УДК 342.9:004
DOI https://doi.org/10.32838/2707-0581/2020.2-2/23

Тарасюк А.В.
Науково-дослідний інститут інформатики і права Національної академії правових наук України

СИСТЕМА СУБ'ЄКТІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Метою статті є дослідження законодавчо визначеної системи суб'єктів забезпечення кібербезпеки в Україні. Бурхливий технічний прогрес зумовив появу нових загроз як соціальної, так і індивідуальної безпеки, внаслідок чого звична людині реальність вперше за всесвітню історію доповнена реальністю віртуальною – кіберреальністю. Кіберзагрози здійснили революцію в уяві людей про безпеку, правила і методи забезпечення національної безпеки тощо. Тож питання кібербезпеки набувають особливого значення, стаючи невід'ємною частиною національної безпеки, а заходи протидії кіберзагрозам розробляються і впроваджуються на державному рівні. У нашій країні для цих цілей був прийнятий Закон України «Про основи забезпечення кібербезпеки України», який, зокрема, вибудовує систему суб'єктів забезпечення кібербезпеки. Система забезпечення кібербезпеки становить органічне поєднання спільною метою державних і недержавних інституцій, а також інших суб'єктів, котрі беруть участь у здійсненні заходів, спрямованих на забезпечення кібербезпеки. Спектр суб'єктів забезпечення кібербезпеки не може обмежуватися виключно державними органами та їх посадовими особами. У складі суб'єктів забезпечення кібербезпеки виділяють загальних і спеціальних суб'єктів. До останніх належать державні органи, які, крім загальних функцій, уповноважені на здійснення боротьби з кіберзлочинністю та кібертероризмом, а також на забезпечення кібернетичного захисту об'єктів національної критичної інфраструктури. Нині ризик кіберзагроз є актуальним для значної кількості суб'єктів: від приватних осіб до великих компаній, окремих галузей економіки та держав загалом, тож ефективна організація системи суб'єктів забезпечення кібербезпеки набуває в сучасному світі непересічного значення.

Ключові слова: *кібербезпека, система забезпечення кібербезпеки, суб'єкти забезпечення кібербезпеки, кіберзагрози.*

Постановка проблеми. Бурхливий технічний прогрес зумовив появу нових загроз як соціальної, так і індивідуальної безпеки, внаслідок чого звична людині реальність вперше за всесвітню історію доповнена реальністю віртуальною – кіберреальністю. Кіберзагрози здійснили революцію в уяві людей про безпеку, правила і методи забезпечення національної безпеки тощо. У нашій країні для цих цілей був прийнятий Закон України «Про основи забезпечення кібербезпеки України», який, зокрема, вибудовує систему суб'єктів забезпечення кібербезпеки.

Постановка завдання. Метою статті є дослідження законодавчо визначеної системи суб'єктів забезпечення кібербезпеки в Україні.

Виклад основного матеріалу дослідження. Передусім слід зазначити, що поняття «система суб'єктів забезпечення кібербезпеки» тісно пов'язане із поняттям «система забезпечення безпеки» як із більш загальним. В. Ліпкан визначає систему забезпечення безпеки як механізм із вироблення, перетворення і реалізації концепції, стратегії та тактики у сфері безпеки за допомогою скоординованої діяльності державних і недержавних структур; сукупність організаційно об'єднаних органів управління, сил і засобів, призначених для вирішення завдань щодо забезпечення національної безпеки [1, с. 314]. На думку І. Тімкіна, система забезпечення національної безпеки виступає як організаційна система державних і недержавних інституцій, інших суб'єктів, покликаних вирішувати завдання забезпечення національної безпеки у визначений законодавством спосіб [2]. М. Гетьманчук, В. Грищук, Я. Турчин вважають, що загальна система забезпечення національної безпеки України – це єдиний державно-правовий механізм, у якому кожний суб'єкт безпеки виконує функції захисту національних інтересів у межах повноважень, що визначаються законодавством України [3, с. 128]. Слід підтримати позицію Т. Ткачука, за якою система забезпечення національної безпеки будується «від інтересів держави», більшість функцій, у т. ч. у сфері забезпечення інформаційної без-

