aut. Jacek Raubo 13.11.2018

NOWA JAKOŚĆ W BEZPIECZEŃSTWIE TRANSPORTU I SZLAKÓW KOMUNIKACYJNYCH W POLSCE [ANALIZA]

W Polsce mamy obecnie do czynienia z kilkoma z pozoru niezależnymi dyskusjami nad bezpieczeństwem komunikacji, które po dłuższym zastanowieniu mają jednak ze sobą wiele punktów stycznych. Przede wszystkim cały czas dokonywane są modernizacje sieci dróg i autostrad, a także części sieci kolejowych. Po drugie, gwałtownie zwiększa się świadomość potrzeb, w tym także logistycznych, wynikających a to z rosnącej funkcji tranzytowej Polski, a to z nowych warunków geostrategicznych związanych choćby z funkcjonowaniem wschodniej flanki NATO. Jednocześnie – po trzecie - dokonuje się istna rewolucja technologiczna w zakresie systemów dozoru i obserwacji, wykorzystywanych do zapewniania bezpieczeństwa na co dzień, ale też właśnie dla potrzeb zabezpieczenia ruchu drogowego i kolejowego. Analiza tych dyskusji skłania do kluczowego pytania - jakie szanse i wyzwania dla bezpieczeństwa niesie ta modernizacyjna synergia sektora komunikacji transportowej i technologii dozoru?

Fala zagrożeń terrorystycznych, która nastąpiła umownie po wydarzeniach z 11 września 2001 r., uzmysłowiła zachodnim państwom wagę i znaczenie nowoczesnych rozwiązań z zakresu bezpieczeństwa miast i ich elementów komunikacji zbiorowej. Nastąpiło dzięki temu m.in. wygenerowanie znacznej presji na inwestowanie w nowoczesne rozwiązania z zakresu obserwacji środków i szlaków komunikacji, transportu publicznego, ale też portów lotniczych, dróg, stacji oraz innych kluczowych miejsc w aglomeracjach miejskich. Takie zdarzenia, jak chociażby ataki terrorystyczne w Madrycie (2004 r.), Londynie (2005 r.), czy też Brukseli (2016 r.) *de facto* raz po raz potwierdzały obrany kierunek w zaawansowanych działaniach R&D (ang. research and development), kupowaniu oraz przede wszystkim użytkowaniu coraz to skuteczniejszych systemów monitoringu i związanej z nimi analityki.

Jednakże, współcześnie mamy do czynienia z nowym wymiarem zagrożeń, motywującym do kolejnych inwestycji w zakresie systemów bezpieczeństwa wewnętrznego. Co więcej, ich zakres może wykraczać daleko poza tereny zurbanizowane. Są one związane z łatwo obserwowalnym wzrostem napięcia w relacjach pomiędzy państwami, prowadzącym do podejmowania operacji o charakterze hybrydowym, innych niż te terrorystyczne, ale mogących zawierać w sobie czynnik militarny, dywersyjny, działania pod fałszywą flagą (np. terrorystów) etc. Co więcej, to właśnie w tym kontekście Polska może stać się swoistym laboratorium, gdyż jest kluczowym elementem flanki wschodniej NATO. Jako państwo sąsiadujemy z obszarem Europy doświadczonej działaniami terrorystów (Wielka Brytania, Belgia, Hiszpania, Niemcy, Francja), a także zagrożeniami hybrydowymi (przede wszystkim w rejonie Ukrainy).

W cieniu wschodniej flanki NATO

Jeśli chodzi o potrzebę inwestowania w systemy na rzecz przeciwdziałania zagrożeniom kryminalnym

oraz potencjalnej aktywności terrorystów panuje niejako szeroki konsensus wśród kluczowych polskich decydentów. Wskazują na to m.in. doświadczenia w przygotowaniu Szczytu NATO w Warszawie, ŚDM w Krakowie, zbliżającej się Konferencji COP24 w Katowicach, które - co najważniejsze - obejmują decyzje na różnych szczeblach władzy państwowej, a także lokalnej. W dodatku wzrasta przekonanie polskiego społeczeństwa, że nowoczesne technologie warto wykorzystywać na użytek eliminacji takich zagrożeń. Przykładowo, rozwiązania monitoringu wizyjnego traktowany jest już nie jako zbytek dla miast lub infrastruktury krytycznej, ale jako ważny wymiar bezpieczeństwa konkretnych, mniejszych społeczności.

