УДК 351.862.224.6

ВЛАДА І ГРОМАДЯНСЬКЕ СУСПІЛЬСТВО В КІБЕР-ПРОСТОРІ

ТЕТЯНА МАЛЯРЕНКО,
доктор наук з державного управління, професор кафедри загального та адміністративного менеджменту Донецького державного університету управління

У статті систематизуються шляхи, за допомогою яких Інтернет змінює політичний дискурс і формат відносин між владою і громадянським суспільством. Особливим дослідницьким фокусом є визначення механізмів, через які громадянське суспільство, що діє в кібер-просторі, впливає на формування державної політики.

Ключові слова: *влада, громадянське суспільство, держава, Інтернет, кібер-простір, конфлікт, соціальні мережі.*

Постановка проблеми. Інформаційна революція внесла корективи у формат відносин між владою й громадянським суспільством. Три аспекти впливу інформаційної революції на взаємодію між владою і громадянським суспільством заслуговують на особливу увагу. По-перше, інформаційна революція сприяє розвитку мережевих форм організації. Зараз мережеві форми є більш ефективними, аніж ієрархічні. Порівняно з бюрократіями, мережеві структури є спроможними ефективно й швидко об'єднувати індивідуумів у мультикультурні, мультирівневі й мультиорганізаційні групи. Зростання мережевих форм організації призводить до трансферу влади до недержавних акторів. У конфлікті з ієрархічно організованими владними інститутами соціально-активні громадяни, об'єднані в мережі, отримують вагомі переваги. По-друге, з поширенням інформаційних технологій перемога в конфлікті все більше залежить від комунікацій. Учасники конфлікту потребують доступу до нових знань й освіти; вони вчаться використовувати "м'яку" владу, що, безумовно, сприяє гуманізації та інтелектуалізації конфлікту. Супротивники спираються на інформаційні технології, вони розробляють ефективні стратегії комунікаційних (зокрема, пропагандистських) кампаній, призначених організовувати або дезорганізовувати окремі соціальні групи або суспільство в цілому. По-третє, соціальні конфлікти, що точаться у віртуальному просторі, можуть матеріалізуватись - перенестись до реального життя й трансформуватись у насильницькі форми. До подій "арабської весни" уряди вважали, що віртуальний простір є місцем, де соціально-активні індивідууми можуть обмінюватись думками, обговорювати політичні події, але конфлікт у кібер-просторі неможливо трансформувати в реальний збройний масовий конфлікт. Недооцінка важливості Інтернет-комунікацій та переваг мережевих організацій над державними бюрократіями призвела до знищення систем національної безпеки й повалення авторитарних (навіть ззовні стабільних) політичних режимів, які забороняли громадянську активність, але виявились не в змозі протистояти їй.

Аналіз останніх досліджень і публікацій. Протягом останніх десятиліть кібер-загрози національній безпеці (особливо, у формі кібер-тероризму) займають чинне місце в спектрі актуальних загроз і ризиків, але сек'юритизація кібер-атак значною мірою пов'язана швидше з очікуванням нових загроз, аніж із руйнуванням, що вже мали місце.

Уперше важливість розробки ефективних механізмів протидії загрозам, що надходять із віртуальних мереж, була обґрунтована американськими аналітичними центрами, що спеціалізуються в галузі безпеки, у 1980-ті рр. Це було викликано розумінням асиметричності майбутніх війн, зростанням потенціалу й бажання недержавних акторів (індивідуумів, громадянського суспільства, політичних партій, корпорацій) завдавати шкоди Сполученим Штатам за допомогою інформаційних кампаній, руйнівних вірусів та шкідливих програм.

