Секція: Державне управління, самоврядування і державна служба

Дзюндзюк Вячеслав Борисович
доктор наук з державного управління, професор
Харківський регіональний інститут державного управління
НАДУ при Президентові України
м. Харків, Україна

Котух Євген Володимирович
кандидат технічних наук, доцент
Університет митної справи та фінансів
м. Дніпро, Україна

ПРОБЛЕМИ УРЯДУВАННЯ У СФЕРІ КІБЕРБЕЗПЕКИ

Політика у сфері кібербезпеки може ґрунтуватися на односторонніх чи багатосторонніх заходах. Проте до тих пір поки код кіберпростору, тобто інструкції, вбудовані в його апаратне та програмне забезпечення [3], в основному ігнорує фізичні кордони, односторонні зусилля, як правило, є дорогими або неефективними. Держави завжди можуть напевно відключити себе від Інтернету. Але тоді їм доводиться нести витрати, пов'язані з економічною (і культурною) ізоляцією. Під час тижневого відключення інтернету в Єгипті у 2010 році, яке уряд навмисно здійснив, єгипетська телекомунікаційна індустрія втратила дохід, оцінюваний в 90-110 мільйонів доларів США [7]. Зведення віртуальних огорож, тобто ізоляція себе на синтаксичному, а не на фізичному рівні кіберпростору також ускладнює міжнародні обміни. Якщо запозичити метафоричний опис ситуації у М. Лібіцкі, то той, хто хоче бути на агорі, не може залишатися в замку весь час [4, с. 62-72].

Як неодноразово наголошувалось вище, співпраця конче необхідна

для забезпечення кібербезпеки, оскільки навіть найбільш дієздатна держава не може сподіватися самостійно передбачити та відобразити всі кібератаки. Співпраця може здійснюватися на разовій або системній основі. Останнє, на наш погляд, найкраще здатне забезпечити врядування. К. Оффе пропонує відрізняти врядування від управління ієрархічними та ринковими структурами [6]. Цей термін також застосовується до діяльності так званих багатосторонніх структур, які забезпечують механізми співпраці різних публічних і приватних акторів [5]. Відповідно до такого розумінням врядування у сфері кібербезпеки включає в себе добровільні спільні зусилля публічних і приватних акторів із забезпечення доступності, автентичності, цілісності та конфіденційності цифрових даних, що зберігаються в кіберпросторі або переданих через нього.

Існують деякі характеристики врядування у сфері кібербезпеки, які можуть як посилювати зазначене вище співробітництво, так і загрожувати йому. Серед цих характеристик найбільш важливими є наступні:

1. Практично всі можливості для атаки або захисту в кіберпросторі залежать від знання про уразливість [3, с. 54]. Як правило, ці уразливості складаються з невідомих властивостей комп'ютерного коду. Але з тим же успіхом вони можуть стосуватися і людей або організацій, схильних до атак соціальної інженерії. В обох випадках саме знання, а не матеріальні можливості, дають здатність протистояти загрозам у кіберпросторі. Однак поширення та використання знань набагато важче виявити і, отже, регулювати, ніж поширення або використання матеріальних можливостей.

2. Оскільки знання є основним ресурсом у сфері кібербезпеки, в цій сфері спостерігається тенденція до зменшення асиметрії влади. Існує безліч суб'єктів, здатних здобувати знання і, відповідно, наносити серйозної шкоди в кіберпросторі. Крім того, географічне положення цих суб'єктів не має значення для більшості операцій. З цих двох причин співпраця з цими суб'єктами або проти них повинна бути всеосяжною. Отже, досягнення

домовленостей утруднено. Це також більш ризиковано, враховуючи той факт, що обмін інформацією може здійснюватися нескінченно. В цьому відношенні управління кібербезпекою структурно дуже схоже на співпрацю в галузі розвідки [2].

