aut. Szymon Palczewski 11.09.2020

CZEKA NAS ERA CHIŃSKIEJ DOMINACJI? RANKING „CYBERPOTĘG" 2020

Stany Zjednoczone znalazły się na czele najnowszego rankingu „cyberpotęg", wyprzedzając największego przeciwnika – Chiny. Państwo Środka nieustannie dynamicznie się rozwija w cyberprzestrzeni, tym samym silnie naciskając na USA i ich globalne przywództwo w wirtualnej domenie. Czołówkę klasyfikacji uzupełnia Wielka Brytania, Rosja oraz... Holandia. Schyłek amerykańskiej dominacji jest kwestią czasu?

National Cyber Power Index 2020 (NCPI), opracowany przez ekspertów Belfer Center for Science and International Affairs z Harvard Kennedy School, określa potencjał 30 państw w obszarze cyberprzestrzeni przy użyciu szerokiej grupy wskaźników, które opierają się na materiałach pochodzących z publicznie dostępnych zasobów i danych.

Specjaliści jednoznacznie podkreślili, że nie da się określić „cybersiły" państwa za pomocą tylko jednej miary czy wartości. „Cyber Power składa się z wielu elementów i należy je rozpatrywać w kontekście celów danego państwa" – czytamy w raporcie. Analiza została przeprowadzona z punktu widzenia całego kraju, uwzględniając wszystkie aspekty znajdujące się pod kontrolą rządu. Istotnym punktem odniesienia podczas badań były między innymi zapisy strategii państw, jego zdolności obronne, siła sektora prywatnego czy poziom rozwoju innowacji. „Nasza ocena jest zarówno miarą udowodnionej siły, jak i potencjału" – wskazują eksperci.

National Cyber Power Index obejmuje siedem głównych „celów krajowych", do których państwo dąży przy wykorzystaniu swoich cyberzdolności. Są to:

1. Nadzór i monitorowanie grup krajowych (Inwigilacja) – odnosi się do kroków, jakie podjęło państwo w celu nadania swoim służbom i innym podmiotom możliwości w zakresie monitorowania, wykrywania i gromadzenia informacji. Jako przykład można wskazać na obserwację obywateli, omijanie szyfrowania komunikacji czy kontrola ruchu internetowego.

2. Wzmacnianie i ulepszanie narodowych sił cyberobrony (Obrona) – działania w tym zakresie obejmują między innymi aktywną obronę aktywów rządowych, promowanie cyberbezpieczeństwa i cyberhigieny w społeczeństwie, a także podnoszenie świadomości obywateli na temat zagrożeń w sieci. Państwo nadaje szczególny priorytet kwestiom cyberobrony i ulepszaniu krajowego systemu cyberbezpieczeństwa.

3. Kontrola i manipulowanie środowiskiem informacyjnym (Kontrola) – obszar ten dotyczy przede wszystkim tworzenia i rozpowszechniania dezinformacji oraz propagandy w kraju i zagranicą. Z drugiej strony odnosi się również do skuteczności działań na rzecz usuwania szkodliwych treści z sieci, takich jak na przykład ekstremistycznych materiałów w social mediach.

4. Zbieranie danych wywiadowczych na rzecz bezpieczeństwa narodowego (Wywiad) – obejmuje

zdolności państwa do „zdobycia” tajemnic i wrażliwych informacji z sieci i systemów przeciwnika (tajemnic handlowych, know-how itd.) za pomocą środków w cyberprzestrzeni.

5. Wzmacnianie rozwoju krajowego przemysłu (Przemysł) – dotyczy działań polegających na wykorzystaniu wirtualnych możliwości do wzmacniania rozwoju krajowego przemysłu technologicznego lub innych gałęzi gospodarki. Mogą one mieć charakter legalny (inwestycje w badania i rozwój) oraz nielegalny (szpiegostwo gospodarcze).

6. Niszczenie lub zakłócanie infrastruktury i możliwości adwersarza (Ofensywa) – w tym miejscu mowa o operacjach z wykorzystaniem wirtualnych środków, aby „odstraszyć, osłabić lub obniżyć zdolności przeciwnika do walki w cyberprzestrzeni lub w tradycyjnej domenie”. Wśród nich można wymienić między innymi cyberataki na infrastrukturę krytyczną.

7. Definiowanie międzynarodowych „cybernorm" i standardów technicznych (Normy) – obszar ten dotyczy aktywnego uczestnictwa państwa w międzynarodowych debatach na rzecz tworzenia „cybernorm” oraz powszechnych zasad postępowania w cyberprzestrzeni. Najprostszym przykładem działań w tym zakresie jest ratyfikacja traktatów dotyczących cyberbezpieczeństwa.

Na podstawie pozyskanych danych specjaliści starali się zmierzyć i opisać „kompleksowość” państwa jako jednego z kluczowych podmiotów funkcjonujących w cyberprzestrzeni. „Najbardziej wszechstronną cybersiłą jest państwo, ponieważ posiada – po pierwsze – zamiar realizowania wielu celów przy użyciu środków cyfrowych oraz – po drugie – zdolności do osiągnięcia tych celów” – czytamy w NCPI.