Американська дослідниця Дороті Денінг виокремлює такі типи політично-мотивованої діяльності у віртуальному просторі: Інтернет-активність, хакерство і кібер-тероризм. Інтернет-активність - це нормальне, неруйнівне використання Інтернету для висловлювання власної позиції, підтримки політичних партій або політиків. Хакерство - це комбінація політичної активності з навичками програмування. Хакери атакують і руйнують обрану ціль. Кібер-тероризм - це сукупність цілеспрямованих незаконних атак проти комп'ютерів або комп'ютерних мереж ворожої країни з метою досягнення політичних або соціальних цілей. Кібер-тероризм призводить до руйнування власності або іміджу [1]. Брюс Шнейдер визначає також інші різновиди людської поведінки в Інтернеті, які можуть завдавати шкоди національній безпеці, - кібер-вандалізм (руйнування або паплюження вебсайтів) та кібер-злочин (крадіжка інтелектуальної власності) [2].

Для розробки стратегії протидії кібер-тероризму фахівці Національної академії оборони Сполучених Штатів пропонують розрізняти "неструктуровані" та "структуровані" загрози безпеці держави, що надходять з Інтернету. Неструктуровані загрози надходять від поодиноких слабко організованих супротивників, які мають обмежені фінансові можливості та короткострокові цілі. Структуровані загрози мають системний характер і надходять від добре організованих супротивників, які мають можливості фінансування своїх дій [2].

Інструменти й тактики, які використовують армії, терористи, злочинці, соціальні активісти в кібер-просторі, є однаковими, але цілі цих груп відрізняються. У той час, коли чи не кожний постріл є актом війни, успішні Інтернет-атаки, незалежно від руйнувань, до яких вони призвели, не обов'язково є кібервійною. Кібер-атака, що руйнує сервер урядової установи, може бути часткою кібер-війни, а може бути кібер-злочином або навіть хуліганськими діями підлітків, які не розуміють, що вони роблять.

Разом з іншими формами соціальних конфліктів кібер-війни характеризуються залученням широкого спектра учасників до ворожих дій: організаторами кібер-атак є підлітки, злочинці, терористи та професійні програмісти на державній службі. Очевидно, що дуже важко розробити універсальні заходи нейтралізації атак, що надходять із таких різних за кваліфікацією та мотивацією супротивників.

Метою статті є систематизація шляхів, за допомогою яких Інтернет змінює політичний дискурс та формат відносин між владою і громадянським суспільством з особливим дослідницьким фокусом на визначення механізмів, через які громадянське суспільство впливає на формування державної політики.

Виклад основного матеріалу дослідження

Великий зрівнювач XXI століття. Відомого конструктора зброї Самюеля Кольта часто називають "великим зрівнювачем". У Сполучених Штатах Америки популярним є висловлювання, що Авраам Лінкольн звільнив усіх людей, а Сем Кольт зробив їх рівними. Інтернет є великим зрівнювачем XXI століття.

Здатність виробляти та обмінюватись інформацією впливає на кожний аспект безпеки держави: починаючи від утворення й функціонування інформаційних систем у державному управлінні ("електронний уряд"), інформаційних війн, у яких бере участь держава, і "м'якої" дипломатії в зовнішній політиці, до загроз і викликів безпеці держави, спричинених посиленням міжнародної організованої злочинності, що діє в кібер-просторі; від кібер-тероризму до дій екстремально налаштованих представників громадянського суспільства, які за допомогою Інтернету можуть об'єднуватись в мережі й мобілізовувати підтримку всередині країни й поза її межами.

За своєю сутністю Інтернет є та зі значною вірогідністю залишиться в майбутньому нестабільною, небезпечною технологією, відкритою для проявів агресії та експлуатації. Інтернет урівнює людей у можливостях, наділяє владою індивідуумів і громадянське суспільство, що кидає виклик державним бюрократіям, домінуванню "офіційної" ідеології та релігії.

