РОЗДІЛ XII. ФІЛОСОФІЯ ПРАВА

УДК 342.1
DOI https://doi.org/10.24144/2788-6018.2023.06.122

АКТУАЛІЗАЦІЯ КІБЕРСТІЙКОСТІ ТА ІСТОРИЧНІ ВИТОКИ КОНЦЕПЦІЇ «СТІЙКІСТЬ»

Користін О.Є.,
доктор юридичних наук, професор,
заслужений діяч науки і техніки України,
ЦСК ННІ ІБСК НА СБ України;
ORCID: 0000-0001-9056-5475

Демедюк С.В.,
кандидат юридичних наук
заступник Секретаря Ради національної
безпеки і оборони України, м. Київ;
ORCID: 0009-0008-1359-5265

Користін О.Є., Демедюк С.В. Актуалізація кіберстійкості та історичні витоки концепції «стійкість».

У цій статті кіберстійкість визначається як здатність протистояти зовнішнім потрясінням, спричиненим кіберризиками, відновлюватися після них та адаптуватися до них. Зазначено на важливості розбудови системи кіберстійкості в сучасних умовах та наведено приклади надзвичайних ситуацій застосування кібератак. Розглядається необхідність забезпечення кіберстійкості на об'єктах та установах, висвітлюються різні типи загроз, спрямовані на різні системи, а також наслідки їх негативного впливу.

Зазначено, що стійкість та управління ризиками хоча і є взаємопов'язаними, все ж відрізняються. Управління ризиками передбачає кількісну оцінку ризиків, що формує рішення про найбільш відповідну стратегію реагування на них. Стійкість має важливе значення, коли ризик не піддається обчисленню, коли небезпечні умови є повною несподіванкою, або коли аналітичні параметри ризику виявилися неефективними.

Акцентовано на тому, що на фундаментальному рівні існують певні розбіжності щодо справжнього значення стійкості: для одних вона передбачає здатність системи витримати шок і повернутися до свого початкового стану, тоді як для інших - це еволюційний процес, що веде до адаптації та нового стану рівноваги.

Стійкість має тривалу і багату історію в різних галузях наукового пізнання, в тому числі в екології, психології та управлінні катастрофами. Однією з її основних переваг є те, що вона дозволяє складним системам підготуватися до несприятливих подій і продовжувати працювати в надзвичайних умовах. Робиться висновок, що парадигма «запобігти і захистити», яка є домінуючою і сьогодні, є недостатньою, і що інструментарій управління ризиками необхідно розвивати в напрямі кіберстійкості.

Ключові слова: кібербезпека, стійкість, кіберстійкість, ризик, кіберризик, управління ризиками.

Korystyn O., Demediuk S. Actualization of cyber resilience and historical origins of the concept of "resilience".

In this article, cyber resilience is defined as the ability to withstand external shocks caused by cyber risks, recover from them, and adapt to them. The importance of building a cyber resilience system in modern conditions is emphasized and examples of emergency situations of cyberattacks are given. The need to ensure cyber resilience at facilities and institutions is considered, different types of threats aimed at different systems, as well as the consequences of their negative impact are highlighted.

It is noted that resilience and risk management, although interrelated, are still different. Risk management involves quantitative risk assessment, which forms a decision on the most appropriate strategy for responding to them. Resilience is important when risk is incalculable, when hazardous conditions are a complete surprise, or when analytical risk parameters have proven ineffective.

It is emphasized that at a fundamental level, there are certain disagreements about the true meaning of resilience: for some, it implies the ability

of a system to withstand a shock and return to its initial state, while for others it is an evolutionary process leading to adaptation and a new state of balance.

Resilience has a long and rich history in various fields of scientific knowledge, including ecology, psychology, and disaster management. One of its main advantages is that it allows complex systems to prepare for adverse events and continue to operate under extraordinary conditions. It is concluded that the "prevent and protect" paradigm, which is still dominant today, is insufficient, and that risk management tools need to be developed in the direction of cyber resilience.

Key words: cybersecurity, resilience, cyber resilience, risk, cyber risk, risk management.

Постановка проблеми. Витонченість та зростаючі частота й інтенсивність кібератак, спрямованих на установи у кіберпросторі, підкреслюють їх високу ризиковість та складність повноти захисту цілісності критично важливих об'єктів та систем. У цьому контексті кіберстійкість пропонує привабливу додаткову альтернативу існуючій парадигмі кібербезпеки. Концепт кіберстійкості є результатом тривалого наукового пошуку та розвитку більш загальної концепції «стійкість», з різним осягненням та сприйняттям різноманітними науковими школами та широкої низки галузей та сфер суспільного буття.

