NCI

Narodowy Instytut Cyberbezpieczeństwa

Opracowanie _kwartalne

PAŹDZIERNIK – GRUDZIEŃ 2020

vol. IV

Sfinansowano przez Narodowy Instytut Wolności - Centrum Rozwoju Społeczeństwa Obywatelskiego ze środków Programu Rozwoju Organizacji Obywatelskich na lata 2018 - 2030.

Spis treści

Adres

ul. Mglista 14a/12,
53-020 Wrocław, Polska

Kontakt

Tel: +48 574 923 305
E-mail: kontakt@nci.org.pl

Online

Strona: www.nci.org
Podcast: wwww.anchor.fm/nci

Info & cyber security: chińsko-rosyjskie zagrożenia i japońska szansa dla Polski i Europy

Drodzy Czytelnicy,

Zbliżający się koniec roku 2020 przyniósł informację o skutecznych szczepionkach na COVID-19, w tym o dopuszczeniu ich do użytku oraz rozpoczęciu stosowania jednej z nich w Wielkiej Brytanii. Podobną ścieżką podążą zapewne wkrótce także i inne państwa. Jednocześnie w Stanach Zjednoczonych Federalna Komisja Handlu oraz 48 stanów i terytoriów USA złożyło pozwy przeciwko Facebookowi, mogące doprowadzić do podziału tej firmy. Sytuacja z firmą Marka Zuckerberg będzie pewnego rodzaju papierkiem lakmusowym dla oceny ewolucji podejścia rządów krajowych do wielkich firm technologicznych. Z racji utrzymującej się wciąż pandemii, aktualny pozostaje temat pracy zdalnej i zagrożeń z nią związanych. W sposób szczególny odnosi się to do organizacji pozarządowych. Z tego też powodu polecamy analizę pt. *Zagrożenia i profilaktyka zagrożeń IT w organizacjach pozarządowych.* Rozwinięciem wątku związanego z cyberbezpieczeństwem użytkowników indywidualnych jest kolejna publikacja o charakterze analitycznym, zatytułowana *Komunikatory – wady, zalety, bezpieczeństwo danych.* Porównane zostają w niej najpopularniejsze aplikacje, jak:
Facebook Messenger, Whatsapp, Telegram, Signal, WeChat czy Threema.

Szczególnie uwzględniona została tu kwestia prywatności danych.
Dalsza część poświęcona została bezpieczeństwu informacyjnemu *Komentarz pt. Mgła tajemnicy i milczenia wokół rosyjskich cyberwojsk* odnosi się do zagadnienia rosyjskich działań i wykładni łączących komponenty informacyjne i cybernetyczne. W sposób szczególny chcemy także polecić wywiad z Alicją Bachulską, poświęcony chińskim oddziaływaniom informacyjnym w Polsce, z uwzględnieniem kontekstu i porównania z bardziej zaawansowanymi (przynajmniej na chwilę obecną) działaniami rosyjskimi.

Na koniec natomiast, przygotowaliśmy obszerną analizę pt. *Bezpieczeństwo informacyjne jako wektor współpracy dla Japonii i Europy,* która porusza temat wspólnych wyzwań, interesów i możliwości dla państw europejskich indywidualnie oraz Unii Europejskiej jako całości oraz Kraju Kwitnącej Wiśni.

Zapraszamy do lektury!

Zespół Narodowego Instytutu Cyberbezpieczeństwa

Zagrożenia i profilaktyka zagrożeń IT w organizacjach pozarządowych

Niezwykle dynamiczny rozwój sektora ICT, powstanie kolejnych kanałów społecznościowych, a zwłaszcza pojawienie się pandemii i wzrost skali pracy czy nauki zdalnej w 2020 roku spowodowały, że pojęcie cyberbezpieczeństwa w NGO nabrało nowego wymiaru. Pojawiły się nowe formy zagrożenia. Z drugiej strony wdrażane są działania profilaktyczne, które mogą skutecznie niebezpieczeństwom przeciwdziałać.

Z pojęciem cyberbezpieczeństwa w organizacji pozarządowej wiąże się sporo zagadnień. To między innymi: dane osobowe, urządzenia, sieci komputerowe, płatności internetowe, bankowość elektroniczna czy profilaktyka w zakresie ochrony przed wirusami i instalacją złośliwego oprogramowania. Niniejsza analiza przedstawia w sposób praktyczny najważniejsze zagadnienia dotyczące potencjalnych zagrożeń i działań profilaktycznych umożliwiających bezpieczne funkcjonowanie NGO w przestrzeni cyfrowej.

Bezpieczne dane osobowe – kategorie, proces administracji, przetwarzanie

Za dane osobowe (DO) uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (Art. 6 ust. 1 UODO). Proces przetwarzania DO dotyczy w szczególności operacji w systemach IT. Można powiedzieć, że to integracja urządzeń, programów, procedur przetwarzania informacji i odpowiednich narzędzi wdrożonych w celu przetwarzania DO.

Dane osobowe możemy podzielić na dwie podstawowe kategorie: dane zwykłe i tzw. szczególna kategoria danych, określana jako dane wrażliwe. Do danych zwykłych zaliczamy: imię i nazwisko, adres zamieszkania, Pesel, NIP, numer i seria dowodu osobistego, wykształcenie, zawód, płeć, numer telefonu. Szczególna kategoria danych (dane wrażliwe/ sensytywne) obejmuje: pochodzenie rasowe lub etniczne; poglądy polityczne; przekonania religijne lub filozoficzne; przynależność wyznaniowa, partyjna; stan zdrowia; kod genetyczny; nałogi; życie seksualne; skazania, orzeczenia o ukaraniu; mandaty, orzeczenia wydane przed sądem lub urzędem.
Integralnymi elementami procesu przetwarzania DO są zdefiniowane czynności, takie jak: zbieranie i pozyskiwanie; utrwalanie i opracowywanie; przechowywanie; modyfikacja; udostępnianie oraz usuwanie danych osobowych. Absolutnie trzeba wspomnieć o przypadkach, w których można zgodnie z prawem przetwarzać dane osobowe (Art. 6 RODO). Będą to m.in. następujące kryteria:

Kryteria zgodnego z prawem przetwarzania danych osobowych

1. Wyrażenie zgody na przetwarzanie,

2. Konieczność realizacji umowy lub podjęcia działań przed jej zawarciem,

3. Wypełnienia obowiązku prawnego nałożonego na administratora,

4. Ochrona żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,

5. Realizacja zadania realizowanego w interesie publicznym,

6. Cele wynikające z prawnie uzasadnionych interesów.

Czy jesteś gotowy na RODO?

6 prostych zasad

» Źródło: grafika CloudForum

Zidentyfikuj jakie dane przechowujesz

Należy wiedzieć, skąd pochodzą różne komponenty danych klientów oraz gdzie są przechowywane. W dużych organizacjach może to oznaczać konieczność śledzenia ścieżki, którą dane przechodzą przez wiele różnych systemów.

Zidentyfikuj, w jaki sposób dane są wykorzystywane

Co dzieje się z danymi, gdy już znajdą się w posiadaniu organizacji? Jak się je wykorzystuje i w jakim celu? Czy i w jaki sposób są przekształcane? Z jakimi procesami w organizacji są powiązane?

Upewnij się, że możesz udowodnić zgodność z RODO

Do tego konieczne jest zapewnienie skutecznego systemu raportowania i kontroli sposobu korzystania z danych osobowych, kolejne wyzwanie logistyczne w dużych organizacjach. Jak można zmodyfikować systemy w organizacji, aby zapewnić pełną ścieżkę audytu informacji wymaganych do raportowania zgodności z RODO.

Upewnij się, że dane są bezpiecznie przechowywane

Należy upewnić się, że każda platforma analityczna w organizacji jest odpowiednio zintegrowana z systemami bezpieczeństwa oraz możliwości skutecznego kontrolowania, tego, kto ma dostęp do danych klientów. Dane klienta muszą być szyfrowane i przechowywane bezpiecznie na wszystkich etapach cyklu analitycznego, nie tylko w miejscu ich gromadzenia.

Pozyskane zgody

Upewnij się, że wyraźnie zażądano zgody tam, gdzie dane zostały zebrane i czy została ona pozyskana. Zgodnie z rozporządzeniem zgoda może zostać odwołana w dowolnym momencie, więc potrzebny jest sposób śledzenia nie tylko tego, czy osoba pierwotnie wyraziła zgodę, ale również czy od tego czasu nie cofnęła zgody.

Upewnij się, że możesz monitorować zgodność z RODO na bieżąco

Czy dysponujemy kompletną wiedzą, dokąd przepływają dane będące przedmiotem analityki i co dzieje się z nimi na każdym etapie? Czy skutecznie monitorujemy każdy z zaangażowanych procesów?

Ochrona danych osobowych w NGO powiązana jest z kilkoma aspektami. Można zacząć od dokumentacji. Pracownicy organizacji powinni mieć podpisane dokumenty formalne: Umowa o poufności, Umowa powierzenia DO, Upoważnienie do przetwarzania DO. W samej organizacji niezbędnymi dokumentami są: Polityka bezpieczeństwa, Ewidencja osób upoważnionych, Polityka prywatności (strona www, profile w mediach społecznościowych, newsletter).

» Grafika 2. Na podstawie :SuperDrob

Ważne jest, aby dane były odpowiednio zabezpieczone. Dokumentacja w formie papierowej powinna być przechowywana w bezpiecznym, niedostępnym dla osób nieupoważnionych miejscu. Dokumenty zawierające informacje podlegające ochronie, przed wyrzuceniem czy zniszczeniem należy zanonimizować. Tak, żeby nie można było odtworzyć treści i zidentyfikować osób, których dotyczą. W zakresie nośników w formie elektronicznej kluczowe są zabezpieczenia techniczne. Na pewno warto wdrożyć następujące rozwiązania:

- Sieć WiFi zabezpieczona unikalnym, silnym hasłem,
- Brak dostępu do sieci WiFi osób nieupoważnionych,
- Dostęp do sieci Internet za pośrednictwem hasła udostępnionego przez Administratora lub osobę upoważnioną,
- Blokada mediów społecznościowych i serwisów rozrywkowych (gaming, erotyka),
- Aktualizacja danych dostępowych do systemów informatycznych (login, hasło) w okresie 1 x miesiąc,
- Szyfrowanie nośników danych (laptop, pendrive, płyta CD).

Wyższy poziom zabezpieczenia to szyfrowanie. Skuteczna, najprostsza i bezpieczna metoda ochrony danych spełniająca wymogi Artykułu 32 RODO (wytyczne dla efektywnego działania strategii *disaster recovery,* odzyskiwania haseł i systemów zarządzania kluczami dostępu) oznacza, że organizacja jest w stanie udowodnić, że dane i systemy są bezpieczne, a zaszyfrowane dane możliwe do odzyskania po awarii technicznej. Najważniejsze czynności, to przede wszystkim:

- Szyfrowanie powierzchni dysku, dysków wymiennych, nośników,
- Szyfrowanie tekstów, dokumentów, plików i folderów na urządzeniu,
- Szyfrowanie poczty i załączników (np. wtyczka dla MS Outlook),
- Korzystanie z dysków wirtualnych, rozwiązań chmurowych,
- Wykorzystanie szyfrowanych pamięci Flash USB.

» Grafika 3. Źródło: Sophos

Bezpieczne urządzenie (PC, laptop, smartfon, tablet), pobieranie plików

Nie ma organizacji pozarządowej, w której nie wykorzystuje się sprzętu komputerowego. W dobie intensywnego natłoku informacji w Internecie, a zwłaszcza mediach społecznościowych łatwo stać się ofiarą hackingu, infekcji wirusa komputerowego czy instalacji złośliwego oprogramowania. Ważne jest przestrzeganie kilku strategicznych zasad. Priorytet #1 to program antywirusowy i cykliczna aktualizacja bazy wirusów. Priorytet #2 to aktualna wersja oprogramowania. Plus niezbędne wtyczki i sterowniki. Przy okazji warto usunąć starsze wersje oprogramowania. Pamiętajmy o ustawieniu poziomu zabezpieczenia. Zarówno samego urządzenia, jak i przeglądarki (Mozilla, Google Chrome, Opera, Safari). Zwracajmy uwagę na treść wyświetlanych monitów bezpieczeństwa, w razie czego warto przywrócić deaktywowane wcześniej opcje. Pomocne będzie czyszczenie pamięci podręcznej urządzenia i historii przeglądania. Ważne jest uruchomienie automatycznych aktualizacji programu urządzenia i systemu operacyjnego. Jeżeli nie jesteśmy pewni zawartości pliku, programu nieznanego wydawcy, zablokujmy opcję pobierania oraz instalacji.

Poczta elektroniczna – zagrożenia, profilaktyka

Wysyłka wiadomości email i bieżąca komunikacja online to rzecz powszechna. Każdej godziny w NGO'sach odbierane i wysyłane są setki tysięcy e-maili. W takim natłoku istnieje duże pole popisu dla cyberprzestępców. Mocno „popularne" są treści email wysyłane z fałszywych stron, imitujących najczęściej bank lub firmę kurierską. Sama treść emaila, podobnie jak SMS, nie jest groźna. Zagrożeniem jest znajdujący się w treści link bądź integralny załącznik.

Jak działać profilaktycznie? Przede wszystkim zachować czujność i zdrowy rozsądek. Każdy email wysyłany jest z konkretnego adresu, zawiera pole nadawcy. Zweryfikujmy kto jest nadawcą i jaki jest tytuł emaila. Warto przyjrzeć się samej treści, sprawdzić styl, format, pisownię. Do niebezpiecznej, potencjalnie zainfekowanej e-przesyłki często dołączane są spakowane załączniki w formacie ZIP czy RAR. Omijajmy to szerokim łukiem. Dobrym zwyczajem jest zainstalowanie czy aktywacja zapory oraz filtru antyspamowego. Tego typu system nie przepuści emaila z zainfekowanym załącznikiem ani treści z niedozwolonymi frazami typu: sex, viagra, dopalacz, hazard.

Bezpieczne płatności internetowe, bankowość elektroniczna– zalecenia

Bankowość elektroniczna i płatności internetowe to tematy, do których trzeba podchodzić z rozwagą i ostrożnością. Z raportu „2020 Cybersecurity Outlook", opracowanego przez VMware Carbon Black, wynika, że hakerzy nie tylko znajdują coraz bardziej zaawansowane sposoby na skuteczne oszustwa i wymuszenia, ale też coraz częściej wdrażają metody służące do maskowania swoich działań. Autorzy raportu podkreślają, że ponad 90 proc. analizowanych cyberataków imituje standardowe zachowania ruchu sieciowego, zaufane procesy lub dezaktywuje rozwiązania zabezpieczające (na podstawie: https://pieniadze.rp.pl).

Istnieją na szczęście dosyć skuteczne metody zapobiegające cyfrowym włamaniom i kradzieżom. Jeżeli realizujesz zakupy online dla NGO pamiętaj, kupuj tylko na stronach z Ceryfikatem SSL (kłódka przy adresie, protokół https). Szczególną czujność zachowaj przy płatnościach kartą bankową czy kredytową.