Користування Інтернетом стає все більш дешевим. Ідеї, інноваційні технології й руйнівне програмне забезпечення поширюється в кібер-просторі швидко й безкоштовно, тому атаки на державну владу надходять не лише з боку урядів ворожих держав, а й з боку опозиції та екстремально налаштованих представників громадянського суспільства. Віруси, шкідливе програмне забезпечення, трояни, пастки, DOS-атаки (denial-of-service) - усе це є зараз ординарною й доступною для кожного зброєю, отримавши яку, протестні групи й навіть індивідууми відчувають себе рівними супердержавам. Ресурси, необхідні для ведення війни в кібер-просторі, стають усе більш доступними - тисячі вебсайтів пропонують складне програмне забезпечення для кібердіяльності й містять детальні інструкції, як це забезпечення повинно бути використано.

Експерти визнають, що сучасні системи безпеки держави здатні ідентифікувати лише окремі кібер-атаки й запобігти їм. По-перше, хакери й кібер-терористи відрізняються від солдат і байдужих до своїх обов'язків державних службовців. Вони є ідеологічно мотивованими інтелектуалами, об'єднаними в мережі однодумців, які розробляють і використовують усе більш досконале програмне забезпечення. По-друге, спроможність незграбних і корумпованих державних бюрократій протистояти кібер-загрозам є низькою. Уряди витрачають усе більше й більше ресурсів для нейтралізації кібер-загроз.

Уряд Сполучених Штатів, діяльність якого є найбільш комп'ютеризованою у світі, використовує понад 10000 комп'ютерних систем, функціонування близько 2000 із яких є критично важливим для безпеки держави. Тоді як тотальний параліч комп'ютерних систем є популярною темою американських фільмів-катастроф, різниця між звичайною соціальною активністю в кібер-просторі, хакерством і кібертероризмом усе більше стирається.

Громадянське суспільство в кібер-просторі. Інтернет є ефективним інструментом мобілізації соціальної активності населення, особливо, якщо його використання є складовою більш масштабної інформаційної стратегії. Для громадських організацій, що протидіють репресивним політичним режимам, використання Інтернету надає важливі переваги порівняно з іншими медіа. По-перше, це можливість подолання урядової цензури. По-друге, використання соціальних мереж дозволяє громадським рухам бути результативними навіть без масштабного фінансування - отримання, поширення інформації через соціальні мережі, освіта членів громадських організацій, поширення петицій, планування, координація дій, мобілізація для висловлення протесту і впливу на політику влади не потребує значних коштів. Соціальні медіа (засоби масової інформації, які побудовані на основі Інтернет-технологій і дозволяють користувачам з обмеженими технічними знаннями утворювати й поширювати

контент [4]) є впливовим інструментом соціальної мобілізації протестних рухів. Соціальні медіа включають блоги, сайти, призначені для соціальних комунікацій (наприклад, Facebook, Linkedin), сайти, призначені для поширення фото і відео (наприклад, Flikr або Youtube), сайти, призначені для акумулювання новин і поширення Інтернет-посилань.

Можна обґрунтувати п'ять форм використання Інтернету для цілей соціальної мобілізації: (1) збір інформації, (2) публікація, (3) налагодження діалогу, (4) координація дій, (5) пряме лобіювання інтересів протестних угруповань у владних установах для впливу на пріоритети внутрішньої й зовнішньої політики [3].

Водночас, такі форми соціального протесту в Інтернеті, як хакерство і кібер-тероризм, є менш дієвими щодо впливу на внутрішню й зовнішню політику держави - хакери й кібер-терористи можуть відчувати свою владу над комп'ютерами уряду, але не в змозі змінити його політику.

