aut. Andrzej Kozłowski 05.07.2019

CYBERBEZPIECZEŃSTWO SYSTEMÓW SATELITARNYCH NATO ZAGROŻONE

Brytyjski think-thank Chatham House opublikował raport "Cybersecurity of NATO's Space-based Strategic Assets" na temat cyberbezpieczeństwa systemów satelitarnych państw NATO. Brytyjczycy ostrzegają, że skuteczny cyberatak przeciwko komponentom systemów satelitarnych może bezpośrednio wpłynąć na bezpieczeństwo narodowe.

Systemy satelitarne są krytyczne dla operacji NATO prowadzonych na morzu, lądzie, w powietrzu oraz w cyberprzestrzeni. Dostarczają one kluczowych informacji potrzebnych do efektywnego wykonywania zadań przez siły zbrojne, to od nich zależy m.in. prawidłowe działanie zaawansowanych systemów uzbrojenia, a w szczególności amunicji precyzyjnej. Autorzy raportu przypominają, że prawie wszystkie obecne interwencje wojskowe opierały się na systemach satelitarnych. W 2003 roku, podczas inwazji na Irak, 68% precyzyjnych pocisków używanych przez Stany Zjednoczone było sterowane za pomocą systemów satelitarnych. W Afganistanie w 2001 roku, liczba ta wyniosła 60%. W dokumencie podkreślono również, że NATO nie posiada własnych satelitów, musi liczyć na dostęp do zasobów państw członkowskich. Ze względu na ich znaczenie narażone są na nowy typ ryzyka, czyli cyberataki.

Zagrożenia dla sektora satelitów

Consultative Committe for Space Data Systems (CCSDS) wymienia zagrożenia pochodzące z cyberprzestrzeni, które mogą być wymierzone w sektor satelitów. Eksperci uwzględniają tu uszkodzenie danych albo ich modyfikację, utratę kontroli nad systemami naziemnymi, przejęcie informacji, zagłuszanie, ataki typu DDoS uniemożliwiające korzystanie z danej usługi, spoofing (podszywanie się pod inny elementy systemu informatycznego), zagrożenia dla oprogramowania oraz nieautoryzowany dostęp. Eksperci wymieniają, że z niektórymi przypadkami ataków na zasoby bazujące na systemach satelitarnych NATO i jego członkowie musieli się już mierzyć. Przykładowo Rosją zakłócała sygnał GPS, podczas ćwiczeń NATO. Państwo to przeprowadziło podobne operacje w trakcie walk na Ukrainie i w Syrii. Było to w szczególności uciążliwe dla bezzałogowych aparatów latających. Autorzy raportu przypominają również, że największe zagrożenie może płynąć ze strony nieświadomych pracowników. Inżyniera społeczna jest bardzo ważnym narzędziem używanym przez przeciwników i często udaje się nabrać ofiarę. Zwracają również uwagę na konieczność zabezpieczenia łańcucha dostaw technologii satelitarnych, upewniając się, że na żadnym etapie nie zainstalowano tylnych furtek. Z ryzykiem zagrożeń pochodzących z cyberprzestrzeni wiąże się również powszechne używanie technologii podwójnego użytku – cywilnego i wojskowego. W sektorze cywilnym potencjalnym hakerom łatwiej jest uzyskać dostęp do takich systemów, przebadać je pod kątem potencjalnych luk, które mogą wykorzystać w atakach przeciwko wojsku.

Cyberataki mogą potencjalnie siać spustoszenie w satelitarnych, wojskowych systemach i w ten sposób osłabić odstraszanie, tworząc sytuację pełną niepewności oraz wprowadzając zamieszanie.

Autorzy piszą, że cyberataki są tak groźne ze względu na swoją szybkość, trudność w określeniu głównego sprawcy czy brak sygnałów o możliwości wystąpienia takiego zagrożenia. Dodatkowo zdolności do prowadzenia działań w cyberprzestrzeni posiadają takie państwa jak Chiny, Rosja, Iran czy Korea Północna, która mają sprzeczne interesy z państwami NATO. Państwa te wśród swoich priorytetów umieściły cyberataki i wojnę elektroniczną. Autorzy raportu twierdzą, że biorąc pod uwagę krytyczne znacznie systemów satelitarnych nie można wykluczyć, że potencjalni przeciwnicy NATO już dawno znajdują się w sieci.

