X kadencja

SEJM RZECZYPOSPOLITEJ POLSKIEJ

KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji Śledczej do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych m.in. z wykorzystaniem oprogramowania Pegasus przez członków Rady Ministrów, służby specjalne, policję, organy kontroli skarbowej oraz celno-skarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od dnia 16 listopada 2015 r. do dnia 20 listopada 2023 r.**
(nr 18)
z dnia 8 lipca 2024 r.

Pełny zapis przebiegu posiedzenia

Komisji Śledczej do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych m.in. z wykorzystaniem oprogramowania Pegasus przez członków Rady Ministrów, służby specjalne, Policję, organy kontroli skarbowej oraz celno-skarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od dnia 16 listopada 2015 r. do dnia 20 listopada 2023 r. (nr 18)

8 lipca 2024 r.

Komisja Śledcza do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych m.in. z wykorzystaniem oprogramowania Pegasus przez członków Rady Ministrów, służby specjalne, Policję, organy kontroli skarbowej oraz celno-skarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od dnia 16 listopada 2015 r. do dnia 20 listopada 2023 r., obradująca pod przewodnictwem poseł **Magdaleny Sroki (PSL-TD)**, przewodniczącej Komisji, zrealizowała następujący porządek dzienny:

– odebranie opinii biegłego Krzysztofa Dyki, powołanego przez Komisję uchwałą z dnia 17 czerwca 2024 r.;

– sprawy bieżące.

W posiedzeniu udział wzięli: **Adam Behan**, **Piotr Binas**, **Filip Curyło**, **Kamil Krajewski**, **Katarzyna Leder Salgueiro**, **Piotr Marciniak**, **Grzegorz Nawrocki** i **Sławomir Śnieżko** – stali doradcy Komisji.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Magda Jedynak**, **Sylwia Łaska** i **Mariusz Pawełczyk** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dzień dobry, witam państwa bardzo serdecznie. Otwieram posiedzenie Komisji Śledczej do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych z wykorzystaniem oprogramowania Pegasus przez członków Rady Ministrów, służby specjalne, Policję, organy kontroli skarbowej oraz celno-skarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od dnia 16 listopada 2015 r. do dnia 20 listopada 2023 r.

Na podstawie listy obecności stwierdzam kworum.

Stwierdzam przyjęcie protokołów z poprzednich posiedzeń Komisji wobec niezgłoszenia do nich zastrzeżeń.

Porządek dzienny dzisiejszego posiedzenia Komisji przewiduje: odebranie opinii biegłego Krzysztofa Dyki, powołanego przez Komisję uchwałą z dnia 17 czerwca 2024 r.; punkt drugi – sprawy bieżące. Czy są jakieś wnioski do porządku dziennego dzisiejszego posiedzenia? Wobec braku zgłoszeń przychodzimy w takim razie do realizacji punktu pierwszego, czyli odebranie zeznań od pana biegłego Krzysztofa Dyki.

Dzień dobry, witam serdecznie.

Na wezwanie Komisji stawił się pan Krzysztof Dyki, powołany uchwałą Komisji na 16. posiedzeniu w dniu 17 czerwca 2024 r. jako biegły sądowy z zakresu informatyki wpisany na listę biegłych sądowych Sądu Okręgowego w Warszawie. Komisja w uchwale powołała pana na biegłego na następujące okoliczności: ustalenie ryzyk korzystania z oprogramowania Pegasus, opinii na temat topologii systemu teleinformatycznego Pegasus, w tym struktury kodu, infrastruktury sieciowej, kryteriów rozliczalności użycia, poufności jego stosowania, miejsca gromadzenia danych logowań, działań użytkownika wykorzystującego licencję oprogramowania Pegasus zakupioną przez CBA, kompletności, nienaruszalności i integralności danych pozyskiwanych za pomocą tego systemu, zakresu kontroli i zabezpieczeń procesów infekcji i transmisji danych, zakresu audytu oprogramowania i urządzeń aktywnych oraz rodzajów testów, którym powinien być poddany tego typu system informatyczny, możliwości dostępu do danych historycznych na atakowanym urządzeniu, możliwości modyfikowania dokumentów w zainfekowanym urządzeniu lub w systemie teleinformatycznym, zdolności do wysyłania dokumentów, wiadomości, wykonywania połączeń w imieniu użytkownika zainfekowanego urządzenia komórkowego, oceny możliwości zachowania integralności, autentyczności i niezabezpieczalności danych stanowiących dowody pobierane z zainfekowanego urządzenia z wykorzystaniem oprogramowania, opinii, czy sposób przechowywania i zapisywania danych przez oprogramowanie Pegasus zapewniał walor procesowego materiału dowodowego na potrzeby postępowania sądowego, sposobu pozyskania przez CBA systemu teleinformatycznego Pegasus za pośrednictwem spółki Matic.

Pouczam pana o treści art. 233 § 4 Kodeksu karnego, na podstawie którego kto jako biegły, rzeczoznawca lub tłumacz przedstawia fałszywą opinię lub tłumaczenie mające służyć za dowód w postępowaniu prowadzonym przez Komisję, podlega karze.

Wymogi proceduralne obligują mnie do zadania panu pytania, czy zrozumiał pan treść pouczenia.

Biegły Krzysztof Dyki:

Tak, zrozumiałem.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Przypominam, że przebieg przesłuchania jest utrwalany za pomocą urządzenia rejestrującego dźwięk i obraz, o czym został pan uprzedzony w wezwaniu.

Proszę o podanie imion, nazwiska, wieku i zajęcia.

Biegły Krzysztof Dyki:

Krzysztof Jan Dyki, 47 lat, prezes spółki ComCERT.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo proszę wszystkich o powstanie. W tej chwili odbierzemy przyrzeczenie.

Proszę za mną powtarzać.

„Świadomy znaczenia moich słów…

Biegły Krzysztof Dyki:

„Świadomy znaczenia moich słów…

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

…i odpowiedzialności przed prawem…

Biegły Krzysztof Dyki:

…i odpowiedzialności przed prawem…

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

…przyrzekam uroczyście…

Biegły Krzysztof Dyki:

…przyrzekam uroczyście…

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

…że powierzone mi obowiązki…

Biegły Krzysztof Dyki:

…że powierzone mi obowiązki…

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

…wykonam z całą sumiennością i starannością".

Biegły Krzysztof Dyki:

…wykonam z całą sumiennością i starannością".

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo dziękuję.

Możemy usiąść. Bardzo proszę sekretariat o pomoc i włączenie mikrofonu. Bardzo dziękuję. Bardzo dziękuję.

W takim razie przystępujemy do zadawania pytań. Szanowni państwo, pozwolicie, że jako pierwsza rozpocznę serię pytań. Kolejna zadawać pytania będzie pani poseł Joanna Kluzik-Rostkowska, następnie pan wiceprzewodniczący Marcin Bosacki, następnie pan Witold Zembaczyński, później pan Patryk Jaskulski i ewentualnie będziemy ustalać dalszą kolejność.

Szanowni państwo, dzisiaj przesłuchujemy biegłego sądowego. Ma pan ogromne doświadczenie eksperckie, ale proszę powiedzieć, jakie ma pan doświadczenie, doświadczenie z zakresu analizy umów IT klasy przedsiębiorstwa, analizy oprogramowania, cyberbezpieczeństwa. Czy w trakcie wykonywania swojego zawodu wykonywał pan pracę operacyjną lub śledczą na poziomie „ściśle tajne"? Czy pana doświadczenie z zakresu… Czy ma pan doświadczenie również z zakresu nabywania systemów niejawnych, systemów do przetwarzania informacji ściśle tajnych? Czy posiada pan doświadczenie z zakresu tworzenia niejawnych systemów przetwarzających informacje? Te pierwsze pytania chciałabym, żeby były również takim momentem, w którym mógłby pan opowiedzieć o swoich możliwościach i doświadczeniu eksperckim.

Biegły Krzysztof Dyki:

Tak, to może pozwolę sobie zacząć od końca. Jeżeli chodzi, jeżeli dobrze pamiętam…

Czy doświadczenie w stosowaniu narzędzi tej klasy: ściśle tajnych? Tak. Czy doświadczenie w nabywaniu narzędzi ściśle tajnych tej klasy? Tak. Czy doświadczenie w tworzeniu narzędzi ściśle tajnych tej klasy? Tak. Doświadczenie praktyczne? Tak. I ta część pierwsza pytania, dotycząca analizy umów oprogramowania, inżynierii wstecznej i cyberbezpieczeństwa: również tak.

W zakresie praktycznym sądowym? Poprzez zakres praktyczny mam na myśli występowanie po stronie wykonawcy, twórcy, ale też po stronie zamawiającego klienta, z obu stron w tym zakresie, o który pani przewodnicząca pyta. W zakresie sądowym, o który padło pytanie, to ok. 20 lat opinii sądowych tej klasy, o którą pani przewodnicząca pyta, czyli spory dotyczące zagadnień, już też abstrahując od tej kwestii techniki operacyjnej i niejawnych, spory dotyczące zagadnień praw autorskich, oceny własności kodów źródłowych, wartości oprogramowania, umów klasy przedsiębiorstwa, o które pani przewodnicząca pyta. Więc to ok. 20 lat doświadczenia przed organami sądowymi jako biegły sądowy, ale w międzyczasie równolegle to samo doświadczenie praktyczne po stronie klienta i po stronie wykonawcy. To się całe życie mieszało, też w tym okresie 20 lat, czyli opinie sądowe plus wykonawca, klient.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję bardzo.

Wiemy, że Komisja pracuje nad wyjaśnieniem kwestii dotyczących stosowania Pegasusa, systemu tego oprogramowania Pegasus. Czy pan dysponował kiedykolwiek oprogramowaniem Pegasus? Kiedy, w jakim zakresie i w jakich okolicznościach?

Biegły Krzysztof Dyki:

Tak, dysponowałem, nie całym oprogramowaniem, tylko modułami infekującymi. Później będę prawdopodobnie posługiwał się trochę bardziej technicznym określeniem „implanty", czyli tak jak implant w rozumieniu medycyny, to również podobnie trochę działa to oprogramowanie. Ja nie dysponowałem całym zestawem systemu Pegasus,

nigdy go nie używałem, natomiast dysponowałem tymi modułami infekcyjnymi, tymi implantami, które są instalowane na smartfonach, odpowiedzialnymi za infekcje.

Pierwszy raz zetknąłem się z tym, jeszcze nie wiedząc, że to jest Pegasus, około dwa, niecałe 2 lata przed wybuchem medialnym tej sprawy na świecie, gdy usłyszałem, że to coś nazywa się Pegasus. Tak to nazwano, taką nazwę nadano temu produktowi. Pierwszy raz… Nie pamiętam dokładnie, kiedy ta sprawa ujrzała światło dzienne, ale nieco wcześniej już w moje posiadanie weszły te komponenty, moduły infekcyjne, które były… Wiadomo, że pochodzą z Izraela – to było dość szybko ustalone – ale jeszcze nie było wiadomo, dokładnie czego dotyczą, czyli zobaczyłem, zetknąłem się z niespotykanym sposobem wyrafinowania. Poprzez wyrafinowanie mam na myśli bardzo wysoki poziom ekspercki i technologiczny nowych, wcześniej niespotykanych zagrożeń. Dość szybko można było ustalić, że to pochodzi z Izraela. I chwilę później, gdy się okazało, że to firma NSO Group, Pegasus, już było wiadomo, że to jest to, czyli to był… nie pamiętam, który rok dokładnie, na pewno ok. 2 lata przed tym, gdy oficjalnie uznano to oprogramowanie za istniejące, medialnie obecne. Wtedy zainteresowały mnie te moduły infekcyjne pod kątem inżynierii wstecznej.

Tak jak powiedziałem, przez blisko 30 lat… Wcześniej mówiłem o doświadczeniu praktycznym, zawodowym, to jest ok. 20 lat, o które pani przewodnicząca pytała, ale 30 lat doświadczenia, nawet więcej niż 30, z zakresu inżynierii wstecznej. Ja się interesując tym od małych lat, młodych lat… Jeżeli się interesujemy takim zagadnieniem, jeżeli mamy kontakty międzynarodowe i jeżeli istniejemy w tym obszarze inżynierii wstecznej, to nie jest trudne pozyskanie takich końcówek infekujących. Pozyskanie oprogramowania jest bardzo trudne, ale pozyskanie tych końcówek infekujących nie jest trudne. W taki sposób wszedłem w ich posiadanie – poprzez kontakty zagraniczne z tego samego środowiska ludzi, pasjonatów, którzy pasjonują się inżynierią wsteczną, ze środowisk ludzi, którzy tworzą oprogramowania antywirusowe. W taki sposób wszedłem.

Ostatni raz, kilka lat temu, może ze 3 lata temu, gdy widząc, jak działa Pegasus, jak innowacyjne metody stosuje, jak nieskuteczne są systemy cyberbezpieczeństwa wobec tego specyficznego zagrożenia, zainwestowałem w kilka technologii. Jedna z nich przeciwdziałała tym technikom infekcji. Nad tym pracowałem, porównując, badając, stąd to moje doświadczenie tylko w zakresie modułu infekującego, który z jednej strony jest najciekawszy, ale pewnie w świetle tej sprawy sprawa będzie dotyczyć całego systemu, więc ja za ten model infekujący… Kontakt miałem, tak.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dobrze. Ja… następne pytanie… Chciałam poprosić i… odpowiedzieć, czym jest i jak działa oprogramowanie Pegasus, ale zanim pan przejdzie do odpowiedzi na to pytanie, bardzo poproszę wyjaśnić wszystkim nam, czym jest technologia wsteczna.

Biegły Krzysztof Dyki:

Ach, inżynieria wsteczna…

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Inżynieria.

Biegły Krzysztof Dyki:

…czasami zwana inżynierią odwrotną, jest procesem odwrotnym do inżynierii, czyli jeżeli mówimy o inżynierii czegoś w produkcji, to produkujemy coś, prawdopodobnie technicznego, technologicznego. Inżynieria wsteczna jest procesem odwrotnym. Dla przykładu, stawiamy myśliwiec F-16 na środku parkingu i mówimy: powiedz mi, jak on powstał, jak go stworzyć, stwórz dokumentację. Nie mamy niczego. Widzimy urządzenie, widzimy myśliwiec, widzimy obiekt, więc inżynier wie, jak go stworzyć. Inżynieria wsteczna to jest parking, myśliwiec i zadanie: powiedz mi, jak on działa, stwórz mi dokumentację. To jest inżynieria wsteczna, odwrotność tworzenia. To jest badanie obiektu – to może być obiekt fizyczny, może być obiekt programowy – w celu ustalenia zasad i sposobów jego działania, żeby go zrozumieć. Czyli jeżeli mówiłem, że stosowałem inżynierię wsteczną wobec Pegasusa, to badałem kod – nigdy źródłowy, nie miałem

do niego dostępu, tylko wynikowy, skompilowany, działający – Pegasusa, żeby zrozumieć, jak on dokładnie działa. To jest właśnie inżynieria wsteczna.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

To teraz proszę nam powiedzieć, czym jest Pegasus.