Jeśli płacisz e-przelewem, to upewnij się, że przekierowanie dokonywane jest na stronę Twojego banku. Dokonuj płatności tylko na zaufanych urządzeniach z aktualnym oprogramowaniem antywirusowym. Nie podawaj danych logowania do bankowości elektronicznej przez e-mail/telefon. Bank nigdy nie prosi klienta o login/hasło do konta online. Ani telefonicznie, ani mailowo. Stwórz silne, unikalne hasło do konta bankowego.

Warto przyjrzeć się opinii i zaleceniom Komisji Nadzoru Finansowego, która tak definiuje najbardziej powszechne zagrożenia w bankowości online:

Wyłudzanie danych (phishing)

01. podszywanie się pod bank w celu wyłudzenia pożądanych informacji lub skłonienia do określonych działań. Hakerzy usiłują poznać nasze dane do logowania do serwisów transakcyjnych. Wysyłają fałszywe maile lub podszywają się pod osobę z banku. Pod pretekstem bezpieczeństwa proszą o podanie danych do bankowości elektronicznej, kliknięcie w link;

Złośliwe oprogramowanie

02. zainstalowanie na komputerze wirusów czy programów szpiegujących, które śledzą informacje pojawiające się na ekranie komputera, czytają znaki wprowadzane na klawiaturze, przejmują kontrolę nad urządzeniem. Wirusy mogą np. podmienić numer konta adresata przelewu na inny;

Kopiowanie kart płatniczych (skimming)

03. jedno z popularniejszych zagrożeń. Polega na skopiowaniu danych z paska magnetycznego karty płatniczej. Instaluje się nakładkę na otwór, w którym umieszczamy kartę, wykradane są dane. PIN można poznać dzięki miniaturowym kamerom umieszczanym nad klawiaturą bankomatu lub fałszywej klawiaturze montowanej na oryginalnym urządzeniu;

Zakupy i płatności internetowe

04. zapłata kartą płatniczą online. Wystarczy imię i nazwisko, numer karty i kod CVC2/CVV2 znajdujący się na odwrocie. Jeśli robimy zakupy w nieznanych sklepach internetowych, możemy pozbyć się środków z konta (złośliwe oprogramowanie przechwyci dane karty);

Aplikacje mobilne

05. jeśli smartfon nie jest odpowiednio zabezpieczony i używany (np. instalacja niezaufanych aplikacji), może zostać wykorzystany do przechwycenia programów do bankowości mobilnej.

Zabezpieczenia techniczne w NGO: sieć komputerowa, WiFi, VPN

Przy korzystaniu z Internetu jesteśmy narażeni na wiele zagrożeń. Wszystkie organizacje pozarządowe korzystają z dostępu do sieci komputerowej. Strategicznym priorytetem jest, aby sieci przewodowe i bezprzewodowe (WiFi), na których pracujemy, były odpowiednio zabezpieczone. Zabezpieczenia to działania mające na celu ochronę sprawnego działania, integralności sieci i danych. To rozwiązania sprzętowe i programistyczne. Ich zadaniem jest przeciwdziałanie zagrożeniem i blokada dostępu do sieci oraz rozprzestrzeniania się wirusów czy złośliwego oprogramowania. Bazując na raporcie Cisco *„Podstawowe informacje o zabezpieczeniach sieci dla średnich i małych firm”* wyróżnić możemy następujące metody zabezpieczeń:

Kontrola dostępu do sieci - aby powstrzymać potencjalnych cyberprzestępców, należy zastanowić się nad funkcją każdego użytkownika i urządzenia. Przykładowo zablokować lub ograniczyć dostęp niezgodnych urządzeń końcowych do sieci.

Oprogramowanie antywirusowe i ochrona przed złośliwym oprogramowaniem – określenie „złośliwe oprogramowanie” oznacza min. wirusy, robaki, trojany, oprogramowanie ransomware oraz spyware (szerzej w dalszej części tekstu). Dobre programy chroniące przed złośliwym oprogramowaniem skanują ruch przychodzący do sieci pod kątem zagrożeń, monitorują pliki sieciowe, usuwają złośliwe oprogramowanie i usuwają szkody.

Analizy zachowania - narzędzia do analizy zachowania automatycznie rozpoznają działania odbiegające od normy. Dzięki temu można skutecznie identyfikować sygnały naruszenia zabezpieczeń i eliminować potencjalne problemy.

Zapobieganie utracie danych - technologie zapobiegania utracie danych umożliwiają zapobieganie pobieraniu, przesyłaniu, drukowaniu istotnych z punktu funkcjonowania organizacji informacji.

Zabezpieczenia poczty e-mail – Bramy poczty e-mail są głównym punktem naruszeń bezpieczeństwa. Wykorzystuje się sposoby, które przekierowują odbiorców do witryn rozsyłających złośliwe oprogramowanie. Aplikacje zabezpieczające e-mail blokują ataki z zewnątrz, kontrolują wiadomości wychodzące.

Zabezpieczenia sieci www – kontrolują, jak personel organizacji korzysta z sieci, blokują zagrożenia, uniemożliwiają dostęp do złośliwych witryn internetowych. Działają profilaktycznie w zakresie ochrony bramy sieci komputerowej organizacji.

Koniecznie trzeba wspomnieć o zabezpieczeniach typu Firewall i VPN. Firewall (Zapora) to system IT, który zabezpiecza komputer podłączony do Internetu przed wprowadzaniem lub wyprowadzaniem danych. Blokuje nieautoryzowane transmisje danych z wnętrza lub do wnętrza sieci komputerowej. Zapora zabezpiecza przed wykradaniem danych oraz umieszczaniem szkodliwych danych w komputerze. Blokuje niepożądane instalacje szkodliwego oprogramowania za pośrednictwem Internetu.

Wyróżnia się dwie podstawowe kategorie Firewall:

Zapory sprzętowe – znajdują się w bramkach internetowych. To klasyczne urządzenia sieciowe takie jak modemy i routery. Jest to dobre rozwiązanie techniczne, jednak sprawia ono trudność przeciętnym użytkownikom komputerów, nie zawsze radzą sobie z konfiguracją. Dlatego też zwykle firewalle sprzętowe konfiguruje się w większych, firmowych sieciach komputerowych;

Firewall programowy to programy pełniące funkcję firewalla. Zapory, które instaluje się na komputerze w systemie ustawień sieci. Kontrolują transmisje danych z i do komputera, sprawdzając co dzieje się pomiędzy komputerem jako urządzeniem i zewnętrznym środowiskiem, z którym dany komputer się komunikuje. Firewalle programowe służą blokowaniu nieautoryzowanej, niechcianej migracji danych.

Wspomniany powyżej VPN (Virtual Private Network) to w tłumaczeniu Wirtualna Sieć Prywatna. Często wykorzystywana przez organizacje w dobie pracy zdalnej. Większość pracowników wykonuje obowiązki na urządzeniu firmowym poza siedzibą organizacji. VPN umożliwia szyfrowanie połączenia między punktem końcowym i siecią. Korzysta z szyfrowanego, dedykowanego protokołu IT do uwierzytelniania komunikacji między urządzeniem i siecią.

VPN ma różnorodne zastosowanie, swoje wady i zalety. Sieci VPN z wbudowaną ochroną pomagają zapobiegać infekcjom, blokując witryny ze złośliwym oprogramowaniem. Większość sieci VPN blokuje reklamy czy moduły śledzące. W momencie połączenia z serwerem VPN, ruch internetowy jest szyfrowany. Oznacza to, że nikt nie widzi co robimy online. Przydaje się to niektórym NGO, na przykład tym zaangażowanym w działalność polityczną czy społeczną. Sporo stron/aplikacji, na przykład Netflix, Facebook czy Steam za pośrednictwem numeru IP urządzenia identyfikuje naszą lokalizację. VPN to maskuje. Możemy dzięki temu omijać różne blokady, cenzurę, korzystać dyskretnie z różnorodnych serwisów.

Sieci VPN mają dostęp do wielu poufnych informacji. Zobowiązane są więc do prowadzenia restrykcyjnej polityki prywatności i wdrażania środków bezpieczeństwa. Przy wyborze sieci trzeba zweryfikować właśnie politykę bezpieczeństwa. Korzystanie z VPN oznacza prawie na pewno spowolnienie ruchu na urządzeniu (szyfrowanie i odszyfrowanie ruchu). Warto przyjrzeć się dostawcy VPN. Jeśli korzystamy z mniej znanej firmy, nie ma pewności, że nie sprawdzi on naszej aktywności związanej z przeglądaniem ani czy nie udostępnia jej osobom trzecim. Jeżeli działa w ramach tzw. Aliansu 5/9/14-Eyes, może nawet udostępniać niektóre informacje rządowi swojego kraju (na podstawie: pl.vpnmentor.com).

Polityka bezpiecznego hasła

Polityka haseł ma zapewniać odpowiedni poziom poufności i dostępności do przetwarzanych danych. Przepisy RODO nie określają wprost polityki haseł w Twojej organizacji. Hasło powinno mieć odpowiednią strukturę. Powinno zawierać co najmniej 8 znaków i składać się z 3-4 typów znaków, którymi są małe i wielkie litery, znaki specjalne i cyfry. Stosuje się dodatkowe zasady: np. hasło nie może się powtarzać, nie może zawierać loginu użytkownika lub nazwiska. Nie może być zmieniane w tym samym dniu, nie może zawierać ciągu identycznych znaków. Polityka haseł powinna także zawierać informacje, gdzie hasła są przechowywane, jaki jest system ewidencjonowania, kto ma do nich dostęp. Dobrym rozwiązaniem może być skorzystanie ze specjalistycznego managera haseł. Program pomaga użytkownikom tworzyć nowe hasła, przechowuje hasła w formie zaszyfrowanej, przypomina o zmianie hasła w odpowiednim odstępie czasowym.

Ataki komputerowe, złośliwe oprogramowanie, wirusy - profilaktyka

Według oceny prof. dr hab. Jana Kościelnego z Politechniki Warszawskiej, liczba cyberataków gwałtownie rośnie. Wszystkie dane światowe to rejestrują, zagrożenie wydaje się być coraz większe. Zgodnie ze sprawozdaniem ESG/ISSA 2019 już ponad 90 proc. organizacji ocenia, że grozi im cyberatak. Raport Black Hat 2019 wskazuje, że 77 proc. liderów bezpieczeństwa przewiduje krytyczne naruszenie infrastruktury, które może mieć niebezpieczne konsekwencje. Globalny koszt cyberprzestępczości osiągnie 6 bln USD do 2021 r., dwukrotnie więcej niż w 2015 r. (źródło: Newseria).

Do zwiększonej liczby cyberataków z całą pewnością przyczyniła się pandemia COVID-19. Większa skala pracy czy nauki online, znaczna liczba urządzeń podłączonych do Internetu, wzmożony ruch w infrastrukturze internetowej. Zainfekowanie komputera czy smartfona w organizacji pozwala na szpiegowanie, wykradanie wrażliwych danych lub ich szyfrowanie.

Celem jest na przykład wyłudzenie albo kradzież pieniędzy. W celach profilaktyki, obrony przed cyberatakami konieczne jest monitorowanie zachowania podejrzanych aktywności. Przykładowe kategorie zagrożeń w sieci w roku 2020 to między innymi: Pharming (fałszywe strony www); Wirus plikowy (dopisuje kod do pliku, np. .exe, .com); Wirus Makro (uruchamia się przy otwieraniu pakietu Office); Wirus Retro (blokuje skaner antywirusowy) czy Keylogger (rejestruje klawisze wciskane przez użytkownika).

Osobna kategoria to programy szpiegujące. Tego typu program zbiera dane o użytkowniku: odwiedzane witryny, hasła dostępowe. Potrafi zmieniać wpisy, ustawienia, pobierać i uruchamiać niechciane pliki. Nie można nie wspomnieć o atakach typu Ransomware, ograniczających dostęp do systemu komputerowego i wymagających zapłacenia okupu w celu zdjęcia blokady. Najbardziej niebezpieczne ataki ransomware zostały spowodowane przez złośliwe oprogramowanie WannaCry, Petya, Cerber, Cryptolocker i Locky. Ransomware może dostać się do urządzenia poprzez załącznik w e-mailu lub przeglądarkę, jeśli odwiedzisz zainfekowaną stronę. Może również uzyskać dostęp do Twojego komputera czy smartfona poprzez sieć.

Jak pracować bezpiecznie i bezstresowo w NGO? W jaki sposób zapobiegać tego typu atakom?

- Na pierwszym miejscu wymienić można ostrożność, rozwagę i postępowanie zgodnie z Polityką bezpieczeństwa w organizacji.
- Jeżeli chodzi o kwestie techniczne, upewnij się, że wszystkie programy na komputerze są aktualne: system operacyjny, przeglądarki oraz paski narzędzi. Upewnij się, że Twój program antywirusowy i zapora ogniowa są zaktualizowane. Wykorzystuj rozwiązania chmurowe i kopie zapasowe.
- Kopia zapasowa to jedno z najważniejszych działań zalecanych jako ochrona przed skutkami ransomware. Gdy jest kopia w chmurze, przywrócenie danych będzie dużo prostsze.
- Nie pobieraj plików z nieznanych źródeł. Zwracaj uwagę na wszelkiego rodzaju sygnały, alerty i ostrzeżenia wysyłane przez systemy zabezpieczenia przeglądarek internetowych.

» **Dariusz Adamczyk**

Komunikatory

wady, zalety, bezpieczeństwo danych.

Ostatnie lata to niezwykle dynamiczny rozwój komunikacji za pośrednictwem kanałów internetowych. Głównym motorem rozwoju stały się komunikatory. Nie ma chyba osoby na ziemi, która nie słyszała o Facebook Messenger czy Whatsapp. Poza tymi najbardziej powszechnymi są też komunikatory mniej znane w Polsce, ale jak najbardziej wykorzystywane przez rzesze użytkowników. Mam tu na myśli takie serwisy jak: Telegram, Signal, WeChat czy Threema. W niniejszej analizie porównane zostaną wybrane komunikatory. Przyjęte kryteria, to przede wszystkim specyfika działania i kwestie prywatności. Nie są brane pod uwagę opcje reklamowe czy marketingowe. Komunikatory, jak sama nazwa wskazuje, służą do komunikacji. W większości posiadają zbliżone funkcjonalności. Różnią się zasadniczo kwestią podejścia do pozyskiwania, przetwarzania i przekazywania danych osobowych oraz podejściem do polityki prywatności. W niektórych przypadkach służą wręcz jako narzędzie do inwigilacji czy monitoringu.