Метою цієї статті є дослідження проблематики кіберстійкості, обґрунтування змісту самого явища на прикладі розвитку наукової думки в різних галузях та сферах, а також аналіз та окреслення основних вимірів стійкості.

Виклад основного матеріалу. Кіберстійкість останнім часом стала однією з найбільш розкручених концепцій в дискусіях про кібербезпеку, незважаючи на її розпливчасте значення, що ускладнює її точне визначення та вимірювання, а можливо, і завдяки йому. Її популярність, безсумнівно, пов'язана з численними заголовками про кібератаки і витоки даних, які рясніють на перших шпальтах ЗМІ і веб-сайтах, повідомляючи про нові і масові зломи, що свідчать про вразливість цифрових інфраструктур і нездатність організацій захистити персональні дані, які ми їм довіряємо. Навіть найбільш технічно підковані та обізнані в питаннях безпеки організації не застраховані від катастрофічних збоїв у кібербезпеці.

Свого часу, у жовтні 2017 року газети New York Times і Washington Post опублікували історію прямо з роману Джона Ле Карре, в якій повідомлялося, що ізраїльські шпигуни проникли в системи компанії з кібербезпеки «Касперський» і ніби-то змогли відстежувати хакерські дії своїх російських колег, які використовували телеметричні можливості антивірусного продукту компанії для пошуку конфіденційних документів американських спецслужб [1, 2]. Витоки, що стосуються хакерських інструментів, розроблених Центральним розвідувальним управлінням та Агентством національної безпеки, хоча і не пов'язані з цим конкретним інцидентом, але, здається, підтверджують, що такий підхід іноді буває успішним. Кілька місяців потому, у менш розголошеній доповіді, голландське агентство внутрішньої розвідки повідомило, що воно зламало комп'ютерну мережу будівлі, з якої команда російських хакерів зі Служби зовнішньої розвідки їхньої країни проникла в електронні поштові скриньки співробітників Державного департаменту США та Національного комітету Демократичної партії. Цифрове проникнення, яке тривало близько року, було настільки повним, що рік голландська команда змогла отримувати доступ до відеозаписів камер відеоспостереження будівлі та ідентифікувати осіб, які заходили до кімнати, з якої працювали хакери [3]. Ці дві історії ілюструють неможливість гарантувати цілісність комп'ютерних систем навіть для організацій, які підтримують найвищі стандарти операційної безпеки і мають, можливо, найдосконаліші програми кібербезпеки.

У цьому контексті концепція кіберстійкості пропонує привабливе доповненням до підходу «передбачити і захистити», який домінував в інформаційній безпеці протягом останніх кількох десятиліть. Зіткнувшись з усвідомленням того, що жодна цифрова система не може гарантувати неприступність перед обличчям постійних атак, організації приходять до висновку щодо необхідності розробляти процеси і технології, які надають допомогу після катастрофічних атак. Це далеко не єдиний випадок, коли кіберзагроза не є унікальною в кіберсфері, дилема, як ефективно реагувати на збої, спричинені непередбачуваними несприятливими подіями, та управляти збоями, які мають потенціал дестабілізувати - і, зрештою, знищити - є центральною проблемою всіх складних екологічних, соціальних, організаційних і технічних систем. Відповіддю є стійкість, яку на даний момент визначатимемо як здатність протистояти, відновлюватися після та адаптуватися до зовнішніх шоків. За словами одного із засновників концепції (К.С. Холлінга, канадського еколога), така зміна перспективи «не вимагає точної здатності передбачати майбутнє, а лише якісної здатності розробляти системи, які можуть поглинати і пристосовуватися до майбутніх подій, яких би несподіваних форм вони не набули» [4].