Biegły Krzysztof Dyki:

Pegasus jest narzędziem dedykowanym – podkreślam, dedykowanym – dla służb specjalnych. To nie jest narzędzie dla wojska. To nie jest narzędzie dla rządu. Jest to narzędzie dedykowane służbom specjalnym stosującym technikę operacyjną, upraszczając, narzędzie do elektronicznej inwigilacji, czyli narzędzie mające… umożliwiające zdalną kontrolę smartfonów i tabletów, nie komputerów. To jest ważne. Jeżeli mówimy o Pegasusie, to są smartfony i tablety. Tablet musi posiadać kartę fizyczną SIM lub elektroniczną eSIM, żeby można było zainfekować tablet. Dla przykładu, tablet z siecią Wi-Fi nie da się zainfekować tym jednym rozwiązaniem. Więc narzędzie dla służb specjalnych umożliwiające elektroniczną inwigilację w zakresie dość szerokim…

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

No właśnie, o tę szerokość zaraz będziemy dalej pytać.

Biegły Krzysztof Dyki:

Aha, dobrze.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Ale jeszcze chciałam dopytać, ponieważ padło takie sformułowanie, że powstał on w Izraelu. Mamy firmę NSO, która sprzedała takie narzędzie. Ale czy całość tego oprogramowania powstała wyłącznie w Izraelu? Ponieważ są bardzo różne informacje, które spływają do nas z różnych stron, że nie wszystkie komponenty, jeżeli mogę to tak określić, powstały na terenie Izraela.

Biegły Krzysztof Dyki:

To jest trudne pytanie, pani przewodnicząca, ponieważ właśnie… Chwilę zamilkłem, ale pani dodała cenną uwagę. Może krótkie tło. Tej klasy oprogramowanie prawie nigdy nie powstaje w jednym kraju. To jest… Tej klasy oprogramowanie, wszystkie tej klasy oprogramowania, które znam, miałem okazję mieć z nimi styczność, żadne nie powstało w jednym kraju. Ono… Oczywiście biuro, back office, obsługa administracyjna i czasami nawet programiści znajdują się w danym kraju. Na przykład Izrael i… Tam jest ta główna działalność ich twórców, tak, to prawda, natomiast w tej klasy rozwiązaniach rzeczywiście dość często – żeby nie powiedzieć standardowo – korzysta się z możliwości globalnych, z możliwości międzynarodowych. Więc nie jestem… nie mam dowodów na to, żeby stwierdzić, że ono nie powstało tylko w Izraelu, natomiast domyślam się, czego dotyczy tło pytania.

Czy mogło powstać również poza Izraelem? Tak, mogło. W jakich krajach? Nie chciałbym spekulować, natomiast lista krajów najlepszych w atakach cybernetycznych i najlepszych specjalistów jest ogólnie znana na świecie, więc… Tylko tu już wchodzimy w spekulacje, a nie jestem upoważniony i nie mam dowodów na to…

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

A jakbyśmy mieli sklasyfikować takie trzy kraje, wymienić…

Biegły Krzysztof Dyki:

Najmocniejsze?

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Najmocniejsze w tworzeniu tzw. exploitów…

Biegły Krzysztof Dyki:

Exploitów. OK, rozumiem.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

…czyli, tłumacząc, tych takich mikroprogramów, które odpowiedzialne są za to, że możemy przełamać zabezpieczenia czy znaleźć te dziury w systemie naszych telefonów komórkowych.

Biegły Krzysztof Dyki:

Ja po prostu jestem zawstydzony, bo dynamika tego naszego dzisiejszego spotkania jest znacznie większa, niż zakładałem, że będzie, więc naprawdę duży szacunek za tak bogate posiadanie tak bogatego tła tego trudnego rynku.

W mojej ocenie, co łatwo odnaleźć w moich wywiadach od lat udzielanych w mediach, na pierwszym miejscu jest to Rosja, absolutnie tak. Jeżeli chodzi o ofensywne zdolności do tworzenia chociażby, tak jak pani przewodnicząca pyta, exploitów, to na pierwszym miejscu jest to Rosja, niedaleko dalej Izrael. Często się przenikają z racji historii tego kraju i też jednak ciągłej… jakieś przenikania się tych nacji, może ostatnio z racji sytuacji geopolitycznej mniej, ale to jest jednak… Ta historia dalej istnieje. Więc Rosja, Izrael. Kolejne miejsce? Należałoby się zastanowić, czy Chiny, czy Stany Zjednoczone. Ciężko by mi było spekulować. Pierwsze dwa miejsca: Rosja, Izrael.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czyli istnieje prawdopodobieństwo, że system Pegasus w całości, w swoich komponentach miał wytworzone na przykład przez rosyjskich hakerów części, które umożliwiały infekcje telefonów komórkowych polskich użytkowników.

Biegły Krzysztof Dyki:

Aż tak daleko nie chciałbym pójść w swojej wypowiedzi. Powiedziałbym raczej, że istnieje prawdopodobieństwo, że na podstawie specyfiki wytwarzania tej klasy produktów… że powstało ono nie tylko w Izraelu. Tak.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dobrze. Czy teoretycznie i technicznie istnieje możliwość kontroli firmy NSO nad tymi danymi pozyskanymi i transmitowanymi na poziomie infekcji?

Biegły Krzysztof Dyki:

To jest bardzo dobre pytanie i wiele razy było do mnie kierowane na przestrzeni ostatnich lat. Odpowiedź jest prosta. W tej kategorii zakupach tak naprawdę nie wiele, ale wszystko wręcz zależy od klienta. Jeżeli klient jest świadomy, jeżeli klient jest kompetentny i jeżeli klient chce zabezpieczyć swoje interesy, to to ryzyko, o które pani przewodnicząca pyta, albo nie ma miejsca, albo jest zminimalizowane. Ja sobie wyobrażam, że nie powinno mieć miejsca, natomiast jeżeli klient kupuje przykładowo karton czegoś, przy czym nie wie, czym to jest, jak to działa, to wtedy takie ryzyko w przypadku tej klasy oprogramowania jest i ono rzeczywiście występuje.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dobrze. To w takim razie… Bo my zastanawiamy się cały czas na temat akredytacji, tego, czy to narzędzie zostało rzeczywiście dobrze zweryfikowane, sprawdzone, zanim trafiło do użytku dla polskich służb. Czy dało się taki system zakredytować, sprawdzić i zabezpieczyć przed ewentualnie możliwością utraty tych danych czy przejęcia tych danych przez izraelską firmę NSO?

Biegły Krzysztof Dyki:

Pani przewodnicząca, szanowni państwo, mamy kilka wątków. W tym pytaniu zawarło się kilka wątków. Zawarło się bezpieczeństwo, zawarła się akredytacja, zawarło się sprawdzenie. Z perspektywy biegłego sądowego to są różne pojęcia, a więc pozwolę sobie je rozpakować i omówić.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

OK. Proszę.

Biegły Krzysztof Dyki:

Jeżeli mówimy o sprawdzeniu, jest to bardzo szerokie pojęcie. Ono nie dotyczy akredytacji. Elementem sprawdzenia może być akredytacja, akredytacja jest procesem

formalnym, regulowanym aktami prawnymi, procedurami, normami, certyfikatami, świadectwami. Natomiast jeżeli wychodzimy od pierwszego pojęcia, właśnie ogólnego „sprawdzenia", to sprawdzenie w tej kategorii nabywaniu narzędzi jest czynnością bardzo otwartą. To od klienta zależy, czy i jak on chce sprawdzić to narzędzie, które nabywa. Akredytacja jest na samym końcu, ponieważ w drugim wymiarze tego pytania dochodzimy do bezpieczeństwa, tak jak pani przewodnicząca zapytała, tego systemu, czyli możemy sprawdzić bezpieczeństwo tego systemu, ciągle abstrahując od akredytacji, bo akredytacja… Zaraz do niej dojdziemy.

Bezpieczeństwo takiego systemu możemy sprawdzić na kilka sposobów, przede wszystkim badając jego bezpieczeństwo, bezpieczeństwo wykonywalnego, tego działającego, *as is*, tak jak mój smartfon, który posiadam. Można zbadać jego bezpieczeństwo bez proszenia Samsunga i innych. Można również poprosić Samsunga: „pokaż mi, drogi Samsungu, kody źródłowe do mojego smartfonu", ale Samsung może powiedzieć: „nie dam ci tych kodów, nie ufam ci", i nie daje kodów, kupujesz smartfon. Tak samo jest w przypadku tego oprogramowania. Możemy poprosić producenta o dostęp do kodów źródłowych. I nie mówię teraz: dajcie nam kody do Polski. Nie. Wsiadamy w samolot, lecimy do Izraela, trzy godziny, jesteśmy na miejscu i tam zapoznajemy się z kodami źródłowymi, nigdy ich nie pozyskując – to jest bardzo ważne. Czyli nie mówimy o pozyskaniu kodów źródłowych, tylko o oględzinach, w wyniku których zapoznajemy się z treścią. Nie wiem, czy wykonano taką prośbę, czy nie, czy doszło do tego, ale być może z jakiegoś powodu nie doszło. Naprawdę nie wiem.

To w takim razie co robimy, gdy producent mówi: „nie udostępnię ci, nawet do wglądu, kodów źródłowych"? Wtedy właśnie stosujemy albo inżynierię wsteczną, albo po prostu testy bezpieczeństwa oprogramowania tzw. wykonywalnego w takiej postaci, w jakiej ono działa. Te testy mogą odbywać się statycznie, analizując kod, pliki, albo też dynamicznie – mówimy: behawioralnie – czyli analizując zachowanie tego w działaniu. Nie potrzebujemy żadnych kodów źródłowych i dokumentacji, żeby zbadać bezpieczeństwo tego rozwiązania. Wtedy badamy protokoły, transmisje, ewentualne dziury, luki, podejrzane zachowania, metadane, artefakty itd., więc jest szereg możliwości do zbadania bezpieczeństwa takiego rozwiązania.

Dopiero, szanowna pani przewodnicząca, na końcu jest akredytacja ewentualna, tylko o akredytacji mówimy wtedy, gdy mamy do czynienia z rozwiązaniem przetwarzającym informacje niejawne. Zakładam, że mówimy o pracy operacyjnej, więc informacje pozyskane w toku kontroli operacyjnej, zakładam, że miały klauzulę „tajne", zapewne „ściśle tajne", więc zakładam, że rzeczywiście powinna być mowa o akredytacji. Jeżeli to urządzenie… Jeżeli Pegasus w Polsce przetwarzał informacje z kontroli operacyjnej, to o akredytacji możemy mówić paradoksalnie wtedy i tylko wtedy, gdy spojrzymy, jaką klauzulę nadawano na informacje pozyskiwane w wyniku działania Pegasusa. I to nam odpowie na pytanie, czy powinna być akredytacja. Trochę zawiła odpowiedź, może być trudna, ale…

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

No dobrze, to ja może też ułatwię, żeby nasi słuchacze też to zrozumieli. Jeżeli były nakładane klauzule „ściśle tajne" na dokumenty wytwarzane przy pomocy systemu Pegasus, to powinna być akredytacja czy nie?

Biegły Krzysztof Dyki:

W mojej ocenie, jeżeli na materiały pozyskiwane w wyniku działania systemu Pegasus były nakładane klauzule, to odpowiedź jest zawarta w pytaniu: oczywiście tak.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

To oczywiście wiemy, natomiast wszystko wskazuje na to, że system działający w Polsce nie posiadał takiej akredytacji. Czy pan, wykorzystując swoje doświadczenie i swoją wiedzę, odpowie na pytanie, czy nabywający licencję Pegasusa może na przykład w takim razie legalnie to narzędzie udostępnić innej firmie? Jeżeli mielibyśmy do czynienia z tym, że nie tylko jedna służba w Polsce korzystała z tego systemu, który, jak już wiemy, działał bez akredytacji, czy on mógł być udostępniany innym służbom?

Biegły Krzysztof Dyki:

To tylko drobna uwaga. Nie znałem oczywiście tego wątku o akredytacji tego stanu faktycznego. Naprawdę nie znałem. Nie znam i nie znałem też treści umowy i jej warunków. Nigdy nie widziałem jej na oczy ani nie słyszałem o jej warunkach, więc odpowiadam zupełnie obiektywnie, abstrahując od tej umowy, o której naprawdę nie mam pojęcia.

Sprawa wygląda następująco w tej kategorii systemach. Polskiej umowy nie widziałem, natomiast miałem okazję widzieć inne umowy z innych krajów. Wiem, że to brzmi paradoksalnie, ale tak było. Naprawdę polskiej umowy nie widziałem, natomiast miałem okazję widzieć umowy z innych krajów, również pozyskiwane w podobny sposób.

Te umowy, które ja widziałem z innych krajów, one dotyczyły z reguły wskazania konkretnej jednostki, która nabywała to narzędzie. Jeżeli jest wskazana jedna jednostka, jeden klient, jedna organizacja, która nabywa to narzędzie, to tylko ona może go używać, jeżeli w treści umowy nie ma upoważnienia do udostępnienia tego samego narzędzia dla innych wskazanych jednostek klientów.

Ponieważ… Szanowni państwo, umowa jest… umowa definiuje i nawiązuje stosunek cywilnoprawny i ten stosunek mamy pomiędzy stronami, więc w standardowej umowie Pegasusa występowały dwie strony. Zdarzały się więcej niż dwie strony, ale one muszą być explicite wskazane w treści umowy, literalnie wskazane w treści umowy. Jeżeli nie są, to z tego oprogramowania może korzystać tylko ta strona, ta instytucja, która jest wskazana w treści umowy.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję bardzo.

Zaraz oddam głos pani poseł Joannie Kluzik-Rostkowskiej.

Oczywiście my dzisiaj przesłuchując pana w charakterze biegłego, gromadzimy wiedzę, żeby właśnie móc odnieść to do tych informacji, które my posiadamy w formie dokumentów objętych klauzulą, ponieważ my dysponujemy umową, która została zawarta, i tym, jak… w jakiej formule to jest… w jakiej formule jest akurat ten system zakupiony przez służby w Polsce, tak? Bo wiemy, że on miał kilka możliwości i mógł mieć różne wersje. Dlatego zadając nasze pytania, czasem będziemy teoretyzować, natomiast my to wszystko jesteśmy w stanie przełożyć na dokumentację, którą posiadamy.

Oddaję w tej chwili głos. Pani poseł Joanna Kluzik-Rostkowska, bardzo proszę.

Poseł Joanna Kluzik-Rostkowska (KO):

Dzień dobry, witam serdecznie. Ponieważ interesujemy się wątkiem zakupu Pegasusa, to chciałam zacząć od samego początku, czyli jak to się wydarzyło, że Pegasus znalazł się w posiadaniu polskiej służby, a później służb. Jarosław Kaczyński, który był pierwszym przesłuchiwanym przez nas świadkiem, wydawać się był szczerze zadziwiony, że w zakupie Pegasusa uczestniczył jakikolwiek pośrednik. Przed chwilą powiedział pan, że miał pan okazję widzieć umowy innych państw. Czy można określić, czy raczej regułą jest zakup bezpośredni, czyli NSO – rząd danego państwa, czy raczej pośrednik jest takim oczywistym instrumentem przy pozyskiwaniu Pegasusa?

Biegły Krzysztof Dyki:

Standardowym modelem sprzedaży Pegasusa przez firmę NSO jest model bezpośredni, który ma na celu bezpieczeństwo transakcji, po pierwsze. Spółkę NSO tworzą byli pracownicy służb specjalnych Izraela, oni ją stworzyli, więc wiedzą, jak się gra w te gry, i to nie są amatorzy. Bezpieczeństwo transakcji, poufność transakcji i kolejny argument to jest jednak marża. Pośrednikowi trzeba oddać marżę, więc w domyślnym modelu sprzedaży standardowym: bezpośrednia sprzedaż.