Facebook Messenger

Zaczynamy od najbardziej popularnej platformy – Facebook Messenger. Ponad 70 mln pobrań w Google Play, 2 mln pobrań miesięcznie w AppStore w samych tylko USA. Od początku bezpłatny, oferuje także elementy płatne. Główne funkcje to rozmowy tekstowe, głosowe i video. Notuje sporo awarii w ostatnich dniach, główne problemy: wysyłanie/odbieranie wiadomości, połączenia z serwerem, synchronizacja po ostatniej aktualizacji (10.12.2020 r.). Już w 2018 r. Facebook musiał przyznać, że narusza standardy prywatności poprzez skanowanie przesyłanych zdjęć, treści czy linków. Nie jest tajemnicą, że dane z Messengera są dostępne dla systemów analitycznych FB, ale także jednostek zewnętrznych, np. służb specjalnych. Sieci neuronowe (tj. systemy do procesowania informacji, prognozowania danych, modelowania procesów, etc.) portalu Facebook przetwarzają treści wiadomości w komunikatorze w celu optymalizacji reklamowej.

W 2020 r. wprowadzono lub w najbliższym czasie będą implementowane nowe funkcje w kontekście ustawień prywatności. Blokowanie dostępu z wykorzystaniem Face ID oraz Touch ID. W skrócie ustawienie blokady, która uniemożliwi wyświetlenie treści przechowywanych czatów. Będą zasłonięte rozmytym tłem. Odblokowanie będzie miało miejsce po użyciu wybranego zabezpieczenia biometrycznego. Rozwiązanie dostępne jest dla użytkowników iOS, w najbliższym czasie korzystać z niego będą mogli posiadacze urządzeń z systemem Android. Twórcy zapowiadają funkcję zamazywania wiadomości od osób spoza listy znajomych oraz kontrolę nad przychodzącymi treściami i rozmowami głosowymi. Nie ma w standardzie szyfrowania komunikacji.
Istnieje teoretyczna możliwość zaszyfrowania konwersacji z użyciem ikonki „Z wykrzyknikiem" oraz „Przejdź do tajnej konwersacji".

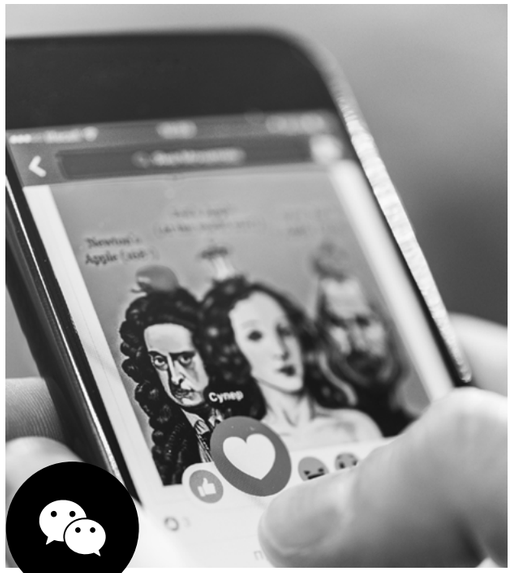
Whatsapp

Whatsapp określany jest czasem jako mix systemów Telegram i Signal. Należy aktualnie do rodziny Facebooka. Właśnie dzięki pojawieniu się w portfolio Facebooka stracił pewną część użytkowników. Zraziło ich chociażby to, że przy instalacji implementuje się baza kontaktów z biało-niebieskiego serwisu. Mimo wszystko jest to wciąż jeden z bardziej popularnych komunikatorów. Prosta konfiguracja. Dostępny dla iOS i Android. Wyróżnikiem jest opcja szyfrowania wiadomości end-to-end. Jak deklaruje na stronie developer Whatsapp: pełne szyfrowanie zapewnia, że jedynie Ty i osoba, z którą się komunikujesz, możecie odczytać lub odsłuchać wysłaną zawartość. Dzieje się tak, ponieważ zaszyfrowane wiadomości są zabezpieczone kodem, do którego przypisany jest klucz umożliwiający odszyfrowanie i przeczytanie. Nie trzeba włączać żadnych ustawień ani konfigurować czatów, aby zabezpieczyć wiadomości. Wbrew pozorom, Whatsapp nie zapewnia pełnej prywatności i zabezpieczenia. Jak donosi Komorkomania.pl nazwa użytkownika w systemie Whatsapp jest pod numerem telefonu. Adres IMEI można uzyskać biorąc urządzenie do ręki, adres MAC można sprawdzić podłączając się do sieci WLAN. Po uruchomieniu aplikacji WhatsApp przesyła całą naszą bazę kontaktową na swoje serwery i sprawdza, które numery są zarejestrowane w sieci. WhatsApp automatycznie ustawia ustawienia prywatności, aby umożliwić każdemu użytkownikowi przegląd przeczytanych, ostatnio widzianych wiadomości oraz zdjęcia i status profilu. Oferuje możliwość wykonania kopii rozmów w usługach iCloud (iOS) i Dysku Google (Android), ale sam developer ostrzega, że nie są one w pełni zabezpieczone. Według serwisu Wynalazca.tv główną zaletą WhatsApp, jest przystępność. Siła kodu używanego do zabezpieczania w niej danych jest o wiele szczelniejsza niż ta Telegramu i porównywalna do Signala. Generalnie Whatsapp uważany jest za komunikator bezpieczny. Ważna rzecz – rozszyfrowanie wiadomości odbywa się na urządzeniu końcowym. Pamiętajmy więc, żeby nasz PC, laptop czy smartfon był odpowiednio zabezpieczony przed ewentualną ingerencją.

Signal

Komunikator Signal uważany jest za najbezpieczniejszy. Dostępny na systemy iOS i Android. Posiada wersję desktop. Należy do Signal Foundation oraz Signal Messenger LLC. Jest bezpłatny, działa w tzw. open source. Signal używa połączenia internetowego do wymiany wiadomości tekstowych i głosowych. Umożliwia rozmowy audio i wideo. Komunikator rejestruje użytkowników na podstawie numeru telefonu i stosuje szyfrowanie end-to-end zapewniające bezpieczeństwo wymienianych wiadomości. Uznawany jest za najbezpieczniejszy komunikator internetowy. Wiadomości wysyłane za pośrednictwem Signal są szyfrowane za pośrednictwem Signal Protocol. Przechwycenie wiadomości przez osobę z zewnątrz jest bezużyteczne, ponieważ deszyfryzacja odbywa się na urządzeniu odbiorcy. Signal oferuje zablokowanie aplikacji z użyciem specjalnego kodu, danych biometrycznych (linie papilarne, skanowanie twarzy).

Według serwisu Wynalazca.tv największą zaletą aplikacji Signal jest poziom zabezpieczania danych, ponieważ zaszyfrowane za jej pomocą wiadomości nie mogą być odczytane przez osoby trzecie. Umożliwiona przez program komunikacja telefoniczna również otrzymała gwarancję ochrony informacji. Dodatkowo pozwala na całkowite usunięcie konta bez możliwości odzyskania. Signal blokuje rozmowy zarchiwizowane, nie ma możliwości ich odczytania. Postrzegany jest jako komunikator, który nie zapisuje naszych danych, oferuje pełną poufność. Jak donosi Cyberdefence24 Signal po najnowszej aktualizacji z 2020 r. ma pozwalać użytkownikom na przechowywanie kontaktów, informacji profilowych, ustawień oraz listy zablokowanych osób w chmurze. Dostęp do informacji przenoszonych do chmury ma być chroniony kodem PIN. Dla niektórych analityków podkreśleniem aspektu bezpieczeństwa aplikacji Signal jest fakt, że korzystał z niej Edward Snowden. Ze względu na trudność złamania kodów aplikacji, Signal został zablokowany w takich krajach jak Egipt, Rosja, Iran.



WeChat

WeChat to aplikacja, która zyskała w ostatnich latach niezwykłą popularność. Gwoli wyjaśnienia, WeChat przedstawiony jest tutaj jako ciekawostka technologiczna, a nie rekomendowane narzędzie.
Popularność WeChat wynika z tego, że jest powszechnie używany w Chinach i niektórych krajach azjatyckich. Wykorzystywany jest często do kontaktów biznesowych, turystycznych czy towarzyskich z chińskimi kontrahentami czy po prostu chińską społecznością. Jeden z pierwszych komunikatorów, używany od 2010 roku. WeChat od kilku lat otrzymuje wsparcie finansowe chińskiego rządu, nie jest więc postrzegany jako system do bezpiecznej, dyskretnej komunikacji.

Nie jest tajemnicą, że algorytmy aplikacji stosują filtry cenzorskie. Skanowana jest treść rozmów pod kątem polityki i spraw społecznych. WeChat uznawany jest powszechnie za jeden z bardziej zaawansowanych technologicznie systemów z tej kategorii. Poza standardowym czatem tekstowym, głosowym, video oferuje na przykład opcję transferów finansowych, płatność za rachunki, wirtualne portfele.
Każdy użytkownik ma dostęp do personalnego QRcode. Z pełnym przekonaniem można stwierdzić, że ze względu na liczbę gromadzonych danych, taką a nie inną Politykę Prywatności, nie ma szans na rozwój poza Chinami i wybranymi krajami azjatyckimi.

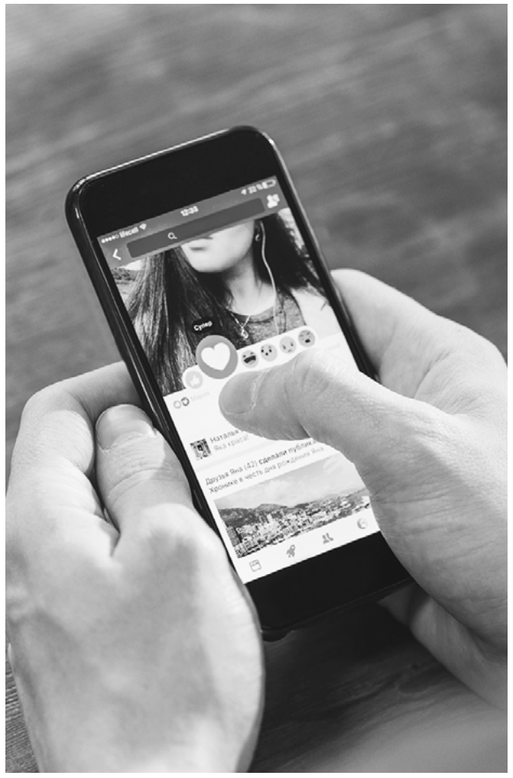
Telegram

Wokół komunikatora Telegram narosło sporo mitów i legend. Legendy przysporzył między innymi fakt, że był (może jest) wykorzystywany przez bojowników tak zwanego Państwa Islamskiego. Telegram jest bezpłatny, ciągle niekomercyjny. Jest dostępny dla systemów Android, iOS, Windows Phone, Windows NT, MacOS, Firefox, OS, Linux. Posiada przede wszystkim funkcje tradycyjnego komunikatora: czat tekstowy, głosowy, opcja rozmów głosowych, przesyłanie multimediów. Testowana jest opcja połączeń video.

To co jest wyróżnikiem, to opcja szyfrowania point-to-point. Dostępna dla pojedynczych rozmówców, niedostępna dla rozmów grupowych. Wdrożony przez twórców model zabezpieczenia Telegramu spotkał się z poważną krytyką specjalistów od kryptografii. Niektórzy wytykają brak dostępności kodu źródłowego systemu szyfrującego i związane z tym niejasności dotyczące aspektów kryptograficznych.
Część specjalistów z kolei podkreśla, że Telegram korzysta z własnego kodu źródłowego o nazwie MTproto oraz szyfruje rozmowy użytkowników. Krytyce poddany został fakt permanentnego przechowywania wszystkich kontaktów, wiadomości i multimediów wraz z kluczami deszyfrującymi domyślnie na serwerach komunikatora. Znaleziono też luki w szyfrowaniu wiadomości. Telegram nie szyfruje wiadomości domyślnie, trzeba tę funkcję uruchomić. Dzięki temu może nastąpić niechciany wyciek informacji. Znana w branży IT Ola Flisbäck udowodniła w swojej wiadomości, że łatwo odszyfrować w Telegramie, czy dany użytkownik jest online, czy offline. Niezależnie od tego, czy włączy funkcję ukrycia. Ale pamiętajmy, żadne oprogramowanie nie gwarantuje 100 proc. poziomu zabezpieczeń.

Według serwisu Niebezpiecznik komunikator Telegram nie szyfruje wszystkich typów komunikacji, jakie są w nim dostępne. Oznacza to, że część użytkowników może nie zdawać sobie sprawy, że przesyłane przez nich informacje są widoczne dla innych.

W dodatku Telegram jest autorstwa Pawła Durowa, Rosjanina (założył go wspólnie z bratem Nikołajem). Toczy się przeciwko niemu proces w Rosji. Sprawa dotyczy właśnie dostępu do danych użytkowników. Co ciekawe, sam Durow oskarża Facebook Messenger i Whatsapp. Nazywa je komunikatorami niebezpiecznymi. Chodzi o słynną sprawę pozyskania danych z konta Jeffa Bezosa, twórcy Amazona. Jest w tym sporo racji. Telegram ma zakaz działania na przykład w Rosji czy Iranie. Whatsapp działa na terenie tych krajów bez żadnego problemu.



Threema

Threema to komunikator najmniej chyba w tym panteonie znany i rozpoznawany. Jako chyba jedyny w tym momencie komunikator płatny (w polskich marketach z aplikacjami kosztuje 13,99 zł). Jest to kompleksowo zaszyfrowana aplikacja do wysyłki szybkich wiadomości i prowadzenia rozmów. Twórcy od początku traktują kwestie prywatności jako priorytet. Nie ma na przykład potrzeby posiadania karty
SIM, aby się do systemu zalogować. W systemie Threema nie jest wymagany numer telefonu ani udostępnianie powszechnych danych osobowych, co jest tak typowe dla innych komunikatorów. Sami twórcy określają swoje dzieło jako „bezpieczny i prywatny posłaniec". Wiadomości, informacje przesyłane w obrębie Threema nie mogą być odczytywane przez dostawców Internetu. Infrastruktura (serwery) według oficjalnej informacji znajdują się na terenie Szwajcarii, tj. kraju znanego z wysoko postawionych priorytetów w zakresie danych osobowych i bezpieczeństwa informatycznego. Istotnym czynnikiem jest funkcja całkowitego czyszczenia, usunięcia wszystkich wiadomości i historii konwersacji. Ciekawa opcja to synchronizacja danych w aplikacji Threema z chmurą. Ułatwia to dostęp pomiędzy różnymi urządzeniami i daje gwarancję, że nasze dane zostaną zapisane na wypadek utraty urządzenia. Aplikacja nie wymaga zakładania konta w celu logowania się i korzystania z dostępnych funkcjonalności. Co ciekawe, z Threema można korzystać anonimowo. Nie trzeba podawać prawdziwej tożsamości. Aplikacja oferuje możliwość oznaczania użytkowników kolorowymi kropkami. W przypadku osoby podejrzanej, zostaje ona oznakowana kolorem czerwonym.

