aut. Fundacja Instytut Bezpieczeństwa i Strategii
10.09.2019

PO CO CBA PEGASUS? [KOMENATRZ]

W ostatnich dniach to słowo (Pegasus - przyp. red.) zdobyło w Polsce ogromny rozgłos, a według powszechnie już znanej wiedzy oznacza jeden z istniejących na rynku systemów pozwalających na operowanie w cyberprzestrzeni. Prawdopodobnie (tak twierdzą dziennikarze, a politycy niezdarnymi zaprzeczeniami, które wyglądają na trochę infantylne kręcenie, nie zmieniają tego przekonania) kupiony przez jedną z polskich służb policyjnych.

Komentarz ten nie ma na celu rozstrzygnięcie, czy istniała podstawa prawna zakupu, który prawdopodobnie miał miejsce ze środków przeniesionych z funduszu przeznaczonego dla ofiar przestępstw. Tym pewnie zajmą się odpowiednie instytucje, jeśli po tych, czy innych wyborach ktoś będzie tym zainteresowany. Zajmijmy się sednem sprawy, czyli tego typu systemami, ich zastosowaniem i zasadnością wykorzystania.

Po publikacjach medialnych donoszących o zakupie przez Centralne Biuro Antykorupcyjne systemu izraelskiej produkcji o nazwie Pegasus rozgorzała polityczna wrzawa. Opozycja zakrzyknęła, że skandal, masowa i totalna inwigilacja. Państwo policyjne o skali opresyjności znanej z poprzedniego ustroju. Po stronie władzy, (politycy i urzędnicy związani z zarządzaniem polskimi służbami) najpierw było niezdarne kręcenie i niejasne zasłanianie się tajemnicą, aż wreszcie wicepremier Sasin palnął głupstwo tygodnia w stylu: jak ktoś jest uczciwy, to nie ma się czego obawiać. Nie sposób tego poważnie komentować, bo w demokratycznym kraju nie jest rolą polityka, a na pewno nie rolą polityka partii rządzącej wystawianie świadectw uczciwości. Jest prawo, normy postępowania, sądy, jasne reguły funkcjonowania w społeczeństwie obywatelskim, gdzie nie opinia nawet najważniejszego polityka, ale jasne reguły rozstrzygają o tym, czy dany obywatel przekracza dopuszczalne granice. Z sympatii do Pana wicepremiera spuśćmy na to zasłonę milczenia. Eksperci natomiast słusznie podkreślali, że nie jest to ani jedyny, ani najdroższy tego typu system oferowany na rynku.

Przyjmijmy na potrzeby tego komentarza założenie, że CBA faktycznie dokonała takiego zakupu i wykorzystuje ten nowiutki nabytek w sobie (i może prokuraturze) znanych celach.

Pytanie pierwsze: czy wykorzystanie tego rodzaju narzędzi mieści się w ramach polskiego prawa?

Każdy, kto zna polskie ustawodawstwo w tej dziedzinie, każdy, kto zna instrukcje operacyjne polskich służb i kto choć raz widział wniosek do sądu o objęcie figuranta X kontrolą operacyjną, bez wahania zaprzeczy. Przepisy dotyczące kwestii kontroli operacyjnej w zdecydowanej większości powstały w czasach, w których nie było jeszcze telefonii komórkowej, o internecie nawet nie wspominając. Nawet ustawa antyterrorystyczna z 10.06.2016 roku niespecjalnie zmieniła ten stan rzeczy.

Czytaj też: "Przygoda życia" w CBA. Biuro szuka talentów

Nie zagłębiając się w techniczne szczegóły, narzędzia typu Pegasus pozwalają na objęcie jednoczesną kontrolą zarówno rozmów telefoniczny, korespondencji mailowej, notatek i zapisów w telefonicznym kalendarzu, treści smsów, zdjęć, historii przeglądarki internetowej, podsłuchiwania w czasie rzeczywistym otoczenia telefonu, jak również podgląd za pomocą kamery w telefonie. Jak to ująć we wniosku do sądu? Kontrola operacyjna (jak większość rzeczy na świecie) musi mieć swój początek i koniec. Jak go określić w przypadku posiadania możliwości czytania całej historii zapisanej w telefonie? O zakresie tematycznym i czasowym służba dowie się dopiero po włamaniu się do systemu w danym telefonie. Samo działanie inwigilacyjne wstecz dotychczas miało bardzo ograniczone możliwości – bilingi są najbardziej oczywistym przykładem, ale i tu we wniosku określa się z góry ramy czasowe.

Krótko mówiąc, zakres tego typu narzędzia w rękach służb dbających o bezpieczeństwo wewnętrzne nie mieści się w obowiązujących ramach prawnych (pamiętamy oczywiście, że tzw. falandyzacja prawa to wynalazek naszego trzydziestolecia wolności). Możemy przyjąć założenie, że służba złoży wniosek do sądu o kontrole operacyjną za pomocą narzędzia typu Pegasus, w którym określi, że przeczyta tylko smsy z tego roku, maile z bieżącego miesiąca, a do zdjęć nawet nie zajrzy. Nie wątpię w uczciwość i rzetelność oficerów operacyjnych, ale na powściągliwość nadzorujących służby polityków i (oczywiście w jednostkowych przypadkach) wyznaczonych przez nich szefów, to już prywatnych pieniędzy bym nie postawił. Coś tam się już w naszym kraju słyszało o przekroczeniu uprawnień itp., bez względu na to kto jest przy władzy. Jak się ma w ręku młotek, to jakoś wszystko bardziej wydaje się być gwoździem.

