CYBERATAK FORMĄ WSPÓŁCZESNEJ WALKI RADIOELEKTRONICZNEJ

Zwyczajny cyberatak może wyeliminować z walki najnowocześniejszy radar z aktywnym skanowaniem elektronicznym. Wystarczy zaaplikować do oprogramowania dane zawierające fałszywe wiadomości lub złośliwe algorytmy, by oślepić systemy wykrywania i naprowadzania na cel samolotów najnowszej generacji – pisze Marek Dąbrowski.

Elektronika i urządzenia zbudowane z wykorzystaniem jej elementów sprawują współcześnie niemal pełną kontrolę nad światem. To one nadzorują cały system energetyczny, ruch lądowy, morski i powietrzny, system finansowy i wiele innych, niezbędnych dla współczesnego człowieka rozwiązań i usług.

Znaczenie elektroniki w siłach zbrojnych jest dzisiaj dominujące i stale rośnie. Systemy wykrywania, dowodzenia czy przesyłania danych to tylko najbardziej znane przykłady zastosowanych w wojsku rozwiązań, w których nowoczesna technologia odgrywa znaczącą rolę.

Jednak, jak to zwykle bywa w armii, korzyści oferowane przez jedne rozwiązania stają się impulsem do budowy nowych systemów, które im przeciwdziałają bazując na wykorzystaniu słabych punktów do zredukowania mocy i potencjału oddziaływania lub całkowitego wyeliminowania ich z użycia.

> *Podstawowym pytaniem jest dzisiaj, czy pozyskiwane przez Wojsko Polskie systemy uzbrojenia z zaawansowanymi rozwiązaniami elektronicznymi w obszarze sterowania i nadzoru są wyposażone w skuteczne zapory, które posiadają zdolność do ograniczenia lub zapobiegania atakom z zewnątrz?*
>
> *Marek Dąbrowski*

W ramach walki radioelektronicznej podejmuje się starania, by zakłócić pracę nowoczesnych systemów elektronicznych takich jak np. radary współczesnych samolotów bojowych czy innych dedykowanych systemów walki. Jedną z współczesnych form walki radioelektronicznej stał się cyberatak, którego wiele form oddziaływania jest wykorzystywana nie tylko w okresie realnych działań, ale nawet w czasie „pozornego" pokoju. Czy zatem obecnie wykorzystywane systemy uzbrojenia są skutecznie chronione przeciw takim zagrożeniom jak powszechnie twierdzą ich producenci, a nawet niektórzy użytkownicy?

Radary z aktywnym skanowaniem elektronicznym AESA (Active Electronically Scanned Array) są powszechnie uważane za najnowocześniejszy system wykrywania i naprowadzania uzbrojenia w samolotach obecnej i kolejnych generacji. Zapewniają one wysoką rozdzielczość, szeroki zakres kąta przeszukiwania/nadzoru, zwiększenie zasięgu wykrywania i śledzenia celów (w tym dużych grup manewrujących obiektów), a także większą od klasycznych rozwiązań odporność na zakłócenia. Główną zaletą AESA nad PESA (Pasive Electronically Scanned Array) jest zdolność generowania wielu wiązek o różnych częstotliwościach.

Jednak, pomimo tak wielu zalet (w tym zwiększonej odporności na zakłócenia), można je wyeliminować z użycia poprzez zwykły cyberatak, np. aplikując do ich oprogramowania dane zawierające fałszywe wiadomości lub złośliwe algorytmy. Takie działania nie tylko „oślepiają" sam radar, ale w dużej mierze wpływają na zdolności wewnętrznych i zewnętrznych sieci i systemów obróbki danych, do których przesyłane są informacje uzyskane za jego pomocą.

AESA z reguły działa w systemie automatycznego przeszukiwania i wychwytywania sygnałów bez analizy ich pochodzenia czy własności. Ta właściwość może zostać wykorzystana do zainfekowania systemów elektronicznych obsługujących radar i nadzorujących cały system uzbrojenia, jakim jest samolot. Zgodnie z wyliczeniami statystycznymi 90 proc. systemów zainstalowanych na pokładzie F-35 działa w systemie sieci informatycznej tego samolotu, którą nadzoruje zespolony system informatyczny. W przypadku F-22 jest to ok. 70 proc. systemów pokładowych, w B-2 ok. 60 proc., a w F-15 już tylko 20 proc.