пеки, здійснюється саме державою, що дозволяє досягти балансу інтересів в інформаційній сфері. Щодо суспільного виміру інформаційної безпеки, то т. зв. «недержавна система безпеки» є не лише суб'єктом власного забезпечення, котрий самостійно визначає мету, принципи та методи забезпечення безпеки відповідно до законодавства України в межах загальної системи, але й становить об'єкт забезпечення інформаційної безпеки з боку держави. У свою чергу, безпека людини є складовою частиною метасистеми національної безпеки, яка об'єднує безпеку особи, суспільства та держави в різних сферах, зокрема в інформаційній [4, с. 102]. Погоджуючись загалом із таким підходом, вважаємо за необхідне уточнити, що система забезпечення кібербезпеки становить органічне поєднання спільною метою державних і недержавних інституцій, а також інших суб'єктів, які беруть участь у здійсненні заходів, спрямованих на забезпечення кібербезпеки.

З цього приводу В. Бухарєв слушно зазначає, що суб'єкти забезпечення кібербезпеки є учасниками не інформаційних, а адміністративних правовідносин, оскільки відносини між ними будуються на основі влади та підпорядкування, до того ж, останні реалізують механізм кіберзахисту шляхом використання примусу, який їм надано чинним законодавством [5, с. 87]. Тож суб'єктами забезпечення кібербезпеки, на думку науковця, є державні органи та їхні посадові особи, наділені владними повноваженнями та відповідними обов'язками щодо охорони об'єктів кібербезпеки, котрі знаходяться у законній підпорядкованості між собою [5, с. 88]. Це твердження є цілком справедливим, водночас вважаємо, що спектр суб'єктів забезпечення кібербезпеки не може обмежуватися виключно державними органами та їхніми посадовими особами. Якщо говорити про систему забезпечення національної безпеки загалом, то слід зазначити, що до її складу традиційно включають сили та засоби забезпечення національної безпеки [6, с. 42]. Це і стосується кібербезпеки.

Загальний перелік і засади розмежування компетенції суб'єктів забезпечення кібербезпеки визначаються у ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України». Зокрема, зазначеною статтею передбачено, що координація діяльності у сфері кібербезпеки здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони (РНБО) України. Робочим органом РНБО України у вказаній сфері є національний координаційний центр кібербезпеки, який здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, котрі забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування й уточнення Стратегії кібербезпеки України [7].

Формування та реалізація державної політики у сфері кібербезпеки, захист прав і свобод людини та громадянина, національних інтересів України у кіберпросторі, боротьба з кіберзлочинністю забезпечується Кабінетом Міністрів (КМ) України. Уряд України також організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України). КМ України є вищим органом у системі органів виконавчої влади, який реалізує свої функції безпосередньо та через міністерства, інші центральні органи виконавчої влади.

Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є: міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні та контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили (ЗС) України, інші військові формування, утворені відповідно до закону; Національний банк України; підприємства, установи й організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України й об'єднання громадян, інші особи, які провадять діяльність та / або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом. Тобто фактично забезпечення кібербезпеки є загальносуспільною справою, і перелік суб'єктів її забезпечення є невичерпним. У межах своєї компетенції суб'єкти забезпечення кібербезпеки здійснюють: заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях; виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків; інформаційний обмін щодо реалізованих і потенційних кіберзагроз; розробку і реалізацію запобіжних, організаційні, освітні та інші заходи у сфері кібербезпеки,

кібероборони та кіберзахисту; проведення аудиту інформаційної безпеки, у т. ч. на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління; інші заходи із забезпечення розвитку та безпеки кіберпростору.

Законодавче підґрунтя забезпечення кібербезпеки, відповідно до якого визначається компетенція суб'єктів її забезпечення, становлять Конституція України, Стратегія національної безпеки України, Стратегія кібербезпеки України, Доктрина інформаційної безпеки України, Закони України «Про національну безпеку України», «Про Раду національної безпеки і оборони України», «Про Службу безпеки України», «Про Державну Службу спеціального зв'язку і захисту інформації України», Положення про Національний координаційний центр кібербезпеки тощо.