Важливо відрізняти стійкість від управління ризиками, хоча вони взаємопов'язані. Управління ризиками передбачає кількісну оцінку ймовірності та серйозності ризиків, що дозволяє підтримувати рішення про найбільш відповідну стратегію реагування на них, наприклад, таких

як бездіяльність, уникнення, зменшення, передача або страхування [5]. Стійкість є ширшим поняттям і «має важливе значення, коли ризик не піддається обчисленню, наприклад, коли небезпечні умови є повною несподіванкою, або коли аналітичні параметри ризику виявилася неефективними» [6]. Стійкість приходить на зміну управлінню ризиками, коли останній виявився неефективним у захисті організації від руйнівних загроз і передбачає постійний цикл дій та реагування - починаючи задовго до несприятливої події і закінчуючи задовго після завершення події, щоб впровадити адаптивні заходи необхідні для протидії наступному непередбачуваному шоку. Іншими словами, в той час як управління ризиками в кібербезпеці спрямоване на мінімізацію загроз, кіберстійкість прагне підтримувати високий рівень продуктивності незалежно від наявності або відсутності загроз [7]. Це пояснює, чому «організація може мати кібербезпеку не будучи стійкою, але не навпаки» [8].

Потреба в застосуванні мислення та практик стійкості до цифрової екосистеми може здатися зайвою, оскільки інтернет був створений як стійка розподілена система, яка може продовжувати працювати в найгірших можливих ситуаціях, таких як ядерний удар [9]. Але ця технічна стійкість, яка обмежується одним з базових рівнів, що складають Інтернет і гарантує, що маршрутизація пакетів даних може проходити декількома альтернативними шляхами [10], досягаючи одержувачів, навіть якщо нетривіальна кількість з'єднувальних вузлів видаляється, ніколи не мала на меті забезпечити надійний рівень безпеки для світу, в якому всі можливі види соціальної активності та бізнес-транзакцій перемістилися в онлайн, мільярди пристроїв підключені до мережі, а люди, процеси та політики регулярно і успішно використовуються зловмисниками. Враховуючи безпрецедентні масштаби та серйозність кібер-ризиків, кіберстійкість повинна виходити за межі глобальної інфраструктури Інтернету, зосереджуючись на окремих організаціях, які стали залежати від неї у виконанні своєї ролі.

Хоча концепція кіберстійкості, безумовно, здається привабливою коли стикається з таким невизначеним і непередбачуваним середовищем, вона має важливі обмеження, які необхідно визнати і подолати, якщо ми хочемо зберегти її концептуальну перевагу. Основна проблема полягає в тому, що міждисциплінарне коріння стійкості може виявитися як прокляттям, так і перевагою: вона забезпечує багатий теоретичний інструментарій, пов'язаних концепцій, з яких суттєві позитивні складові можуть бути перенесені в кіберпростір, але відсутність єдиного визначення і різноманітність підходів, які вона тягне за собою, сприяє фрагментації, що заважає фахівцям з питань стійкості та політикам розробити узагальнюючий підхід [6, 7, 11]. На фундаментальному рівні, наприклад, існують певні розбіжності щодо справжнього значення стійкості: для одних вона передбачає здатність системи витримати шок і повернутися до свого початкового стану, тоді як для інших - це еволюційний процес, що веде до адаптації та нового стану рівноваги [7]. На більш практичному рівні кіберстійкість, замість того, щоб розумітися як всеохоплююче поняття, іноді розглядається вузько. Наприклад, у звітах компаній, вихваляючи її переваги, часто плутають кіберстійкість з практиками та методологіями реагування на інциденти, з якими знайомі їхні автори і які легше продати потенційним клієнтам. З тієї ж причини, галузеві стандарти, які намагалися формалізувати концепцію кіберстійкості переважно зосереджені на її інженерних аспектах і рідко приділяють когнітивним і соціальним аспектам стільки ж уваги. Стійкість занадто часто залишається «риторичним прийомом, який мало впливає на фактичне прийняття рішень» [12].

Це частково пояснює, чому багато експертів скептично ставляться до концепції кіберстійкості, відкидаючи її як одну з останніх примх кібербезпеки, що має на меті привернути увагу довірливих клієнтів. Але мислення про стійкість може забезпечити дуже корисну теоретичну і практичну основу, яка допоможе нам вирватися з колії кібербезпеки, в якій ми опинилися. Тому важливо проаналізувати міждисциплінарні засади, що стосуються вивчення кіберстійкості, щоб зрозуміти як її численні виміри, так і критерії, які можуть бути використані для полегшення її впровадження та вимірювання. Для досягнення цієї мети варто звернути увагу на численні значення стійкості через її використання в різних дисциплінах, вказуючи на теоретичні аспекти, які є особливо актуальними для кібербезпеки.