Хактивізм. "Хактивізм" є специфічною формою громадянської активності у кібер-просторі: хакерство використовується як інструмент висловлення політичної позиції. Хактивізм - це використання комп'ютерів, часто незвичним або нелегальним способом, для досягнення цілей, які ідеологічно мотивовані індивідууми й групи вважають важливими для суспільства. Вікілікс (Wikileaks) є найбільш відомим прикладом хактивізму. Сайт Wikileaks (і його численні копії в багатьох країнах) призначені для публікації матеріалів, що викривають корумпованість і злочинність державної влади. Діяльність Вікілікс не спрямована проти конкретної держави; вона покликана довести, що уряди навіть у найбільш демократичних країнах є корумпованими й несуть загрозу для суспільства. Вікілікс поширює інформацію про дії репресивних урядів і чиновників, яких активісти Вікілікс уважають злочинцями. Діяльність активістів Вікілікс була підтримана світовим громадянським суспільством і незалежними мас-медіа, але ставлення владних еліт до цієї організації є різним: наприклад, парламент Ісландії підтримав захист свободи слова, у той час як Сполучені Штати визнали засновника сайту Вікілікс ворогом держави, а сайт Вікілікс - загрозою безпеці Сполучених Штатів.

Іншим відомим прикладом хактивізму є діяльність групи Anonymous. Anonymous є групою Інтернет-користувачів без постійного складу та членства, які виступають за свободу слова. У групи Anonymous немає визнаних лідерів; це - індивідууми й групи, розташовані в різних країнах світу, об'єднані спільною системою цінностей, які координують свої дії за допомогою соціальних мереж.

У протистоянні з репресивними урядами хактивісти знаходяться в авангарді громадянського суспільства, тому що мають стратегічним завданням змінити сутність суспільства і взаємовідносин між громадянами й владою. Вони намагаються зруйнувати ієрархічну вертикальну структуру урядування й запровадити горизонтальну мережеву структуру, яка дозволить організувати ефективний зворотній зв'язок влади з громадянським суспільством і запровадити прямі механізми тиску на владу. Джон Перрі Барлоу, засновник адвокатської групи Electronic Frontiers Foundation, вважає, що уряди недостатньо або неправильно оцінюють наміри хактивістів, розглядають їх як примітивних злочинців або хуліганів, тоді як хактивізм є громадянським рухом, який має серйозне ідеологічне підгрунтя й бачення власної місії в суспільстві: "Групи хактивістів об'єднує вірування, що майбутнє - не за ієрархічними бюрократичними, а за горизонтальними структурами й урядами експертів. Це вірування й намагання зруйнувати бюрократії робить активістів ворогами урядів, концепція яких була сформульована в індустріальну добу. Фактично, хактивісти завжди перемагають уряди, тому що вони вже живуть в інформаційну епоху, а державні бюрократії - усе ще в індустріальну" [5].

Державна влада в кібер-просторі. Тим не менше, Інтернет не може бути повністю вільним від урядової цензури. Міжнародна громадська організація "Репортери без кордонів" зазначає, що більш ніж у 45 країнах світу (у т.ч. в Україні) уряди намагаються обмежити доступ громадян до політичних новин, що розміщені в Інтернеті. Авторитарні уряди визнають переваги, що надає глобалізація інформаційних потоків економіці, але побоюються безпрецедентної свободи слова й демократії в кібер-просторі. Деякі дії активістів у кібер-просторі й сигнали, що надсилає громадянське суспільство владі, розглядаються як загрози національній безпеці. Серед найважливіших загроз називаються: руйнація інформаційних потоків, економічних трансакцій, логістики, функціонування інфраструктури, отримання секретних або приватних даних, поширення яких може спричинити політичну нестабільність або соціальні конфлікти, маніпулювання інформацією для політичних, економічних або військових цілей.