Skutki cyberataków

W dalszej części raportu autorzy podają skutki cyberataków na zdolności bazujące na systemach satelitarnych. Cyberataki wymierzone w nawigację czy pozycjonowanie bazujące na technologiach satelitarnych mogą wpłynąć na bezpieczeństwo cywilnych lotów pasażerskich, które wprawdzie nie podlegają NATO, ale mogą istotnie wpłynąć na przebieg konfliktu. Dodatkowo zakłócenia mogą wpłynąć negatywnie na kontakt z siłami sojuszników, w szczególności w fazie rozmieszczenia wojsk za granicą czy ze wsparciem nawodnym i lotniczym, co może decydować o powodzeniu operacji. Ponadto taki cyberatak może zakłócić poprawną pracę pocisków samosterujących, które uderzą w zupełnie inny cel. Zakłócenie GPSu ma również negatywne konsekwencje dla cywilnego, sektora finansowego, który jest w dużej mierze uzależniony od tej technologii.

Cyberataki mogą też wpłynąć na zdolności określane terminem ISR czyli wywiadu, inwigilacji i rozpoznania (Intelligence, Surveillance, Reconnaissance - ISR) opartego na zdolnościach satelitarnych. Może to doprowadzić do błędnej analizy zagrożeń, albo nawet przetrwania możliwości transmitowania informacji przez potencjalne terytorium przeciwnika. Ponadto zarówno na poziomie strategicznym jak i operacyjnym grozi to utratą świadomości sytuacyjnej przez dowództwa i może skutkować błędnymi decyzjami. Ponadto manipulowanie ISR może zakłócić systemy obronne, poprzez przesyłanie fałszywych informacji albo ich nadmiernej ilości do osób podejmujących decyzje.

Biorąc pod uwagę, że systemy obrony rakietowej są w dużym stopniu uzależnione od systemów satelitarnych, to utrata takich zdolności w czasie pokoju może doprowadzić do napięć, a w czasie konfliktu do eskalacji działań. Autorzy raportu wskazują na spoofing, który oszukuje systemy dowodzenia rakietami balistycznymi. W raporcie ostrzeżono również, że cyberatak może doprowadzić do nieudanego przechwycenia rakiety balistycznej, co doprowadzi do ofiar.

Opisane w raporcie przykłady, jak cyberataki mogą wpłynąć na zdolności NATO oparte na systemach satelitarnych pokazuje kluczowe znaczenie tych systemów dla operacji prowadzonych przez Sojusz.

Rekomendacje

W raporcie znalazły się również rekomendacje działań, które powinno się podjąć. Konieczne są inwestycje w środki zmniejszające ryzyko ze strony cyberataków oraz we wzmocnienie używanych systemów. Jest to kluczowe dla zabezpieczenia operacji w przestrzeni kosmicznej, a tym samym działań w innych obszarach. Autorzy postulują wprowadzenie zawansowanych technik takich jak sztuczna inteligencja czy uczenie maszynowe w celu efektywniejszej odpowiedzi na zagrożenia. Rekomendowane jest również przyjęcie wyższych, wojskowych progów bezpieczeństwa dla technologii podwójnego użytku oraz wdrożenie koncepcji security-by-design do elementów satelitów oraz komponentów w stacjach bazowych. Autorzy dokumentu sugerują również stworzenie narodowych centrów podobnych do Information Sharing and Analysis Centers (ISACs), których celem byłaby wymiana informacji o zagrożeniach dla systemów satelitarnych. Ponadto zdaniem autorów NATO powinno również powołać NATO Centre of Excellence dla przestrzeni kosmicznej, stworzyć komórkę operacyjną odpowiedzialną za monitorowanie sytuacji w kosmosie oraz oficjalnie uznać przestrzeń kosmiczną za obszar prowadzenia działań wojennych. Najważniejsza jest jednak świadomości tego, że

systemy satelitarne są narażone na cyberataki i nie jest do żadne science-fiction.