Poseł Joanna Kluzik-Rostkowska (KO):

To otwiera całe pole do dużych znaków zapytania, dlaczego akurat w Polsce wykorzystano pośrednika. Historycznie rzecz biorąc, firma Matic, która tym pośrednikiem była… Gdzieś wyczytałam w którejś pana wypowiedzi, że takich firm… już abstrahując od tego, że, rozumiem, z takiego operacyjnego punktu widzenia byłoby lepiej, gdyby to była sprzedaż bezpośrednia, to takich firm w Polsce jest przynajmniej kilkanaście, które ewentualnie mogłyby oferować swoje pośrednictwo. Firma Matic spotkała się z NSO

na jednym z targów międzynarodowych i tam zawarła umowę o to właśnie pośrednictwo. Rzeczywiście marża była duża, ponieważ zapłaciliśmy jako budżet państwa 8 mln dodatkowych za to, że firma Matic była właśnie pośrednikiem. Czy z punktu widzenia tego, kim się… czym ta firma Matic się zajmuje, czy ona mogła dać jakąś wartość dodaną do tego zakupu, czy po prostu była pośrednikiem, który zainkasował 8 mln zł?

Biegły Krzysztof Dyki:

To pytanie trochę mnie krępuje, ponieważ należy zaznaczyć, że firma Matic nie jest firmą obcą dla mnie. Też jako ComCERT zdarza się nam współpracować z tą firmą przy innych projektach, również niejawnych, ale nie tej klasy oprogramowania, to chciałbym wyraźnie zaznaczyć.

Natomiast jeżeli skorzystano z pośrednika, to trudno jest mi sobie wyobrazić sytuację, w której nie ma wartości dodanej w postaci usług tej firmy. Nie mam niestety wiedzy na temat… Wiem o tym z doniesień medialnych, oczywiście wiedziałem, że wystąpiła firma pośrednik, w tym przypadku Matic. To należy zaznaczyć, że firma Matic jest firmą poważną. To nie jest firma anonimowa, to nie jest firma bez doświadczenia. Jest to firma o ugruntowanej pozycji i wiarygodności, również, co ważne, szanowni państwo, firma z doświadczeniem w dostarczaniu oprogramowania dla służb specjalnych.

Jednak rzeczywiście, tak jak wspomniała pani o moich wypowiedziach medialnych, należy rozgraniczyć dostarczanie oprogramowania dla służb specjalnych od oprogramowania klasy Pegasus. To są dwa różne zupełnie światy. Jest szereg firm – i o tych zapewne mówiłem nie w jednym miejscu, mówiąc, że kilkanaście firm mogłoby to dostarczyć – ponieważ tej klasy oprogramowanie, które dostarcza firma Matic na przykład z jawnych informacji, o których mogę mówić, dostępnych publicznie, to jest oprogramowanie i2, wcześniej firmy IBM. To jest oprogramowanie analityczne wspierające służby. Firma Matic jest dobrym rzemieślnikiem, który wykonuje dobrze tę pracę dla służb specjalnych. To należy uznać.

Natomiast usłyszałem teraz, czego nie wiedziałem wcześniej, że jakaś umowa została zawarta na targach. Samo to wskazuje… Nie wiedziałem o tym, że… ile firm mogło taką umowę zawrzeć, bo na targach… Ale upraszczając, firm, które… Ile mogło być firm, które mogły dostarczyć to oprogramowanie? Tyle, ile jest zdolnych do kupna biletu do Izraela i wyjazdu na 2, maksymalnie 3 dni, bo tak to się odbywa. Ja również często tam bywam, więc jeżeli ktoś ma upoważnienie, jest w stanie udowodnić, że ma w pewnym sensie legitymację, nie zawsze formalną, ale jednak organów państwa, które wyrażają chęć zakupu, to wsiada w samolot albo zaprasza tutaj przedstawicieli NSO, oni bywali i bywają tutaj dalej, w Warszawie, ostatnio nawet właściciel, w ubiegłym miesiącu… przepraszam, udziałowiec główny, nie właściciel, to można to spotkanie zorganizować na miejscu, można tam. Ile firm? Zapewne co najmniej kilkanaście mogło to zrobić.

Firma Matic zapewne z jakiegoś względu została wybrana. Tej wysokości marży nie znałem. Słyszałem o niższej, ale czy to jest 2–3 mln więcej, nie zmienia faktu, że jakaś usługa musiała być wykonana, skoro na fakturze znalazła się jakaś pozycja i klient potwierdził jej realizację. Więc bardziej, myślę, to jest pytanie do klienta, jaka usługa była zrealizowana, bo szczerze mówiąc, nie wiem. Nie kwestionuję, że żadna, absolutnie nie, natomiast Matic specjalizuje się w innej kategorii rozwiązań.

Poseł Joanna Kluzik-Rostkowska (KO):

Tak, bo my tutaj zajmujemy się również tym. Staramy się wyjaśnić, dlaczego, po to, żeby zakupić Pegasusa, sięgnięto do Funduszu Sprawiedliwości w myśl ustawy o CBA. Było to po prostu wyjście poza to, co jest tam zapisane, czyli że do funduszu operacyjnego można wkładać tylko pieniądze z budżetu państwa i tak naprawdę to była prostsza droga, czyli po prostu poproszenie ówczesnego ministra finansów o to, żeby wyasygnował sumę 25 mln zł na ten podstawowy zakup. Czy pan… Nie wiem, czy pan zwracał na to uwagę, ale czy w przypadku tych innych umów i innych państw te pieniądze pochodziły z budżetów państwa, czy też pochodziły z jakichś innych form finansowania?

Biegły Krzysztof Dyki:

Dokładnie tego nie pamiętam, nie badałem, ale przypominam sobie, że co najmniej w jednym kraju wystąpił fundusz, ale to nie był Fundusz Sprawiedliwości oczywiście,

był to fundusz inwestycyjny, coś na wzór naszego PFR, państwowego funduszu rozwoju. To taka instytucja wystąpiła, z tym że to był specyficzny kraj. Z pewnych względów nie chciałbym w części jawnej ujawniać jego nazwy, w części niejawnej jak najbardziej. I w tym kraju posłużono się funduszem klasy PFR do realizacji zakupu. W tamtym kraju to było absolutnie unormowane, legalne. Ten fundusz był upoważniony do takich zakupów. Ale w innych? Bezpośredni zakup przez służby, tak.

Poseł Joanna Kluzik-Rostkowska (KO):

To w takim razie otwiera nam się kolejne pytanie. Po co w ogóle pośrednik? Po co wydatkowanie tych dodatkowych pieniędzy, skoro akurat zajęła się ta firma, która jest mocno na rynku usytuowana, ale zajmuje się absolutnie czymś innym? I dlaczego sięgnięto po pieniądze funduszu, ale nie pieniądze budżetu państwa? Czyli podsumowując, generalna zasada jest taka, że zawiera się umowę… że państwo zawiera bezpośrednio umowę z firmą za pieniądze budżetowe.

Biegły Krzysztof Dyki:

Generalna zasada jest taka, że kupuje służba ze środków… w naszym kraju się mówi, tak, operacyjnych, konkretnie funduszu operacyjnego. To jest taka zasada. Należałoby spojrzeć… Oczywiście, są różne kraje, mają różne systemy, ale patrząc na nasz kraj, to środki funduszu operacyjnego…

Natomiast ja mam taką uwagę, refleksję z wielu lat. Tak jak zostałem zapytany i powiedziałem zgodnie z prawdą, że też miałem doświadczenie w tworzeniu różnej klasy narzędzi, to doświadczyłem w naszym kraju wiele razy takiego – co może jakieś tło stanowić tej problematyki, o którą jestem pytany – strachu przez zwiększaniem środków, przed zwiększaniem budżetu służby operacyjnej w ciągu roku. Jakiś u nas jest paraliż, bardzo dziwny. W krajach rozwiniętych, zachodnich, transparentnych to się dzieje, to jest po prostu bardzo szybkie, naturalne i nikt nie protestuje. U nas jest jakiś potężny problem, którego ja osobiście nie rozumiem, ale byłem świadkiem kilkukrotnie, gdzie były podobne potrzeby i był strach ze strony głównie ministerstwa spraw wewnętrznych przed zwiększeniem budżetu służby specjalnej. I wielokrotnie ja sam będąc…

Poseł Joanna Kluzik-Rostkowska (KO):

W ciągu roku?

Biegły Krzysztof Dyki:

W ciągu roku.

Poseł Joanna Kluzik-Rostkowska (KO):

Można to zrobić…

Biegły Krzysztof Dyki:

Pomimo bezwzględnie potrzeby transparentnej, uczciwej, bezwzględnej, pilnej był strach przed zwiększaniem – to dalej jest – przed zwiększaniem budżetu służby specjalnej, nawet nieważne której, po prostu przed zwiększaniem budżetu służby specjalnej. Jest coś takiego w naszym kraju, takie brzemię.

Poseł Joanna Kluzik-Rostkowska (KO):

No tak, dobrze, ale po jednym roku następuje kolejny rok.

Biegły Krzysztof Dyki:

Tak, tak.

Poseł Joanna Kluzik-Rostkowska (KO):

Można to wpisać w budżet.

Biegły Krzysztof Dyki:

…czy zaplanować, oczywiście.

Poseł Joanna Kluzik-Rostkowska (KO):

Ostatnie pytanie w tym wątku. Na pewno będziemy się jeszcze tym zajmować. Będziemy pytać pana o to, czy ten system był bezpieczny, czy możliwe były wycieki, czy ktoś niepożądany mógł mieć dostęp do tych informacji. Czy można założyć, że kupienie Pegasusa

przez pośrednika dodawało do tych ryzyk dodatkowe? Bo jest to taki kolejny element, który mógł być generatorem kłopotów dodatkowych.

Biegły Krzysztof Dyki:

Z perspektywy technicznej w mojej ocenie nie. Z perspektywy biznesowej, rozumiejąc interes klienta… Z perspektywy biznesowej mi osobiście… Gdybym ja odpowiadał za transakcję, nie chciałbym – oczywiście jeśli nie musiałbym go posiadać – pośrednika, taką transakcję, to z pewnością tak. Więc z perspektywy dlaczego bym nie chciał? Dlatego że nie chciałbym, żeby żadna firma wiedziała, co ja kupuję na potrzeby tak wrażliwych operacji. To z tego względu tak. Więc z perspektywy technicznej ryzyk nie widzę, ponieważ zakładam, że pośrednik nie powinien mieć – nie wiem, czy miał, ale nie powinien mieć – żadnego dostępu do tego narzędzia, żadnego. I w tym kontekście nie widzę ryzyk. Z perspektywy biznesowej, gdyby to ode mnie zależało, to chciałbym zrealizować tę transakcję bezpośrednio jako osoba odpowiedzialna za służbę specjalną z NSO.

Poseł Joanna Kluzik-Rostkowska (KO):

Dziękuję. W tej rundzie to już wszystkie moje pytania.

Biegły Krzysztof Dyki:

Dziękuję.

Poseł Joanna Kluzik-Rostkowska (KO):

Chcę tylko powiedzieć, że firma Matic miała organizować szkolenia, więc nie wiem, czy mogło się to odbywać bez dostępu do systemu.

Biegły Krzysztof Dyki:

To pytanie to trochę takie flirtowanie z prawem. Szkolenia… Pytanie: Dotyczące czego? Nie wykluczam, że jakieś były. Dziękuję.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję.

Teraz pan poseł Witold Zembaczyński, bardzo proszę.

Poseł Witold Zembaczyński (KO):

Wielce szanowna pani przewodnicząca, Wysoka Komisjo, państwo eksperci, szanowny panie biegły, proszę zatem powiedzieć, czy według biegłego wiedzy materiały operacyjne pozyskane przy użyciu Pegasusa znajdowały się w całości i na wyłączność w komputerach CBA, na tych konsoletach, czy z uwagi na charakter kodu źródłowego migrowały one również do wewnętrznych serwerów, pośredniczących serwerów. Czy może były tam całe klastry serwerów, które obsługiwały te dane pozyskiwane z urządzeń końcowych?

Biegły Krzysztof Dyki:

W standardowym modelu Pegasusa występują cztery główne komponenty. Pierwszym komponentem jest stacja robocza. Jej może być więcej niż jedna sztuka, z reguły była więcej niż jedna, czyli komputer klasy desktop lub laptop to jest ten pierwszy komponent. Stacje operatorskie, de facto końcówki odbierające…

Poseł Witold Zembaczyński (KO):

Czyli agent operator CBA siedzi przed nim, tak?

Biegły Krzysztof Dyki:

Agent operator, dokładnie, operator.

Poseł Witold Zembaczyński (KO):

Dokonuje infekcji z poziomu tej konsoli, tak?

Biegły Krzysztof Dyki:

Sterowania, operator sterowania, dokładnie tak.

Drugim modułem jest serwer, który znajduje się… najczęściej fizyczny serwer znajdujący się w dyspozycji klienta, czasami nawet w pomieszczeniu tego samego, co operator. Nie wiem, jak było w Polsce.

Poseł Witold Zembaczyński (KO):

Czyli miejsce, gdzie te dane będą zgromadzone, przez które przepływają.

Biegły Krzysztof Dyki:

Dokładnie tak.

Trzecim modułem… I tu już zależy architektura, konfiguracja od tego, jak dany klient zakupił ten produkt. Trzeci moduł to jest sieć anonimizująca. Ona jest nazywana skrótem PATM, sieć anonimizująca systemu Pegasus. Tu się zaczyna ciekawa rzecz, bo to jest więcej niż jeden serwer, fizyczny lub wirtualny, w ostatnich latach to były tylko wirtualne.

Poseł Witold Zembaczyński (KO):

Proszę biegłego, o co chodzi z tą siecią anonimizującą? O to, żeby od urządzenia końcowego, zainfekowanego nie dotrzeć po nitce do kłębka…

Biegły Krzysztof Dyki:

Tak.

Poseł Witold Zembaczyński (KO):

…czyli do konsolety, z której dokonywana jest infekcja? Więc wiele serwerów po drodze anonimizuje ten kierunek, tak?

Biegły Krzysztof Dyki:

Tak. Ten trzeci moduł to jest taka grupa serwerów, które pan słusznie doprecyzowuje, która odpowiada za anonimizację komunikacji w obie strony i ukrycie operatora, lokalizacji operatora. Ta grupa serwerów z reguły obecnie występuje jako serwery wirtualne wykupywane w różnych krajach, płacone kryptowalutami. I teraz… Ale przez kogo zarządzany ten trzeci moduł, sieć anonimizująca? I to już zależy od…

Poseł Witold Zembaczyński (KO):

To znaczy, to było zarządzane przez CBA, czy było zarządzane przez NSO?

Biegły Krzysztof Dyki:

I to właśnie zależy od tego, w jakim modelu kupiono to oprogramowanie. Jeżeli klient mówi: „ja chcę tylko kluczyki od samochodu, reszta mnie nie interesuje", to będzie to zarządzane domyślnie przez NSO.

Poseł Witold Zembaczyński (KO):

OK, ale… Proszę biegłego, natomiast te informacje pozyskane z końcowego urządzenia elektronicznego, które w wyniku infekcji trafiają do operatora za pośrednictwem tego serwera…

Biegły Krzysztof Dyki:

Dokładnie.