Наукові концепції стійкості сягають корінням у фізику та матеріалознавство, де стійкість позначає властивість матеріалу поглинати енергію, коли він піддається деформації, і зберігати або відновлювати свою початкову форму або положення після згинання, розтягування або стискання [13]. У розширеному розумінні це значення застосовується в медичній та ветеринарній науках для визначення природної еластичності частин тіла, таких як шкіра, легені або грудна клітка. У цьому контексті стійкість відноситься до обмеженого набору вимірюваних параметрів, які визначаються їхньою передбачуваністю і мало змінюються в часі та просторі. У 1970-х роках ця концепція стала більш привабливою, особливо в межах двох дисциплін, які спричинили її нинішню популярність - екології та психології.

В екології основоположна стаття Холлінга представила більш динамічне розуміння поняття стійкості, застосовуючи його до ситуацій коли

система стикається з глибокими та неочікуваними змінами не може, на відміну від матеріалів, підтримувати постійний стан рівноваги [4]. Натомість Холлінг стверджував, що вивчення стійкості має зосередитися на «стійкості систем та їхній здатності поглинати зміни і збурення, зберігаючи при цьому незмінними взаємозв'язки між популяціями або змінними стану» [4]. На практиці персистентність є протилежністю стабільності, яка означає здатність системи повертатися до стану рівноваги після збурення. Персистентність, наприклад, може бути досягнута у випадках екстремальних коливань чисельності популяції і забезпечує меншу ймовірність її вимирання порівняно з популяціями, які є більш стабільними, але менш гнучкими у своїй здатності поглинати екстремальні зміни навколишнього середовища. Важливо пам'ятати, що такий погляд на стійкість є характерним для екології, де, на відміну від організацій, головною метою не є обов'язковим максимізувати ефективність, а просто залишитися в грі. Коли ця концепція переноситься в організаційне середовище, вона створює напруженість, оскільки, на відміну від стійких екологічних систем, які покладаються на різноманітність і мінливість, гомогенність, яка сприяє організаційній ефективності, не терпить високих коливань, а отже, демонструє меншу стійкість. У наступній статті, Холлінг формалізував свої міркування щодо ознак - ефективності, постійності та передбачуваності - які відрізняють інженерну (або економічну) стійкість від екологічної стійкості, яка зосереджена на стійкості, змінах і непередбачуваності [14]. Виходячи за межі теоретичних тонкощів одно- та багатостабільних рівноваг, практичним наслідком цього напряму міркувань є те, що ефективність і стійкість не завжди узгоджуються між собою. Умови, які призводять до короткострокової економічної продуктивності (наприклад, зменшення різноманітності і надмірність, які дозволяють досягти економії на масштабах і оптимізації ресурсів), можуть бути шкідливими для стійкості і підвищувати вразливість [14]. Хоча Холлінг не мав наміру узагальнювати свою роботу за межами управління екологічними системами, його розуміння є важливим для осіб, які приймають рішення в інших сферах, які повинні усвідомлювати, що досягнення стійкості вимагає від них балансу між суперечливими пріоритетами. Його новаторський внесок знайшов відгук, зокрема, серед екологів, містобудівників та експертів з управління катастрофами, які розширили їх для концептуалізації та картографування адаптаційних стратегій, доступних для сучасних суспільств та їхніх складних, але крихких соціально-технічних систем, з особливим акцентом на катастрофічні наслідки прискореної зміни клімату [11, 15]. Дехто навіть стверджує, що ця концепція є настільки універсальною і стала настільки помітною, що «вона допомогла уніфікувати екологію як дисципліну» [16].

Психологія є другою дисципліною, яка зробила значний внесок у популяризацію стійкості. У 1970-х роках, коли екологія розглядала стабільність, стійкість і адаптацію екологічних систем, психологія намагалася зрозуміти, чому деякі люди і сім'ї, які опинилися в зоні ризику або зіткнулися з широким спектром несприятливих обставин (таких як бідність, розпад сім'ї, травматична втрата або стихійне лихо), здаються відносно не зачепленими і здатні впоратися з ними і нормально функціонувати [17], а в деяких випадках стають навіть сильнішими [18]. Психологія розробила концепцію життєстійкості як спосіб вийти за межі своєї природної тенденції зосереджуватися на факторах ризику та їхніх негативних наслідках для психічного здоров'я, розширивши свої перспективи до вивчення особистісної сили, позитивних форм адаптації, пом'якшувальних факторів та захисних впливів [17, 19]. Річардсон [19] виокремлює три хвилі психологічних досліджень життєстійкості. Перша хвиля визначила особистісні характеристики та захисні фактори, які підтримують людей під час несприятливих життєвих подій, створивши довгий список індивідуальних, сімейних, громадських та культурних факторів, таких як самооцінка, ефективність, навички вирішення проблем, турбота, гумор або теплі особисті стосунки, якщо назвати лише деякі з них [18]. Друга хвиля намагалася зрозуміти, як ці якості набуваються, тоді як третя хвиля намагалася змоделювати силу або мотивацію, яка спонукає людину до розвитку або посилення цих якостей.