Влада використовує різні інструменти для забезпечення власної стабільності, нейтралізації загроз і викликів, що надходять із кібер-простору, починаючи із запровадження цензури й заборони небажаного політичного контенту (прикладом може слугувати недавнє рішення уряду Росії щодо утворення переліку вебресурсів, заборонених до відвідування) до більш складної стратегії утворення системи "віртуальної керованої демократії" - активного, часто закамуфльованого втручання влади в життя кібер-простору. "В епоху віртуальної демократії, - зазначає канадський дослідник Антон Олійник, - влада отримує нечувану раніше, в епоху "звичайної" демократії, автономію по відношенню до громадян. Забезпечення економічної стабільності та активне використання засобів масової інформації для утворення сприятливого іміджу влади в Інтернеті, маніпулювання масовою свідомістю є ключовими елементами стратегії влади" [6]. Тенденція утворення віртуальної демократії спостерігається в усіх країнах світу, але слабкість громадянського суспільства робить цю систему вразливою до зовнішніх шоків. Економічна криза є чинником, що підриває стабільність віртуальної керованої демократії.

Висновки

Перед викликом зростання потужності громадянського суспільства і зростання різноманітності стратегій, що використовує громадянське суспільство в кібер-просторі для впливу на політику урядів, державна влада в Україні може запровадити деякі тактичні механізми захисту власної стабільності:

1) сприяти утворенню аналітичних центрів, які збирають, аналізують і поширюють інформацію про стратегії поведінки різних акторів у кібер-просторі, оцінюють вразливості, загрози, атаки й можливі механізми захисту;

2) організувати дискусію між представниками державної влади, бізнесу й громадянського суспільства у сфері інформаційної політики;

3) розробляти державну політику, яка фокусується не лише на реагуванні на загрози в кібер-просторі та покаранні порушників, а на запобіганні загрозам шляхом запровадження узгоджувальних механізмів і превентивних дій;

4) удосконалювати освіту урядовців у галузі інформаційної безпеки, запроваджувати спеціальні освітні програми в університетах;

5) розробляти більш гнучке й досконале законодавство, що регулює виробництво, використання й поширення інформації тощо.

Але пропозиції, що наводяться вище, і подібні до них заходи державної політики будуть мати лише короткостроковий вплив і не зможуть зберегти стабільність державних бюрократій у стратегічній перспективі. Інформаційна доба вимагає нових підходів до побудови відносин влади із громадянським суспільством, що базуються на горизонтальних зв'язках й участі громадян у державному управлінні.

ЛІТЕРАТУРА:

1. Denning D. Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy / D. E. Denning // Networks and netwars: the future of terror, crime, and militancy. - Washington DC : RAND, 2011. - P. 239-240.

2. Arquilla John. In Athena's camp: preparing for conflict in the information age / John Arquilla, David Ronfild. - Washington DC : RAND, 2012. - 525 p.

3. Borchgrave A. de. Cyber threats and information security: meeting the 21st century challenge: a report of the CSIS homeland defense project / A. de Borchgrave. - CSIS, 2001. - 40 p.

4. Social media: definition [Електронний ресурс]. - Режим доступу : http://www.merriam-webster.com/dictionary/social%20media.

5. Barlow John Perry. Hacktivists in the frontline battle for the Internet [Електронний ресурс] / John Perry Barlow // The Guardian, 2012. - Режим доступу : http://www.guardian.co.uk/technology/2012/apr/20/hacktivists-battle-internet.

6. Олейник А. Н. Урок испанского: как свернуть с дороги к виртуальной демократии / А. Н. Олейник // Неприкосновенный запас. - 2004. - № 2 (34). - С. 64-69.

T. Malyarenko

THE STATE POWER AND CIVIL SOCIETY IN A CYBER-SPACE

This article is aimed at a thorough analysis of the ways through which the Internet has been enriching a political discourse and, thus, it has been changing the format of the relations between the state power and civil society with the particular focus on the mechanisms that civil society employs to influence domestic and foreign policy. The article explores the links between a civil society activism and an openness of public policy. The main conclusion is that the Internet empowers everyone that poses a significant challenge to the state power. The Internet gives additional benefits for politically-motivated individuals and groups with low access to the financial resources. It facilitates social mobilization of protesters, both individuals and groups through educating the public and media, rising funds, forming coalitions across geographical boundaries, as well as coordination of the events on a national and international level.

Надійшла до редакції 12.10.2012