Одним із перших нормативно-правових актів, котрий визначив систему суб'єктів забезпечення кібербезпеки, є Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України» [8] – в цьому документі вперше зустрічається термін «національна система кібербезпеки», куди входять головні учасники процесу захисту прав і свобод осіб у відносинах із приводу обробки й обміну інформацією у кіберпросторі [5, с. 90]. Зокрема, у Стратегії зазначається, що основу системи суб'єктів забезпечення кібербезпеки становлять Міністерство оборони (МО) України, Державна служба спеціального зв'язку та захисту інформації (ДСС) України, Служба безпеки (СБ) України, Національна поліція (НП), Нацбанк України, розвідувальні органи, на які мають бути покладені в установленому законом порядку спеціальні завдання. Натомість ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» передбачає дещо інший перелік основних суб'єктів забезпечення кібербезпеки, що окремо виділяються в рамках загальної системи суб'єктів забезпечення кібербезпеки, передбаченої ст. 5 того ж Закону. До їх кола віднесено: РНБО України, Міністерство внутрішніх справ (МВС) України, МО України, Генеральний штаб ЗС України, СБ України, ДСС України, розвідувальні органи тощо [7]. Ключова роль цих відомств у забезпеченні кібербезпеки зумовлена специфікою їх компетенції та основних напрямів діяльності, зокрема можливістю вживати спеціальні заходи (у т. ч. й заходи примусу) для підтримки належного рівня кібербезпеки, реалізуючи відповідну монополію держави.

Призначенням ДСС України є забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону. ДСС України входить до складу сектору безпеки і оборони України. У сфері забезпечення кібербезпеки ДСС України займається формуванням і реалізацією політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення і реагування на кіберінциденти та кібератаки й усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури тощо [9].

НП і СБ України наділенні повноваженнями щодо припинення правопорушень, що посягають на кібербезпеку, та притягнення винних осіб до відповідальності. Зокрема, НП у сфері забезпечення кібербезпеки наділена повноваженнями щодо: забезпечення прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі [7; 10]. У своїй діяльності НП підпорядковується КМ України і спрямовується та координується через МВС України, на яке покладається реалізація повноважень щодо: створення і забезпечення функціонування підрозділів із протидії кіберзлочинності; розробки та реалізації комплексу організаційних і практичних заходів, спрямованих на боротьбу з кіберзлочинами; створення і забезпечення функціонування цілодобової контактної мережі для надання невідкладної допомоги у розслідуванні кіберзлочинів тощо [7; 11].

СБ України наділена повноваженнями щодо протидії правопорушенням у кіберпросторі відповідно до своєї компетенції. Призначенням СБ України є забезпечення державної безпеки, тож

у Законі України «Про основні засади забезпечення кібербезпеки України» закріплено, що СБ України здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні й оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом і кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак і кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки [7; 12].

Якщо говорити про повноваження МО України та Генерального штабу ЗС України у сфері забезпечення кібербезпеки, то слід зазначити, що відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» вони є майже ідентичними: зазначені державні органи здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану [7; 11]. Водночас відповідні повноваження реалізуються кожним із цих державних органів у межах його законодавчо визначеної компетенції, відтак МО є координаційним політичним центром, котрий реалізує політику держави у сфері забезпечення кібербезпеки, тоді як Генеральний штаб є оперативним органом, діяльність якого спрямована на подолання реальної агресії та виконання бойових завдань у випадках, передбачених законодавством [5, с. 99].

Розвідувальні органи (Служба зовнішньої розвідки України, розвідувальні органи МО, розвідувальні органи спеціально уповноваженого центрального органу виконавчої влади у справах охорони державного кордону [5, с. 200]) здійснюють у сфері забезпечення кібербезпеки розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки [7; 11].