Pytanie drugie: czy tego typu narzędzia są skuteczne i czy powinno się z nich korzystać?

Nie jest żadnym odkryciem, że zarówno przestępcy, terroryści, czy ludzie prowadzący działalność szpiegowską znaczą część swojej aktywności prowadzą w „świecie cyfrowym”, a ich przywiązanie, aktywność i uzależnienie od urządzeń elektronicznych nie odstaje znacząco od przeciętnej. Działania w cyberprzestrzeni to bardzo istotny element działań na rzecz bezpieczeństwa państwa. Należy się jednak zastanowić, gdzie i w jakiej skali? Zapytać o dobór zastosowanych środków, do faktycznego poziomu zagrożenia. Państwo prawa narzuca wszystkim określone ograniczenia. Bez nich, lub gdy uznamy, że w pewnych aspektach, wybrane podmioty (np. służby policyjne, nawet te wyspecjalizowane w jakimś rodzaju przestępczości jak CBA) nie muszą się w tych ramach mieścić, to znajdziemy się na krótkiej, acz pochyłej drodze do sytuacji znanych nam z historii, a obecnie obserwowanych w krajach, które nie stanowią wzorca demokracji. Czy policjant celujący do przestępcy ma zadanie strzelać tak aby zabić, czy tak aby obezwładnić go, minimalizując ryzyko śmierci. Tak szkoli się policję na całym świecie, a przecież ma broń i może sprawę załatwić ostatecznie. Nie zawsze „prostsze” i skuteczniejsze rozwiązanie może być wykorzystane. W innym przypadku mamy dziki zachód, a nie państwo prawa.

Czytaj też: CBA komentuje sprawę Pegasusa

Służby wewnętrzne, zarówno te policyjne (Policja, CBA) jak i specjalne (ABW, SKW) mają wystarczająco dużo innych skutecznych narzędzi pozwalających na wykrycie, udokumentowanie i zneutralizowanie zagrożeń ze strony przestępców. Oczywiście w przypadku działań antyterrorystycznych czy kontrwywiadowczych prowadzonych przez służby specjalne można, a nawet trzeba, możliwie szybko i w sposób ciągły budować ramy prawne pozwalające na poszerzenie wachlarza ich narzędzi operacyjnych, tak by możliwie blisko trzymały się za przeciwnikiem.

Pytanie trzecie: czy w naszym kraju istnieje potrzeba posiadania takiego systemu jak Pegasus?

Bezwzględnie, oczywiście, bez wątpienia – tak. Trzeba tylko zrozumieć, że nie jest to odpowiednie narzędzie do ścigania krętacza, który unika płacenia VATu! Tego rodzaju systemy do operacyjnej penetracji cyberprzestrzeni powstają z myślą i są wykorzystywane przez służby wywiadowcze. Wywiad, który po pierwsze zbiera za granicą informacje o strategicznym znaczeniu politycznym i gospodarczym, a z drugiej strony stanowi pierwszą linię obrony dla państwa (terroryzm), musi w obecnych warunkach poza osobowymi źródłami informacji, korzystać z najnowocześniejszych osiągnięć technicznych.

Kwestie prawne? Oficer wywiadu prowadzący działania operacyjna na terytorium przeciwnika zawsze działa poza prawem. Nie występuje przecież do miejscowego prokuratora czy sędziego o zgodę na włamanie do czyjegoś pokoju hotelowego i skopiowanie zawartości twardego dysku jego laptopa, albo werbując obcokrajowca w jego kraju unika materiałów nacisku (potocznie zwanych czasem szantażem), bo to nie zgodne z miejscowym prawem!

Czytaj też: Wywiad 3.0, czyli służby wywiadowcze w czasach globalnego przyspieszenia

Szpiegostwo, to w każdym kodeksie karnym jedno z najcięższych przestępstw. Zorientowani w tej branży czytelnicy doskonale wiedzą jaką skuteczność mają narzędzia typu Pegasus w działaniach zagranicznych. Środki i metody pracy wywiadu różnią się jednak od innych i niewybaczalnym błędem jest przenoszenie ich na teren własnego państwa (poza wszystkim jest niezgodny z naszym prawem).

Politycy decydujący w Polsce o kwestiach związanych ze służbami specjalnymi, wywiadowczymi i policyjnymi muszą jedynie zrozumieć, że bezpieczeństwo kraju, to nie jest statystyka zatrzymań, ale złożony system, w którym każdy element ma do odegrania swoją równie ważną rolę.

Czytaj też: Jak uniemożliwić służbom zawłaszczenie systemu ochrony tajemnic państwa?

Bartosz Orlicz-Rabiega przez kilkanaście lat pełnił służbę jako oficer operacyjny w Agencji Wywiadu, realizując zadania zarówno w kraju jak i poza granicami. W latach 2011 – 2012 pełnił funkcję Radcy Ministra Spraw Zagranicznych d.s. bezpieczeństwa polskich przedstawicielstw dyplomatycznych. Służbę w Agencji Wywiadu zakończył na stanowisku Dyrektora pionu odpowiedzialnego za bezpieczeństwo kontrwywiadowcze i bezpieczeństwo operacji wywiadowczych. Jest ekspertem Fundacji Instytut Bezpieczeństwa i Strategii.