Cyberpotęgą jest…

Na przestrzeni lat wiodącą rolę w cyberprzestrzeni odgrywała Wielka Brytania. Potwierdzają to między innymi „Cyber Power Index 2011” oraz „Global Cyber Security Index 2018”, gdzie widniała na pierwszym miejscu, plasując się nad USA. W najnowszym zestawieniu sytuacja jest nieco odmienna.

W pierwszej dziesiątce indeksu „National Cyber Power Index 2020” znalazły się cztery europejskie państwa. Liderem zostały jednak Stany Zjednoczone, a za nimi Chiny, Wielka Brytania, Rosja i… Holandia. To te państwa są obecnie najpotężniejszymi krajami w cyberprzestrzeni. Stawkę uzupełnia Francja, Niemcy, Kanada, Japonia oraz Australia. Poniżej znajduje się wykaz państw wraz z ich łącznym wskaźnikiem „cybersiły”

Każdy z krajów z pierwszej dziesiątki posiada szeroki zakres cyberzdolności w różnych obszarach. Na podstawie powyższej grafiki widać jednak, że Stany Zjednoczone są państwem, które najskuteczniej wykorzystuje wirtualne zdolności i środki do osiągania celów politycznych. Analiza wykazała, że USA zajęły czołowe miejsce w czterech z siedmiu celów: Kontrola, Normy, Wywiad oraz Ofensywa. Taka sytuacja nie może zaskakiwać, ponieważ Waszyngton silnie stawia na rozwój swoich cyberzdolności, co obrazuje między innymi strategia USCYBERCOM i ofensywne operacje prowadzone przez dowództwo.

Warto jednak zaznaczyć, że Chiny regularnie podnoszą swoje „cybermożliwości”, tym samym „windując” pozycję w rankingu. Wydaje się, że pozycja Stanów Zjednoczonych jako „cyberpotęgi” staje się coraz bardziej zagrożona.

Chińscy hakerzy w ostatnim czasie „dali o sobie znać”, prowadząc szeroko zakrojone operacje wymierzone między innymi w protestujących w Hongkongu, rząd na Tajwanie czy społeczność Ujgurów. Były to głośnie działania, jednak nie świadczą one o jedynej specjalizacji Państwa Środka w

cyberprzestrzeni. Według indeksu Chiny posiadają szeroki ekosystem „cyberpotęgi". Potwierdzeniem tak śmiałej tezy może być bardzo wysoka pozycja Chin w zakresie Inwigilacji, Kontroli, Wywiadu i Obrony.

Rosja stale utrzymuje wysoką pozycję w całym zestawieniu. Wynika to z faktu między innymi realizowanych kampanii dezinformacyjnych w skali globalnej, cyberataków wymierzonych w sieci i systemy innych państw oraz ścisłej kontroli prowadzonej przez Moskwę w sieci. Kreml trzyma się „ścisłej czołówki" i należy sądzić, że w najbliższym czasie sytuacja nie ulegnie zmianie.

Równocześnie należy wskazać na rozwój innych państw w cyberprzestrzeni. Przykładem może być Malezja, Szwecja czy Szwajcaria, które uplasowały się w pierwszej dziesiątce zestawienia w obszarze Wywiadu, Inwigilacji, Kontroli i Przemysłu.

Co z Koreą Południową i Iranem?

Wydaje się, że jednym z państw, którego brakuje w czołówce (top 10) zestawienia jest Iran. Hakerzy Teheranu są bardzo aktywni w środowisku i znani ze swoich niszczycielskich kampanii. Indeks jednak nie koncentruje się wyłącznie na cyberprzestępczości i cyberatakach jako miarodajnych wskaźnikach, decydujących o dominacji w wirtualnej domenie. Są one jedynie jednym z elementów, jaki specjaliści brali pod uwagę podczas analizy. Dodajmy, że elementem najmniej punktowanym w całym zestawieniu.

Zgodnie z wynikami badań Iran został zaliczony do grupy państw, które „aktywnie sygnalizują swoje zamiary", na przykład rozwijanie cyberbroni, ale publicznie nie odkryto żadnych dowodów potwierdzających taki stan rzeczy. Są to kraje, które „nie są w stanie stać się współcześnie wszechstronną siłą w cyberprzestrzeni" – czytamy w NCPI.

Podobna sytuacja ma miejsce w przypadku Korei Północnej. Dlaczego nie znalazła się ona w klasyfikacji? Eksperci wskazują, że Pjongjang posiada cyberzdolności na wysokim poziomie, lecz próbuje je wykorzystać w „tajemnicy". W związku z tym specjaliści nie byli w stanie znaleźć wiarygodnych zasobów informacyjnych, jakie mogłyby zostać użyte do oceny i rzetelnego pomiaru siły tego państwa. „Badacze i praktycy powinni pamiętać, że Korea Północna jest szczególnym przypadkiem" – tłumaczą twórcy indeksu.

Czytaj też: Spektakularny rozwój cyberwojsk Korei Północnej. Hakerzy rozmieszczeni poza granicami kraju