Важливе місце у системі забезпечення кібербезпеки займає Нацбанк України, який розробляє та впроваджує у свою діяльність сучасні електронні банківські технології, новітні платіжні й облікові системи тощо. Оскільки основною функцією Нацбанку відповідно до Конституції України [13] є забезпечення стабільності грошової одиниці України, у сфері забезпечення кібербезпеки на нього покладається: формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері; визначення порядку, вимог і заходів із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, контроль їх виконання; створення центру кіберзахисту Нацбанку, забезпечення функціонування системи кіберзахисту у банківській системі України тощо [7].

Як зазначає В. Бурячок, досвід іноземних країн та особливості українських реалій свідчать, що розв'язання основних завдань кібербезпеки неможливе без створення: міжвідомчого структурного органу, який на постійній основі забезпечував би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки; центральних органів у структурі певних відомств, правоохоронних і силових структур України з функціями виявлення й оцінювання рівня (визначення ступеня) критичності стороннього кібервпливу, розроблення концептуальних засад і надання рекомендацій щодо протидії його проявам, а також активної протидії кібератакам протиборчих сторін і впливу на їх інформаційно-телекомунікаційні системи; органів власної інформаційної та кібербезпеки – державних установ (відомств) і комерційних структур, які повинні тісно взаємодіяти із зазначеними центральними органами з питань вироблення єдиної політики щодо захисту як власного, так і спільного національного інформаційного і кіберпросторів [14, с. 8–9].

Необхідно зазначити, що координаційні структури, які об'єднують і спрямовують діяльність суб'єктів забезпечення кібербезпеки, нині створені й успішно працюють вже у багатьох країнах. Так, у 2017 р. в Таллінні був створений Об'єднаний центр передових технологій із кібероборони НАТО. Центр отримав акредитацію НАТО, налічує 20 учасників – 17 членів НАТО і 3 – держави-партнера. Основне завдання Центру – тренування фахівців із різних країн, які забезпечують безпеку в національному кіберпросторі. У Литві Міністерству оборони надано право координувати національну політику з кібербезпеки, передбачається

установа Національного центру кібербезпеки, створення Консультативної ради з кібербезпеки при Міністерстві оборони. У Чехії у 2017 р. створено Національний офіс із кібербезпеки та інформації, до функцій якого входить вирішення проблем кібербезпеки, підтримка державних установ і підприємств в разі кібератак, профілактика злочинів у кіберпросторі, забезпечення безпеки інформаційної інфраструктури [15].

У 2017 р. Президент України підписав Указ «Про Національний координаційний центр кібербезпеки», яким затверджено Положення про вказаний центр. До його основних завдань належить аналіз стану кібербезпеки, результатів проведення огляду національної системи кібербезпеки, стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам, стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури, даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо. Відповідно до Указу Президента України № 27/2020 [16] штат апарату РНБО розширено до 190 співробітників для забезпечення інформаційно-аналітичного, експертного, організаційного, матеріально-технічного забезпечення Центру, розширено повноваження Центру, який координує та контролює роботу суб'єктів сектору безпеки і оборони у сфері кібербезпеки.

Втім, слід зауважити, що відповідні законодавчі новації, особливо у контексті змісту внесеного Президентом України законопроекту № 3196 [17], зумовлюють ризик взаємного дублювання повноважень Центру кібербезпеки, СБ України та ДСС України. Тож відповідна проблема підлягає врегулюванню в ході подальшого вдосконалення системи суб'єктів забезпечення кібербезпеки. Так само потребують вдосконалення та розвитку питання державно-приватного партнерства у сфері кібербезпеки.

Висновки. Ризик кіберзагроз є актуальним для значної кількості суб'єктів: від приватних осіб до великих компаній, окремих галузей економіки та держав загалом. На національному та міжнародному рівні наявне усвідомлення того, що проблеми кібербезпеки можуть завдати шкоди національній безпеці та дієвому функціонуванню економіки держави. Тож ефективна організація системи суб'єктів забезпечення кібербезпеки набуває в сучасному світі непересічного значення. Вдосконаленню її діяльності має сприяти розмежування компетенції державних органів, які є суб'єктами забезпечення кібербезпеки, та розвиток державно-приватного партнерства.