3. Наявні та діючі кодекси в кіберпросторі явно не сприяють відповідальності за інциденти. Таким чином, заохочується порушення правил і, відповідно, не заохочується їх дотримання. Можлива також і неправильна атрибуція, за якої треті сторони будуть проводити операції «під фальшивим прапором» і, таким чином, спричиняти взаємні звинувачення «всіх проти всіх». Отже, quid pro quo як основний принцип встановлення та стабілізації співробітництва [1] не працює добре в кіберпросторі.

4. Феномени, що відрізняються в фізичному світі, такі як злочинність, війна та інтелект, як правило, досить схожі в кіберпросторі. Отже, існує більший ризик неправильної класифікації поведінки й серйозного неправильного сприйняття намірів. Крім того, важко точно визначити межі співпраці та забезпечити, щоб актори не використали свої законні права в одній сфері в якості прикриття для негативних дій в інших сферах.

Зрозуміло, що ці характеристики не впливають однозначно негативно на співробітництво різних акторів у сфері кібербезпеки, але ускладнюють його, спричиняючи певні проблеми, які можна вирішити лише через запровадження ефективного врядування у даній сфері.

Але тут слід мати на увазі, що врядування у сфері кібербезпеки – це нова і методологічно складна сфера досліджень. З огляду на мізерність емпіричних даних, предметна сфера в кращому випадку дозволяє проводити тільки розумові експерименти і рудіментальну перевірку правдоподібності. Отже, всі види висновків можуть бути тільки попередніми і до них слід ставитися з граничною обережністю. З огляду на ці застереження, можна

стверджувати, що кібербезпека за своїми основними характеристиками меншою мірою сприяє міжнародному співробітництву, ніж інші проблемні сфери, і це може призвести до загострення різного роду проблем співробітництва. Але більш проблематичним є те, що багато держав зі слабким кіберзахистом просто серйозно не дбають про вирішення цієї проблеми і тим самим створюють суспільну шкоду. На щастя, існує група держав та міжнародних організацій, готових і здатних надати допомогу в забезпеченні кібербезпеки. Чого досі не вистачає, так це надійних санкцій проти тих, хто нехтує питаннями забезпечення кібербезпеки.

Ініціативи щодо зміцнення довіри в кіберпросторі вимагають наявності надійних режимів моніторингу, якими проте можна легко зловживати з метою шпигунства, тому політика колективного стримування кіберзагроз потребує інституційних гарантій від такого ризику. Нарешті, існує проблема орієнтації на відносні вигоди: держава страждає від різних рівнів уразливості, можливостей і публічно-приватних відносин. Через це глобальне регулювання будь-якого окремого аспекту кібербезпеки супроводжується асиметричним розподілом відносних вигод. І знов-таки подолати цю проблему можна лише через вибудовування довірчих відносин співпраці між різними, як глобальними, так і національними, акторами.

Література

1. Axelrod R. Die Evolution der Kooperation. München: Oldenbourg, 2009.
2. Daun A. Auge um Auge: Intelligence-Kooperation in den deutsch-amerikanischen Beziehungen. Wiesbaden: VS Verlag für Sozialwissenschaften, 2011.
3. Gaycken S. Cyberwar: Das Internet als Kriegsschauplatz. München: Open Source Press, 2011.
4. Libicki M.C. Conquest in Cyberspace: National Security and Information Warfare, Cambridge: Cambridge University Press, 2007.

5. Mathiason J. Internet Governance: The new Frontier of Global Institutions. London/New York: Routledge, 2009.
6. Offe C. Governance – 'Empty Signifier' oder sozialwissenschaftliches Forschungsprogramm / Schuppert G. F., Zürn M. (Eds.). Governance in einer sich wandelnden Welt. Wiesbaden: VS Verlag, 2008. PP. 61-76.
7. Olson P. Egypt's Internet Blackout Cost More than OECD Estimates // Forbes, 03.02.2011. URL: http://blogs.forbes.com/parmyolson/2011/02/03/how-much-didfive-days-of-no-internet-cost-egypt/