Ця робота стала інструментом у розвитку позитивної психології, яка відмовляється від патологізації ризиків на користь більш цілісного підходу, в якому розуміється, що найнесприятливіші ситуації можуть дозволити людям процвітати і знаходити креативні рішення [20]. Така перспектива може бути відкинута як занадто оптимістична для суворих реалій нашого складного світу, але, навпаки, психологічні дослідження виявили, що життєстійкість трапляється набагато частіше, ніж прийнято вважати. Основним висновком є те, що життєстійкість - це далеко не виключна сфера компетенції невеликої групи «невразливих» або «непереможних» людей, є дуже поширеним набором здібностей і практик, які демонструє значна частина населення [19, 21, 22]. Психології вдалося демістифікувати надзвичайну силу життєстійкості та виділити її «звичайну магію» [23].

Третя, більш розрізнена, група вчених, які вивчали управління катастрофами та стійкість міст, також знайшла концепцію стійкості дуже привабливою. У «суспільстві ризику», в якому ми живемо [24], антропогенні фактори спричи-

няють дедалі частіші та сильніші стихійні лиха (посухи, пожежі, повені, спеку), які є надзвичайно руйнівними і впливають на наші складні технологічні та міські системи. Крім того, «штучні ризики», категорія ризиків, створених наукою і технікою і щодо яких є обмеженими знання, стали повсюдними [25]. Штучні ризики, такі як фінансові крахи, ядерні катастрофи, розливи нафти чи скандали у сфері охорони здоров'я, зазвичай розгортаються в глобальному масштабі і завдають надзвичайної шкоди. Враховуючи такий радикально ворожий і невизначений контекст, не дивно, що дослідники як антропогенних, так і техногенних ризиків прийняли концепцію стійкості. Зокрема, у розробці та застосуванні концепції стійкості були задіяні дві сфери, що перетинаються, а саме: стійкість міст та стійкість до стихійних лих. У той час як перша стосується спроможності міст протистояти широкому спектру стресів і потрясінь, друга фокусується на конкретних великомасштабних несприятливих подіях і на тому, як з ними справляються організації та місцеві громади. Обидва напрямки висвітлені у численних публікацях, в яких варто виділити два висновки.

По-перше, складні організації та соціоекологічні системи по-різному інтерпретують поняття стійкості, залежно від рівня їхньої зрілості. На базовому рівні стійкість передбачає спроби зберегти статус-кво і зменшити виникнення або вплив збурень шляхом поглинання, тоді як більш адаптивна форма стійкості спирається на здатність до самоорганізації та прийняття нових практик без шкоди для структури та функцій. Найбільш просунутою формою стійкості є трансформаційна, яка передбачає перехід до нового набору функцій, структур, зворотного зв'язку та результатів, які краще відповідають мінливому середовищу [11]. Друге розуміння полягає в тому, що неможливо зрозуміти - і, відповідно, сприяти підвищенню - стійкості складних систем, не звертаючи уваги на міжмасштабну взаємодію між низкою географічних, часових, функціональних і технологічних вимірів [26]. Обидва висновки видаються особливо актуальними для нової сфери кіберстійкості.

Висновки. Таким чином, хоча стійкість та управління ризиками є взаємопов'язаними, все ж вони відрізняються. Управління ризиками передбачає кількісну оцінку ймовірності та серйозності ризиків, що дозволяє підтримувати рішення про найбільш відповідну стратегію реагування на них, наприклад, таких як бездіяльність, уникнення, зменшення, передача або страхування. Стійкість є ширшим поняттям і має важливе значення, коли ризик не піддається обчисленню, наприклад, коли небезпечні умови є повною несподіванкою, або коли аналітичні параметри ризику виявилися неефективними.