Jednocześnie należy zauważyć, że nie nastąpiła jeszcze debata o tym, jakie ostatecznie miejsce mogą mieć efektywne systemy obserwacji, wsparte odpowiednią analityką, dla całej wschodniej flanki NATO. Chodzi przede wszystkim o dopasowanie się do ustaleń, wynikających z kolejnych szczytów NATO – tj. w Walii, Polsce, Belgii - w obliczu konfliktu na Ukrainie, gdzie wskazano, że oprócz dyslokacji wojsk kluczowe są zmiany w sferze poruszania się wojsk sojuszniczych na kontynencie, a co za tym idzie – należy zrewidować podejście do transportu kołowego i kolejowego, wykorzystania sieci logistycznych,
portów itd.

W tym właśnie miejscu pojawia się możliwość wykorzystania współczesnych doświadczeń wynikłych z przeobrażeń systemów zabezpieczenia miast oraz infrastruktury krytycznej. Jeśli bowiem mowa o wzmocnieniu ochrony szlaków komunikacyjnych w celach innych niż tylko bezpieczeństwo cywilne, warto głęboko zastanowić się przede wszystkim nad efektywnym zastosowaniem wspomnianych technologii dozoru. Obecne inteligentne, sieciowe systemy dozoru, np. od Axis Communications, wraz z odnośnym oprogramowaniem analitycznym, są rozwiązaniami elastycznymi i można je również zaadaptować na potrzeby wojska oraz służb specjalnych, m.in. w celach ochrony logistyki, czy na wypadek wystąpienia sytuacji kryzysowej. Należy przy tym wskazać, że obejmuje to już nie tylko adaptację istniejących rozwiązań – np. systemów kamer monitorujących skrzyżowania, bramki na autostradach - ale też budowę nowych systemów, czy to w sferze rozpoznawania tablic rejestracyjnych, czy obserwacji wielosensorowej miejsc przeładunku, a nawet rozpoznania powietrznego z wykorzystaniem bezzałogowych statków powietrznych ze zróżnicowanymi głowicami optoelektronicznymi oraz innymi czujnikami.

Tego typu rozszerzone podejście będzie wymagało większego nasycenia oraz skali zastosowanych rozwiązań, opartych na równie innowacyjnych, co bezpiecznych technologiach. Nasycenie to wymagać będzie oczywiście odpowiedniej integracji i synchronizacji urządzeń, aplikacji i procedur. Przy czym, odnośna debata, co do priorytetów i kierunków rozbudowy systemów monitoringu na specjalny nie-cywilny użytek, a także późniejsze wdrożenia muszą być wkomponowane w dobrze zdiagnozowane potrzeby militarne państwa oraz potrzeby współczesnego NATO.

Przydatny głos ekspertów

Ważną praktyką, towarzyszącą inwestycjom drogowym, powinno być dokładne wsłuchiwanie się w głos wojskowych, w tym przedstawicieli wojsk specjalnych, odpowiadających za logistykę oraz transport wojska, ale też specjalistów w zakresie dozoru. Chodzi o dobre rozpoznanie i zabezpieczenie potencjalnych punktów krytycznych, widzianych z perspektywy działań nieregularnych i specjalnych przeciwnika. Trzeba również realnie zastanowić się, jak systemy obserwacyjne synchronizować nie tylko z codzienną aktywnością Policji, PSP, OSP, czy systemu ratownictwa medycznego, ale też z chociażby budowanym zapleczem Wojsk Obrony Terytorialnej (WOT) w poszczególnych rejonach Polski.

Najlepszym kazusem, obrazującym nowe potrzeby w tym zakresie, jest sprawa odpowiedniego monitorowania w sytuacjach kryzysowych rejonów tzw. Drogowych Odcinków Lotniskowych. W

warunkach współczesnych zagrożeń hybrydowych obserwacja wizyjna DOL`i – dokonywana w warunkach dzień/noc - a także stosowanie systemów kontroli przed wejściem intruzów na obszar wykorzystywany przez lotnictwo (np. systemy zabezpieczeń obwodowych) powinny stać się czymś oczywistym. Tym samym, w tego typu miejscach obserwacja wizyjna powinna stanowić rozwiązanie równie łatwo wdrażane, co fizyczne przystosowanie dróg do przyjęcia samolotów. Równoległa inwestycja w zaawansowaną technologię monitoringu w przypadku takiej infrastruktury transportowej oznacza mniejsze koszty ludzkie i sprzętowe w przypadku zaistnienia realnej sytuacji kryzysowej – wyjaśnia Karol Dominiczak z Axis Communications, w rozmowie z Infosecurity24.pl.