Już obecnie nowoczesne samochody, w których zastosowano zarządzający wszelkimi procesami związanymi z jazdą i bezpieczeństwem procesor, posiadają wewnętrzny system bezpieczeństwa (np. CarShark). Chroni on pojazd przed próbą interwencji z zewnątrz nie aprobując wykonania żadnych poleceń związanych z jazdą z wyjątkiem tych, które pochodzące od samego kierowcy. Zawsze jednak możliwa jest ingerencja z zewnątrz (np. poprzez urządzenia diagnostyczne), która spowoduje zainfekowanie nadzorującego samochodem procesora, tak by przekazywał on błędne dane kierującemu pojazdem. Kierowca popełni wówczas nieświadomie błąd doprowadzając do wypadku.

Taki system działania zastosowano w czasie ataku wirusem Stuxnet na irańskie wirówki do wzbogacania uranu. Ich zniszczenie nastąpiło samodzielnie w czasie rutynowego monitoringu pracy przez personel zarządzający nieświadomy, że wykonywane przez niego standardowe procedury zostały zmienione poprzez ingerencję w oprogramowanie. Przykład z Iranu obrazuje jak trudno jest przeciwdziałać zagrożeniu nawet dostosowując się do ściśle opracowanych wytycznych, które dotyczą rutynowego postepowania ze sprzętem nadzorowanym przez system czy sieć informatyczną.

Od uzbrojenia i wyposażenia wojskowego wykorzystującego różne klasy elektronicznych systemów nadzoru i przetwarzania danych wymaga się dużej szybkości i wydajności. Prawie nic natomiast nie mówi się o uodparnianiu tych rozwiązań na niepożądane lub szkodliwe oddziaływanie strony przeciwnej.

Radary typu AESA charakteryzują się tym, że skanują cały zadany im obszar „na raz" w przeciwieństwie do rozwiązań stosowanych w konwencjonalnych radarach. Pozyskane w tym trybie dane po przetworzeniu są albo odrzucane albo zbierane w bazie danych. To sprzyja „przemyceniu" do systemu danych niepożądanych/zainfekowanych.

Zdając sobie sprawę z tego zagrożenia, specjaliści w sposób ciągły modyfikują i opracowują systemy informatyczne nadzorujące ten proces, m.in. poprzez aktualizację oprogramowania. Wymaga to jednak wysokich kosztów związanych z tego typu działaniem i ciągłego nadzoru. Zaawansowane czujniki nadzorujące ten proces wymagać będą ciągłego udoskonalania i zwiększania możliwości przetwarzania sygnałów, tak by eliminować te niepożądane. Największym zagrożeniem jest wysoka

szybkość przetwarzania danych, która wymusza jeszcze większą szybkość ich monitoringu. Kolejne ryzyko wiąże się z tym, że niepożądane sygnały są odrzucane będąc już w systemie.

Opracowując i modyfikując radary typu AESA nieustannie dąży się do zbudowania „inteligentnego" systemu nadzoru/czujników wszelkich danych wpływających, który je zbiera i klasyfikuje. W przypadku, gdy nie odpowiadają one znanym charakterystykom, czujnik bezustannie dąży do pozyskania informacji na temat aktualnego stanu takiego sygnału.

Brak nadzoru i blokady sygnału o nieznanej charakterystyce stanowi dogodną sposobność do ataku z zewnątrz (np. cyberataku). Jako że radary stanowią bazę wszelkich danych nie tylko dla systemów ich przetwarzania, analizy i nadzoru, ale także systemów uzbrojenia, pilotażu i samoobrony, jest to otwarta droga do ich neutralizacji lub przejęcia nad nimi kontroli.

> *Zgodnie z wyliczeniami statystycznymi 90 proc. systemów zainstalowanych na pokładzie F-35 działa w systemie sieci informatycznej tego samolotu, którą nadzoruje zespolony system informatyczny. W przypadku F-22 jest to ok. 70 proc. systemów pokładowych, w B-2 ok. 60 proc., a w F-15 już tylko 20 proc.*
>
> *Marek Dąbrowski*

Zbieranie i klasyfikacja danych zewnętrznych musi odbywać się z bardzo dużą prędkością, która zapewnia przechwytywanie, zmianę i retransmisję sygnałów radarowych pozwalając na ich szybkie zmiany. Oznacza to, że procesory analizy sygnałów muszą być równie adaptacyjne i zdolne do dostosowania się do zmiennej emisji.

Dlatego ok. 90 proc. prac związanych z modyfikacjami obecnych rozwiązań i tworzeniem nowych sprowadza się do zwiększenia możliwości przetwarzania sygnałów wejściowych.

Wielu specjalistów zatrudnionych przez amerykański Departament Obrony, jak i samych wojskowych, dostrzega potrzebę finansowania rozwoju zdolności komunikacyjnych i modyfikacji całego szeregu istniejących systemów w celu ich wzmocnienia lub przywrócenia im ochrony wobec takich zagrożeń jak walka radioelektroniczna (w tym cyberatak).