Poseł Witold Zembaczyński (KO):

…macierzystego, nazwijmy to, są anonimizowane przez te serwery pośrednie, które de facto posługują się szyfrowaniem. I teraz moje pytanie: Czy jest technicznie możliwe wykradzenie tego procesu między urządzeniem końcowym a konsoletą, gdzie dochodzi do tego szyfrowania, bądź czy NSO dokonując tej usługi anonimizacji, jest w stanie posiąść informacje wykradane z telefonu użytkownika?

Biegły Krzysztof Dyki:

Sieć anonimizująca ma za zadanie anonimizować samą transmisję, nie dane, nie ruszać danych, tylko samą ich transmisję. Więc ten, kto ma kontrolę nad siecią anonimizującą, ma kontrolę nad danymi, które przez nią przechodzą. Oczywiście te dane mogą być tam transmitowane w postaci zaszyfrowanej, ale to nie zmienia faktu, że ten, kto ma kontrolę nad siecią anonimizującą Pegasusa, kontroluje bezpieczeństwo tych danych.

Poseł Witold Zembaczyński (KO):

A przekładając to na przypadek polskiego customowego Pegasusa kupionego przez CBA, czy może biegły tutaj przełożyć to na funkcjonalność tego systemu? Jak to się odbywało

konkretnie w tym przypadku według biegłego wiedzy?

Biegły Krzysztof Dyki:

Nie wiem, w jaki sposób zakupiła Polska, natomiast jeżeli zakupiła system Pegasus bez kontroli nad siecią anonimizującą, to w tym obszarze, o który pan pyta, nie ma kontroli nad danymi Polska.

Poseł Witold Zembaczyński (KO):

Czy to byłby warunek do braku udzielenia akredytacji przez ABW?

Biegły Krzysztof Dyki:

Kilka lat temu zmieniły się przepisy. Ja dokładnie ich nie śledzę, ale była w ostatnich latach zmiana – nie wiem, ok. 2 lata temu – która… wprowadzono zapis mówiący, że jeżeli którykolwiek z komponentów infrastruktury jest poza siedzibą klienta, naszą nomenklaturą mówiąc, to chyba nie. Należałoby sprawdzić, jak w chwili transakcji… który przepis obowiązywał.

Poseł Witold Zembaczyński (KO):

W dalszym ciągu mówimy o stanie prawnym takim, który umożliwiał certyfikację systemu w sytuacji, kiedy wszystkie jego zasoby były pod kontrolą operatora.

Biegły Krzysztof Dyki:

Tak. Tak, bo trudno mówić, trudno mówić o certyfikacji czegoś, co nie jest pod naszą kontrolą.

Poseł Witold Zembaczyński (KO):

Proszę powiedzieć, czy sam Pegasus był możliwy do dostarczenia stronie polskiej, CBA, w wersji, w której wszystkie jego elementy są po stronie operatora, czyli CBA.

Biegły Krzysztof Dyki:

NSO… Nie wiem, jak było w przypadku Polski, ale NSO w przypadku niektórych innych krajów dopuszczało kontrolę, całkowitą kontrolę klienta nad całą infrastrukturą.

Poseł Witold Zembaczyński (KO):

Po swojej stronie?

Biegły Krzysztof Dyki:

Całkowitą kontrolę klienta…

Poseł Witold Zembaczyński (KO):

Przez klienta?

Biegły Krzysztof Dyki:

Przez klienta, wyłącznie przez klienta. Pytanie… Nie wiem, jak było w Polsce, w jaki sposób…

Poseł Witold Zembaczyński (KO):

Co Komisja potrzebuje, żeby to rozstrzygnąć… Czy dane kradzione – użyję takiego kolokwializmu „kradzione” – dane pozyskiwane w wyniku pracy techniki operacyjnej z elektronicznych urządzeń końcowych trafiały wyłącznie, bez pośrednictwa na serwer w siedzibie CBA, czy były szyfrowane poprzez wielopiętrowe przenikanie przez inne serwery, które były poza jurysdykcją CBA?

Biegły Krzysztof Dyki:

Troszkę uproszczę. W przypadku systemu Pegasus sieć anonimizująca nie jest komponentem fakultatywnym. Ona jest obligatoryjna. Ona musi wystąpić. Pytanie jest proste: Kto sprawował nad nią kontrolę? Bo to nie jest pytanie, czy była sieć…

Poseł Witold Zembaczyński (KO):

To jest coś, co my powinniśmy ustalić, tak żeby odpowiedzieć na to pytanie?

Biegły Krzysztof Dyki:

Gdzie i pod czyim nadzorem funkcjonowała sieć anonimizująca systemu Pegasus? To odpowie na to pytanie, bo ona musiała istnieć. Pegasus nie działa bez sieci anonimizującej. Nie jest możliwe.

Poseł Witold Zembaczyński (KO):

Komisja już ma jakąś wiedzę na ten temat. Natomiast cały czas poszukujemy tej odpowiedzialności w zakresie dopuszczenia użytkowania systemu bez certyfikacji ABW i tu istotą jest właśnie, można powiedzieć, ustalenie tych faktów, jak przebiegał proces anonimizacji również przy użyciu tych ewentualnie zewnętrznych zasobów. Czy, proszę powiedzieć, teoretycznie istniała możliwość wglądu do tych danych przez NSO w tym układzie?

Biegły Krzysztof Dyki:

Jeżeli dany klient zakupił Pegasusa, oddając kontrolę nad transmisją, siecią anonimizującą do NSO, to oczywiście tak.

Poseł Witold Zembaczyński (KO):

Proszę powiedzieć, czy według świadka NSO tworzyło lustrzane kopie materiałów pozyskiwanych przy użyciu technik operacyjnych przez poszczególne wywiady.

Biegły Krzysztof Dyki:

Nie mam takiej wiedzy. Nie posiadam takiej wiedzy.

Poseł Witold Zembaczyński (KO):

Proszę świadka, co według świadka… przepraszam, biegłego – proszę wybaczyć, to przyzwyczajenie komisyjne – było powodem odebrania licencji stronie polskiej przez NSO na użytkowanie Pegasusa?

Biegły Krzysztof Dyki:

Z informacji, które ja posiadam, sytuacja wiązała się… mogła się wiązać albo wynikać z okoliczności medialnych upublicznionych co do stosowania tego oprogramowania w kraju i za granicą przez Polskę, czyli pojawił się szereg wątpliwości, szereg…

Poseł Witold Zembaczyński (KO):

O użycie pozalicencyjne, czyli pozaumowne użycie oprogramowania.

Biegły Krzysztof Dyki:

Nie… sposobu wykorzystania. Nie było… nie spotkałem się z wątkiem licencyjnym. Dzisiaj po raz pierwszy od państwa słyszę tę problematykę licencyjną, jak się domyślam. Nie, z tych informacji, które ja posiadam, problem licencji, Polski i nastawienia NSO do naszego kraju wynikał głównie z pozycji Polski na arenie międzynarodowej w tzw. aferze Pegasusa. Otóż nie wiem, czy to jest ogólnie wiadome, ale my sporo nabroiliśmy jako kraj w interesach wobec NSO i samego Izraela. Czyli mamy dwie płaszczyzny: problem wobec Izraela, bo to oprogramowanie rzutuje na sytuację geopolityczną Izraela… Firmie NSO odebrano wszelkie licencje i możliwość sprzedaży czegokolwiek w Stanach Zjednoczonych, więc ta firma została, mówiąc technicznie, zbanowana, tak? Nie może zakupywać żadnych rozwiązań amerykańskich. Na tle czego? Między innymi Polski, czyli…

Poseł Witold Zembaczyński (KO):

A o jaką sytuację chodziło według biegłego wiedzy konkretnie?

Biegły Krzysztof Dyki:

Szereg publikacji medialnych dotyczących podejrzeń o… podkreślam, publikacji medialnych dotyczących podejrzeń o wykorzystywanie, prawdopodobne wykorzystywanie prawdopodobnie niezgodne z prawem wobec polityków, którzy…

Poseł Witold Zembaczyński (KO):

No właśnie dlatego tu się spotykamy. Właśnie to chcemy wyjaśnić.

Biegły Krzysztof Dyki:

I na tym tle Polska odegrała i odgrywa istotną rolę w dwóch płaszczyznach, jednej wobec Izraela, bo to jest problem już nie tylko firmy NSO, ale wizerunku również Izraela, po drugie, firmy NSO. Pamiętajmy, że oprogramowanie, o które szanowni państwo mnie pytają, to nie jest zwykły program, jeden z setek bardzo dobrych programów, świetnych, tworzonych w Izraelu. To jest szczególny program, bo jego sprzedaż nie odbywała się na podstawie decyzji firmy NSO komercyjnej. Jego sprzedaż za każdym razem musiała być uzgadniana z rządem Izraela i tak to się odbywało.

Poseł Witold Zembaczyński (KO):

Z ministerstwem obrony tam odpowiednio…

Biegły Krzysztof Dyki:

Na przykład czasami wręcz z premierem i…

Poseł Witold Zembaczyński (KO):

Z czego to wynikało? Z uwagi na to, że jest to cyberbroń?

Biegły Krzysztof Dyki:

Jest to świetne określenie. Kolejny raz jest mi bardzo miło słyszeć takie przygotowanie. Tak, jest to narzędzie… Nie jest to wprost cyberbroń, ale jest to narzędzie o znamionach cyberbroni, tak.

Poseł Witold Zembaczyński (KO):

Rozumiem. Proszę świadka, proszę jeszcze o troszkę większą dawkę informacji w zakresie pośrednictwa, dlatego że też Komisja ustaliła w pewnych źródłach również takie informacje, że to właściwie strona izraelska często w tej transakcji sprzedażowej między służbami specjalnymi poszczególnych krajów a wytwórcą NSO oczekiwała pośrednika w celu zatarcia tego bezpośredniego powiązania między dostawcą usługi a jej wykonawcą czy operatorem i również w celu wprowadzenia dodatkowego ogniwa, jakim jest tajemnica przedsiębiorstwa, tajemnica handlowa gdzieś pomiędzy… wynikająca z umów i samego faktu wprowadzania produktu na rynek przez przedmioty… przez podmioty komercyjne.

W związku z tym precyzując moje pytanie do biegłego: Czy zatem NSO działało dwutorowo w zależności od klienta, czyli albo spółki pośredniczące… co zresztą w świecie służb jest bardzo często praktykowane, że korzysta się z różnych fasadowych spółek pośredniczących, czy ta sprzedaż bezpośrednia jednak dominowała, powiedzmy sobie, w całym wolumenie sprzedaży NSO?

Biegły Krzysztof Dyki:

Sprzedaż bezpośrednia, co wynika chociażby ze strony… Nie wiem, jak ona dzisiaj wygląda, ale NSO można znaleźć w archiwach, to jest dostępne, internetowych. NSO na swojej stronie wyraźnie manifestuje, co sprzedaje, dla kogo sprzedaje, więc trudno mi mówić o tajemnicy przedsiębiorstwa czy handlowej, skoro to oni krzyczeli wręcz, namawiali również, tak jak ktoś z państwa dzisiaj słusznie powiedział, na różnych konferencjach, wydarzeniach… Oni oficjalnie przedstawiali: my się nazywamy NSO Group, mamy oprogramowanie do techniki operacyjnej do inwigilacji. Więc w mojej ocenie trudno tu mówić o ukrywaniu czegoś, skoro oficjalna ich działalność, oficjalny produkt…

Poseł Witold Zembaczyński (KO):

Był interes po stronie rządów, żeby utrudnić na przykład drogę przez dostęp do informacji publicznej w zakresie nabywania takiego oprogramowania. Co innego, kiedy z budżetu operacyjnego byłoby to kupione, wtedy de facto są to informacje klauzulowane, natomiast nie wynikało to z jakiegoś etosu funkcjonowania firmy, tylko, rozumiem, to użycie pośrednika było według biegłego, jeżeli dobrze to interpretuję, musiało być inicjatywą polską, tak? Czy nie był to warunek *sine qua non* umowy, żeby obsłużyć tę część Europy i sprzedać Pegasusa?

Biegły Krzysztof Dyki:

Myślę, że obiektywnie oceniając, trzeba by było spojrzeć na kategorie pośrednika i odpowiedzenie sobie na pytanie, czy i od kiedy był on pośrednikiem autoryzowanym NSO. Firma Matic nie była wcześniej pośrednikiem ani partnerem, więc trudno mówić o tym, że… trudno byłoby mówić o tym, że NSO oczekiwało akurat takiej firmy czy pośrednika. Raczej jeżeli w takiej sytuacji występuje, a czasami się zdarzała sytuacja, że musiał wystąpić pośrednik, to o tych sytuacjach, o których ja słyszałem, abstrahując od Polski, to były inicjatywy klienta, że klient z jakiegoś powodu chciał.

Poseł Witold Zembaczyński (KO):

W tym wypadku klientem jest CBA. Proszę powiedzieć, proszę biegłego, czy zatem CBA miało jakieś deficyty, które dawały tę przewagę Maticowi, żeby posłużyć się tym Matikiem w zakresie doboru osprzętu do tego, żeby zainstalować stanowisko operatorów w zakresie możliwości konfiguracji tego systemu. Z czego wynikało to de facto, oprócz tego, że Matic stale obsługuje polskie służby specjalne i państwo polskie od tam kilkudziesięciu lat? Czy to była taka… taki nawyk po prostu w tych służbach, które doprowadziły w CBA konkretnie do Matica? Czy jakieś deficyty po stronie CBA do tego doprowadziły? Co według biegłego było tym impulsem do użycia Matica?

Biegły Krzysztof Dyki:

Niestety nie potrafię odpowiedzieć na to pytanie, ale potrafię odpowiedzieć na kapitał intelektualny, kompetencje, które znajdują się w służbach specjalnych…

Poseł Witold Zembaczyński (KO):

O to też pytam.

Biegły Krzysztof Dyki:

…na przykładzie również CBA. Te kompetencje w przypadku CBA akurat są – są, czy też były na tamten moment, bardziej były, niż są – bardzo wysokie, bardzo wysokie, więc to nie są amatorzy. Część z tych osób to są moi koledzy i to są bardzo doświadczone osoby, które… Trudno jest mi sobie wyobrazić, żeby potrzebowały wsparcia jakiegokolwiek podmiotu innego niż producent, i trudno by mi było sobie wyobrazić, że ktoś inny niż producent to instaluje, jeżeli fizycznie ten zespół osób, które mam w głowie, by sobie nie poradził. Ale, znowu wracam, niektóre osoby znam i te osoby są bardzo kompetentne, więc przy tym poziomie wysokich kompetencji, jakie ówcześnie posiadało biuro, pracując tam, nie potrafię odpowiedzieć na pytanie, dlaczego pośrednik…

Poseł Witold Zembaczyński (KO):

Rozumiem. Sprawa jest jak gdyby niezamknięta.

Proszę powiedzieć, czy znał pan na tyle dobrze dyrektora Biura Techniki Operacyjnej CBA, Piotra Klimczuka, żeby się wypowiedzieć na temat mojego pytania, czy jego śmierć miała jakikolwiek związek z pracą w CBA.

Biegły Krzysztof Dyki:

Jak miałem przyjemność poznać pana dyrektora i to chcę zaznaczyć, że bardzo – w mojej ocenie personalnej – bardzo uczciwa osoba i oddana temu krajowi… To chciałem, żeby wyraźnie wybrzmiało. Postać, która… wyróżniająca się bardzo pozytywnie w mojej ocenie na tle naszej biało-czerwonej flagi, nie tylko samego biura.