Jak podkreśla ekspert szwedzkiego koncernu – zalety monitoringu to nie tylko racjonalizacja kosztów, ale przede wszystkim funkcjonalność. Zastosowanie chociażby systemów rozpoznawania obiektów mobilnych i tablic rejestracyjnych może dać wiele informacji np. kontrwywiadowi lub Policji i Żandarmerii Wojskowej, przydatnych w pracy operacyjnej, czy dochodzeniowej. Można dzięki nim weryfikować, czy nie dąży się m.in. do niebezpiecznego zablokowania dróg przez konkretne pojazdy, legitymujące się rejestracjami obcych państw lub należącymi do bazy danych pojazdów skradzionych. To ważne, ponieważ dość niepokojące są doświadczenia z obserwacji blokowania przejazdu pojazdów ratowniczych w trakcie wypadków (tzw. korytarz życia). Można również założyć, że monitoring przysłużyłby się skoordynowaniu oraz ochronie transportu jednostek i ładunków wojskowych, optymalizując możliwości ich przerzutu.

Karol Dominiczak zwraca uwagę również na inny kluczowy wymiar funkcjonalności monitoringu w komunikacji i transporcie. Chodzi o sprzężenie systemów kamer z systemem informowania użytkowników dróg o zmianach na trasach, wynikających bądź to ze zdarzeń typu wypadek, bądź z przemieszczania się pojazdów uprzywilejowanych, lub wspomnianych kolumn wojskowych.

W militarnym kontekście, nie mniej ważny jest aspekt zabezpieczenia tras i węzłów kolejowych na wschodniej flance NATO, odgrywających przecież kluczową rolę dla sojuszu i to nie tylko w przypadku sytuacji kryzysowych, ale też rutynowych ćwiczeń poszczególnych komponentów sił zbrojnych, manewrów narodowych i międzynarodowych, rotacji w ramach np. wysuniętej obecności. Dziś w Polsce mamy już rzeczywiście pewne środki i doświadczenia w zakresie zwalczania wandalizmu na kolei, albo też przeciwdziałaniu próbom kradzieży znacznych ilości np. węgla (w tym przypadku stosuje się chociażby bezzałogowe statki powietrzne). Wydaje się, że te dobre praktyki i narzędzia niekoniecznie wystarczą na użytek zabezpieczenia sił sojuszniczych. W zakresie ochrony logistyki wojsk należy bowiem brać pod uwagę szersze spektrum wyzwań i zagrożeń. Przepływ żołnierzy chociażby ze Stanów Zjednoczonych oraz ich sprzętu może być celem działań grup pacyfistycznych, antyzachodnich, itp. Nie wspominając o próbach kinetycznego blokowania możliwości sieci kolejowych w Polsce w przypadku eskalacji sytuacji w regionie.

Ważnym doświadczeniem, studiowanym oraz odpowiednio rozpoznanym, powinny być dla nas w Polsce dotychczasowe próby blokad składów kolejowych przewożących materiały radioaktywne w Niemczech oraz innych państwach Europy Zachodniej. Nie można też zapominać o potrzebie kontroli nad rozległą infrastrukturą kolejową planowaną w związku z możliwym udziałem Polski w lądowych, szeroko zakrojonych inicjatywach infrastrukturalnych Chin - Jedwabnym Szlaku (Inicjatywa Pasa i Szlaku). Już dziś postrzeganie bezpieczeństwa kolei winno być rozszerzone z walki z kradzieżami elementów infrastruktury, ładunków, etc. na sprawy wspomnianych zagrożeń hybrydowych – i oto apelują także przedstawiciele sił specjalnych.

Ogólnie, w sektorach transportu i logistyki – zaznacza Karol Dominiczak - co raz wyraźniej w Europie inwestuje się w skalowalną ochronę obwodową podpartą zaawansowanymi algorytmami, obsługującymi różne scenariusze detekcji. Takie rozwiązania w sferze wsparcia wojska również mogłyby się sprawdzić, po odpowiednim dostosowaniu kamer i aplikacji analitycznych, zwłaszcza w zakresie cyberbezpieczeństwa. Kluczem jest to, aby działać profilaktycznie i przed szkodą; poza tym,

aby zaoszczędzić w późniejszym czasie środki, które potencjalnie będzie trzeba wydatkować w przypadku wymuszonej modernizacji po zdarzeniu, czy w kryzysie.