Список літератури:

1. Ліпкан В.А., Ліпкан О.С. Національна і міжнародна безпека у визначеннях та поняттях. Київ : Текст, 2008. 400 с.
2. Тімкін І.Ф., Новікова Н.Є. Структурно-функціональна характеристика системи забезпечення національної безпеки України. URL: er.nau.edu.ua.
3. Політологія : навчальний посібник. Київ : Знання, 2010. 415 с.
4. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 422 с.
5. Бухарєв В.В. Адміністративно-правові засади забезпечення кібербезпеки України : дис. ... канд. юрид. наук : 12.00.07. Суми, 2018. 221 с.
6. Ткачук Т.Ю. Суб'єкти забезпечення інформаційної безпеки держави: функціональний аналіз. *Jurnalul juridic national: teorie şi practică.* 2017. № 6. С. 42–46.
7. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19.
8. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України». URL: https://zakon5.rada.gov.ua/laws/show/96/2016.
9. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України». URL: https://zakon.rada.gov.ua/laws/show/3475-15.
10. Закон України «Про національну поліцію». URL: https://zakon.rada.gov.ua/ laws/show/580-19.
11. Закон України «Про національну безпеку України». URL: https://zakon.rada.gov.ua/laws/show/2469-19.
12. Закон України «Про Службу безпеки України». URL: https://zakon.rada.gov.ua/laws/show/2229-12.
13. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/ 254%D0%BA/96-%D0%B2%D1%80.
14. Бурячок В.Л., Гнатюк С.О., Корченко О.Г. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки. *Інформаційна безпека: виклики і загрози сучасності* : зб. матеріалів наук.-практ. конф., 5 квітня 2013 р., м. Київ. Київ : Наук.-вид. центр НА СБ України, 2013. 416 с.

15. Ковалев А.А., Балашов А.И., Международно-правовые аспекты политики кибербезопасности некоторых европейских стран бывшего советского блока. *Вестник Поволжского института управления.* 2018. Т. 18. № 5. С. 105–114.

16. Указу Президента України № 27/2020 «Про внесення змін до Указів Президента України від 27 січня 2015 р. № 37 та від 7 червня 2016 р. № 242». URL: https://www.president.gov.ua/ documents/ 272020-32041.

17. Проект Закону про внесення змін до Закону України «Про Службу безпеки України» щодо удосконалення організаційно-правових засад діяльності Служби безпеки України (реєстр. № 3196). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68347.

Tarasuk A.V. CYBER SECURITY SYSTEM SUBJECTS IN UKRAINE

The aim of the article is to study the legally defined system of cybersecurity entities in Ukraine. The rapid technological progress has led to the emergence of new threats to both social and individual security, resulting in a familiar reality for the first time in world history, augmented by virtual reality – cyber reality. Cyber threats have revolutionized people's perceptions of security, rules and methods of national security. Therefore, cyber security issues are of particular importance, becoming an integral part of national security, and cyber threats are being developed and implemented at the state level. In our country, the Law of Ukraine "On the Fundamentals of Cybersecurity of Ukraine" was adopted for these purposes, which, in particular, establishes a system of cybersecurity entities. The cybersecurity system is an organic combination of the common goal of governmental and non-governmental institutions, as well as other entities involved in cybersecurity activities. At the same time, the spectrum of cybersecurity entities cannot be limited solely by government agencies and their officials. Cybersecurity entities distinguish between general and special entities. The latter include public authorities that, in addition to general functions, are empowered to combat cybercrime and cyber-terrorism, as well as to provide cybernetic protection for national critical infrastructure. Currently, cyber threats are relevant to a large number of entities, from individuals to large companies, individual industries, and states as a whole, so effective organization of the cybersecurity entities is of paramount importance in the modern world.

Key words: *cybersecurity, cybersecurity systems, cybersecurity entities, cyber threats.*