Nie znam… Słyszałem oczywiście o tej wielkiej tragedii. Ogromne wyrazy współczucia dla członków rodziny, ogromna strata, również merytoryczna. Myślę, że poziom stresu, który towarzyszył zakupowi tego i nie tylko tego oprogramowania w tamtym obszarze, był na pewno niemały, ale nie chcę spekulować, czy miał związek, natomiast wiem, że poziom stresu, adrenaliny, jednak głównie stresu, był rzeczywiście w tamtym obszarze bardzo duży, co można łatwo prześledzić na podstawie ruchów kadrowych. One pokazują, oczywiście ja o nich nie mogę, nie chcę mówić, ale one pokazują, co się w którym momencie dzieje. Jeżeli jest dobrze, stabilnie, to kadry są stabilne, a jeżeli sytuacja jest niestabilna, nerwowa, stresująca, to te kadry się zmieniają, więc myślę, że była to bardzo trudna komórka. Zakładam, że chodzi o Biuro Techniki Operacyjnej.

Poseł Witold Zembaczyński (KO):

Tak, dokładnie tak.

Biegły Krzysztof Dyki:

OK, dobrze. To na pewno było to niełatwe miejsce nie tylko w tamtym okresie. Od tej komórki organizacyjnej oczekiwano cudów i to jest… Na tym się kończy moja wiedza. Podkreślam, sam pan dyrektor Piotr – absolutnie wzorowa postać.

Poseł Witold Zembaczyński (KO):

Bardzo dziękuję za tę odpowiedź.

Proszę biegłego, to przejdźmy teraz do dla mnie bardzo istotnych pytań. Czy według biegłego wiedzy Pegasus w tej customowej polskiej wersji, dostarczonej dla polskiego odbiorcy, miał możliwość wgrywania danych poza przestrzenią pamięci operacyjnej, modyfikacji np. SMS-ów, modyfikacji zdjęć w galerii, wgrywania zdjęć do galerii, modyfikacji treści maili, wysyłania wiadomości w celu… jak gdyby w miejsce autora? Ale głównie chodzi mi o modyfikacje treści.

Biegły Krzysztof Dyki:

Jak rozumiem, pytanie dotyczy możliwości operatora, czyli klienta, bo sam Pegasus… To pytanie ma dwa wymiary. Pierwszym wymiarem są techniczne możliwości Pegasusa. Na każde pytanie odpowiedź brzmi: tak, Pegasusa jako systemu NSO, tak.

Poseł Witold Zembaczyński (KO):

W tej, powiedzmy, najwyższej wersji dostępnej?

Biegły Krzysztof Dyki:

W każdej wersji.

Poseł Witold Zembaczyński (KO):

W każdej?

Biegły Krzysztof Dyki:

W każdej wersji Pegasus…

Poseł Witold Zembaczyński (KO):

To, proszę biegłego… Czyli, powiedzmy, ma możliwość wgrywania poza pamięcią operacyjną danych?

Biegły Krzysztof Dyki:

Tylko ważne rozróżnienie: Pegasus z perspektywy narzędzia. Abstrahujemy na razie od klienta, nie mówimy o kliencie. Narzędzie technologiczne, sposób, w jaki działa – tak, absolutnie tak. Ale teraz, jeżeli pytamy, czy klient miał taką możliwość, to w standardowej wersji Pegasusa, nabywanej standardowo, domyślnie nie było takiej funkcjonalności dla klienta. Ale Pegasus technologicznie dla jego producenta…

Poseł Witold Zembaczyński (KO):

Miał tę możliwość.

Biegły Krzysztof Dyki:

Oczywiście, że miał taką możliwość, czyli domyślnie standardowo nie udostępniał jej klientowi, Pegasus miał taką możliwość i co więcej…

Poseł Witold Zembaczyński (KO):

A zna może biegły przykłady klientów, którzy posiadali tę wersję, jakichś państw? Nie chodzi mi o nazwę, ale potrafi to umocować, że ktoś był nabywcą akurat tej wersji bądź tym się posłużył? Bo znamy przypadki zabójstwa dziennikarza, prawda, tam, gdzie korzystano z jego lokalizacji czy podsłuchiwano jego otoczenie, żeby ustalić pewne fakty. Natomiast czy tam dochodziło stricte do wgrywania danych poza przestrzenią pamięci operacyjnej, która była niezbędna, Pegasusowi, jeżeli się tutaj zgadzamy co do tego, żeby móc rozpocząć infekcję?

Biegły Krzysztof Dyki:

Tu bym chciał powtórzyć moją odpowiedź, że Pegasus sam technicznie miał taką możliwość. Nie mam wiedzy, informacji o klientach, którzy posiadali taką funkcjonalność. Słyszałem, że byli klienci, którzy żądali takiej funkcjonalności. Nie słyszałem o Polsce w tym gronie, nie, natomiast słyszałem, że byli klienci, którzy żądali takiej funkcjonalności, co wynikało z istnienia alternatywnych narzędzi posiadających standardowo taką funkcjonalność. Upraszczając…

Poseł Witold Zembaczyński (KO):

Konkurencyjnych narzędzi wobec Pegasusa?

Biegły Krzysztof Dyki:

Tak, istnieją konkurencyjne narzędzia, które standardowo… I niektórzy klienci – ale tu nie słyszałem o Polsce, absolutnie nie – niektórzy klienci pytali. Produkt X z kraju Y posiada coś takiego, natomiast nie wiem, nie mam informacji o tym, czy takie funkcjonalności były udostępniane, czy nie.

Poseł Witold Zembaczyński (KO):

A czy moglibyśmy się skupić na konkretnym kazusie? Mamy tę słynną wiadomość z telefonu Krzysztofa Brejzy i w jego telefonie ona wygląda inaczej, a inaczej wyglądała na ekranie TVP w tamtym czasie. Czy jako biegły jest pan w stanie mniej więcej przybliżyć moment, w którym dochodzi do tej modyfikacji?

Biegły Krzysztof Dyki:

Jako biegły musiałbym w pierwszej kolejności ustalić, czy mam kontrolę nad tym, co pozyskuję, czyli jeżeli jestem operatorem, to czy jestem pewien, skąd ja to pozyskuję, czyli jaki jest zakres infrastruktury, nad którą ja mam kontrolę. Tam, gdzie on się kończy, tam się kończy moja wiedza i wszystko jest możliwe, czyli nie można wykluczyć, bo, jak rozumiem, pytanie dotyczy niezgodności materiału posiadanego przez osobę inwigilowaną z materiałem opublikowanym w mediach.

Poseł Witold Zembaczyński (KO):

Tak, dokładnie o to chodzi. Jest rozbieżność. Ta wiadomość w mediach jest jak gdyby przedstawiana jako spod palca właściciela telefonu, a de facto była do niego wysyłana, a nie on ją wysyłał. Na przykład taka różnica, prawda?

Biegły Krzysztof Dyki:

To jest pytanie o to, czy klient nabył oprogramowanie w modelu gwarantującym integralność i autentyczność danych, bo…

Poseł Witold Zembaczyński (KO):

Procesowo jaką to ma wartość?

Biegły Krzysztof Dyki:

Taką, jaką… wprost proporcjonalną do zakresu wiedzy i kontroli klienta nad systemem, czyli wracamy do sieci anonimizującej. Jeżeli mamy kontrolę nad całą infrastrukturą, to ma to bardzo dużą wartość. Jeżeli zbadaliśmy bezpieczeństwo, wiemy, jak zweryfikować materiał, wiemy, jak ustalić, czy on rzeczywiście pochodzi z mojego smartfonu, ale jeżeli nie wiemy, skąd on dokładnie pochodzi, czy on w ogóle pochodzi ze smartfonu, to trudno mówić w tym aspekcie o walorze procesowym czy trudno odpowiedzieć na pytanie, który materiał jest prawdziwy. Wiemy tak dużo, jak wiemy o samym systemie. Trochę wracamy do pierwszych państwa pytań. Ten początek chronologiczny był słuszny, czyli jaki jest zakres wiedzy klienta o posiadanym systemie, bo możliwość odpowiedzi na pana pytanie kończy się tam, gdzie kończy się wiedza klienta o systemie.

Poseł Witold Zembaczyński (KO):

Czyli wiedza CBA o systemie, tak żeby to sprecyzować.

Biegły Krzysztof Dyki:

Tak.

Poseł Witold Zembaczyński (KO):

Czyli nawet dzisiaj, z perspektywy dnia dzisiejszego, czy jest możliwe uzyskanie tych odpowiedzi, mając to urządzenie końcowe i mając zabezpieczone konsolety Pegasusa przez prokuraturę?

Biegły Krzysztof Dyki:

Tak, jeżeli jest umowa, jeżeli jest dokumentacja techniczna ukazująca architekturę systemu, kto nad czym ma kontrolę, za jaką część kto odpowiada, to tak. Oczywiście osoby, które to obsługiwały, one mają tę wiedzę, jaki zakres infrastruktury kontrolowały. Operator wie, czy… Proste pytanie do operatora: W jaki sposób mogę zweryfikować materiał pobrany z urządzenia osoby inwigilowanej? Innymi słowy, w jaki sposób możemy udowodnić, że ten materiał z pana smartfonu jest, po pierwsze, materiałem z pana smartfonu…

Poseł Witold Zembaczyński (KO):

Pan to jako biegły ocenia w swojej pracy na przykład, tak?

Biegły Krzysztof Dyki:

Jeżeli były takie zagadnienia, tak. Jeżeli były problematyki procesowe, czasami oczywiście, w operowaniu w różnych sprawach, gdzie są materiały wykorzystywane z kontroli operacyjnej, czasami dochodzi do problematyki procesowej, do polemiki, w której trzeba rozstrzygnąć, czy dany materiał pochodził, czy nie pochodził z urządzenia ofiary. To po pierwsze. To jest ważne, czy pochodził, skąd on pochodził. Dopiero w drugim kroku – czy on jest oryginalny. Pana pytanie dotyczy tych dwóch zagadnień dla mnie. Przypominają mi się właśnie sprawy sądowe, w których należało rozstrzygnąć, czy on pochodzi z tego miejsca i skąd wiemy, czy on pochodzi z tego smartfonu osoby inwigilowanej. Stąd, jaką mamy pewność o tym, co kontrolujemy. Jeżeli kontrolujemy całą infrastrukturę i wiemy, jak to działa, to…

Poseł Witold Zembaczyński (KO):

Mamy pewność.

Biegły Krzysztof Dyki:

… mamy tę pewność, potrafimy to udowodnić.

Poseł Witold Zembaczyński (KO):

Rozumiem. Proszę powiedzieć, kończąc odpowiedź na to pytanie. W sytuacji hipotetycznej, kiedy CBA posiada te uprawnienia w postaci konsolety, oprogramowania, serwera tego finalnego, na którym to zbierają, z którego zgrywają na płytę… ale jednak szyfrowanie odbywa się gdzieś tam, NSO coś musi zrobić, żeby to zapewnić, żeby jak gdyby od urządzenia nie dotrzeć do operatora, to wtedy ta kontrola nie jest zapewniona. Jaki jest walor dowodowy takich dowodów z tego Pegasusa, który kupiło CBA? Proszę powiedzieć. W polskim porządku prawnym… pan jako biegły sądowy jest w tym świetnie zorientowany. Jakie są walory dowodowe właśnie tak pozyskanych materiałów, przedstawionych w formie aktu oskarżenia, wycinka pracy operacyjnej służb, kiedy jest tak wiele pytań dla sądu? Czy sąd w ogóle kiedykolwiek jest w stanie się dowiedzieć, czy ta infrastruktura jest na wyłączność operatora, czy na przykład poszczególne serwery pośredniczące-uczestniczące w szyfrowaniu przesyłu danych, co już ustaliliśmy, są zewnętrzną infrastrukturą bądź jeszcze – najgorzej, jeżeli tak jest – pośredniczy w tym NSO, bo do końca nie wiemy z uwagi na brak znajomości kodu źródłowego? Jaki to ma walor dowodowy w polskim postępowaniu karnym?

Biegły Krzysztof Dyki:

Jedna drobna uwaga. Nie trzeba znać kodu źródłowego, żeby ocenić, kto nad czym ma kontrolę. Kod źródłowy jest zupełnie niepotrzebny.

Poseł Witold Zembaczyński (KO):

OK. To jeszcze pana dopytam o ten kod za chwilę.

Biegły Krzysztof Dyki:

Dobrze. Jaką to ma wartość? To jest pytanie na pewno do radcy prawnego. Rzeczywiście z tytułu posiadanych uprawnień to ja odpowiem technicznie. Dla mnie technicznie dowód o walorze procesowym jest wtedy dowodem, gdy oczywiście jest legalny, to po pierwsze…

Poseł Witold Zembaczyński (KO):

Tu jest fundamentalne pytanie, czy był legalny z Pegasusa.

Biegły Krzysztof Dyki:

…jest autentyczny, po drugie, i po trzecie, jest weryfikowalny. Więc z perspektywy biegłego sądowego legalność, weryfikowalność, autentyczność, ale…

Poseł Witold Zembaczyński (KO):

Czy Pegasus to dawał? Czy Pegasus w polskim procesie karnym to dawał, te trzy kryteria?

Biegły Krzysztof Dyki:

Pegasus mógł to dawać, jeżeli kontrolowaliśmy te trzy aspekty. Jeżeli jesteśmy w stanie jako… Jeżeli klient Pegasusa, ten, który to nabył, był w stanie udowodnić, że to było weryfikowalne i autentyczne, to tak. I to zależy ciągle od tego, nad czym miał kontrolę. Jeżeli miał kontrolę nad całą infrastrukturą Pegasusa, to tak, i przeprowadzono testy, to jak najbardziej tak. Jeżeli nie, to nie.

Poseł Witold Zembaczyński (KO):

Jeżeli nie, to nie. Bardzo dziękuję. Reszta pytań w drugiej turze.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję.

Teraz pan przewodniczący Marcin Bosacki, bardzo proszę.

Poseł Marcin Bosacki (KO):

Dziękuję bardzo, pani przewodnicząca.

Wysoka Komisjo, szanowny panie biegły, ja zacznę od takich podstawowych rzeczy, żeby ustalić pana stan wiedzy. W przestrzeni medialnej pojawiły się informacje na temat tego, że pan badał kod źródłowy Pegasusa. Czy to prawda?

Biegły Krzysztof Dyki:

Kod źródłowy? Nie. To jest błąd, omyłka pisarska skorygowana przez wydawnictwo w wersji elektronicznej, w wersji papierowej omyłka pisarska. Nie było to autoryzowane przeze mnie, więc stąd omyłka. W wersji elektronicznej ten sam wywiad jest już ze słowem „kod", nie „źródłowy".

Poseł Marcin Bosacki (KO):

OK. Czy według pana wiedzy odbiorca systemu Pegasus w Polsce, czyli służba specjalna CBA, miał dostęp do tego kodu źródłowego, czy nie?

Biegły Krzysztof Dyki:

Nie mam wiedzy na ten temat. Jeżeli poprosiło, mogło próbować uzyskać, jeżeli nie poprosiło, na pewno nie uzyskało.

Poseł Marcin Bosacki (KO):

Czy pan ma wiedzę na temat tego, jakie funkcjonalności polski operator Pegasusa uzyskał? Powiedział pan, że nie widział pan umowy. Natomiast czy ma pan wiedzę, co polski operator Pegasusa mógł, a czego nie mógł?

Biegły Krzysztof Dyki:

Nie mam takiej wiedzy.

Poseł Marcin Bosacki (KO):

W takim razie będę pana pytał o możliwości Pegasusa jako takiego, bo skoro nie wiemy, jaką wersję i na jakich zasadach uzyskało w 2017 r. CBA, to będziemy opierali się na pana wiedzy o całym tym systemie.