Odrębna kwestią jest zapewnienie zdolności do pokonania wspomnianych form ataku poprzez zbudowanie skutecznego systemu zagłuszania i neutralizacji.

Jedną z rozważanych opcji jest również separacja systemów sterowania (np. samolotem poprzez wprowadzenie odrębnych systemów nadzoru i wykorzystania uzbrojenia czy łączności i przekazywania danych, tak by w przypadku zainfekowania jednego z nich można było nadal używać pozostałych). Jest to jednak proces zwiększający koszty pozyskania i eksploatacji. Poza tym nie zapewnia w 100 proc. bezpieczeństwa załodze czy maszynie.

Dlatego przyszłe systemy powinny posiadać wewnętrzną świadomość istniejących zagrożeń oraz własnych możliwości i ograniczeń. Już obecnie funkcjonuje kilka systemów (np. "Trusted Boot" i jego kolejne modyfikacje), których zadaniem jest ograniczenie/uodpornienie sieci informatycznych wobec

nowych zagrożeń. Systemy te działają na różnych poziomach operacyjnego wykorzystania)

"Trusted Boot" jest programem na małej płycie, która może być umieszczona w dowolnym komputerze. Po ponownym uruchomieniu komputer izoluje zaufany system operacyjny, przeglądarki czy Adobe Reader od nieznanej/niepożądanej infrastruktury, sieci czy oprogramowania. Już na poziomie zmiany oprogramowania następuje blokada wykonania niektórych operacji. Może to stanowić najniższy poziom ochrony. Na pozór „niezmienny" system informatyczny oferuje pewną wewnętrzną funkcję losową, która go zabezpiecza przed niepożądaną infiltracją.

Niektóre firmy w procesie rozwoju systemów zapewniających ochronę przed cyberatakiem próbują wykorzystać znane im obszary oprogramowania czy sieci z lukami w zabezpieczeniach. Mogą one bowiem rzutować na stan samego systemu jak i sieci, z którą jest on połączony.

Jednym ze sposobów takiej ochrony jest zbudowanie działających w ich obrębie zapór, których zadaniem jest ostrzeganie, zapobieganie i przeciwdziałanie ingerencjom.

W wypadku wykrycia zagrożenia, np. w postaci kasowania danych, jednym ze środów zapobiegawczych jest rozdrobnienie pakietów danych na osobne części, dystrybucja ich w poszczególnych kawałkach i szyfrowanie każdego z nich inaczej. Ponownego scalenia tak przetworzonych danych może dokonać jedynie system znający specjalny kod z instrukcją, która zawiera informacje o lokalizacji poszczególnych kawałków.

Systemy przeznaczone do takiej ochrony są łatwe w instalacji, podobnie jak inne powszechnie dostępne programy, a całość zadania, do którego służą, wykonują w zasadzie samodzielnie. W przyszłości tego typu programy można będzie aktualizować automatycznie przez Internet, skąd zostaną ściągnięte pakiety danych wzbogacające możliwości ochrony dzięki wykorzystaniu bieżących doświadczeń z cyberataków czy innych form interwencji. Sama sieć śledząc takie interwencje może uczyć się reagowania na nie i zapobiegania czy przeciwdziałania atakom.

Podstawowym pytaniem jest dzisiaj, czy pozyskiwane przez Wojsko Polskie systemy uzbrojenia z zaawansowanymi rozwiązaniami elektronicznymi w obszarze sterowania i nadzoru są wyposażone w skuteczne zapory, które posiadają zdolność do ograniczenia lub zapobiegania atakom z zewnątrz?

W jaki sposób chcemy zabezpieczyć tworzącą się sieć, która służy do przekazywania danych i dowodzenia (np. w postaci BMS czy innych systemów C4ISR) czy szkolenia (sieć symulatorów i trenażerów) na wypadek cyberataku bądź agresji z użyciem innych metod współczesnej walki radioelektronicznej?

Już dzisiaj należy szukać rozwiązań takich jak "Trusted Boot", tworzyć specjalistyczne zespoły nadzoru i zbierania danych oraz intensywnie szkolić użytkowników.

W ramach prac naukowych należy również rozwijać inteligentne systemy przeciwdziałania cyberatakom, które uczą się same tworząc nieustannie modyfikowaną sieć zapór przeciw zagrożeniom tego rodzaju.

I na koniec należy pamiętać, że najsłabszym ogniwem pozostaje człowiek, który poprzez nieumyślne lub celowe działanie może doprowadzić do katastrofalnych dla danego kraju czy społeczności skutków zarówno w wymiarze politycznym jak i gospodarczym czy militarnym.

Marek Dąbrowski