Зінченко Олександра Ігорівна

Аспірантка кафедри політології Філософського факультету ХНУ ім. В.Н.Каразіна

Харків

https://orcid.org/0000-0003-1623-957X

КОМПЛЕКСНИЙ ВПЛИВ КІБЕРТЕРОРИЗМУ НА ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО

Оскільки епоха цифрових технологій продовжує розвиватися, змінюється і ландшафт загроз, які її супроводжують. Кібертероризм, загрозливий привид, що переслідує коридори Інтернету, створює значні проблеми для політичної, економічної технологічної та інших структур нашого суспільства. У цифрову еру кібертероризм постає як комплексна загроза, яка кидає виклик основам нашого інформаційного суспільства. У цій роботі досліджується багатогранна природа кібертероризму, розкриваються його економічні, технологічні та політичні наслідки в усьому світі. Вплив кібертероризму охоплює значну частину проблем від порушення критичної інфраструктури до маніпулювання громадською думкою, що підкреслює необхідність комплексних стратегій для пом’якшення його ризиків [1].

Досліджуючи феномен кібертероризму, можно побачити значну еволюцію від простих незручностей до складних атак, здатних паралізувати критичну інфраструктуру. Спочатку кібертерористи брали участь у актах цифрового вандалізму, псуючи веб-сайти для поширення політичних чи ідеологічних повідомлень. Однак з тих пір ця тактика посилилася, включивши атаки програм-вимагачів, розподілені напади на відмову в обслуговуванні (DDoS) і злами, спрямовані на викрадення конфіденційної інформації [2, c.11]. Ці передові загрози використовують вразливі місця в нашій цифровій інфраструктурі, підкреслюючи нагальну потребу в надійних заходах кібербезпеки.

Критичні інфраструктури, такі як електромережі, транспортні мережі та фінансові установи, особливо вразливі. Атака на ці системи може призвести до повсюдного хаосу, порушуючи основні послуги та завдаючи значних економічних збитків. У відповідь на ці нові загрози швидко розвиваються оборонні технології та стратегії. Штучний інтелект і алгоритми машинного навчання розгортаються для виявлення аномалій і прогнозування потенційних атак.

Говорячи про економічні наслідки кібертероризму, важливо зазначити, що вони є глибокими та далекосяжними. Прямі фінансові втрати від атак можуть бути приголомшливими, включаючи витрати на відновлення, втрату доходу через простої та витрати, пов’язані з посиленням заходів безпеки. Компанії та уряд однаково несуть основний тягар цих витрат, які можуть досягати мільйонів або навіть мільярдів доларів. Крім безпосереднього фінансового впливу, кібертероризм завдає шкоди економіці в цілому, адже довіра споживачів може різко впасти внаслідок резонансних атак, що призведе до зменшення витрат та інвестицій. У довгостроковій перспективі повторювані інциденти кібертероризму можуть підірвати довіру до цифрових платформ і послуг, потенційно затримуючи зростання цифрової економіки. За іронією долі, загроза кібертероризму також стимулювала зростання ринку кібербезпеки. Оскільки організації намагаються захистити себе, попит на інноваційні рішення безпеки стрімко зростає. Ця динаміка відкриває можливості для технологічних інновацій та економічного зростання в секторі кібербезпеки, хоча й на тлі підвищеного ризику.

Вплив кібертероризму поширюється й на політичну сферу, зриваючи вибори, поширюючи дезінформацію та вторгаючись у приватне життя, тим самим підриваючи довіру до політичних інститутів.

Отже, можемо зробити висновок, що кібертероризм представляє собою складний виклик інформаційному суспільству зі значними економічними, технологічними та політичними наслідками. Подолання цієї загрози потребує багатогранного підходу, який використовує технологічні інновації, регулятивні дії та залучення суспільства. Оскільки ми переходимо в епоху цифрових технологій, сприяння стійкості проти кібертероризму буде ключовим фактором для збереження нашого економічного процвітання, технологічного прогресу та політичної стабільності. Завдяки постійним дослідженням, співпраці та пильності ми можемо сподіватися пом’якшити ризики та використати можливості, які надає наш все більш взаємопов’язаний світ.

Література

1. Iftikhar S. Cyberterrorism as a global threat: a review on repercussions and countermeasures. PeerJ Comput Sci. 2024 Jan 15;10:e1772. doi: 10.7717/peerj-cs.1772. PMID: 38259881; PMCID: PMC10803091. (date of access: 05.08.2024).
2. NAZARIO J. Politically Motivated Denial of Service Attacks. Arbor Networks, United States. URL: https://ccdcoe.org/uploads/2018/10/12\_NAZARIO-Politically-Motivated-DDoS.pdf (date of access: 05.08.2024).