Bardzo często poruszaną kwestią – także prawnie, także w sprawach sądowych znanych już opinii publicznej – jest to, czy system Pegasus instalowany w urządzeniu końcowym, czyli na smartfonie albo tablecie, może mieć wgląd do danych, wiadomości, filmów, zdjęć, maili, informacji szyfrowych itd. przed datą zarządzenia przez sąd czynności operacyjnych.

Biegły Krzysztof Dyki:

Tak.

Poseł Marcin Bosacki (KO):

A jak… Jeśli chodzi o czas prowadzenia kontroli operacyjnej, na którą zgodę wyraził sąd, co wówczas… Czy Pegasus w praktyce funkcjonowania służb, którą pan bardzo dobrze zna, jest odinstalowywany automatycznie? W jaki sposób to przebiega? Czy on dalej może zbierać dane?

Biegły Krzysztof Dyki:

Te parametry definiuje operator w chwili zlecania w swojej stacji operatorskiej infekcji, takie parametry, jakie zdefiniuje operator, ta osoba, która obsługuje, dany agent, funkcjonariusz. W takich parametrach będzie działało to oprogramowanie na urządzeniu osoby inwigilowanej. Również dotyczy to dat.

Poseł Marcin Bosacki (KO):

Myśmy zadawali to pytanie prof. Kosińskiemu. On odpowiedział na nie bardzo zdecydowanie, że raz zainfekowany Pegasusem smartfon praktycznie jest we władaniu operatora Pegasusa. Ja trochę odwrócę to pytanie i zadam panu pytanie: Czy operator Pegasusa, który zainfekował telefon czy tablet, ma jakiekolwiek ograniczenia, tzn. czy on czegoś nie może zrobić z tym telefonem?

Biegły Krzysztof Dyki:

W standardowej konfiguracji nie może wysyłać plików do osoby zainfekowanej – w standardowej konfiguracji – natomiast w standardowej konfiguracji może przeszukiwać zasoby, smartfon. W zależności od exploita, o którym tu… Jestem mile zaskoczony, że państwo macie aż taką wiedzę o tych aspektach technologicznych. W zależności od danego exploita, który jest wykorzystywany w danym ataku – a to się bardzo zmienia również w czasie – może uzyskać pełną kontrolę nad smartfonem… do wszystkich danych, czasami ograniczoną do uprawnień danej aplikacji, czyli, upraszczając, najczęściej to wygląda tak, że infekcja może nastąpić wobec jednej aplikacji. Teraz w zależności od tego, jak państwo… jakie macie smartfony, systemy, konfiguracje, różnie to będzie wyglądać. W niektórych smartfonach infekcja aplikacji jednej pozwoli na uzyskanie wszystkich… dostępu do wszystkich państwa danych, a w niektórych smartfonach, jak mój, niestety nie, umożliwi uzyskanie aplikacji tylko do danej… dostępu do danych tylko danej aplikacji.

Poseł Marcin Bosacki (KO):

Może nie „niestety”. Może na szczęście.

Biegły Krzysztof Dyki:

Tak. Więc to zależy od exploita, dokładnie exploita wykorzystywanego przez Pegasusa. Operator nie miał wpływu standardowo na exploity. Operator wydawał polecenie. Wpływ na exploity miało głównie NSO. Czasami jest tak, że jeżeli jest coś, czego dany system nie ma, to się dzwoni, dosłownie dzwoni do NSO, że jest jakiś problem, i NSO potrafi dosłać, dostarczyć w jakiś sposób, różnie to bywa, aktualizację, która już obsługuje jakiś smartfon, i w zależności od tego exploita uzyskuje się uprawnienia do aplikacji lub do całego smartfonu. Przegląda się po prostu pliki.

Poseł Marcin Bosacki (KO):

Jeśli chodzi o umieszczanie danych w telefonie osoby zaatakowanej, to rozumiem, że pana odpowiedź jest taka: generalnie system ma takie możliwości, ale to, czy miał używane w Polsce, to zależy od tego, jaką wersję kupiono.

Biegły Krzysztof Dyki:

Tak. W standardowej nie miał tej opcji.

Poseł Marcin Bosacki (KO):

OK. Czy według pana wiedzy producent urządzenia, czyli NSO Group, przewiduje ograniczenia co do ilości urządzeń, na których może być stosowany Pegasus w tym samym czasie?

Biegły Krzysztof Dyki:

Rozumiem, że chodzi o perspektywę uprawnień dla klienta. Tak. NSO różnie licencjonuje i najczęściej występują w politykach licencyjnych NSO dwie kategorie uprawnień. Jedna kategoria to jest liczba infekcji niezależna od osób, numeru smartfonów. A druga kategoria? Liczba numerów smartfonów – nie wiem, jak Polska zakupiła – najczęściej spotykana kategoria. Liczba infekcji niezależna od numeru smartfonów, a druga kategoria – liczba numerów smartfonów.

Poseł Marcin Bosacki (KO):

Czyli jeśli… Ja w tej chwili przedstawiam wiedzę nie z jakichkolwiek źródeł niejawnych, tylko taką, która była przedstawiana przez media. Czyli jeśli dokupywano kolejne pakiety możliwości infekowania Pegasusem, to to mogło wynikać też z tego, że niektóre osoby infekowano tym Pegasusem wielokrotnie, tak…

Biegły Krzysztof Dyki:

Raczej miałem na myśli…

Poseł Marcin Bosacki (KO):

…i zużyto pierwotnie przyznaną liczbę infekcji?

Biegły Krzysztof Dyki:

Tak też mogło być. W swojej wypowiedzi miałem na myśli raczej sytuację, w której ze względów technicznych potrzebna jest jakaś aktualizacja. Nie płacimy wtedy za taką aktualizację. Jeżeli mamy wykupione uprawnienia, nie zużyliśmy jeszcze ich, podnosimy telefon, mówimy: drodzy przyjaciele, mam pacjenta, który ma niekompatybilne urządzenie, potrzebuję wsparcia. Wtedy NSO sprawdza. OK. Czy mamy aktualne uprawnienia? Jeżeli mamy aktualne uprawnienia, w ramach już upłaconych środków finansowych bezpłatnie dostarcza, potrafi dostarczyć aktualizację nie nowych uprawnień, nie nowych uprawnień licencyjnych, tylko kompatybilności z nowym smartfonem. Kompatybilności. Tak to działa, że… I to jest w ramach posiadanych uprawnień licencyjnych. Nie płaci się za to, ale oczywiście jeżeli klient wcześniej wyczerpie uprawnienia, to jak najbardziej może dokupić dodatkowe uprawnienia.

Poseł Marcin Bosacki (KO):

Z czego wynika to, że wiemy już – mam nadzieję, że to też potwierdzimy podczas prac naszej Komisji – że niektóre z ofiar Pegasusa w Polsce, nawet wziąwszy pod uwagę rodzinę i środowisko państwa Brejzów… Wiemy, że niektórzy z nich, na przykład pani posłanka Łośko albo pan Brejza senior, były prezydent, ówczesny prezydent Inowrocławia, musieli kliknąć w fałszywie podesłane linki do konkretnych firm, których byli klientami, na przykład do systemu obsługującego autostrady albo do sklepu z zabawkami dla dzieci pani Łośko, a w wypadku innych osób na razie przynajmniej taka jest wiedza, że sam pan Krzysztof Brejza był infekowany bez tego systemu, który wymaga kliknięcia na to. Z czego wynika ta różnica?

Biegły Krzysztof Dyki:

To ciekawe pytanie, bo ono dotyczy mojej wcześniejszej odpowiedzi, pewnie nieświadomie. Wynika właśnie z kategorii exploitów. NSO… Pegasus nie jest urządzeniem, które potrafi wszystkie nasze urządzenia zainfekować bez interakcji z nami. Potrafi w wybranych okresach czasu zainfekować wybrane modele smartfonów – nie chciałbym mówić absolutnie jakich – bez interakcji z użytkownikiem, ale są wybrane modele smartfonów, które wymagają interakcji z użytkownikiem. Więc jeżeli zaszła taka sytuacja, o którą pyta pan przewodniczący, to w tamtym okresie czasu Pegasus wobec urządzenia jed-

nej osoby miał możliwość infekcji bez żadnej interakcji z tą osobą, a wobec urządzenia drugiej osoby wymagał kliknięcia. Standardowa sytuacja na rynku tej klasy rozwiązań, nie tylko Pegasusa, co zależy od tych exploitów w danym czasie.

Poseł Marcin Bosacki (KO):

Na koniec tej pierwszej rundy z mojej strony pytanie będące kontynuacją pytań kolegów, jeśli chodzi o akredytację systemu Pegasus. Z tego, co wiemy, jej nie było. Tymczasem jasno mówi ustawa z 2010 r. o ochronie informacji niejawnych, że „ABW albo SKW" – ja w tej chwili cytuję – „udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji o klauzuli «poufne» lub wyższej". Wiemy, że ten system nie tylko przetwarzał, ale tworzył informacje niejawne o klauzuli „tajne" i „ściśle tajne", nie mówiąc o „poufne". Z czego mogło wynikać według pana wiedzy… Ja nie chcę, żeby pan spekulował, tylko zrekapitulował swoje doświadczenia wieloletnie z tego, nazwijmy to, rynku. Z czego mogło wynikać to, że wbrew tej jasnej ustawowej normie tej akredytacji nie było?

Biegły Krzysztof Dyki:

Nie miałem tej wiedzy, że jej nie było. Być może z architektury samego systemu, czyli być może z niepełnej kontroli nad nim. To jedyne, co mi przychodzi do głowy, bo jeżeli mamy komplet systemu, nad którym mamy kontrolę, i ja jestem odpowiedzialny za ten obszar, to dokonuję tych czynności. Być może niepełna kontrola nad systemem? To jedyne, co mi przychodzi do głowy. Bo chyba nic innego, zakładając to, o czym pan przewodniczący mówi, że te dane miały określoną klauzulę. Oczywiście jeszcze można rozważyć czysto hipotetycznie i teoretycznie, że dane pozyskiwane za pomocą tego systemu… Dopiero później nadawano im w innym systemie klauzulę, ale to już jest daleko idąca teoria, ale ona teoretycznie mogłaby tłumaczyć, że być może gestor tego systemu, klient wychodził z założenia, że w chwili, gdy operator uzyskuje te dane, to one jeszcze na przykład nie są klauzulowane i wtedy to nie podlega akredytacji, a dopiero po przeniesieniu na inną maszynę to jest klauzulowane.

Poseł Marcin Bosacki (KO):

To raczej mało możliwe. Natomiast zapytam pana… i to jest już moje ostatnie pytanie. Jeśli część tego systemu była poza kontrolą polskich służb i z tego powodu nie udzielono akredytacji, to czy takiego systemu należy używać do pozyskiwania informacji, które mają klauzule „poufne", „tajne" i „ściśle tajne"?

Biegły Krzysztof Dyki:

To jest pytanie, wydaje mi się, bardziej dla radcy prawnego, ale ja odpowiem technicznie. Ze względów technicznych, abstrahując od wątku prawnego, bo tu by była potrzebna ocena eksperta z zakresu prawa, ze względów technicznych mnie by interesowały po prostu testy bezpieczeństwa. Czyli abstrahując od akredytacji, mnie, gdybym ja odpowiadał za tę transakcję, interesują testy bezpieczeństwa, które by technicznie skonsumowały akredytację nie prawnie, ale technicznie skonsumowałyby akredytację i mogłyby być nawet szersze niż sama akredytacja. Czyli z mojej perspektywy jako osoby technicznej ważne są testy bezpieczeństwa, ich wykonanie. A czy to było legalne? Tu już niestety poproszę o wyrozumiałość w zakresie braku moich kompetencji co do oceny wątków prawnych.

Poseł Marcin Bosacki (KO):

Na razie dziękuję.

Biegły Krzysztof Dyki:

Dziękuję bardzo.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję.

Pan poseł Patryk Jaskulski teraz. Poproszę.

Poseł Patryk Jaskulski (KO):

Bardzo dziękuję, pani przewodnicząca.

Wysoka Komisjo, panie biegły, pozwolą państwo, że zacznę od cytatu: „Pegasus jest tak drogi, ponieważ pozwala władzom zrobić to, czego od dawna nie mogły: zdalnie włamać się do smartfonów, dzięki czemu wszystko, co się w nich znajduje, jest całkowicie widoczne". To powiedział jeden z założycieli grupy NSO.

Przypomnijmy. Polscy podatnicy zapłacili za Pegasusa 25 mln zł. W przeliczeniu po aktualnym kursie jest to ok. 6 mln dolarów. Jeżeli odejmiemy od tej sumy jeszcze tę sumę prowizji 8 mln, 6–8 mln prowizji, to zastanawiam się, czy ten Pegasus, który my kupiliśmy, faktycznie był tak drogi, skoro jest to cena trzech, czterech autobusów elektrycznych.

Padło też stwierdzenie, które pan potwierdził, że można traktować Pegasusa jako cyberbroń. Doskonale wiemy, ile najnowocześniejsza broń kosztuje. Czołg typu Abrams to jest koszt rzędu 12 mln dolarów. I też jeszcze, jeżeli nałożymy na to fakt, że jeden zero-day, który jest potrzebny do przełamania luk systemowych, czyli wejścia do danego smartfona, kosztować potrafi na rynku – czarnym rynku – nawet kilka milionów dolarów, to czy ta cena, którą my zapłaciliśmy, 17 mln zł, to była duża cena, wysoka cena? Jak pan to oceni?

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Ja przepraszam. Tylko zanim jeszcze pan odpowie, chciałabym, żebyśmy nie wprowadzali w błąd opinii publicznej. 20… 33 mln to są te faktury, którymi mieliśmy możliwość… z którymi mieliśmy możliwość zapoznać się po raporcie Najwyższej Izby Kontroli, czyli 25, sam system, plus 8, prowizja, tak że tak to mniej więcej wyglądało.

Poseł Patryk Jaskulski (KO):

Przepraszam bardzo, ale OK. Niezmiennie uważam, że jest to kwota, która faktycznie odbiega trochę od cen chociażby najnowocześniejszego sprzętu dla armii.

Biegły Krzysztof Dyki:

To jest bardzo szerokie pytanie, bardzo profesjonalne, ponieważ ono dotyka tych znamion cyberbroni, o których mówiliśmy, natomiast ono dotyka też trochę geopolityki. Zaznaczyłem, że ono ma znamiona cyberbroni, ale to nie jest cyberbroń. Gdyby to była cyberbroń, to zgadzam się, że cena byłaby znacznie, znacznie wyższa, gdyby to była cyberbroń dla wojska, natomiast to jest narzędzie – tak jak powiedziałem na początku, podtrzymuję – dedykowane dla służb specjalnych, nie dla wojska. Nie jest mi wiadoma informacja o posiadaniu tego narzędzia przez jakiekolwiek wojsko, co, nawiasem mówiąc, jest wątkiem na odrębne dyskusje.