W dobie powszechnego korzystania z Internetu, mediów społecznościowych, komunikatorów, kwestia nadrzędna to bezpieczeństwo i prywatność. Nie wszystkie komunikatory mogą nam to zagwarantować. Oczywiście pamiętać należy o dwóch sprawach. Po pierwsze, systemy widzą i potencjalnie udostępniają dane, które sami ujawniamy. Wiele osób dzieli się w sposób nadmierny informacjami dotyczącymi życia prywatnego i zawodowego.

Pamiętajmy, na bazie danych zebranych w komunikatorach, programy internetowe i aplikacje profilują reklamy wyświetlane użytkownikom. Po drugie kwestią priorytetową jest zabezpieczenie urządzenia, za pośrednictwem którego aktywnie używamy komunikatorów. Tak, żeby nie dostało się w niepowołane ręce. Z kilku wymienionych wcześniej powodów coraz większą popularnością będą się cieszyły komunikatory szyfrowane. Zawierające dedykowane programy z opcją kodowania wiadomości i zaimplementowanych danych. W zasadzie twórcy wszystkich komunikatorów podają oficjalne informacje o wdrożonych procedurach bezpieczeństwa i polityce prywatności. Rzeczywistość tego nie potwierdza. Przykładem może być platforma Facebooka. Według doniesień CNBC Mark Zuckenberg i Facebook wykorzystali dane ponad 87 mln użytkowników, przekazując zdjęcia i prywatne rozmowy na czatach do działu zajmującego się analizą osobowości i wywieraniem psychologicznego wpływu w skali masowej na zachowania wyborców danej partii politycznej. Niektórzy analitycy twierdzą, że mocno przyczyniło się do wyborczego sukcesu Donalda Trumpa.

Generalnie za trzy najbardziej bezpieczne komunikatory szyfrujące uważane są Whatsapp, Telegram i Signal. W tej trójce prym wiedzie Signal. Cały czas pojawiają się pytania: czy dane zbierane przez komunikatory wykorzystywane są przez służby specjalne? Odpowiedź jest twierdząca. Przykład Polski. Zgodnie z polskim prawem telekomunikacyjnym operatorzy są zobowiązani do rejestrowania i archiwizowania numerów IP oraz rejestru połączeń numerów telefonów komórkowych przez pięć lat. Sądy, Prokuratura i służby mają potencjalną możliwość analizy historii rozmów użytkowników WhtasApp z pięciu lat. Inny, drastyczny przykład. Słowacja, śledztwo w sprawie zabójstwa dziennikarza Jána Kuciaka i jego narzeczonej Martiny Kusznírovej. Śledczy bez problemu dotarli do zawartości telefonu (treści w aplikacji Threema) podejrzanego o zabójstwo, M. Kocznera. W konsekwencji afery pedofilskiej w Niemczech (Bergisch Gladbach) w drugiej połowie 2021 roku w Parlamencie Europejskim ma pojawić się projekt ustawy, która zobliguje operatorów wszystkich komunikatorów do stworzenia w nich tzw. tylnej furtki dla organów ścigania.
W USA planowana jest ustawa EARN IT Act, która przewiduje wprowadzenie furtek do szyfrowanych połączeń i obowiązek zawiadamiania organów ścigania oraz służb specjalnych w zakresie poufnych informacji dotyczących aktywności wybranych użytkowników. Pamiętajmy więc, zdrowy rozsądek i rozwaga przede wszystkim.

Wywiad: Chińskie oddziaływania informacyjne w Polsce

> „Nic nie wskazuje na to, żeby Pekin miał rezygnować z obecnego asertywnego kursu i międzynarodowej ekspansji. Chińskie władze chcą mieć większy wpływ na kształtowanie obrazu ChRL na świecie, mają również środki, by promować własny model ustrojowy jako alternatywę dla liberalnej demokracji".

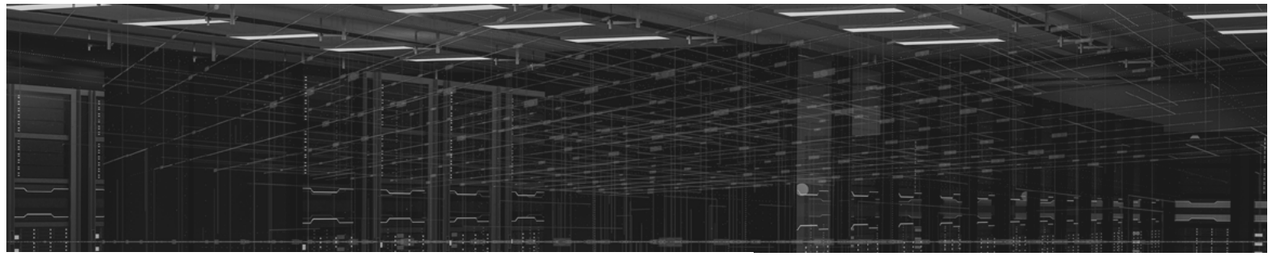
– mówi w rozmowie z Narodowym Instytutem Cyberbezpieczeństwa analityczka ds. polityki Chin w Ośrodku Badań Azji Centrum Badań nad Bezpieczeństwem Akademii Sztuki Wojennej i ekspertka międzynarodowego projektu MapInfluenCE monitorującego chińskie i rosyjskie wpływy w państwach Grupy Wyszehradzkiej Alicja Bachulska.

Adam Lelonek: Zachód, w tym Polska, od wielu lat doświadcza rosyjskich działań informacyjnych i psychologicznych. Można powiedzieć, że rosyjskie zagrożenie jest czymś, co jest nam w jakiś sposób znane. Kiedy jednak mówi się o chińskim oddziaływaniu na polską przestrzeń informacyjną, może wywoływać to wciąż zdziwienie u wielu odbiorców. Dlaczego temat zagrożeń informacyjnych pochodzących z Chin nie przebija się w Polsce do szerszej świadomości społecznej i mediów mainstreamowych?

Alicja Bachulska: Zarówno z powodów geograficznych, jak i historyczno-kulturowych Chiny są nam odległe, a jako społeczeństwo wiemy o nich bardzo mało. Nawet w środowiskach eksperckich i akademickich Chińską Republiką Ludową (ChRL) zajmuje się w Polsce garstka ludzi. W ostatnich latach można zaobserwować znaczne zwiększenie zainteresowania chińską tematyką, ale w dalszym ciągu jest to kwestia niszowa. Często mówi się również o Chinach bardzo jednowymiarowo, a kraj ten przedstawiany jest głównie jako biznesowy raj czy kulturowo-społeczna ciekawostka. Zakładając dalszy wzrost znaczenia Chin w przestrzeni międzynarodowej, musimy być gotowi rozmawiać o znaczeniu tych procesów dla Polski. Debata ta powinna wyjść poza wąskie grono ekspertów i osób zainteresowanych Azją Wschodnią. A Chiny już są nad Wisłą, nie musimy na nie czekać – również w obszarach mniej oczywistych niż np. inwestycje zagraniczne. Mowa tutaj np. o współpracy medialnej czy chińskiej obecności w polskojęzycznych mediach społecznościowych, które mają bezpośrednie przełożenie na postrzeganie ChRL w Polsce.

Porozmawiajmy więc o konkretach. W jaki sposób ChRL stara się wpływać na kształt debaty publicznej w Polsce? O jakim poziomie zaawansowania takich działań mówimy na chwilę obecną?

Obecnie nie są to zaawansowane działania, ale ich intensywność szybko wzrasta, w szczególności w kontekście pandemii COVID-19. Strona chińska jest aktywna w polskiej przestrzeni informacyjnej na kilku poziomach: w mediach tradycyjnych, społecznościowych oraz w wymiarze dyplomacji publicznej. W tradycyjnych mediach współpraca ta jest najlepiej widoczna w dzienniku „Rzeczpospolita", w którym od lat publikowane się artykuły autorstwa chińskich dyplomatów w Polsce oraz wywiady z nimi. Pojawiają się też teksty sponsorowane, np. promujące chińską politykę pod rządami Xi Jinpinga. Na poziomie retorycznym są one pełne partyjnej nowomowy i wyglądają na bezpośrednie tłumaczenia materiałów propagandowych Komunistycznej Partii Chin (KPCh) na polski. Ciężko powiedzieć do jak szerokiego grona odbiorców trafiają te publikacje – wydaje się, że w Polsce mogą one raczej budzić ambiwalentne uczucia ze względu na wrażliwość Polaków na komunistyczną nowomowę, którą starsze pokolenia rozpoznają z autopsji, a młodsze odbierają raczej z przymrużeniem oka. Teksty tego rodzaju pojawiają się również w mediach historycznie wywodzących się ze środowisk związanych z reżimem komunistycznym w Polsce, np. w dzienniku „Trybuna". Tego typu treści można również coraz częściej znaleźć w najbardziej popularnych mediach społecznościowych – ambasada ChRL w Warszawie ma swoje oficjalne konta na Twitterze i Facebooku, tak samo jak sam ambasador Chin. Natomiast jeśli chodzi o dyplomację publiczną, to strona chińska wychodzi z atrakcyjną ofertą stypendialną skierowaną ku polskim studentom. Młodzi Polacy coraz częściej wyjeżdżają na studia do ChRL zarówno na krótkoterminowe kursy językowe, jak i na dłuższe programy licencjackie, magisterskie czy nawet doktorskie. Rok temu w Chinach studiowało ok. 2000 Polaków i chociaż pandemia zmusiła część z nich do kontynuowania nauki zdalnie z Polski, można spodziewać się, że w przyszłości zainteresowanie wyjazdami tego rodzaju będzie dalej rosnąć. W zamyśle zagraniczni absolwenci chińskich uczelni mają zostać „ambasadorami" kraju, chociaż doświadczenia ze studiów w ChRL są zróżnicowane i niekoniecznie przekładają się na bezkrytyczny stosunek wobec władz w Pekinie. Również Instytuty Konfucjusza współfinansowane przez Chiny działają na kilku polskich uczelniach bez większych problemów, chociaż w wielu krajach są one postrzegane coraz częściej jako narzędzia chińskiej propagandy za fasadą promocji języka i kultury.



Rosjanie do swoich działań przeciwko państwom zachodnim powszechnie wykorzystują m.in. farmy trolli, media społecznościowe i rządowe ośrodki medialne, w tym zwłaszcza Sputnik i RT. Jak w tym kontekście wyglądają działania informacyjne Chin?

Obecnie wygląda na to, że Chiny działają w polskiej przestrzeni informacyjnej przy pomocy lokalnych mediów, które świadomie lub nieświadomie pośredniczą w promocji oficjalnego przekazu rządu w Pekinie. Chińska państwowa agencja prasowa Xinhua współpracuje również z Polską Agencją Prasową, a na stronach PAP nierzadko współdzielone są treści tworzone przez ten chiński podmiot. Publikacje tego rodzaju często są pełne odniesień do kluczowych pojęć propagandowych promowanych przez Chiny, jak np. „wspólnota dzieląca ten sam los" – odniesienie do wizji ładu międzynarodowego forsowanego przez Pekin – czy „pragmatyczna współpraca" – eufemizm na kooperację niezależną od demokratycznych norm i wartości.

Z perspektywy wielu lat widać wyraźnie, że działania rosyjskie dostosowywane są do bieżących wydarzeń i aktualnych w danym momencie potrzeb polityki zagranicznej i bezpieczeństwa Kremla, lecz mają mniej więcej podobne wektory oddziaływania w długim okresie. Odnoszą się do określonych przekazów czy narracji, jak np. anty-USA, anty-NATO czy anty-UE. Czy w długim okresie Chiny mają swoje preferowane obszary oddziaływań informacyjnych, poza bieżącą tematyką COVID-19?

Zacznijmy od tej bieżącej tematyki, bo pandemia podziałała jako katalizator zmian, które rozpoczęły się wcześniej, ale globalny kryzys zdrowia publicznego na pewno je przyspieszył. Intensyfikacja chińskich działań mających na celu rozmycie odpowiedzialności za rozprzestrzenienie się nowego koronawirusa w początkowej fazie pandemii zaczęła się już w pierwszym kwartale 2020 r. Chińskie media nakierowane na zagranicznych odbiorców publikowały wtedy treści odwracające uwagę od spóźnionej reakcji władz ChRL w obliczu epidemii oraz sugerujące, że koronawirus mógł powstać w amerykańskim laboratorium wojskowym. Przekaz tego rodzaju wzmacniali chińscy dyplomaci, którzy zaczęli coraz agresywniej angażować się w obronę własnego kraju – stąd wzięło się też popularne obecnie pojęcie „dyplomacji wilczych wojowników", odnoszące się właśnie do ich ofensywnej retoryki.

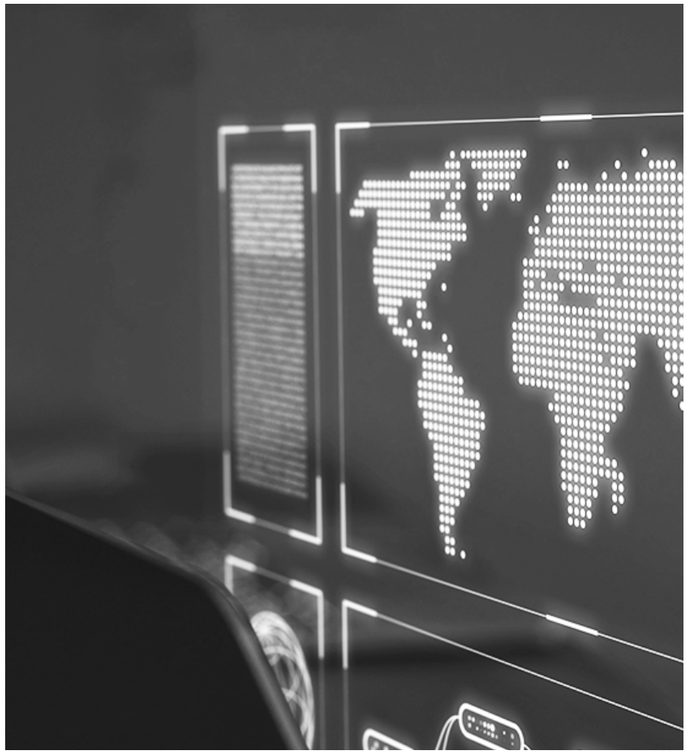
Natomiast odnosząc się do preferowanych długofalowych obszarów oddziaływań informacyjnych Pekinu, należy zauważyć, że przez wiele lat chińska polityka zagraniczna była uważana za reaktywną, jednak obecnie szybko się to zmienia. Widać to właśnie na poziomie oficjalnego przekazu – Chiny z defensywy przeszły w ofensywę i coraz aktywniej forsują własną wizję ładu międzynarodowego. Wizja ta niekoniecznie jest zbieżna z tą preferowaną przez Moskwę, chociaż łączą je pewne elementy, jak np. imperatyw rywalizacji ze Stanami Zjednoczonym. Rozgrywa się ona zarówno na płaszczyźnie gospodarczej, przez tzw. wojnę handlową, ale również w wymiarze strategicznym i ideologicznym.

