Biuletyn Informacji Publicznej Szkoły Głównej Gospodarstwa Wiejskiego

Adres artykułu: https://bip.sggw.edu.pl/artykul/cyberinformacja-wspolczesna-bron

Cyberinformacja – współczesna broń

Nieustanny rozwój technologii informacyjnych, społeczeństwa informacyjnego oraz cyberprzestrzeni niesie ze sobą wiele nadziei, ale także obaw. Pandemia COVID-19 czy pełnoskalowa wojna w Ukrainie doprowadziły do intensyfikacji działań w cyberprzestrzeni i uwidoczniły wiele zagrożeń. Jednym z nich jest negatywne wykorzystanie informacji, o czym

opowiedział dr Wojciech Mincewicz z Katedry Socjologii Instytutu Nauk Socjologicznych i Pedagogiki Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie.

Współczesna broń

Współczesne środowisko informacyjne podlega dynamicznym przemianom. Ich źródłem jest przede wszystkim postęp technologiczny i stały wzrost znaczenia cyfrowych kanałów komunikacji. W rezultacie zagrożenia w przestrzeni informacyjnej przyjmują formę cyberzagrożeń, które nie tylko zagrażają infrastrukturze teleinformatycznej, ale także podważają zaufanie do instytucji publicznych, procesów demokratycznych i spójności społecznej. Cyberzagrożenia w warstwie informacyjnej obejmują szerokie spektrum działań, od technicznych ataków typu DDoS, Ransomware, przez szpiegostwo elektroniczne, po zaawansowane kampanie dezinformacyjne nakierowane na manipulowanie opinią publiczną. Za tego typu działania odpowiada szerokie grono aktorów. Cyberprzestrzeń stała się bowiem dziś polem operacyjnym dla wielu graczy o często sprzecznych interesach – od rządów i służb specjalnych, przez korporacje i zorganizowane grupy hakerskie, aż po indywidualnych aktywistów i przestępców działających anonimowo.

– *Na podstawie analiz i doświadczeń z ostatnich lat można wyróżnić konkretne narzędzia i systemy wykorzystywane w działaniach prowadzonych w cyberprzestrzeni, zwłaszcza w obszarze walki informacyjnej* – mówi **dr Wojciech Mincewicz** z Katedry Socjologii Instytutu Nauk Socjologicznych i Pedagogiki Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie. – *Do takowych zalicza się: narzędzia informatyczne służące do testowania luk w zabezpieczeniach; ukryte sieci wykorzystywane do globalnego cyberszpiegostwa; oprogramowania do eksploracji danych zarówno jawnych, jak i ukrytych; sieci Internetów zapewniające anonimowość działań oraz szyfrowanie. Wszystkie wymienione pozwalają na skuteczne prowadzenie operacji wywiadowczych, destabilizowanie systemów państwowych, a także dezinformowanie społeczeństwa. Co istotne, wiele z tych rozwiązań pozostaje niewidocznych dla przeciętnego użytkownika, co dodatkowo zwiększa ich skuteczność i trudność w przeciwdziałaniu. Ich użycie często odbywa się poniżej progu otwartego konfliktu, co sprawia, że trudno przypisać odpowiedzialność i podjąć adekwatną reakcję.*

Socjotechniki w manipulacji

Wymiar technologiczny zagrożeń bezpieczeństwa informacyjnego cyberprzestrzeni w sposób integralny uzupełniany jest o socjotechniczne narzędzia oddziaływania. Cyberzagrożenia coraz częściej opierają się na manipulacji emocjami, tożsamością i przekonaniami odbiorców. Techniki inżynierii społecznej, *phishing* (fałszywe wiadomości wyłudzające dane), *spoofing* (podszywanie się pod zaufane źródła) czy *deepfake'i* (realistycznie podrobione nagrania) stają się narzędziami w rękach zarówno przestępców, jak i państwowych agencji wywiadowczych. Skuteczność tych metod zwiększa się w środowisku nadmiaru informacji i spadku zaufania do tradycyjnych źródeł wiedzy. W kontekście bezpieczeństwa informacyjnego państw, szczególne zagrożenie stanowi możliwość masowego wycieku wrażliwych danych oraz rosnące znaczenie whistleblowingu. Historyczne przykłady takie jak WikiLeaks, Edward Snowden czy Chelsea Manning wskazują, że jednostki dysponujące odpowiednią wiedzą i narzędziami mogą realnie wpływać na politykę międzynarodową, ujawniając nielegalne lub nieetyczne praktyki rządów i organizacji.