Więc cena Pegasusa… Ją w mojej ocenie jako biegłego powinniśmy oceniać przez dwa pryzmaty. Pierwszy pryzmat to jest wartość samego Pegasusa. Rzeczywiście tło pana pytania jest prawidłowe. Wartości exploitów, które pan podał, są również prawidłowe. Kilka milionów złotych potrafi kosztować jeden exploit, który może być… który może działać kilka dni albo kilka miesięcy – maksymalnie pewnie kilka miesięcy – więc koszt produkcji takiego oprogramowania jak Pegasus jest ogromny. O czym mało kto wie, sama firma NSO jeszcze przed wybuchem afery Pegasusa, czyli w swoim szczycie chwały i swojego biznesu, miała pół miliarda dolarów długu. To pokazuje, jak gigantyczne koszty są związane z wytworzeniem tej klasy oprogramowania i funkcjonowaniem na takim rynku.

Więc koszt Pegasusa w tym pierwszym pryzmacie, oceniany przez sam ten produkt i innych jego klientów może wydawać się, wręcz możemy uznać, że rzeczywiście jest niski. Jest niski. I teraz można się zastanawiać, czy mamy takich negocjatorów w kraju, którzy potrafią negocjować takie dobre ceny.

Ja powiem inaczej. Dodam drugi pryzmat. Są jeszcze inne produkty na rynku, to prawda, że gorsze, ale jednak robiące bardzo podobne rzeczy, bardzo podobne, gorsze, ale porównywalne. One kosztują taniej niż Pegasus, więc co do wartości Pegasusa na tle innych klientów to jest to bardzo dobra cena i jest to… nie chcę powiedzieć niska, powiedziałbym biznesowo atrakcyjna cena. Polska zakupiła to w mojej ocenie w atrakcyjnej kwocie. Abstrahuję już od wątków… Jeżeli weźmiemy pośrednika, to jest to bardzo atrakcyjna wręcz kwota. Jeżeli odejmiemy koszt pośrednika, to ja uznaję ten zakup za kwotę bardzo atrakcyjną, ale z drugiej strony pamiętajmy, że trzeba spojrzeć na szer-

sze spektrum, na tło rynkowe. Pegasus jest najdroższym narzędziem, więc ta cena, w której kupiono Pegasusa, jest porównywalna z najdroższymi ofertami innych narzędzi. Tak bym to ujął.

Poseł Patryk Jaskulski (KO):

Powiedział pan, że widział pan umowy z innych krajów. Czy zna pan ceny transakcji innych krajów, które kupiły Pegasusa? Jak to wygląda na tle właśnie naszego kraju?

Biegły Krzysztof Dyki:

Te umowy… Dzisiaj nie pamiętam z głowy wszystkich krajów, ale były chyba rzeczywiście… wszystkie były wyższe kwoty, a niektóre kilkukrotnie wyższe. Tylko pamiętajmy, trzeba porównywać jabłka z jabłkami. Trzeba porównać uprawnienia licencyjne, bo łatwo mówić o kwotach. Znam klientów, którzy zapłacili pięciokrotnie więcej niż Polska, ale uzyskali większe uprawnienia, więc kwota będzie pięciokrotnie wyższa, nawet sześciokrotnie, jeszcze więcej. Znam klientów, którzy jeszcze więcej zapłacili.

Poseł Witold Zembaczyński (KO):

Zależy od licencji.

Biegły Krzysztof Dyki:

Właśnie, zależy od licencji, więc trzeba by porównać – nigdy tego nie robiłem – licencje i zobaczyć te wartości. Natomiast zakup Polski? Bezsprzecznie cena była w mojej ocenie atrakcyjna.

Poseł Patryk Jaskulski (KO):

Czy dobrze rozumiem, że cena uzależniona była też od ilości osób, które mogliśmy inwigilować, czyli tych licencji?

Biegły Krzysztof Dyki:

Przede wszystkim. Tak.

Poseł Patryk Jaskulski (KO):

Dobrze. Panie biegły, NSO Group jest firmą prywatną, ale, tak jak to też już chyba dzisiaj tutaj padło, część pracowników tej firmy wywodzi się bezpośrednio ze służb specjalnych Izraela. I wiemy – albo proszę mnie wyprowadzić z błędu – że Izrael kontrolował, musiał wyrazić zgodę, żeby sprzedać to oprogramowanie danemu krajowi.

Biegły Krzysztof Dyki:

Tak.

Poseł Patryk Jaskulski (KO):

Czy, biorąc pod uwagę też tę atrakcyjną cenę, mogło to być w interesie Izraela, żeby sprzedać nam to oprogramowanie nie dlatego, żeby firma zyskała finansowo, ale żeby właśnie przez na przykład tę sieć animizującą pozyskiwać część danych wywiadowczych?

Biegły Krzysztof Dyki:

To jest daleko idące pytanie, na które chciałbym móc odpowiedzieć nieco inaczej. Nie jestem w stanie na tak postawione pytanie odpowiedzieć, natomiast rzeczywiście nie jest tajemnicą, jest to faktem wiadomym w wielu kręgach, że Pegasus był traktowany – był, bo już nie jest – traktowany przez rząd Izraela jako narzędzie wspierające ich działania geopolityczne, politykę zagraniczną. Czyli w niektórych krajach na najwyższych poziomach władzy zgoda na sprzedaż Pegasusa rzeczywiście była tzw. dealbreakerem, na najwyższych poziomach władzy pomiędzy Izraelem a danym krajem. Jest to prawda, że to było to, tak jak pan powiedział, narzędzie prywatnej firmy, tak, ale ono nie miało rangi normalnego narzędzia, jakich jest bardzo wiele. Jest wiele fantastycznych technologii w Izraelu, ale one są zwykłymi technologiami rynkowymi. Pegasus nigdy takim czymś nie był. On był narzędziem geopolitycznym w polityce Izraela, przy czym ja to rozumiem, popieram, tak samo bym robił na miejscu premiera Izraela, tak samo bym się zachowywał. Uznałbym to narzędzie i tę firmę za kartę do gry w mojej geopolityce. I ono było wykorzystywane, ale w grze geopolitycznej.

Natomiast czy Izrael mógł sięgać do tych danych technicznie, tylko i wyłącznie technicznie? Oczywiście mógł, ale nie mam takich informacji ani wiedzy o tym, żeby to robił.

Poseł Patryk Jaskulski (KO):

W jednym z wywiadów powiedział pan o tych problemach finansowych, dzisiaj pan to potwierdził… problemów finansowych grupy NSO, firmy NSO. Ten dług, ta strata wynosi, pan powiedział, pół miliarda dolarów. Czy ten fakt może wpływać i mieć wpływ na bezpieczeństwo korzystania z systemu Pegasus?

Biegły Krzysztof Dyki:

Ten fakt ma wpływ bardziej, bym powiedział, na wiarygodność tej firmy, ponieważ w chwili, w której mamy tak potężne problemy finansowe, szuka się inwestorów i ta presja rośnie wraz z upływającym czasem, ponieważ koszt obsługi długu rośnie. W pewnym momencie dochodzi się do sytuacji, w której koszt obsługi długu jest tak wysoki, że bieżące wpływy z licencji nie są w stanie pokryć nie tylko kosztów kredytu/długu, ale nie są nawet w stanie, mogą nie być w stanie pokryć kosztów obsługi tego długu.

W tym znaczeniu z mojej perspektywy należałoby uznać, że rzeczywiście firma NSO powinna być bacznie obserwowana jako dostawca takich technologii. Ale pamiętając o tym, o czym powiedziałem wcześniej, że NSO jest traktowane jako narzędzie… było traktowane jako narzędzie geopolityczne w rękach rządu Izraela, jednak to mnie by uspokajało. Wiedziałbym, że Izrael nie pozwoli – i nie pozwolił – upaść NSO. To by mnie uspokajało. Natomiast gdyby to nie była firma… co do stabilności tej firmy… Natomiast gdyby to nie była firma ważna strategicznie dla rządu Izraela, wtedy tak, to byłoby poważne zagrożenie chociażby w naszej procedurze uzyskiwania poświadczenia bezpieczeństwa, czy osobowego, czy przemysłowego, krajowego. Jest to jeden z fundamentalnych czynników oceny wiarygodności i bezpieczeństwa osoby bądź firmy, której udziela się takiego poświadczenia.

Poseł Patryk Jaskulski (KO):

Powiedział pan o tym dzisiaj, że Departament Handlu USA wciągnął NSO na czarną listę, zakazując sprzedawania tej firmie amerykańskiej technologii. Jeżeli tak, to może pan powtórzyć to, przytoczyć dlaczego? Czy to można wiązać właśnie z faktem tego długu, tej straty, którą wygenerowała ta firma i…

Biegły Krzysztof Dyki:

Nie…

Poseł Patryk Jaskulski (KO):

…newralgicznych danych, które może posiadać?

Biegły Krzysztof Dyki:

Nie, nie chodziło o stratę. Są dwa wątki, jeżeli chodzi o Stany Zjednoczone. Pomijając pozew wytoczony przez firmę Meta, Apple i inne firmy, to dwa główne wątki. Jeden to jest to, o co pan pyta, czyli to zablokowanie możliwości sprzedaży amerykańskich technologii firmie NSO.

Jest jeszcze drugi wątek: dekret prezydenta Bidena z marca 2023 r. zakazujący kupna i stosowania takiego oprogramowania jak Pegasus, niewskazujący w treści dekretu go wprost, ale wiadomo, że chodzi o to oprogramowanie i inne z zagranicy. Czyli prezydent Biden zabronił w marcu 2023 r. kupna oprogramowania tej klasy od zagranicznych firm, które, cytuję, może stwarzać zagrożenie dla bezpieczeństwa państwa. Z przyczyn chociażby, o których rozmawiamy, uznano tam, że może stwarzać, więc nie ma możliwości.

Wątek finansowy nie miał znaczenia przy… Wątek długów nie miał znaczenia. Paradoksalnie jeden z pierwszych inwestorów, którego szukali i znaleźli, to był w Stanach Zjednoczonych, który później się wycofał.

Jeżeli chodzi o tę blokadę możliwości zakupu amerykańskich technologii, oprogramowania, urządzeń przez firmę NSO, ona była związana raczej z wynikiem trochę prac podobnych, które państwo prowadzicie, do zbadania, czym jest to oprogramowanie, jak ono działa i czy… Nie że… Nie chodziło o to, że ono istnieje. Nie chodziło o to, że ono jest nabywane. Fakt potrzeby istnienia takiego narzędzia nie jest kwestionowany w Stanach

Zjednoczonych. Fakt potrzeby posiadania takiego narzędzia nie jest również kwestionowany. Co zakwestionowano i legło u podstaw tego, o co pan mnie pyta, to był sposób sprzedaży, po pierwsze, tego oprogramowania i po drugie, sposób wykorzystania przez klientów tego oprogramowania. To legło u podstaw decyzji Stanów Zjednoczonych.

Poseł Patryk Jaskulski (KO):

Czyli de facto Stany Zjednoczone w swojej decyzji kierowały się bezpieczeństwem swojego kraju. Można tak to określić?

Biegły Krzysztof Dyki:

I wartościami demokratycznymi, ochroną praw człowieka. Tak, te podstawy legły: bezpieczeństwo kraju, wartości demokratyczne, ochrona praw człowieka.

Poseł Patryk Jaskulski (KO):

I do tego zmierzam, panie biegły. Pegasus to narzędzie crackerskie, a więc przełamujące kod oprogramowania, a nie zabezpieczeń sieci. Moje pytanie jest następujące: Czy w Polsce znajdują się eksperci znający się na crackingu na tyle, żeby posiadać wiedzę i umiejętności, żebyśmy my sami na własny użytek potrafili wytworzyć podobne narzędzie?

Biegły Krzysztof Dyki:

Oczywiście tak, szanowni państwo, o czym często zapominamy w naszym kraju. Są różne rankingi, ale jeżeli weźmiemy… Ostatnio wróciłem wprost z delegacji zagranicznej specjalnie na tę Komisję i jutro ponownie wyjeżdżam. Jakież zaskoczenie było w bardzo bogatym kraju, w którym pokazywałem rankingi Polski, abstrahując zupełnie od tego wątku. To nie był ten wątek, ale pokazałem slajd, w którym wyświetliłem, dlaczego my, dlaczego uważam, że powinni z nami współpracować, bardzo bogaty kraj. Według rankingu, który wskazałem, źródła, w programowaniu jesteśmy drudzy na świecie, w cyberbezpieczeństwie – trzeci na świecie. To jest odpowiedź na pana pytanie i to są rankingi, które można zweryfikować, to nie jest moja opinia. W *cyber defense*, czyli w takiej cyberobronie trochę o znamionach wojny – pozycja szósta na świecie. W naszym kraju często zapominamy, kim my jesteśmy, jaki potencjał mamy, więc tak. O tym świadczą niezależne rankingi, również nasze cyberwojsko, bardzo wysoka pozycja naszego cyberwojska, ogromna praca, ogromny sukces. To się nie bierze znikąd, więc jak najbardziej tak.

Poseł Patryk Jaskulski (KO):

Czyli rozumiem, że zakupując system Pegasus od obcej firmy obcego państwa, mając jednocześnie tak bogaty zasób ludzki, de facto naraziliśmy bezpieczeństwo naszego kraju.

Biegły Krzysztof Dyki:

Tego nie chciałbym powiedzieć. Powiedziałbym, że nie wykorzystujemy potencjału tkwiącego od lat w naszym kraju. To nie dotyczy okresu ówczesnego szefostwa biura czy ówczesnego rządu. To jest zarzut szerszy, mentalnościowy, ale aktualny, że nie wykorzystujemy potencjału tkwiącego w naszym kraju, tak.

Poseł Patryk Jaskulski (KO):

Dziękuję.

Biegły Krzysztof Dyki:

Dziękuję.

Poseł Patryk Jaskulski (KO):

Na ten moment tyle.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo dziękuję.

Pan przewodniczący Tomasz Trela teraz zadaje pytania.

Poseł Tomasz Trela (Lewica):

Dziękuję bardzo. Ja tylko tak na wstępie, gwoli ścisłości, bo myśmy sprawdzali z panem przewodniczącym Pawłem Ślizem te wszystkie wydatki związane z oprogramowaniem Pegasus i myśmy dotarli do informacji, z których… i o tym też publicznie mówiliśmy, ale z racji, że dzisiaj padają te kwoty, a pan był uprzejmym powiedzieć, że ta kwota 25 mln zł

to nie jest taka… czy 33 nie jest taka wysoka, to Skarb Państwa przeznaczył na Pegasusa ponad 60 mln zł, dlatego że to były dodatkowe faktury, które wystawiała firma Matic, i to fizycznie była wypłata ponad 60 mln zł, więc to są takie dane. Myśmy o tym 9 kwietnia też informowali. Więc to tak tylko precyzując, bo 25 mln zł poszło z Funduszu Sprawiedliwości, 8 mln z Centralnego Biura Antykorupcyjnego, ale pewnie jak to każda umowa miała swoje zapisy i swoje możliwości, że każda dodatkowa usługa czy dodatkowy element tej usługi kosztował i to było w ramach tej umowy pewnie wykorzystywane. To tak precyzując.

Natomiast ja chciałbym o dwóch wątkach… dwa wątki jak gdyby może nie tyle poszerzyć, ale jeszcze uporządkować. Pan powiedział, że tego typu oprogramowania na ogół nie są w pełni produkowane przez jeden kraj, że tak to ujmę. Była wymiana między innymi Rosji jako tego kraju, Federacji Rosyjskiej jako tego kraju, który jest takim hegemonem czy potentatem, jeżeli chodzi o tego typu oprogramowania. Czy należy to rozumieć, że mogła być taka sytuacja, że ściągając te dane przez Pegasusa, które mogły być przechowywane na obcym serwerze, na przykład w Izraelu, one mogły być też przechowywane na serwerze jakiejś służby czy jakiejś instytucji w Federacji Rosyjskiej? Czyli gdybyśmy nie mieli tej takiej supermocnej aplikacji, to można byłoby spodziewać się, że te dane nie są tylko w dostępie dla aparatu władzy naszego kraju czy służb specjalnych naszego kraju, tylko one gdzieś są również pochowane, niekoniecznie wykorzystywane, ale również przetrzymywane.