Czy poza kwestiami gospodarczymi i własnego wizerunku mogą pojawić się w Polsce jakieś inne tematy o znaczeniu strategicznym dla Chin?

Tak, wspomniane przed chwilą kwestie rywalizacji strategicznej z USA są również widoczne w Polsce, m.in. w dyskusji na temat potencjalnego ograniczania obecności chińskiej firmy Huawei na naszym rynku. Huawei jest największym producentem sprzętu telekomunikacyjnego na świecie i jest również najtańszym dostarczycielem sprzętu niezbędnego do budowy internetu piątej generacji (tzw. 5G). Chociaż nominalnie prywatny, Huawei jest wspierany przez chińskie państwo dzięki subsydiom, a jego założyciel Ren Zhengfei przez lata pracował w jednostkach podległych chińskiej armii, co budzi obawy o jego powiązania z wojskiem i chińskim aparatem bezpieczeństwa. USA pod rządami Donalda Trumpa zaangażowały się w globalną kampanię osłabiania wpływów Huawei. Temat technologicznej dominacji jest kluczowy z pespektywy rywalizacji Pekinu z Waszyngtonem i odcisnął swoje piętno w Polsce, gdzie w tym roku przedstawiciele obu tych państw wdali się w publiczną, wielomiesięczną wymianę poglądów i opinii na temat roli Chin i USA w przestrzeni międzynarodowej. W licznych artykułach, m.in. na portalu Onet.pl oraz w treściach publikowanych na Twitterze, ambasadorowie USA i Chin obwiniali się nawzajem za globalne rozprzestrzenianie się COVID-19, poruszali również kwestię Huawei i problem braku zaufania do firm pochodzących z autorytarnego państwa. Ciężko powiedzieć, która ze stron tej dyskusji zyskała dzięki temu więcej zwolenników, ale na pewno aktywność tego rodzaju jest nowością w polskiej przestrzeni informacyjnej.

W swoim policy paper pt. „Chińska obecność w Polsce: przerwany romans między Pekinem a Warszawą" piszesz, że Pekin korzysta w swojej dyplomacji z różnych metod, w tym obietnic i zachęt, czyli „marchewki" oraz gróźb i prób wymuszeń zachowań, czyli „kija". W przypadku Polski jednak stwierdzasz, że bardziej jednak mamy do czynienia z „marchewką". Czy możemy spekulować jakie więc obietnice i zachęty kierowane są w stronę Warszawy?

Jeśli chodzi o obietnice, moje wnioski wypływają z analizy oficjalnych dokumentów i oświadczeń publikowanych przy okazji wizyt wysokiego szczebla czy innych wydarzeń tego typu. Intensyfikacja stosunków polsko-chińskich miała miejsce tak naprawdę w ostatniej dekadzie: w 2011 r. podpisaliśmy z ChRL umowę o partnerstwie strategicznym, a w 2016 r. została ona podniesiona do. rangi wszechstronnego partnerstwa strategicznego. W międzyczasie Polska poparła również flagowy projekt Xi Jinpinga, czyli Inicjatywę Pasa i Szlaku, znaną również jako Nowy Jedwabny Szlak. Dołączyliśmy też do wielostronnego mechanizmu współpracy między Chinami a państwami Europy Środkowo-Wschodniej, znanego obecnie jako format 17+1. Wszystkim tym działaniom towarzyszyła atmosfera „miodowego miesiąca" relacji Warszawy z Pekinem, a deklaracje obu stron były pełne odniesień do tzw. współpracy o charakterze win-win czy napływu chińskich inwestycji bezpośrednich oraz infrastrukturalnych. Oczekiwania po stronie polskiej były bardzo wysokie i można odnieść wrażenie, że dyplomatyczną retorykę Pekinu traktowano przez pewien czas jako pewnik. Z czasem jednak okazało się, że rzeczywistość nie dorasta do oczekiwań. Jednocześnie postrzeganie ChRL w przestrzeni międzynarodowej zaczęło się powoli zmieniać z nastawienia na bezwarunkową współpracę na bardziej krytyczną ocenę polityki Pekinu. Ryzyko związane ze współpracą z Chinami akcentuje się obecnie coraz częściej, a tematy takie jak zagrożenie uzależnieniem od chińskich technologii czy łańcuchów dostaw wychodzą na pierwszy plan, np. w unijnej debacie na temat znaczenia ChRL dla Europy. W Polsce widać właśnie na przykładzie debaty o udziale Huawei w budowie infrastruktury krytycznej i sieci 5G. Na razie jednak strona chińską nie zastosowała wobec Warszawy żadnych „kijów".



Jak z Twojego punktu widzenia mógłby jednak wyglądać hipotetyczny „kij" zastosowany wobec Polski? I z jakiego powodu mogłaby pojawić się groźba jego użycia w Twojej ocenie?

Wrócę tutaj do tematu Huawei. W międzynarodowej debacie dużo spekuluje się na temat potencjalnych kroków odwetowych, które mógłby podjąć Pekin na wypadek zablokowania tej firmy np. w państwach UE. Wielka Brytania jest w tym kontekście ciekawym przykładem: Londyn długo nie mógł podjąć decyzji w tej sprawie, ale w połowie 2020 r. zadecydował o całkowitym wykluczeniu Huawei z lokalnych sieci 5G. Strona chińska na poziomie retorycznym zareagowała ostro, ale koniec końców Pekin nie zdecydował się na żadne konkretne sankcje wobec Brytyjczyków. Mamy jednak również przykład Australii, której relacje z Chinami przechodzą obecnie poważny kryzys, a Canberra oskarża Pekin o ingerencję w sprawy wewnętrzne i vice versa. Strona chińska posunęła się w tym przypadku nie tylko do pogróżek słownych, ale również do sankcji gospodarczych, m.in. zwiększając taryfy celne na australijskie wina. Doprowadziło to nawet do potrojenia cen tego produktu na chińskim rynku. Pamiętajmy, że ChRL jest największym partnerem handlowym Australii oraz największym rynkiem zbytu dla australijskich win – trafia tam prawie 40% produkcji. Z tej perspektywy widać, że pogłębianie współpracy handlowej z Chinami działa jak obosieczna broń: z jednej strony generuje zyski, ale też częściowo uzależnia dane państwo od chińskiego rynku, co na wypadek napięć politycznych może okazać się bardzo kosztowne w skutkach. Jeśli chodzi o Polskę, to zważywszy na niski poziom zależności ciężko powiedzieć, jakie kroki mógłby podjąć Pekin, by znacząco uderzyć w nas gospodarczo.

Studiowałaś w Chinach i mieszkałaś tam trzy lata. Jak wygląda dla Ciebie to praktyczne doświadczenie wschodzącego mocarstwa, pozycjonującego się na lidera transformacji technologicznej i globalną potęgę rzucającą wyzwanie Stanom Zjednoczonym w skali globalnej? Na ile odczuwalna była druga strona medalu, tj. totalna inwigilacja mieszkańców, brak prywatności, ograniczenie wolności słowa i wypowiedzi i wciąż panujący tam komunizm?

Po raz pierwszy pojechałam do Chin na kurs językowy w 2011 r., studiowałam tam również w latach 2014-2016. Teraz również odwiedzam Chiny regularnie i mogę powiedzieć, że moje doświadczenia z ostatniej dekady potwierdzają tezę, że tempo zmian zachodzących tam jest niezmiernie szybkie. Ma to swoje dobre i złe strony: jeśli chodzi o pozytywy, to np. walka z zanieczyszczeniem powietrza w miastach rzeczywiście przyniosła pewne skutki, ale nie obyło się bez efektów ubocznych, jak np. „wyeksportowania" smogu z miast do obszarów podmiejskich przez relokację działalności przemysłowej. Niestety moje doświadczenia z tej dekady potwierdzają również tezę, że przestrzeń relatywnej wolności w Chinach nieustannie się kurczy: mówię tutaj o ogólnym kształcie debaty publicznej czy nawet tak pozornie trywialnej kwestii jak wybór tytułów w księgarniach czy uniwersyteckich bibliotekach. W 2011 r. byłam w stanie znaleźć w pekińskich księgarniach książki o krytycznym wydźwięku wobec chińskich władz, natomiast w ostatnich latach jest to po prostu niemożliwe.

Jednocześnie trzeba zauważyć, że indywidualny odbiór tej „przestrzeni wolności" w Chinach może znacząco różnić się w zależności od zainteresowań danej osoby. Jeśli twoja działalność mieści się w „bezpiecznych" z perspektywy chińskich władz ramach, represyjne elementy chińskiego systemu politycznego mogą wydawać się mało znaczące czy wręcz demonizowane przez szeroko pojęty Zachód. Jednak jeśli twoja działalność wykroczy nagle poza ten „neutralny obszar", szybko może okazać się, że chińskie władze mają wszelkie narzędzia niezbędne do ograniczenia twojej aktywności w przestrzeni publicznej. Jest to coraz bardziej widoczne pod rządami Xi Jinpinga, które charakteryzuje zwrot ku ideowym źródłom chińskiego marksizmu-leninizmu i zakłada m.in. ograniczanie wpływu zachodnich idei na społeczeństwo ChRL.

Wiele osób, które spędziły w Chinach niewiele czasu, np. biznesowo, wraca z przeświadczeniem, że poglądy o autorytarnej naturze tego państwa są przesadzone – wynika to jednak z niezrozumienia politycznych uwarunkowań różnych aspektów działalności społecznej w ChRL i tego jak są one postrzegane przez władze. Warto również podkreślić, że obcokrajowcy w Chinach są na uprzywilejowanej pozycji: na wiele kwestii związanych z aktywnością osób spoza ChRL władze „przymykają oko", chociaż i to się zmienia. Najtrudniej mają oczywiście chińscy dziennikarze, naukowcy, aktywiści, prawnicy czy szerzej intelektualiści, którzy zajmują się drażliwymi kwestiami – to dla nich autorytarnych charakter chińskiego ustroju jest najbardziej dotkliwy, gdyż może potencjalnie dotknąć nie tylko ich samych, ale również ich bliskich. Nie wspominam tutaj nawet o sytuacji niektórych mniejszości etnicznych, jak np. Ujgurów w regionie Xinjiang, którzy poddawani są obecnie represjom na masową skalę.

Znowu wrócę do porównania z Federacją Rosyjską. Mimo faktu, że dokonuje się tam jednej z największej ilości aborcji, kraj trawiony jest przez korupcję, alkoholizm i narkomanię, a wolności obywateli są wciąż ograniczane, Rosja zbudowała dla wielu zachodnich odbiorców wizerunek obrońcy religii, tradycji i chrześcijańskich wartości, a poprzez stację RT poucza Zachód o niedostatkach jego systemów demokratycznych. Czy widzisz podobne „rozdwojenie jaźni" po chińskiej stronie?

Tak, Chiny od lat starają się promować jako tzw. „odpowiedzialny gracz", chociaż patrząc na obecną politykę tego kraju można szybko zauważyć, jak wiele decyzji Pekinu wcale nie wydaje się tak odpowiedzialna. Podkreśla się m.in. rzekomo pokojową naturę chińskiej cywilizacji czy antyimperializm reżimu KPCh. W historii oczywiście nie brakuje przykładów chińskich działań przeczących tym tezom, niemniej jednak tego rodzaju pacyfistyczna narracja wydaje się atrakcyjna przynajmniej dla części partnerów zagranicznych ChRL, np. z państw rozwijających się lub z innych państw niedemokratycznych, którym taka retoryka jest po prostu na rękę, gdyż pośrednio legitymizuje ich własną politykę.

W raportach wielu służb specjalnych, zwłaszcza tych z państw bałtyckich i skandynawskich regularnie pojawia się wątek rosyjskiej aktywności wywiadowczej wobec studentów i absolwentów. Rosja działa również aktywnie na płaszczyźnie kulturalnej i naukowej. Jak z Twojego punktu widzenia, po praktycznych doświadczeniach studiów, postrzegasz ryzyka wynikające z rozwijania współpracy i wymiany naukowej polskich uczelni czy instytucji z tymi z Chińskiej Republiki Ludowej?

Nie chcę tutaj demonizować wszelkich form współpracy z Chinami – sama byłam beneficjentką chińskiego stypendium rządowego, a doświadczenia zdobyte podczas studiów tam są dla mnie obecnie nieocenione. Jednakże czym innym jest demonizowanie, a czym innym szerzenie świadomości odnośnie zagrożeń związanych ze współpracą z podmiotami z państwa autorytarnego. Wiedza na temat politycznych uwarunkowań współpracy z chińskimi uczelniami w Polsce wydaje mi się niestety ograniczona. Bezkrytyczne podejście w tym wymiarze może poskutkować tym, że np. nasze uczelnie mogą nieświadomie stać się narzędziami szerzenia chińskiej propagandy, w szczególności, jeśli chodzi o nauki polityczne czy społeczne. Również współpraca uczelni technicznych i ścisłych z ChRL z ich zachodnimi odpowiednikami jest coraz częściej przedstawiana jako potencjalne zagrożenie w związku z oskarżeniami o szpiegostwo technologiczne.

Na koniec może jeszcze pytanie o przyszłość. Jak prognozujesz ewolucję chińskich działań informacyjnych w najbliższych latach? Obecnie te działania nie są jeszcze tak zaawansowane jak te rosyjskie, ale Chiny szybko się uczą, a do tego mają nieporównywalnie większe zasoby od Rosji.

Spodziewałabym się, że chińskie działania w przestrzeni informacyjnej będą kontynuowane. Nic nie wskazuje na to, żeby Pekin miał rezygnować z obecnego asertywnego kursu i międzynarodowej ekspansji. Chińskie władze chcą mieć większy wpływ na kształtowanie obrazu ChRL na świecie, mają również środki, by promować własny model ustrojowy jako alternatywę dla liberalnej demokracji. Powstają kolejne międzynarodowe inicjatywy mające na celu rozprzestrzenianie tego typu narracji, np. w formule BRICS, w ramach której organizowane są szczyty przedstawicieli mediów z ChRL, Rosji, Brazylii, Indii i RPA. Również w naszym regionie Chiny podejmują podobne działania: 2017 r. był oficjalnym rokiem współpracy medialnej we wspomnianym wcześniej formacie 17+1. Chińska państwowa agencja prasowa Xinhua podpisała umowy z wieloma podmiotami z Europy Środkowo-Wschodniej, a dziennikarze z regionu wyjechali na szereg wizyt studyjnych do Chin. Również polskie państwowe podmioty, jak np. TVP, podpisały umowy o współpracy z chińskimi mediami.

Chociaż chińska motywacja do kształtowania przestrzeni informacyjnej na własną korzyść nie słabnie, moja ocena tych działań jest niejednoznaczna. Tak jak wspomniałeś, Pekin szybko się uczy, jednak najnowsze badania wskazują, że w ostatnich latach stosunek opinii publicznej do Chin w wielu państwach Europy uległ drastycznemu pogorszeniu. Czas pokaże, czy chińskie władze będą w stanie zmodyfikować przekaz, aby odpowiadał on bardziej zachodnim gustom. Osobiście nie wydaje mi się jednak, by leżało to w polskim czy europejskim interesie, zważywszy na destrukcyjny charakter tego typu narracji dla demokratycznych standardów współpracy.