Хоча концепція кіберстійкості і здається привабливою, та коли стикається з невизначеним і непередбачуваним середовищем, вона має важливі обмеження, які необхідно визнати і подолати, якщо необхідно зберегти її концептуальну перевагу. Враховуючи безпрецедентні масштаби та серйозність кібер-ризиків, кіберстійкість повинна виходити за межі глобальної інфраструктури Інтернету, зосереджуючись на окремих організаціях. Мислення про стійкість може забезпечити дуже корисну теоретичну і практичну основу, яка допоможе вирватися з колії кібербезпеки. Тому важливо проаналізувати міждисциплінарні засади, що стосуються вивчення кіберстійкості, щоб зрозуміти як її численні виміри, так і критерії, які можуть бути використані для полегшення її впровадження та вимірювання у кіберпросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Nakashima E. Israel hacked Kaspersky, then tipped the NSA that its tools had been breached, The Washington Post, 2017. https://www.wash ingtonpost.com/world/national-security/israel-hacked-kaspersky-then-tipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html.
2. Perlroth N, Shane S. How Israel caught Russian hackers scouring the world for U.S. secrets, The New York Times, 2017. https://www. nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking. html.
3. Gallagher S. Candid camera: Dutch hacked Russians hacking DNC, including security cameras, Ars Technica, 2018. https://arstechnica.com/information-technology/2018/01/dutch-intelligence-acked-video-cameras-in-office-of-russians-who-hacked-dnc/
4. Holling CS. (1973) Resilience and stability of ecological systems. Annu Rev Ecol Syst.
5. Button M. Doing (2008) Security: Critical Reflections and an Agenda for Change. Basingstoke: Palgrave Macmillan.
6. Linkov I, Eisenberg DA, Bates ME, et al. (2013) Measurable resilience for actionable policy. Envir Sci Tech.
7. Bagheri S, Ridley G. Organisational cyber resilience: research opportunities. Australasian Conference on Information Systems 2017.
8. Conference Board of Canada. Building Cyber Resilience. Ottawa: Conference Board of Canada 2018.
9. Castells M. (2001) The Internet Galaxy: Reflexions on the Internet, Business, and Society. Oxford: Oxford University Press.

10. Kuehl D. (2009) From cyberspace to cyberpower: defining the problem. In: Kramer F, Starr S, Wentz L (eds.), Cyberpower and National Security. Washington DC: National Defense University Press.
11. Davidson JL, Jacobson C, Lyth A, et al. (2016) Interrogating resilience: toward a typology to improve its operationalization. Ecol Soc.
12. Benson MH, Craig RK. (2014) The end of sustainability. Soc Natur Resour.
13. OED Online. Resilience, OED Online 2018. www.oed.com/view/Entry/163619.
14. Holling CS. (1996) Engineering resilience versus ecological resilience. In: Schulze P (ed.). Engineering within Ecological Constraints. Washington DC: National Academy Press.
15. Downes BJ, Miller F, Barnett J, et al. (2013) How do we know about resilience? An analysis of empirical research on resilience, and implications for interdisciplinary praxis. Environ Res Lett.
16. Olsson L, Jerneck A, Thoren H, et al. (2015) Why resilience is unappealing to social science: theoretical and empirical investigations of the scientific use of resilience. Sci Adv.
17. Masten AS. (2018) Resilience theory and research on children and families: past, present, and promise. J Fam Theor Rev.
18. Waller MA. (2001) Resilience in ecosystemic context: evolution of the concept. Am J Orthopsychiat.
19. Richardson GE. (2002) The metatheory of resilience and resiliency. J Clin Psychol.
20. Seligman MEP, Csikszentmihalyi M. (2000) Positive psychology: an introduction. Am Psychol.
21. Werner E, Smith RS. (1992) Overcoming the Odds: High Risk Children from Birth to Adulthood. Ithaca: Cornell University Press.
22. Bonanno GA. (2004) Loss, trauma, and human resilience: have we underestimated the human capacity to thrive after extremely aversive events? Am Psychol.
23. Masten AS. (2001) Ordinary magic: resilience processes in development. Am Psychol.
24. Beck U. (1992) Risk Society: Towards a New Modernity. London: SAGE Publications.
25. Giddens A. (1999) Risk and responsibility. Mod Law Rev.
26. Ansell C, Boin A, Keller A. (2010) Managing transboundary crises: identifying the building blocks of an effective response system. J Conting Crisis Man.