Przemysł przychodzi z gotowymi rozwiązaniami

Ekspert Axis Communications podkreśla, że w zakresie bezpieczeństwa komunikacji odpowiednio skonfigurowane kamery powinny mieć przede wszystkim możliwości wspomnianego rozpoznawania pojazdów, w tym tablic rejestracyjnych, ale i – gdy zajdzie potrzeba - detekcji twarzy kierujących. Jednocześnie systemy dozoru powinny być odpowiednio przystosowane do łączenia się z bazami danych służb, tak aby w dogodny i bezpieczny sposób identyfikować i rozróżniać te pojazdy, które stanowią zagrożenie; szczególnie, że takie rozwiązania są oferowane i nie są one już żadną nowością. W dodatku, Karol Dominiczak wskazuje, że kamery już teraz mogą wykrywać takie anomalie, jak porzucone samochody, albo takie, które stają w miejscach, w których nie powinny, mają zbyt długie postoje w miejscu objętym ochroną, itp.

W tym kontekście trzeba przypomnieć, że po, doświadczeniach ekstremalnych - przede wszystkim z Iraku - gdzie zagrożenie stanowiły IED, VBIED, takie funkcjonalności są nader istotnym czynnikiem zapewniającym ochronę dla konwojów wojska (zagrożenia hybrydowe oraz powiązane z terroryzmem). W obu przypadkach jest to szczególnie istotne, gdy bierzemy pod uwagę wzmocnioną obecność wojsk sojuszniczych, m.in. wojsk amerykańskich w danym państwie. W Polsce jest to oczywiście baza w Redzikowie, wysunięta obecność EFP na kierunku przesmyku suwalskiego oraz państw nadbałtyckich, rotacyjna brygada US Army, wykorzystanie baz w Mirosławcu oraz Powidzu, a w przyszłości być może stała infrastruktura.

W dodatku, mając na uwadze problemy kadrowe w sferze ochrony w Polsce nowoczesne rozwiązania w zakresie monitoringu pozwalają również zmniejszyć liczbę osób zaangażowanych w zabezpieczenie logistyki oraz zredukować obciążenia w przesyłaniu danych. Inteligentne kamery, wykorzystywane w kontekście obserwacji dróg, są już złożonymi i zautomatyzowanymi systemami w takim stopniu, że mogą w pewnym zakresie samodzielnie analizować konkretne zdarzenia, ostatecznie wysyłając alerty jedynie w przypadku wykrycia czegoś podejrzanego. Ta technologia – wyjaśnia ekspert Axis - idealnie odpowiada warunkom tras i szlaków komunikacyjnych o dużej rozległości i skomplikowaniu, szczególnie gdy chodzi chociażby o zabezpieczenie mostów, wiaduktów, nasypów, etc.

Przy czym, podkreśla dalej Karol Dominiczak, nadal analizowanie skomplikowanych anomalii odbywa się niejako poza kamerą, w oparciu o dane z serwerów, gdzie kamera stanowi jeden z wielu możliwych do integracji sensorów, wychwytujących te dane. Coraz ważniejsze są zatem rozwiązania brzegowe, czyli rozwiązania analityczne zaimplementowane w kamerze, dzięki temu można ograniczyć zapotrzebowanie na przepustowość sieci i pamięć masową. Podsumowując, istotne jest ujęcie systemowe, obejmujące zarówno system kamer-sensorów, jak i system odpowiednio zabezpieczonego i szybkiego przesyłu informacji oraz ich gromadzenia i analizy.

Dostrzegalne zmiany

Należy zauważyć, że w zakresie nowego podejścia do ochrony szlaków komunikacyjnych w Polsce dokonuje się już pewnego rodzaju diametralna zmiana, wynikająca chociażby z rozwijania przez Generalną Dyrekcję Dróg Krajowych i Autostrad (GDDKiA) Krajowego Systemu Zarządzania Ruchem. Co więcej, samo wojsko monitoruje ruch własnych oraz sojuszniczych konwojów w oparciu o nowoczesne technologie. Jednak już na tym etapie, patrząc na skalę zmian infrastrukturalnych w obrębie dróg oraz kolei, trzeba podnieść świadomość potrzeb na wypadek zagrożeń terrorystycznych, a przede wszystkim hybrydowych, wykraczający poza dotychczasową definicję zagrożeń. Szczególnie, że potencjalna, umowna druga strona rywalizacji na flance wschodniej NATO, zapewne bardzo dobrze zna wszelkie mankamenty również i w tym aspekcie funkcjonowania Polski oraz całego Sojuszu.

