проект

РІШЕННЯ

Міжнародної науково-практичної конференції
«Глобальні виклики європейської безпеки. Роль громадських організацій у протидії екологічному, аерокосмічному і кібертероризму»
(Україна, Київ, 5 жовтня 2018 г.)

Ми, учасники Міжнародної науково практичної конференції «Глобальні виклики європейської безпеки. Роль громадських організацій у протидії екологічно-му, аерокосмічному і кібертероризму» переконані, що стрімкий розвиток глобалізованого інформаційного простору спричинює загрози для суспільства у випадку своєчасно не розроблених заходів безпеки новітнім технологіям, які беруть на озброєння адепти міжнародного тероризму.

Сьогодні спостерігається сплеск розширення масштабів тероризму, різноманітності його форм і засобів реалізації на морі, на суші, у повітрі, в інформаційному просторі. Особливу загрозу всьому живому становить погіршення екології, перенесення у космічний простір сфер збройної, інформаційної, радіоелектронної боротьби і розвідки.

Уважаємо за необхідне невідкладно розпочати розроблення нової архітектури європейської системи безпеки, в якій найважливішим складником протидії тероризму має стверджуватися активна позиція громадських інститутів суспільства.

Як першочергові заходи пропонуємо:

у галузі екологічної безпеки:

- вирішення проблеми запобігання «екологічному тероризму» у тісній взаємодії всіх страт суспільства кожної країни за умови обов'язкової координації дій з представниками світової спільноти;
- визнання прямого зв'язку між «екологічною безпекою» і «екологічним тероризмом» (відповідно до Статуту ООН і принципів міжнародного права у контексті національної безпеки держави, Європейського товариства);
- введення у право термінологічної дефініції «екологічний тероризм», що означає незаконне або зумисне заподіяння значної шкоди довколишньому природному середовищу з метою залякування населення, примусу уряду, міжнародних організацій до здійснення певних дій або утримання від їх вчинення. Поняття «екологічний тероризм», як кримінальний злочин, вимагає або виділення його зі складу поняття «тероризм» або введення нової кваліфікаційного ознаки у його тлумачення;
- запровадження більш жорстких санкцій за шкоду екології конкретної країни, оскільки такі збитки мають не лише регіональні, але й глобальні наслідки;
- розроблення на основі застосовування методів системного аналізу стратегії і заходів запобігання і боротьби з екологічним тероризмом (еколого-правові, кримінально-правові, міжнародно-правові аспекти), використання соціологічних методів (соціологічне опитування у формі анкетування та інтерв'ювання), а також

проведення моніторингу об'єктів критичної інфраструктури та навколишнього середовища, комп'ютерного моделювання;

- проведення системних попереджувальних заходів і боротьби з «екологічним тероризмом» у будь-яких його проявах: біологічний, хімічний, техногенний, радіаційний тощо;
- розмежування на законодавчому рівні понять «екологічний тероризм» та «екологічний активізм» (радикалізм), яким характеризують надмірні дії представників «зелених», засобів масової інформації, пов'язані з прагненням привернути увагу суспільства до певної екологічної проблеми і сформувати громадську думку щодо неї;
- інформування населення щодо екологічної безпеки, зокрема про стан довколишнього середовища, рівень безпеки потенційних об'єктів екологічних терористичних атак;
- ініціювання створення «Екологічної конституції Землі» із залученням фахівців світового рівня з правової та міжнародної екологічної безпеки;

у галузі кібербезпеки:

- завершення законодавчого врегулювання питань забезпечення кібербезпеки і протидії кібертероризму, зокрема, щодо визначення та захисту об'єктів критичної інфраструктури, ушкодження яких може створювати ситуацію, загрозливу для національної безпеки;
- удосконалення законів і нормативно-правових актів України у сфері кібербезпеки і запровадження практики застосування дієвих механізмів міжнародно-правової відповідальності за кібертероризм;
- ініціювання невідкладного створення Національного центру оперативно-технічного управління мережами телекомунікацій України в умовах надзвичайної ситуації, надзвичайного та воєнного стану, та забезпечення його дієвої взаємодії з центрами управління операторів телекомунікацій, в тому числі й іноземних;
- організацію підвищення кваліфікації фахівців з питань кібербезпеки (кіберзахисту) в державних органах влади, у CERT-UA – підрозділі Державного центру кіберзахисту Держспецзв'язку;
- забезпечення переходу України в пост-антивірусний простір і створення національного антивірусного продукту;
- створення належної навчальної бази спеціалістів у галузі кібербезпеки та забезпечити підготовки висококваліфікованими фахівцями з питань кібер- та інформаційної безпеки у закладах освіти;

у галузі аерокосмічної безпеки:

- встановлення загроз і чинників ризику можливих кіберінцидентів, пов'язаних з польотами і діяльністю критично важливих систем цивільної авіації і космонавтики, визначення можливих наслідків таких інцидентів;
- окреслення кола обов'язків національних органів у галузі аерокосмонавтики щодо вжиття заходів із забезпечення кібербезпеки;
- заохочення вироблення державами-членами аерокосмічного клубу спільного розуміння проблем кібербезпеки і чинників ризику, загальних критеріїв визначення важливості об'єктів і систем, що потребують захисту;
- заохочення координації дій між державними органами та аерокосмічної галуззю з вироблення стратегії, політики і планів забезпечення кібербезпеки, а

також обміну інформацією, необхідною для виявлення критично вразливих аспектів, які потрібно усунути;

- створення державно-галузевого партнерства і механізмів взаємодії на національному та міжнародному рівнях задля систематичного обміну інформацією у галузі кібербезпеки щодо інцидентів, тенденцій і заходів протидії;
- використання гнучкого, ґрунтованого на оцінці ризиків, підходу до захисту критично важливих авіаційних систем, виробленого на основі єдиного розуміння кіберзагроз та чинників ризику, шляхом упровадження управління кібербезпекою;
- заохочення розвитку в національній аерокосмічній галузі стійкої культури кібербезпеки на всіх рівнях, підвищення ролі громадських організацій у забезпеченні кібербезпеки;
- сприяння розробленню та впровадженню міжнародних стандартів, стратегій і кращих практик у сфері захисту критично важливих систем інформації та зв'язку, що застосовуються у цивільній авіації, від актів втручання, які можуть загрожувати безпеці польотів цивільної авіації;
- співпраця у розробленні програми ІКАО в сфері кібербезпеки згідно з єдиним, комплексним і функціональним підходом, що включає галузі аеронавігації, зв'язку, спостереження, експлуатації повітряних суден, професійної (льотної) придатності та інші відповідні дисципліни, на основі реалізації Глобального плану з авіаційної безпеки, прийнятого ІКАО у 2017 р. і Резолюції ІКАО (А39-19);

Пропонуємо країнам-учасницям космічного клубу:

- об'єднати зусилля щодо запобігання фактів космічного тероризму, як у близькому, так і в далекому Космосі;
- розробити стратегію запобігання незаконним «захопленням» космічних апаратів на робочих орбітах з метою їх використання у подальшому для атаки космічних і наземних об'єктів;
- виступити з ініціативою розроблення правил поведінки в космічному просторі запобігання незаконному наближенню до космічних об'єктів інших країн з метою інформаційного тероризму;
- заборонити на міжнародному рівні приватним космічним компаніям запускати в космічні апарати, які не мають необхідних ліцензій і дозволів на розміщення таких апаратів у космічному просторі.

За дорученням учасників Конференції

Президент МГО «Международна антитерористична єдність», доктор філософії
Олександр Дічек

Президент ГО «Соціальна справедливість», доктор філософії
Алла Шлапак