна почала працювати над розвитком цієї сфери. Україна, Естонія, Грузія сприйняли це як питання національної безпеки. Те ж стосується Ірану. Одна із найбільш відомих та можливо найбільш скандальних типів кібератак, який трапився в ядерному центрі в Ірані, а сама операція, на думку Ірану, могла бути пов'язана з Ізраїлем та США. Загалом це уповільнило систему збагачення урану і вірус працював роками.

Ось чому вони відкликали Олімпійські ігри, з'явилася купа вірусів, які могли б бути прямою атакою на критичну інфраструктуру і проблема полягала в тому, що впродовж тривалого часу це була нульова сума. Тобто ніхто не міг зрозуміти, що це таке. Зараз найбільшою проблемою є те, що існує стереотип стосовно того, що кібератаки трапляються лише тоді, коли є підключення до мережі інтернет. Вірус може потрапити через магнітну систему комп'ютера, при цьому не будучи навіть підключеним до мережі Інтернет. Такі атаки існують, були також атаки на банківські системи США зі сторони Ірану. Були так звані кібератаки Кореї на Sony Productions США, тому що ця компанія глузувала з лідера Північної Кореї. Безперечно, прикладом є вплив Російської Федерації на американські вибори. Основна проблема усіх кібератак полягає в тому, що завжди потрібна серйозна судова експертиза і не завжди можливо зрозуміти, хто стояв за кібератакою.

Що можна порекомендувати країнам, в яких відбуваються конфлікти чи воєнні дії?

Ну, найголовніше - це кампанія з підвищення обізнаності громадян. Ми користуємось новими інструментами, але справа в тому, що в школі ми навчаємо дітей переходити вулицю, те ж саме кажуть

колір означає, що можна йти, жовтий – очікувати, а червоний означає стояти нерухомо. Такі ж правила повинні бути і в кампаніях з підвищення рівня обізнаності в кіберпросторі. Але справа в тому, що ні батьки, ні бабусі, ні дідусі, ні вчителі не знають, що потрібно розповідати з цього питання. Саме тому важливо, щоб відбувались масові національні кампанії з підвищення рівня обізнаності з кібербезпеки, які повинні починатись зі школи. Окрім навиків письма та читання, повинні також надаватись навики як захистити себе в кіберпросторі. Так, до прикладу ті люди, які мають «розумний дім», повинні також розуміти, як убезпечити його.Це, звичайно, підвищення рівня обізнаності щодо кібербезпеки прискорить важливість і, знаєте, інтерес до цих продуктів, і люди будуть знати, що якщо у них буде розумний дім, вони також повинні бути дуже безпечними. Люди повинні думати про те, які емейли вони читають, що вони отримують і яку інформацію надають, чи на які медіа підписуються.

Припустимо, колись за допомогою кондиціонерів чи навіть тостерів може буде зламати чийсь будинок. Тобто, зчинити двері та без додаткових інструкцій не

відчиняти систему. Це якщо ми говоримо про особистісний рівень. Те ж саме може трапитись на системному рівні. Може трапитись ситуація, коли держслужбовці використають персональні флеш-накопичувачі на роботі і це призведе до краху всієї системи. І найголовніше, що це все відбудеться ненавмисно.

Багато представників влади надсилають важливі документи через месенджери соціальних мереж просто тому, що так простіше. Але такі дії можуть призвести до збою роботи всієї владної структури.Тому, кампанії з підвищення обізнаності громадян – це надзвичайно важливий елемент. Окрім цього, повинна існувати стратегія кібербезпеки. На національному рівні повинні функціонувати спеціальні центри, до яких громадяни могли б звернутись у випадку небезпеки. І останнє, але не менш важливе: питання кібербезпеки - це питання міжнародної співпраці.

Можна порівняти кібервіруси та кібервійни з вірусом Еболи. Якщо він існує в одній частині світу, то потрібно спільно боротись з тим, щоб він не прийшов в іншу частину світу. Те саме стосується й кібербезпеки. Я думаю, що нам потрібно періодично проводити кіберщеплення, щоб очистити всі механізми від вірусу у всьому світі.

А яким чином працює модель е-урядування в Китаї?

В Китаї органи державної служби дуже модернізовані. У більшості розвинених частинах Китаю у сфері охорони здоров'я можна побачити яким чином насправді працює E-Health. Ви користується єдиною карткою, яка прив'язана до вашого посвідчення особи. Китай модернізує свої технології, розвиває «розумні» міста. Звісно і в інших частинах світу є розумні міста,можливо, навіть із більшою кількістю додатків для управління. Проте, говорячи про Китай, міста у ньому більш розумні. Чому? Тому що населення прагне використовувати ці технології, тоді як у багатьох частинах світу люди консервативні і не так швидко звикають до їх використання.

Я багато разів помічала як старші жінки в Китаї користуються додатками для кешбеку (повернення коштів після покупок). Це їхній спосіб життя і він їм подобається. Китай розвиває свій електронний ринок. Електронна комерція, Fintech, Regtech є загальновживаними поняттями, які широко використовуються. І вони виходять за межі Китаю відповідно до ініціативи цифрової шовкової дороги.

Зрештою, де б ви не жили, зараз справді надзвичайно важливо бути підключеним до Інтернету. І щодня ми все більше використовуємо технології, тому ми повинні дбати про механізми безпеки та захисту даних.

Я б хотіла, щоб у моїй країні функціонував центр відкритих даних. В той же час це має бути захищений центр обробки даних, але на національному рівні, щоб жодна міжнародна компанія не могла втрутитись. Ми всі переважно використовуємо Facebook, проте всі дані, які збираються у цій мережі, зберігаються в США. І це досить складне питання.

І наостанок, сферу кібербезпеки ще потрібно досліджувати, створювати та впроваджувати проекти задля підвищення обізнаності у сфері кібербезпеки, щоб мати можливість себе захистити.

З інтерв'ю з Анахіт Паж'ян