Zintegrowana, długotrwała kampania generuje konsekwencje, które mogą mieć różny charakter, poczynając od zniszczenia autorytetu instytucji państwowych, przez polaryzację społeczną, po osłabienie spoistości informacyjnej państw.

Polityka cyberbezpieczeństwa

– *W warunkach współczesnego społeczeństwa informacyjnego skuteczna polityka bezpieczeństwa wymaga nie tylko rozwiązań technologicznych, ale także dogłębnego rozpoznania procesów kulturowych, edukacyjnych i psychologicznych, które wpływają na podatność społeczną na manipulację informacyjną* – tłumaczy dr W. Mincewicz. – *Z tego względu cyberzagrożenia w warstwie informacyjnej nie mogą być traktowane jedynie jako problem techniczny. Konieczne jest, aby były rozpatrywane w szerszym kontekście ładu informacyjnego, suwerenności poznawczej oraz nowoczesnych form konfliktu, w których granica między wojną a pokojem staje się coraz bardziej nieostra. Rozwój technologii cyfrowej, postępująca globalizacja komunikacji oraz rosnąca rola danych w życiu społecznym i politycznym sprawiły, że informacja stała się jednym z kluczowych zasobów w nowoczesnych konfliktach, zarówno na poziomie jednostkowym, jak i systemowym*. *W tym kontekście cyberzagrożenia informacyjne stanowią poważne wyzwanie dla państw, organizacji i społeczeństw, prowadząc do zniszczenia zaufania, destabilizacji ładu publicznego oraz rozmycia granic między informacją a dezinformacją.*

Cyberzagrożenia informacyjne obejmują działania prowadzone za pośrednictwem przestrzeni cyfrowej, których celem jest naruszenie integralności, poufności lub dostępności informacji. Zagrożenia te nie wynikają wyłącznie z ataków na

infrastrukturę techniczną, lecz rozwijają się dynamicznie, między innymi poprzez manipulację treścią komunikatów, kształtowanie percepcji oraz wpływanie na procesy decyzyjne. W praktyce przejawiają się one między innymi w stosowaniu botów funkcjonujących także w ramach farm trolli, rozpowszechnianie fałszywych informacji (fake news) oraz wykorzystanie deepfake. Mechanizmy te służą do polaryzowania opinii publicznej, osłabiania zaufania społecznego oraz podważania legitymizacji instytucji państwowych.

Psychologia społeczna

Równolegle stale na znaczeniu zyskują działania wykorzystujące psychologię społeczną, jak np. inżynieria społeczna, która, operując na błędach poznawczych i emocjach użytkowników, skutecznie obchodzi zabezpieczenia technologiczne. W tym kontekście człowiek nadal pozostaje najsłabszym ogniwem systemu bezpieczeństwa. Studium przypadku poszczególnych incydentów oraz realizowane w następstwie analizy jednoznacznie wskazują, że zdecydowana większość incydentów informacyjnych wynika z błędów ludzkich, a nie przełamania zabezpieczeń technologicznych.

Szczególnie niepokojącym obszarem cyberzagrożeń są działania ukierunkowane na informację niejawną oraz poufną, których wyciek może prowadzić do utraty kontroli państwa nad obiegiem strategicznych danych.

W odpowiedzi na te wyzwania niezbędne staje się podejście holistyczne: integrujące działania legislacyjne (np. RODO), technologiczne (monitoring, szyfrowanie, wykorzystanie AI w analizie zagrożeń) oraz edukacyjne (budowanie świadomości i odporności poznawczej użytkowników) – dodaje dr Wojciech Mincewicz z SGGW.

Konsultacja merytoryczna i materiały:

dr Wojciech Mincewicz

Katedra Socjologii

Instytut Nauk Socjologicznych i Pedagogiki SGGW

Metryczka

Opublikował w BIP:	Dorota Sokół

Data opublikowania:	28.07.2025 15:59
Data ostatniej aktualizacji:	28.07.2025 16:03
Liczba wyświetleń:	6