Alicja Bachulska

Analityczka ds. polityki Chin w Ośrodku Badań Azji Centrum Badań nad Bezpieczeństwem Akademii Sztuki Wojennej. Koordynuje w Polsce międzynarodowy projekt MapInfluenCE monitorujący chińskie i rosyjskie wpływy w państwach Grupy Wyszehradzkiej. Jest absolwentką londyńskiej uczelni School of Oriental and African Studies (SOAS) oraz Uniwersytetu Fudan w Szanghaju. Przez rok uczyła się również języka mandaryńskiego na Beijing Normal University w Pekinie. Obecnie pracuje nad doktoratem w Szkole Nauk Społecznych Polskiej Akademii Nauk.

Twitter: @a_bachulska

Komentarz:

Mgła tajemnicy i milczenia wokół rosyjskich cyberwojsk

Temat rosyjskich cyberwojsk, a precyzyjnie Wojsk Operacji Informacyjnych jest od 2017 roku praktycznie nieporuszany i nie ma o nim praktycznie żadnych publikacji. Co ciekawe jednak, na koniec 2019 roku Ministerstwo Obrony Federacji Rosyjskiej ogłosiło rozmieszczenie oddziałów cybernetycznych w każdym z okręgów wojskowych Rosji w połowie 2020 roku. Od tamtej pory nie ten wątek nie pojawił się publicznie. Co to może oznaczać dla Zachodu, biorąc pod uwagę, że do rosyjskich działań jest wciąż więcej pytań niż odpowiedzi?

Dla Rosji cyberwojska oznaczają coś zupełnie innego niż dla Zachodu. Pierwszym, kto publicznie mówił o potrzebie stworzenia cyberdowództwa Federacji Royjskiej był wicepremier Dmitri Rogozin. Miało to miejsce w 2012 roku. Zostało ono utworzone w 2014 roku w Sztabie Generalnym Sił Zbrojnych FR. Oficjalnie jego głównym zadaniem była ochrona przed zewnętrznymi ingerencjami w wewnętrzne systemy komunikacji i dowodzenia. Od tego właśnie czasu datuje się powstanie formalnych struktur cyberwojsk w Rosji.

W 2017 roku na posiedzeniu Dumy Państwowej, odpowiadając na pytanie o potrzebie odtworzenia wydziału kontrpropagandy, Minister Obrony FR Siergiej Szojgu poinformował już publicznie, że stworzone zostały Wojska Operacji Informacyjnych *(ros. Войска Информационных Операций)*. Miały być one znacznie silniejsze i skuteczniejsze od wcześniejszych rozwiązań z czasów sowieckich. Co ciekawe przez pewien czas oficjalnie niektórzy przestawiciele państwa rosyjskiego zaprzeczali istnieniu jakichkolwiek cyberwojsk.

Stanem na 2017 rok oficjalna liczba rosyjskich cyberżołnierzy wynosiła 1000 osób. Dla porównania, z rosyjskich danych wynikało, że inne mocarstwa dysponowały wtedy odpowiednio:

Cała klasyfikacja stworzona była przez stronę rosyjską i zgodnie z tamtejszymi przekazami Rosja weszła wtedy do pierwszej piątki najbardziej rozwiniętych państw świata pod kątem komponentu cybernetycznego w strukturach wojskowych. Ten ranking zbudowany był bowiem pod kątem realnego potencjału, a nie pod kątem ilościowym. Biorąc pod uwagę rosyjskie działania informacyjne, a zwłaszcza dezinformację, nie należałoby przeceniać znaczenia danych pochodzących od samych Rosjan. Na tamten moment można było traktować taki ranking jako projekcję rosyjskich aspiracji w tym zakresie.

Należy też zauważyć, że zagadnienie rosyjskich cyberżołnierzy i ich liczby związane jest z kilkoma płaszczyznami. Jedną z najistotniejszych z punktu widzenia Zachodu jest fakt podejścia do działań informacyjnych jako takich, czyli łączenie aspektów cybernetycznych z informacyjnymi. Dla Rosji nie ma bowiem rozróżnienia pomiędzy przestrzenią informacyjną (infosferą) a cyberprzestrzenią, tak jak jest to powszechne w zachodnich koncepcjach czy rozwiązaniach. Innym, nie mniej ważnym zagadnieniem jest tajność prowadzonych działań i wynikająca z niej blokada informacyjna, a więc i niedostępność danych nawet o liczebności Wojsk Operacji Informacyjnych. Te dwa czynniki utrudniają analizę działań rosyjskich w tym obszarze. Nawet gdyby znana była szacunkowa ilość komponentu stricte militarnego, to wciąż nie byłoby jasne jaki procent tej formacji pracuje na odcinku cybernetycznym (np. w obszarze twardego cyberbezpieczeństwa), a jaki rzeczywiście nad operacjami informacyjnymi.

Warto również podkreślić, że obok jednostek wojskowych, w rosyjskich operacjach przeciwko państwom zachodnim biorą także udział i inne struktury. Doskonałym przykładem na to będzie jednostka wojskowa 54777 Głównego Zarządu Wywiadowczego Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej, która odpowiada m.in. za działania psychologiczne. Co więcej, inne podmioty państwowe również biorą aktywny udział w operacjach informacyjnych i na odcinku cyber, jak chociażby wywiad cywilny, tj. Służba Wywiadu Zagranicznego Federacji Rosyjskiej czy kontrwywiad, tj. Federalna Służba Bezpieczeństwa.

Z informacji ukraińskich wiemy, że oddziały wojsk informacyjnych wchodzą w skład centrów wojny informacyjnej, obecnych w okręgach wojskowych Sił Zbrojnych Federacji Rosyjskiej. W operacjach przeciwko Ukrainie bezpośrednio brała udział sieć ośrodków Południowego Okręgu Wojskowego Sił Zbrojnych RF w składzie w 8. Armii Obrony Powietrznej z dowództwem w Nowoczerkasku. W Kijowie wyróżniono cztery oddzielne wydziały centrów wojny informacyjnej:

a) Wydział I - „Izolacji informacyjnej pola walki”, który odpowiada za neutralizację systemów telekomunikacyjnych, systemów podtrzymywania życia czy emisję sygnału telewizyjnego i radiowego na określonych terenach,

b) Wydział II – „Osłony informacyjnej wojsk, dezinformacji i kontrpropagandy”, który jest odpowiedzialny za dokumentację bojową (w tym fotograficzną i wideo), dezinformację i kontrpropagandę,

c) Wydział III – „Interakcji cywilno-wojskowych, pracy z ludnością na kontrolowanych terytoriach i rozstrzygania konfliktów”, który współpracuje z władzami, ludnością i jest odpowiedzialny za prowadzenie działań humanitarnych,

d) Wydział IV – „Wsparcia informacyjnego”, który odpowiada za wsparcie lingwistyczne i tzw. „materiały specjalne”.

Przy ocenie sytuacji bezpieczeństwa związanej z działaniami Federacji Rosyjskiej nie należy zapominać o szerszym kontekście politycznym i geopolitycznym. Jednym z nich jest Organizacja Układu o Bezpieczeństwie Zbiorowym (OUBZ), do której poza Rosją należą: Armenia, Białoruś, Kazachstan, Kirgistan i Tadżykistan. W ciągu ostatnich lat obserwujemy starania Rosji mające na celu aktywizację komponentu bezpieczeństwa informacyjnego w ramach OUBZ. Na przykład w 2019 roku weszła w życie Umowa o współpracy w zakresie bezpieczeństwa informacyjnego *(ros. Соглашение о сотрудничестве в области обеспечения информационной безопасности).* Natomiast na początku grudnia tego roku miała miejsce wspólna deklaracja Rady OUBZ w kwestii możliwości stworzenia centrum informacyjno-analitycznego Co więcej, państwa członkowskie mają zintensyfikować współpracę w celu wspólnego przeciwdziałania zagrożeniom i wyzwaniom w przestrzeni informacyjnej, w tym w ramach Operacji PROXY *(ros. операция „ПРОКСИ”).*

Innymi słowy do faktu utrzymywanej w tajemnicy liczby rosyjskich żołnierzy informacyjnych można uwzględniać także i hipotetyczne działania państw Organizacji Układu o Bezpieczeństwie Zbiorowym i ich analogicznych struktur militarnych, które mogą być instrumentalnie wykorzystywane przez Rosję. W ten sposób Kreml byłby w stanie udowadniać brak swojego rzekomego zaangażowania w pewne operacje, np. przeciwko państwom zachodnim. Niezależnie od tego, że realne zdolności rosyjskie w cyberprzestrzeni są trudne do zmierzenia i oszacowania, widać wyraźnie, że Kreml od lat buduje i wzmacnia swoje zasoby w tym obszarze. Coraz bardziej zaawansowane stają się również prace w wymiarze prawno-instytucjonalnym. Wykorzystywany jest do tego także i fakt, iż zachodni sepołeczeństwa wciąż nie zdają sobie sprawy z natury zagrożeń informacyjnych i psychlogicznych oraz aspektu traktowania łącznie infosfery i cyberprzestrzeni przez Rosję.

Adam Lelonek, Denys Kolesnyk

Analiza:

Bezpieczeństwo informacyjne jako wektor współpracy dla Japonii i Europy

Wyzwania informacyjne, psychologiczne i cybernetyczne idą w parze z tymi gospodarczymi i politycznymi. Rosnąca aktywność Pekinu powoduje, że rozważanie pogłębiania i zacieśniania relacji ekonomicznych i politycznych przez Japonię i Europę staje się coraz bardziej zasadne. Tak jak państwa europejskie od wielu lat zmagają się z zagrożeniem ze strony rosyjskiej, a przez ostatnie lata dopiero rozpoczynają badania nad aktywnością Chin, tak Japonia od wielu lat zmaga się z wyzwaniami pochodzącymi tak z Rosji, jak i Chin oraz Korei Północnej. Doświadczyła ich zresztą w zupełnie innej skali i dysponuje swoim własnym *know how* oraz możliwościami technologicznymi, które mogłyby być wykorzystane w Europie.

Wprowadzenie

Na przestrzeni ostatnich lat Zachód prowadził działania reaktywne wobec zagrożeń informacyjnych. Do dnia dzisiejszego wciąż powszechne jest nadmierne skupianie się na skutkach oraz niesystemowych próbach neutralizacji konsekwencji tych zagrożeń, a nie na badaniu i przeciwdziałaniu ich przyczynom, jak chociażby podatności odbiorców informacji i ewolucji modeli konsumpcji informacji. Dezinformacja stała się synonimem fałszywych informacji (fake news), a ich demaskowanie ukonstytuowało mainstreamową perspektywę na wysiłki mające na celu przeciwdziałanie zagrożeniom informacyjnym w krajowych przestrzeniach informacyjnych. Innymi słowy interdyscyplinarne i wielowymiarowe zagadnienie bezpieczeństwa informacyjnego zamknięte zostało w jednej tylko płaszczyźnie – dziennikarskiej. Ogranicza to nie tylko skuteczność odpowiedzi na wyzwania w tym obszarze, ale także możliwości budowania prawdziwej odporności społecznej, gdyż społeczeństwa zachodnie pozostają wciąż nie w pełni świadome skali i natury zagrożeń.

Identyfikacja i ekspozycja fałszywych informacji czy weryfikacja faktów (fact checking), choć potrzebne, okazały się dalece niewystarczającymi narzędziami do budowy realnej odporności na poziomie społecznym. Mają one też ograniczone efekty w kwestii neutralizacji negatywnych tendencji wynikających z wrogich oddziaływań informacyjnych i psychologicznych. Między innymi dlatego, że zjawisko tzw. baniek informacyjnych, tj. funkcjonowania zamkniętych obszarów poznawczych, wraz z innymi tendencjami i trendami obecnymi w krajowych przestrzeniach informacyjnych ogranicza docieranie z takimi działaniami do podatnych grup odbiorców. Potwierdzają to kolejne badania czy ewaluacje projektów, prowadzonych w skali krajowej, regionalnej czy globalnej i są to wnioski czołowych ośrodków badawczych na świecie. Przez lata zresztą to samo powtarzało spore grono ekspertów po obu stronach Oceanu Atlantyckiego. Obecnie podobnego zdania są już i autorzy oraz wykonawcy szeregu projektów poświęconych demaskowaniu fałszywych informacji.

Inter-dyscyplinarna natura zagrożeń informacyjnych

Bezpieczeństwo informacyjne jest pojęciem interdyscyplinarnym, łączącym wiele aspektów – od nauk humanistycznych, przez psychologię, kognitywistykę, nauki o bezpieczeństwie i komponent militarny, aż do obszaru IT i cyberbezpieczeństwa. Najczęściej w przestrzeni informacyjnej dominuje tylko jedna wykładnia interpretacyjna, tj. wywodząca się ze świata dziennikarskiego. Jest ona poniekąd fundamentem dla poznania i rozumienia środowiska informacyjnego i jego mechanizmów, lecz pozostaje niewystarczająca dla zrozumienia złożonej natury zagrożeń informacyjnych. Tym bardziej nie pozwala ona na przygotowanie adekwatnej i skutecznej odpowiedzi na poziomach krajowych.

W przestrzeni publicznej najczęściej używanymi pojęciami związanymi z zagrożeniami informacyjnymi są wspomniane już **fałszywe informacje** oraz **dezinformacja.** Od początku prezydentury Donalda Trumpa w świecie anglosaskim na popularności zyskało również określenie **narracje**. Używane jest tam jednak najczęściej wyłącznie w rozumieniu działań politycznych i w kontekście wewnętrznym Stanów Zjednoczonych. Oprócz tego pojawia się wątek cyberbezpieczeństwa, jak chociażby wykorzystanie algorytmów i kont o różnym poziomie automatyzacji **(botów)** oraz tzw. **trolle** (realni użytkownicy, działający celowo, świadomie, a w przypadku zorganizowanych działań także odpłatnie, rozpoczynając konflikty czy wpływając na dyskusje w sieci). Dodatkowo częściowo odnoszono się do pojęcia **deepfake**, czyli realistycznego materiału audio lub wideo, przygotowanego za pomocą programu komputerowego, mającego wprowadzać w błąd odbiorców.

Z punktu widzenia zagrożeń informacyjnych, wszystkie te działania są różnymi formami manipulacji informacją. Mimo faktu, że większość tych działań prowadzonych jest w cyberprzestrzeni, zachodnie koncepcje cyberbezpieczeństwa nie łączą w sobie komponentów bezpieczeństwa informacyjnego. Wciąż rozdzielnie traktuje się sferę informacyjną (tzw. infosferę), rozumianą jako przestrzeń mediów tradycyjnych oraz cyberprzestrzeń, która rozpatrywana jest głównie wyłącznie przez pryzmat twardego bezpieczeństwa. Jest tak i na poziomie NATO, Unii Europejskiej, ale i na poziomach krajowych. Odróżnia to Zachód od Rosji, Iranu czy Chin.

