6.2. Państwa były już hakowane

W naszym postrzeganiu hakowano już państwa lub ich elementy składowe, newralgiczne: instytucje, ludzi, urzędników, polityków. Można powiedzieć, że atakowanie tych elementów było właśnie hakowaniem państwa. To obszary właśnie takie jak sytuacja polityczna lub działania z wpływem na nią, bezpośrednim lub pośrednim, z ingerencją w lokalne sprawy państwowe. Wpływ na wewnętrzną sytuację polityczną to mogą być wręcz kwestie suwerenności państwa.

Cyberoperacje wymierzone w państwa, np. w proces wyborów, to także **nowa rzeczywistość geopolityczna**, nowe ryzyko, z którego trzeba zdawać sobie sprawę. Naturalne i zrozumiałe jest, gdy celem operacji jest pozyskiwanie informacji, działania wywiadowcze, co w świetle prawa międzynarodowego jest legalne; nawet za pośrednictwem czegoś, co potocznie nazywa się cyberatakami, choć w tym wypadku o wiele lepszym określeniem jest rzeczywiście „cyberoperacja". Ale zupełnie innego wymiaru nabierają działania mogące (potencjalnie, przypadkowo lub celowo) mieć wpływ na sytuację polityczną, także na wybory. Wtedy są to działania bardziej agresywne, ingerencja, być może nawet naruszenie suwerenności państwa. Zdarzyło się to chociażby w Stanach Zjednoczonych (2016 r.), Francji (2017 r.), a nawet w Polsce (2020, 2021 r.).

6.2.1. Cyberoperacje wymierzone w system polityczny w USA

Zacznijmy od najbardziej znanego przykładu, czyli cyberoperacji w wyborach prezydenckich w USA w 2016 r. oraz związanych z nią upublicznieniem danych i zaprzęgnięciem ich w operację informacyjną wymierzoną w konkretną kandydatkę (a także szerzej, bo w Partię Demokratyczną). Była to bardzo sprytna operacja, która uwidoczniła, że hakowanie polityków, dyplomatów czy też innych osób związanych z państwem stało się rzeczywistością.

6.2.2. Wybory, wywiad i ludzka natura

To zresztą zrozumiałe, że w wypadku wyborów czy też w czasie poza wyborami zewnętrzni aktorzy są zainteresowani tym, co dzieje się lub będzie się działo w przyszłości w państwie. To jest przedmiot działań wywiadowczych, a od pewnego czasu także cyberwywiadowczych.

Na tym tle wydarzenia z 2016 r. w Stanach Zjednoczonych miały nieco odmienny charakter. Nastąpiły cyberataki, ale zostały one zaprzęgnięte w aktywną cyberoperację umożliwiającą działania o charakterze informacyjnym. Wyciek danych został przeprowadzony w taki sposób, że zainteresowała się tym tematem opinia publiczna. Nie było to trudne, ponieważ działo się to po raz pierwszy, wcześniej świadomość problemu nie była powszechna, a media potraktowały ten temat jako sensację.

6.2.3. Celowe wycieki danych i ich efekty

Dane, które wyciekły, były stale wałkowane przez opinię publiczną, także w mediach. Były analizowane, opisywane bardzo dokładnie. Trudno, żeby media przepuściły taką okazję, w końcu uzyskano wgląd w wewnętrzną politykę, w polityczną „kuchnię", potencjalnie w „afery" lub też wrażenie ich istnienia. Chociażby rozumując w prosty sposób: skoro powstaje wyciek, a do tego danych niepublicznych, to z pewnością „musi" być w środku coś kompromitującego, prawda? Bo inaczej by nie wyciekło. W tym sensie kompromitujący może być sam fakt wycieku – nawet jeśli w środku niczego konkretnego nie ma, da się to wykorzystać informacyjnie lub propagandowo. Tym bardziej gdy takich danych jest dużo, bo wtedy być może nikt nie będzie dokładnie ich wszystkich analizować, zwłaszcza gdy istnieje presja czasu (ten motyw miał z kolei znaczenie we Francji w 2017 r.).

W USA doprowadziło to do znacznych strat, a wszystko zaczęło się od zhakowania jednej osoby – Johna Podesty, polityka zaangażowanego w kampanię wyborczą po stronie Partii Demokratycznej. Klikając tam, gdzie nie powinien, uczynił coś, czego nie powinien. Dał się zwieść; nie ma znaczenia, czy zrobił to z nieświadomości, czy z pośpiechu. W efekcie przejęto jego dane, jego e-maile. Dane te następnie bardzo kreatywnie wykorzystano. Miało to zresztą prawdopodobnie wpływ na zwycięstwo w wyborach prezydenckich w 2016 r. Donalda Trumpa. Niekoniecznie na sam wynik. Jednak podczas całego okresu jego prezydentury wypominano te przeszłe zdarzenia i zajścia, przypominano je, analizowano, czyniono z nich zarzut.

Nie ma więc wątpliwości, że cyberatak bezpośrednio wpłynął na sytuację wewnętrzną w Stanach Zjednoczonych, bez względu na to, czy uznaje się, że rzeczywiście zdecydował o wyniku wyborów w 2016 r.

6.2.4. Cyberoperacje wymierzone w system polityczny we Francji

Podobnego rodzaju cyberoperacją były działania z elementami operacji informacyjnej we Francji, w kampanii wyborczej do wyborów prezydenckich w 2017 r., kiedy to wykradziono dane ze sztabu Emmanuela Macrona i je ujawniono. Dane te, podobnie jak w Stanach Zjednoczonych, były analizowane i wywołały zamieszanie, choć na znacznie mniejszą skalę – nie zajęły się nimi duże media. Choćby dlatego, że wyciek nastąpił stosunkowo późno, ale być może także z powodu pewnego rodzaju większej dojrzałości mediów lokalnych we Francji.

W każdym razie, jeśli nawet wyciek ten doprowadził do strat, to niewielkich. Zresztą nie było możliwości, żeby takie zajście mogło mieć wpływ na wynik wyborów w państwie takim jak Francja. Choćby dlatego, że opinia publiczna i media głównego nurtu bardziej sprzyjały kandydatowi Emmanuelowi Macronowi niż jego kontrkandydatce Marine Le Pen z opcji skrajnie prawicowej. To nie było tak jak w USA, że wyścig był wyrównany. I taka operacja nie mogła realistycznie mieć wpływu na wynik wyborów prezydenckich, natomiast hipotetycznie mogła mieć znaczenie dla następujących po nich wyborów parlamentarnych (w praktyce jednak wydaje się, że nie miała, zresztą i w nich wygrała partia zwycięskiego prezydenta Macrona, ale to wiadomo dopiero po fakcie!).