Nie wolno zapominać, że oprócz szeroko ujmowanych kwestii natowskich, trzeba w Polsce rozważać, wspomniany wcześniej zwiększony tranzyt dóbr z Azji, a także takie strategiczne inicjatywy regionalne, jak chociażby koncepcja Trójmorza. W jej kontekście, analitycy Axis Communications zwracają uwagę, że obecnie można zauważyć w Polsce wyzwania technologiczne, związane m.in. ze scalaniem systemu opłat autostradowych w obrębie państw regionu, gdzie już teraz wiele państw południa regionu używa systemów cyfrowych, a w Polsce nadal bazujemy na bramkach opłat. Integracja strategicznych szlaków komunikacji kołowej w tym aspekcie będzie *de facto* dobrym testem i wnioski z niego powiedzą wiele o możliwościach zabezpieczenia ważnych tras oraz szlaków komunikacyjnych na innych, wcześniej omawianych płaszczyznach, zarówno cywilnego, jak i wojskowego transportu osób i ładunków.

Jednakże, nawet przy olbrzymich możliwościach oferowanych przez technologie zabezpieczeń istnieją widoczne ograniczenia. Ekspert Axis stwierdza, że nadal stoi przed nami wyzwanie przenoszenia rozwiązań „smart city" na obszar pozamiejskich szlaków drogowych i kolejowych, gdzie ciągle brakuje odpowiedniej ciągłości obserwacji. Aby taki transfer standardów uzyskanych w naszych miastach mógł się powieść, trzeba na wstępie zagęścić sieć samych kamer, a także inwestować w droższe rozwiązania software'owe. Przy czym, zauważa Karol Dominiczak, warto wiedzieć, że pod kątem dostępu sprzętu, jak i oprogramowania Polska na taką modernizację lądowych kanałów logistycznych jest gotowa i taka integracja jest wykonalna; należy bardzo wysoko ocenić choćby polskie software house`y, oferujące swoje produkty zarówno na rynek wewnętrzny, jak i zewnętrzny.

Ta uwaga jest o tyle istotna, że wskazuje na posiadanie przez Polskę istotnego potencjału i kapitału ludzkiego, wystarczającego, aby samodzielnie budować odpowiednie rozwiązania, gwarantujące określony poziom zabezpieczeń względem zdefiniowanych zagrożeń. Dziś już wiemy, że działania hybrydowe mogą być rozpoczęte od uderzeń na wszelkie urządzenia sieciowe, przekazujące dane. Co więcej, dla obcych wywiadów wojskowych informacje z naszych kluczowych szlaków komunikacyjnych w wypadku sytuacji kryzysowej również będą celem. Stąd technologia winna być dobierana oczywiście pod zadania i uwzględniać kwestie finansowe, zawsze z odpowiednim podejściem do kwestii zabezpieczenia kontrwywiadowczego, przede wszystkim w sferze cyberzagrożeń.

Realne potrzeby i realne wyzwania

Konkludując, należy zwrócić większą uwagę na bezpieczeństwo naszych dróg oraz sieci kolejowych pod kątem zastosowanej technologii dozoru, wizyjnego i wielosensorowego, przy jednoczesnej perspektywie „nie wyspowego" a sieciowego rozkładania elementów składowych ochrony w obrębie kraju, ale też regionu. Warto skorzystać z koniunktury oraz swoistego bumu w sferze inwestycji infrastrukturalnych, i uzupełnić je o odpowiednie systemy monitoringu, spełniające współczesne wyzwania logistyki cywilnej i wojskowej, jak i te z niedalekiej przyszłości, przede wszystkim związane z ciągłą ewolucją architektury bezpieczeństwa europejskiego. Warto rozwijać świadomość, że pewne rozwiązania w systemach obserwacji posiadają taką wielofunkcyjność, która z pewnością przyda się operatorom dróg, służbom takim jak Policja, PSP, Straż Graniczna, itp., ale również wojsku.

I chyba to ujęcie wielopodmiotowe powinno być mocniej zaakcentowane w dobie debaty o implementacji postanowień ostatnich trzech szczytów NATO. Szczególnie, że w działania hybrydowe idealnie można wpisać całe spektrum możliwych akcji wymierzonych w kluczowe węzły komunikacyjne. Nie wspominając już nawet o zwiększonych potrzebach w zakresie dozoru wizyjnego w sytuacji, gdy nastąpiłoby rozmieszczenie większej liczby wojsk amerykańskich w Polsce i potrzeba transportu oraz ochrony towarzyszącej im stałej infrastruktury na terytorium Polski.

Tym mocniej już teraz należy naciskać na sprawdzone rozwiązania technologiczne, ograniczające potrzeby osobowe, a zwiększające możliwości realnego zabezpieczenia wspomnianych dróg i szlaków kolejowych. Nie zapominajmy też o wymaganiach względem dostawców sprzętu oraz

oprogramowania, tak aby nie narażać się na wrogie działania szczególnie w cyberprzestrzeni, m.in. poprzez ryzykowne pod względem zabezpieczeń, „dziurawe” technologie, otwierające drogę do backdoor’owych ataków.