Wielu ekspertów od lat zwraca uwagę na sztuczność wydzielania infosfery i cyberprzestrzeni jeżeli chodzi o współczesne zagrożenia informacyjne. Manipulacja informacją z kolei ukierunkowana jest na wpływanie na procesy poznawcze (kognitywne). Chodzi tu więc o to, jak patrzymy na świat i nasze otoczenie (w tym np. na procesy polityczne czy sytuację w kraju), jak przetwarzamy informacje, które do nas docierają, ale także na pamięć, analizę, postrzeganie nas samych i innych oraz myślenie. Przenosząc to na poziom ogólny dla znalezienia analogii, w przypadku wojny informacyjnej na poziomie politycznym, działania z nią związane podejmowane dla osiągnięcia przewagi informacyjnej poprzez wpływanie na informacje przeciwnika, procesy oparte na przetwarzaniu informacji, systemy informacyjne oraz sieci komputerowe przy jednoczesnej ochronie własnych informacji, procesów opartych na przetwarzaniu informacji, systemów informacyjnych oraz sieci komputerowych. Analogicznie więc, na indywidualnym, poznawczym poziomie jednostek, działania wymierzone w sferę kognitywną są w rzeczywistości aktywnościami podejmowanymi przeciwko naszej świadomości, tj. umysłowi. Tak właśnie do tej kwestii podchodzi Federacja Rosyjska na oficjalnym poziomie państwowych doktryn bezpieczeństwa i polityki – wojna informacyjna jest skierowana przeciwko umysłowi przeciwnika.

Aby prawdziwie zmienić społeczną percepcję zagrożeń informacyjnych warto rozważyć odchodzenie od zawężania tego tematu do wyłącznie pewnych form manipulacji informacją (fake news, dezinformacja, deepfake) i rozszerzania terminologii dla odbiorcy masowego. Walka o umysły czy walka o świadomość są formą, którą Japończycy w swoich strategiach określają jako **naruszenie domeny kognitywnej** (ang. infringement on cognitive domain). Poszukiwanie nowych form docierania do odbiorcy masowego związane będzie więc nie tylko z mechanicznym usprawnianiem komunikacji strategicznej państw i instytucji, ale będzie znajdować realne przełożenie na poziom bezpieczeństwa krajowego, w tym bezpieczeństwo informacyjne i cyberbezpieczeństwo. Adaptacja używanego języka i sposobu przedstawiania informacji powinna być uzupełniona nie tylko o kontekst potrzeb i nawyków różnych grup odbiorców informacji, ale i trendy oraz sytuację w danej sferze na poziomie praktycznym.

Inter-dyscyplinarna natura zagrożeń informacyjnych

Militaryzacja kwestii cyber-bezpieczeństwa i bezpieczeństwa informacyjnego

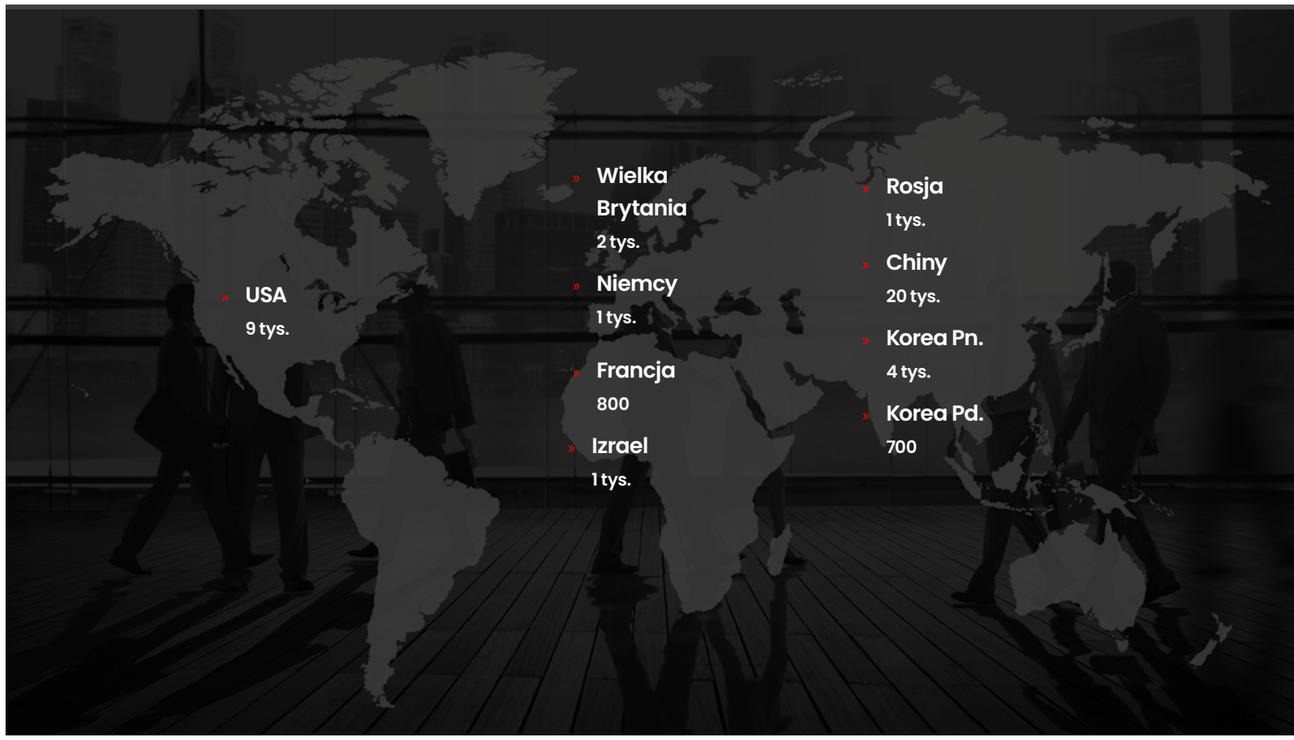
Najlepszym przykładem do analizy skali i poziomu zagrożenia w obszarze bezpieczeństwa informacyjnego będzie polityka rosyjska. Dla Kremla przestrzeń informacyjna stała się jedną z priorytetowych domen nie tylko dla współczesnych konfliktów zbrojnych, ale i w czasie pokoju. Wskutek braków w innych obszarach, komponent walki informacyjnej rozwijany jest od czasów Związku Radzieckiego i wykorzystuje szereg rozwiązań i doświadczeń z tamtego okresu, które zostały rozwinięte i zaadaptowane do nowych realiów technologicznych. Rosyjska koncepcja wojny informacyjnej zakłada także prowadzenie działań psychologicznych z wykorzystaniem komponentów cybernetycznych. Całościowo więc powinno mówić się o współczesnej wojnie informacyjnej i psychologicznej, prowadzonej w cyberprzestrzeni. Co więcej, w rosyjskich koncepcjach taka forma walki traktowana jako alternatywa dla wojny konwencjonalnej, w tym konfliktu nuklearnego.

Istotnymi krokami praktycznej materializacji tych koncepcji było powołanie Cyberdowództwa w Sztabie Generalnym Sił Zbrojnych Federacji Rosyjskiej w 2014 roku. Od tego właśnie czasu datuje się także utworzenie tzw. Wojsk Operacji Informacyjnych w strukturach Sił Zbrojnych Federacji Rosyjskiej, do czego Rosja przyznała się oficjalnie dopiero w 2017 roku. Wojska Operacji Informacyjnych to praktyczne połączenie i materializacja rosyjskich koncepcji w spójną całość. Potwierdza to, że dla Rosji nie ma rozróżnienia pomiędzy cyberbezpieczeństwem a bezpieczeństwem informacyjnym, gdyż te dwie domeny traktowane są łącznie. Należy też pamiętać, że nowa formacja wojskowa to tylko jeden z elementów rosyjskich zdolności w cyberprzestrzeni. Inne, analogiczne działania prowadzone są przez służby specjalne, cywilne i wojskowe oraz inne podmioty, w tym niepaństwowe czy prywatne, a także mogą być prowadzone przez podmioty zagraniczne.

Wojna informacyjna jest dla Rosji narzędziem realizacji celów w polityce zagranicznej. Takie działania prowadzone były już w kilkunastu państwach na świecie, w tym m.in. w Stanach Zjednoczonych, Wielkiej Brytanii, Francji, Hiszpanii, Niemczech czy Polsce. Szerokie spektrum rosyjskich operacji informacyjnych i psychologicznych prowadzonych w cyberprzestrzeni ujrzało światło dzienne podczas wyborów prezydenckich w USA w 2016 roku, które poprzedziły bezprecedensowe działania strony rosyjskiej, zwłaszcza te niejawne, z wykorzystaniem służb specjalnych. Szczególnie istotny jest fakt, iż działania w cyberprzestrzeni były ściśle koordynowane z tymi w infosferze. Przykład Ukrainy z kolei pokazuje ścisłą koordynację operacji informacyjnych i psychologicznych z działaniami militarnymi, politycznymi i ekonomicznymi, co składa się na definicję tzw. wojny hybrydowej, wykorzystującej różne komponenty działań przeciwko przeciwnikowi.

Rozwijanie koncepcji wojny informacyjnej z wykorzystaniem komponentu cyber, w tym prowadzenie jej w cyberprzestrzeni to nie tylko domena rosyjska. Podobne prace prowadzone są przez Chińską Republikę Ludową, Iran czy Koreę Północną. Państwa te wykorzystują struktury cywilne i wojskowe, a także podmioty prywatne, grupy i indywidualnych hakerów, narzędzia oparte na sztucznej inteligencji, algorytmy i zautomatyzowane konta w mediach społecznościowych, ataki cybernetyczne oraz przypominające pracę agencji informacyjnych tzw. farmy trolli. Wszystko to koordynowane jest na poziomie państwowym i służy oddziaływaniu na inne społeczeństwa poprzez dostarczanie określonych treści, ukierunkowywanie debaty publicznej lub jej zakłócanie, a docelowo także i wpływanie na percepcję całych społeczeństw lub wybranych grup odbiorców. Kształtuje to odpowiednie uwarunkowania dla innych działań w obszarze militarnym, politycznym, kulturowym, społecznym lub ekonomicznym. Nie pozostaje to również bez wpływu na atakowane środowisko informacyjne, tym bardziej, że wiele z takich operacji planowane jest na lata, a nawet dziesięciolecia.

Wszystko wskazuje także na to, że te zdolności będą tylko rozwijane, a proces ich zaawansowania i profesjonalizacji będzie tylko wzrastał. Według rosyjskich danych, czyli takich, co do których można podchodzić jednak z pewną dozą sceptycyzmu, w 2017 roku szacunki liczebne dla wyłącznie komponentu militarnego czołowych państw na świecie to odpowiednio:



Dla porównania według aktualnych szacunków Japońskich, stanem na 2020 rok Chiny dysponują już 30 tys. cyberżołnierzy, a Korea Północna ok. 7 tys. Można zakładać, że inne państwa z tej listy także zwiększyły stan liczebny swoich zasobów. Sama Japonia planuje przekroczyć kontyngent 1 tys. cyberżołnierzy dopiero w 2023 roku. Dane na temat Rosji czy Iranu są utajnione.

Doktryny militarne odnoszą się do uzyskania przewagi nad przeciwnikiem w przestrzeni informacyjnej na różnych etapach prowadzonego konfliktu. Także przed jego rozpoczęciem. Długofalowe aktywności skierowane na podważanie zaufania obywateli do instytucji państwowych, procedur demokratycznych, elit, polityków, sojuszy i systemu międzynarodowego, a wreszcie i budowanie antagonizmów w regionie, na poziomie krajowym czy lokalnie spełnia kryteria wojny informacyjnej. Docelowo operacje informacyjne i psychologiczne prowadzone w cyberprzestrzeni mogą być także uzupełniane o komponenty kinetyczne, jak działania dywersyjne czy wykorzystanie tzw. zielonych ludzików, jak miało to miejsce na Ukrainie.

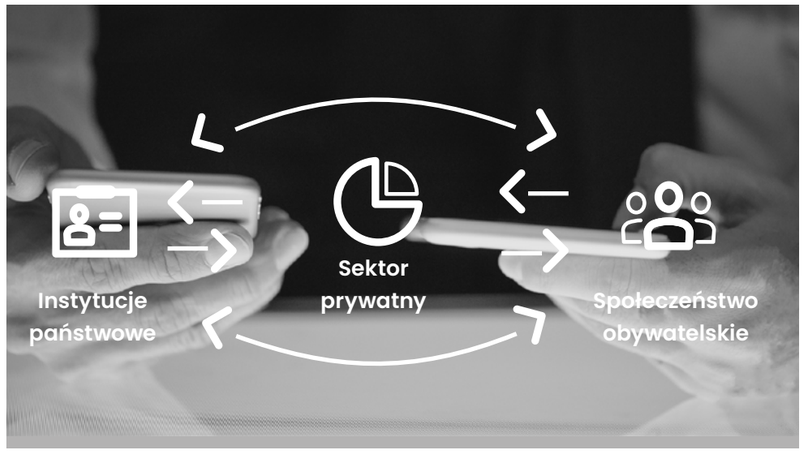
Bezpieczeństwo informacyjne obejmować będzie budowanie odporności na poziomach krajowych, ale i przygotowanie proaktywnej odpowiedzi we wszystkich płaszczyznach życia społecznego i funkcjonowania państw. Działania Zachodu, ograniczające odpowiedź na te wyzwania wyłącznie do kuluarowych rozmów czy prac w zamkniętych środowiskach, a zwłaszcza analogiczna ich militaryzacja w warunkach systemów demokratycznych tylko utrudniają procesy wzmacniania odpowiedzi społecznej. Nie da się bowiem zamknąć sfer: gospodarczej, społeczno-politycznej, kulturowej, naukowej, dyplomatycznej i informacyjnej w ramach wyłącznie struktur państwowych, w tym jedynie militarnych. Nie jest również realne przygotowanie odpowiedzi społecznej na jednoczesne wyzwania związane z komponentami technologicznymi, cybernetycznymi, informacyjnymi i psychologicznymi bez ścisłej współpracy i dialogu ze społeczeństwem obywatelskim, a w szerszym ujęciu – rozwijania transparentnej współpracy międzynarodowej.

Poza bezpieczeństwem informacyjnymi obywateli, bezpieczeństwem krajowej infosfery i ekosystemu informacyjnego (w sposób szczególny funkcjonowania mediów), a także komponentami militarnymi, celami mogą być wreszcie inne obiekty, jak chociażby Infrastruktura krytyczna, w tym elektrownie, szpitale, infrastruktura komunikacyjna czy energetyczna, ale i funkcjonowanie różnych gałęzi przemysłu czy systemów krytycznych państwa – od komunikacji po opiekę medyczną. W sposób szczególny odnieść się można także do bezpieczeństwa wyborów i zabezpieczenia procedur demokratycznych. Sytuacja z globalną pandemią SARS-CoV-2 pokazała także, że określone działania informacyjne i psychologiczne stanowią bezpośrednie zagrożenie dla funkcjonowania państw na każdej jego płaszczyźnie. Zaawansowanie i rozwój technologiczny, zwłaszcza sieci 5G i 6G będą wymuszać na demokracjach szczególne podejście do kwestii cyberbeczpieczeństwa, prace nad identyfikacją podatności, ale i edukację społeczeństw, aby redukować negatywne skutki oddziaływań infoagresorów, dążących do destabilizacji sytuacji wewnętrznej. Poza więc sferą wojskową i psychologiczną, pojawia się komponent fizycznego bezpieczeństwa, ładu i porządku publicznego. Rosnący poziom współzależności i komunikacji powoduje, że coraz trudniej będzie radzić sobie z tymi wyzwaniami państwom indywidualnie, bez rozwijania zaawansowanej współpracy strategicznej.

Odporność społeczna *(societal resilience)*

W doktrynach wojskowych psychologiczne komponenty odporności na poziomie państwowym:
- poziom patriotyzmu
- poziom optymizmu
- stopień spójności społecznej
- zaufanie do instytucji publicznych i politycznych

W szerokim ujęciu rozpatrywać należy także m.in.: poziom wiedzy i świadomości społecznej na temat zagrożeń informacyjnych, funkcjonowanie mediów, uwarunkowania historyczno-kulturowe, podejście elit, wolę polityczną, stan komunikacji strategicznej, ramy prawno-systemowe, działania i poziom współpracy państwa z sektorem prywatnym, działania korporacji technologicznych oraz współpracę pomiędzy społeczeństwem obywatelskim a instytucjami państwowymi.



Działania związane z podnoszeniem poziomu odporności społecznej są nie tylko wyłączną domeną, w której aktywne mogą być wyłącznie państwa narodowe i struktury krajowej administracji. Szereg inicjatyw w tym obszarze jest prowadzonych, finansowanych i koordynowanych przez instytucje zagraniczne, w tym komórki administracji państwowej innych państw, w tym przez ambasady czy fundacje. Głównymi obszarami, w których jest to na chwilę obecną rozwijane w Polsce, to edukacja medialna, fact checking i identyfikacja fałszywych informacji. W związku z tym jest ogromny potencjał dla rozwoju współpracy międzynarodowej w regionie, ale i w skali globalnej. Indywidualne doświadczenia krajowe pozwolą bowiem na precyzyjniejsze analizy, dokładniejsze prognozy oraz szybszą identyfikację potrzebnych aktywności i rozwiązań.

Możliwości rozwoju współpracy pomiędzy Europą a Japonią

Państwa demokratyczne wybierają zupełnie inną ścieżkę prawno-systemową dla rozwoju komunikacji, w tym sieci internet. Koncepcja cyfrowej suwerenności staje się właściwa dla państw autorytarnych i niedemokratycznych, dążących do ograniczania wolności i swobód obywatelskich. Przeciwległym biegunem do tego modelu jest podejście państw zachodnich, a zwłaszcza Unii Europejskiej, Stanów Zjednoczonych i Japonii. Ewolucja w tym obszarze wymaga zacieśniania współpracy na poziomie międzynarodowym oraz koordynacji i implementacji pewnych rozwiązań w całym świecie zachodnim, które mogą służyć za wzór i standard dla innych, a jednocześnie pomogą wzmocnić rządy indywidualnie wobec potencjalnych agresywnych działań Chin oraz podmiotów prywatnych.

Mamy tu do czynienia nie tylko z aspektem wewnątrzpaństwowym, ale i globalnym, a nawet z płaszczyzną idei i filozofii. Konkurencja w obszarze technologicznym i innowacji nie jest bowiem w geopolitycznej próżni. Zmiany zachodzące w środowisku bezpieczeństwa powodują, że z konkurentów Europa i Japonia stają się bliskimi sojusznikami tak w obszarze wysokiej technologii, jak i informacji, ale i bezpieczeństwa, w tym cyberbezpieczeństwa. Jednym z aspektów, który przez lata kształtował postrzeganie Zachodu i determinował atrakcyjność jego rozwiązań prawno-systemowych był kapitalizm oraz wolności i swobody obywatelskie. Podobnie należałoby długoterminowo podchodzić do wykładni funkcjonowania cyberprzestrzeni, w odróżnieniu od państw, które dążą do cenzury i ograniczania wolności komunikacji, prezentować swój własny model, korzystając z zaplecza technologicznego i we współpracy z największymi firmami technologicznymi świata, przywiązanymi do zachodnich wartości.

Podczas zamkniętych debat Japan-Europe Core Group in Warsaw, zorganizowanych przez European Council on Foreign Relations Warsaw, podkreślono, że elementy związane z rosnącą militaryzacją cyberprzestrzeni przestały być abstrakcyjnymi i hipotetycznymi zagadnieniami, ale stały się codziennym wyzwaniem już nie tylko dla armii na całym świecie. Nie tylko przestępcy podejmują aktywne działania w cyberprzestrzeni. Rośnie liczba celowych ataków hakerów i zorganizowanych grup, ale także udział podmiotów państwowych, w tym służb specjalnych. Do tego w przypadku krajów autorytarnych powszechne jest wykorzystywanie cywilów oraz osób innych narodowości do realizacji określonych zadań (taki model wykorzystany był np. przez Koreę Północną, która wynajęła rosyjskich obywateli do przeprowadzania cyberataków na Sony Pictures w 2014 roku). Z punktu widzenia działań aktorów państwowych, szczególnie niebezpieczne są długoterminowe działania, w tym instalacja złośliwego oprogramowania w krytycznych systemach oraz inne formy ich penetracji do wykorzystania w przyszłości. Nie ulega wątpliwości, że zarówno Europa jak i Japonia stoją obecnie przed analogicznymi wyzwaniami w obszarach: bezpieczeństwa, technologii, prawno-instytucjonalnym, a nawet politycznym.

Możliwości rozwoju współpracy pomiędzy Europą a Japonią

Mimo różnic kulturowych stajemy przed podobnymi zagrożeniami na poziomie wewnętrznym i międzynarodowym. Szczególnie istotne będzie tu opracowanie strategii przeciwdziałania zagrożeniom w cyberprzestrzeni i tym związanym z oddziaływaniami informacyjnymi i psychologicznymi. Rozwój zdolności obronnych i ofensywnych wymagać będzie w pierwszej kolejności syntezy i adaptacji szerokiego spektrum czynników, w tym przede wszystkim bezpieczeństwa informacyjnego i cyberbezpieczeństwa, z czym Japonia, podobnie jak państwa europejskie, wciąż sobie nie poradziła. Wśród priorytetowych tematów będą również kwestie: wykorzystania sztucznej inteligencji, sieci 5G i 6G oraz internet rzeczy *(ang. Internet of things , IoT)*.

Istnieje ogromny potencjał współpracy w obszarze wymiany doświadczeń z zakresu identyfikacji, analizy i przeciwdziałania zagrożeniom informacyjnym i cybernetycznym. Tak jak państwa europejskie od wielu lat zmagają się z zagrożeniem ze strony rosyjskiej, a przez ostatnie lata dopiero rozpoczynają badania nad aktywnością Chin, tak Japonia od wielu lat zmaga się z wyzwaniami pochodzącymi tak z Rosji, jak i Chin oraz Korei Północnej. Doświadczyła ich zresztą w zupełnie innej skali i dysponuje swoim własnym *know how* oraz możliwościami technologicznymi, które mogłyby być wykorzystane w Europie.

Wyzwania informacyjne, psychologiczne i cybernetyczne idą poniekąd w parze z tymi gospodarczymi i politycznymi. Rosnąca aktywność Pekinu powoduje, że rozważanie pogłębiania i zacieśniania relacji ekonomicznych i politycznych przez Japonię i Europę staje się coraz bardziej zasadne. „Tektoniczna zmiana" potęgi państw w stronę nowych technologii będzie miała znacznie poważniejsze konsekwencje niż poprzednie, bardziej tradycyjne zmiany wynikające z kwestii politycznych i gospodarczych. Widać tu nową rolę dla Europy, której przyszłość zdeterminowana zostanie przez rozwój wysokiej technologii, ale i poziom kooperacji ze Stanami Zjednoczonymi i Japonią.

Biorąc pod uwagę rywalizację amerykańsko-chińską, ale i różne scenariusze geopolityczne, w tym m.in. potencjalny sojusz chińsko-rosyjski przeciwko USA, otwierają się nowe wymiary dla analizy kierunków współpracy. Poza odpornością społeczną, już teraz należy myśleć także o **odporności technologicznej** (technological resilience). Związane to będzie także z budowaniem wizerunku marek i produktów, ale i budową zaufania tak na poziomie politycznym, jak i do prywatnego biznesu. Dalej istotne będzie też kształtowanie zwyczajów, norm, standardów oraz rozwiązań prawnomiędzynarodowych w cyberprzestrzeni. Są to elementy, które kształtować będą nowy ład międzynarodowy. Na tych wszystkich odcinkach Japonia i Europa mają sobie dużo do zaoferowania.

Wnioski i zalecenia

- Działania Zachodu mające na celu identyfikację i ekspozycję różnych form manipulacji informacją, a zwłaszcza fact checking i demaskowanie fake news były i pozostają ograniczone z punktu widzenia realnych efektów na odbiorców informacji na poziomie krajowym i międzynarodowym,
- Budowanie świadomości społecznej na poziomie krajowym jest działaniem obliczonym na dziesięciolecia, a ich skutki będą widoczne w perspektywie co najmniej dwóch pokoleń,

- Skuteczność działań państwowych w obszarze informacyjnym zależy od szeregu czynników, w tym w szczególności:

  - a) ponadinstytucjonalnej i interdyscyplinarnej współpracy na linii państwo, media, sektor prywatny i społeczeństwo obywatelskie,
  - b) rozwoju prac nad komunikacją strategiczną i jej wdrażania na odcinku bezpieczeństwa informacyjnego i cyberbezpieczeństwa,
  - c) identyfikacji podatności różnych grup społecznych,
  - d) przebadania realnej skuteczności i wpływu oddziaływań informacyjnych i psychologicznych na społeczeństwa i różne grupy odbiorców informacji oraz zaadaptowania wniosków do bieżących strategii i działań różnych instytucji państwowych i międzynarodowych,
  - e) działań edukacyjnych, w tym edukacji medialnej i wprowadzenia przedmiotów związanych z krytycznym myśleniem od poziomu wczesnoszkolnego oraz reform programów nauczania, w tym na poziomie uniwersyteckim,
  - f) adaptacji systemów prawnych do nowych wyzwań związanych z cyberbezpieczeństwem oraz bezpieczeństwem informacyjnym,
  - g) modyfikacji programów finansowania i wspierania badań w obszarze bezpieczeństwa informacyjnego i cyberbezpieczeństwa.

- Istotną rolę w obszarze cyberbezpieczeństwa i bezpieczeństwa informacyjnego odgrywają i wciąż jeszcze długo będą odgrywać media społecznościowe – kształtują one postawy i nawyki odbiorców informacji, a od woli ich właścicieli zależy możliwość rozprzestrzeniania się zmanipulowanych treści; W związku z tym to od postawy prywatnych firm technologicznych zależeć będzie skuteczność działań instytucji państwowych na poziomach krajowych i międzynarodowym; W ramach systemów demokratycznych wypracować należy nowe zasady i reguły dla funkcjonowania gigantów technologicznych w ramach państwowych przestrzeni informacyjnych, ale i w lokalnych systemach prawnych (Unia Europejska ma tu szansę stać się światowym liderem jeżeli chodzi o wdrażanie takich rozwiązań)

- Współpraca pomiędzy Japonią a Unią Europejską (w tym na poziomach bilateralnych) ma szczególną przyszłość w obszarze dyplomacji technologicznej, wysokiej technologii, współpracy politycznej, naukowej, gospodarczej, kulturalnej, ale i eksperckiej, zwłaszcza w obszarach cyberbezpieczeństwa i bezpieczeństwa informacyjnego (także na odcinku militarnym),

- Istnieje szeroka możliwość wykorzystania doświadczeń inicjatywy „Wolnego i Otwartego Indo-Pacyfiku" (Free and Open Indo-Pacific, FOIP) dla Europy, w tym dla głębszego rozumienia działań Pekinu w regionie, jak i globalnie, w tym także w cyberprzestrzeni oraz w obszarze bezpieczeństwa dla całego Zachodu,

- Największe zagrożenia informacyjne, które długoterminowo wpływają na stabilność systemów demokratycznych oraz są najbardziej destrukcyjne dla krajowych systemów informacyjnych, ale i dla różnych grup społecznych czy konsumentów informacji to narracje i teorie spiskowe,

- Działania związane z bezpieczeństwem informacyjnym i budowaniem odporności społecznej są apolityczne i nie powinny stawać się zakładnikami wewnętrznych czy międzynarodowych sporów politycznych czy ideologicznych, tym bardziej, że niektóre działania rządów mogą tylko wzmacniać zewnętrzne, wrogie wpływy informacyjne i psychologiczne,

- Operacje informacyjne i psychologiczne Chin i Rosji skierowane przeciwko Zachodowi ulegać będą zaawansowaniu oraz możliwe są różne scenariusze dla współpracy Pekinu i Moskwy w tym obszarze z silnym wektorem antyamerykańskim (a docelowo i antyzachodnim), co tym bardziej wymusza konieczność pogłębionej współpracy politycznej, gospodarczej, militarnej oraz technologicznej,

- Wśród priorytetowych obszarów współpracy pomiędzy Japonią a Europą wymienić można badanie i neutralizacja polaryzacji społecznej i innych niebezpiecznych trendów (jak np. bańki informacyjne), które są wzmacniane przez wrogie podmioty państwowe i niepaństwowe zwłaszcza w cyberprzestrzeni (jak narracje, teorie spiskowe, radykalne ideologie czy poglądy antysystemowe), a także przeciwdziałanie rozprzestrzenianiu się innych form manipulacji informacją oraz identyfikacja i wypracowanie dobrych praktyk i skutecznych rozwiązań na tym odcinku,

- W sposób szczególny tak dla Japonii jak i Europy kluczowa będzie analiza negatywnych zjawisk, tendencji, trendów i manipulacji związanych z pandemią COVID-19 oraz przygotowanie rozwiązań prawno-systemowych, adaptacji systemów edukacyjnych oraz usprawnienia komunikacji strategicznej, a także wymiany informacji i doświadczeń w tym obszarze, co mogłoby stworzyć nowe modele dla radzenia sobie z wyzwaniami informacyj-nymi w cyberprzestrzeni i na poziomach społecznych.

- **Adam Lelonek**

Dziękujemy za zainteresowanie!

Narodowy Instytut Cyberbezpieczeństwa

www.nci.org.pl

vol. IV

Sfinansowano przez Narodowy Instytut Wolności - Centrum Rozwoju Społeczeństwa Obywatelskiego ze środków Programu Rozwoju Organizacji Obywatelskich na lata 2018 - 2030.