Biegły Krzysztof Dyki:

Tu ponownie dotykamy tego wątku sieci anonimizującej. Ten, kto ma kontrolę nad siecią anonimizującą, ten, kto ma do niej dostęp, osobiście nie wiem kto, nie mam pojęcia, ten ma dostęp do tych danych. Wszyscy, którzy mogą mieć dostęp do tej sieci anonimizującej, ci będą mieli te dane. To może być NSO lub inne podmioty trzecie, za zgodą NSO lub bez zgody NSO. Wszyscy, którzy uzyskają dostęp do tej sieci, pamiętajmy, że sieć anonimizująca to serwery w różnych krajach, nie wiemy w których. Kluczem jest kontrola nad siecią anonimizującą. Więc…

Poseł Tomasz Trela (Lewica):

Czyli rozumiem to w ten sposób, że gdyby jakieś elementy, moduły tego oprogramowania pochodziły z Federacji Rosyjskiej i Federacja Rosyjska miałaby dostęp do tych sieci, to również u nich to mogłoby być przechowywane.

Biegły Krzysztof Dyki:

Byłbym zaskoczony, gdyby Federacja Rosyjska tworzyła sieć anonimizującą, bo wbrew pozorom to jest prosta operacja. Z perspektywy nawet kompetencji posiadanych przez nasze służby specjalne one są w stanie same wytworzyć przy kawie, herbacie, dobrym ciastku, bez szkoleń taką sieć anonimizującą, naprawdę. To brzmi może zawile, ale to nie jest trudne. Na to są gotowe komponenty otwartego oprogramowania, często darmowego, można taką sieć zbudować samemu. Mamy mnóstwo specjalistów, którzy potrafią sieć anonimizującą zbudować. Więc byłbym zaskoczony, gdyby Rosjanie budowali dla Izraela taką sieć. Mniej zaskoczony byłbym, gdyby w exploitach tworzonych i skupowanych z rynku znalazł się autor na przykład z takiego kraju. Tak, to by mnie mniej zaskoczyło, samego exploita.

Poseł Tomasz Trela (Lewica):

Z tego, co pan mówi, pan ma pełną wiedzę, doświadczenie w tym zakresie. Powiedział pan, udzielając odpowiedzi na jedno z pytań, że w Centralnym Biurze Antykorupcyjnym byli świetni specjaliści, żeby przeprowadzić taką procedurę zakupową i mogli to znakomicie sami zrobić. Proszę powiedzieć tak, jednym zdaniem, jasno dla opinii publicznej, według pana dlaczego tego nie zrobiono. Dlaczego, skoro mamy specjalistów, których opłacamy, którym polski podatnik płaci, to Centralne Biuro Antykorupcyjne jeszcze dodatkowo bierze firmę pośredniczącą, płaci jej niemałe pieniądze, bo to 8 mln, to podejrzewam, że to jest tam kwota, która będzie przy pełnej weryfikacji większa? Dlaczego to jest zrobione?

Biegły Krzysztof Dyki:

Problem, który widzę w kraju, od lat narastający, a w tej chwili apogeum jest tego problemu, to jest postępująca bardzo dynamicznie degradacja zdolności do realizacji niestandardowych zakupów przez organy państwa, w szczególności służby specjalne. Czyli mamy specjalistów, coraz mniej, ale mamy i oni są dobrzy w tych kompetencjach technicznych. Natomiast pytanie pana przewodniczącego dotyka…

Poseł Tomasz Trela (Lewica):

…spraw proceduralnych.

Biegły Krzysztof Dyki:

Tak, procesu zakupowego. I tu już ci specjaliści, oni patrzą na dział zakupów i inżynierowie tej klasy wysokiej, podtrzymuję, w kontakcie z prawnikami i ludźmi od Prawa zamówień publicznych… niekoniecznie będzie to wymarzone grono na grilla w weekend. Jest problem z komunikacją.

Poseł Tomasz Trela (Lewica):

Ja rozumiem, że pan chce powiedzieć, że o ile mamy znakomitych ekspertów od technologii i tych kwestii informatycznych…

Biegły Krzysztof Dyki:

Tak.

Poseł Tomasz Trela (Lewica):

…to generalnie Centralne Biuro Antykorupcyjne mogłoby sobie nie poradzić, przynajmniej szybko nie poradzić z procesem zakupowym, tak?

Biegły Krzysztof Dyki:

Jak niestety dzisiaj również, również dzisiaj, nie chodzi o dzień dzisiejszy, ale również dzisiaj większość służb specjalnych w tym kraju, tak, to jest poważny problem.

Poseł Tomasz Trela (Lewica):

Czyli firma pośrednicząca była według pana opinii i oceny wzięta po to, żeby to zrobić szybko i sprawnie.

Biegły Krzysztof Dyki:

Nie, myślę, że raczej jest jakieś zaufanie do firmy rozpoznawalnej, wiarygodnej, legalnej, która dostarczała, nie było problemów z innymi, mniejszej klasy, bardziej przyziemnymi rozwiązaniami i ktoś być może na gruncie wypracowanych schematów, standardów, pewnie też procesów zakupowych wpadł na pomysł, że być może skoro mamy zaufaną, wiarygodną firmę, która wywiązuje się ze swoich obowiązków, to może w samej instytucji mniej będzie przeszkadzać ta firma niż jakakolwiek inna i może ona pomoże rozwiązać jakieś problemy, które powstały w toku zakupu. Wyobrażam sobie, że mogły powstać jakieś problemy związane z samym zakupem, ale nie mam informacji na ten temat.

Poseł Tomasz Trela (Lewica):

Nie, bo wie pan, to jest o tyle istotne i ważne, że… tych pytań akurat ja nie będę do pana kierował, ale tutaj wszyscy świadkowie, którzy byli wcześniej, byli pracownikami Ministerstwa Sprawiedliwości, to to była taka błyskawiczna decyzja, jeżeli chodzi o przesunięcie tych pieniędzy, że to wszystko wskazuje na to, że to było tak naprawdę skrzętnie zaplanowane, umówione i… bo szybka decyzja, szybkie przelewy, szybka transakcja. W momencie, gdyby te pieniądze do Centralnego Biura Antykorupcyjnego trafiły w taki sposób budżetowy, to pewnie by trzeba było rozpocząć całą procedurę przetargową, poszukiwanie pewnie jakichś firm itd. Pewnie w tym przypadku takiego oprogramowania specjalnego… nie byłoby to w formie jawnej, bo wiemy, jak to powinno działać.

Natomiast mnie osobiście zastanawia to, że Centralne Biuro Antykorupcyjne, które jest jednostką publiczną, ma pewnie też swoich specjalistów do tego typu działań, nie robi tego indywidualnie, tylko korzysta z innych firm. Tym bardziej, że pan powiedział, że co do zasady państwa kupowały tego typu oprogramowania, jak nie państwa, to specjalne fundusze, które działały w oparciu o środki publiczne. Tutaj jednak

było to trochę zrobione inaczej, bo wiemy, że pieniądze z Funduszu Sprawiedliwości pieniędzmi budżetowymi nie są w rozumieniu przepisów.

Biegły Krzysztof Dyki:

Prawdopodobnie ta presja czasu, o której pan mówi, skutkowała jakimiś błędami… błędnymi decyzjami mogła skutkować.

Poseł Tomasz Trela (Lewica):

Zapytam pana jeszcze o taką rzecz, dlatego że ta presja czasu tak naprawdę miała przestrzeń wrzesień, październik, listopad, grudzień 2017 r. Czy według pana doświadczenia te 4 miesiące… 4 miesiące, jeżeli chodzi o decyzję, bo oprogramowanie było odebrane w 2018 r., na początku, miały tak kluczowe znaczenie, czy mogły mieć takie kluczowe znaczenie dla bezpieczeństwa państwa, że należało to tak szybko kupić? Bo gdyby to wpisano w budżet Centralnego Biura Antykorupcyjnego, w budżet operacyjny, to pewnie mało kto by o tym w ogóle kiedykolwiek się mógł dowiedzieć. Więc to mogło mieć takie znaczenie według pana, pana doświadczenia?

Biegły Krzysztof Dyki:

Świetna uwaga. Planowanie budżetów operacyjnych to jest ogromny problem. I teraz, z mojego doświadczenia czy w mojej pracy zawodowej widziałem takie działanie, pod taką presją w zakresie zakupów techniki operacyjnej o klauzuli „ściśle tajne" – tak, widziałem. Jeżeli jest uprawdopodobniona, a już na pewno wieloźródłowa informacja wskazująca na popełnienie bądź przygotowywanie jakiegoś ciężkiej kategorii wagowej czynu przestępczego, to wtedy zdarza się, że jest działanie w takim pośpiechu. Oczywiście na tym poziomie, o którym pan mówi – Fundusz Sprawiedliwości – to nie widziałem. To jest pewne novum, ale działanie pod taką presją…

Poseł Tomasz Trela (Lewica):

…czasową.

Biegły Krzysztof Dyki:

…czasową zdarza się, tak. Natomiast tu problem w mojej ocenie jest wieloletni, przewlekły. Ta choroba ma charakter przewlekły, czyli brak wyposażenia tej i innych służb w fundamentalne i bezpieczne narzędzia do wykonywania ich pracy, bo tu jest według mnie główny problem. Nie to, że oni to… ktokolwiek to posiadał, tylko co posiadał i jak to nabywał. Tu się zgadzam. Bo to, że powinien posiadać, to w mojej ocenie nie ulega wątpliwości.

Poseł Tomasz Trela (Lewica):

Wie pan, co do tego to my też jak gdyby specjalnie nie dyskutujemy, bo na każdym kroku to podkreślamy. Natomiast tutaj jak to wykorzystywał i w jaki sposób to nabywał, to otwierają się wszystkim i zapalają lampki, że tutaj było coś jednak nie tak, bo proces decyzyjny, jeżeli chodzi o przekazanie 25 mln zł, bardzo dużej kwoty, bardzo szybko, zawile, niejaśnie, w niejasny sposób, daje dużo do myślenia.

Ja w tej rundzie dziękuję.

Biegły Krzysztof Dyki:

Dziękuję.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo dziękuję.

Przechodzimy w takim razie do drugiej tury zadawania pytań. Czy przerwa… Jeżeli chciałby pan skorzystać z przerwy, to proszę tylko o sygnał. Dobra, jeżeli nie widzę potrzeby przez nikogo zgłaszanej przerwy, to przechodzimy do drugiej tury.

Ja mam takie pytanie. Ono pewnie na tym etapie… już gdzieś to wybrzmiało, ale chciałabym, żeby bardzo jednoznacznie stwierdził pan, czy Pegasus w standardowej konfiguracji dawał klientowi, czyli w naszym przypadku Centralnemu Biuru Antykorupcyjnemu, bezpieczeństwo, to znaczy pełną kontrolę nad gromadzonymi materiałami pozyskanymi w wyniku tego systemu, czy za pomocą tego systemu, czy transmisji tych danych. Czy Pegasus w standardowej konfiguracji…

Biegły Krzysztof Dyki:

W standardowej konfiguracji, abstrahując teraz od klienta, naszego kraju, służby, która to zakupiła, w standardowej nie, ponieważ w standardowej konfiguracji nie dawał takiego bezpieczeństwa, ponieważ występowała sieć anonimizująca, jak wspomniałem, PATM, nad którą właśnie rozmawialiśmy o sposobach zakupu. Jeżeli realizujemy szybko w pośpiechu zakup, to chcemy standardową konfigurację, nie ma czasu, nie zadajemy zbędnych pytań. I w tym przypadku takiego bezpieczeństwa nie gwarantuje, ponieważ nie mamy bezpieczeństwa nad siecią anonimizującą. A kiedy je posiadamy? Gdy zadbamy o bezpieczeństwo nad infrastrukturą całego systemu i on jest pod naszą kontrolą.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czyli jeżeli Centralne Biuro Antykorupcyjne zakupiło system Pegasus w standardowej konfiguracji, to nie posiadało dostępu do danych PATM, do tej sieci anonimizującej. Ta sieć anonimizująca była we władaniu NSO Group.

Biegły Krzysztof Dyki:

W standardowej konfiguracji, nie wiem, jak było w Polsce. Tak, była we władaniu, pod zarządem, całkowitym praktycznie, NSO Group, tak.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czy tak pozyskiwane dane na potrzeby procesu, postępowania, czy to przed prokuraturą, czy przed sądami, są danymi wiarygodnymi w pana ocenie, ocenie biegłego?

Biegły Krzysztof Dyki:

Jeżeli mówimy o standardowej konfiguracji, w której klient…

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Tak, o tym mówimy.

Biegły Krzysztof Dyki:

…nie ma kontroli nad siecią anonimizującą, trudno by mi było odnaleźć walor procesowy, ponieważ nie mógłbym zweryfikować źródła materiału dowodowego oraz jego autentyczności.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czy w standardowej konfiguracji system Pegasus mógł włączyć kamerę, mógł zrobić zdjęcie, nagrywać w czasie rzeczywistym obraz i dźwięk?

Biegły Krzysztof Dyki:

Tak.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czy w standardowej konfiguracji mógł modyfikować SMS-y na danym telefonie komórkowym?

Biegły Krzysztof Dyki:

Nie.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czy w standardowej konfiguracji system Pegasus pozwalał na infekcję numerów z prefiksem np. rosyjskim? Czyli czy mogliśmy podsłuchiwać, inwigilować obywateli posługujących się telefonami z sieci rosyjskiej?

Biegły Krzysztof Dyki:

Według doniesień medialnych istniały pojedyncze przypadki inwigilacji opozycjonistów na Białorusi i w Rosji. Z informacji przeze mnie posiadanych i próbek przeze mnie badanych nie spotkałem się z infekcją numerów rosyjskich.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czyli badał pan fragment systemu Pegasus i w tym badanym przez pana fragmencie stwierdza pan, że nie ma możliwości infekcji prefiksu rosyjskiego.

Biegły Krzysztof Dyki:

Fragmenty systemu Pegasus, ten implant instalowany na urządzeniu osoby inwigilowanej oraz czasami dostawałem tak zwane dumpy, językiem technicznym mówiąc, a w prostszym ludzkim zrzuty smartfona osoby X, Y, tak na tej podstawie… Czyli nie spotkałem się z infekcją telefonu rosyjskiego. Chodzi o prefiks, tak jak pani przewodnicząca słusznie mówi, nie o produkcję, miejsce jego, ale prefiks abonenta, co nie oznacza, że to nie miało miejsca. Natomiast tak, jak patrzę na mapę miejsc i krajów ofiar, to rzeczywiście, ja osobiście nie spotkałem się z zainfekowaną ofiarą w Rosji.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dobrze.

Biegły Krzysztof Dyki:

Ale podkreślam, wiem o informacjach medialnych, że podobno wybrani opozycjoniści w Rosji czy w Białorusi według informacji medialnych byli inwigilowani.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

A dlaczego według pana nie było takiej możliwości?

Biegły Krzysztof Dyki:

Nie wiem, czy nie było, i z materiałów, przeze mnie posiadanych informacji nie odnalazłem takich dowodów. Natomiast być może… Relacje Rosji z Izraelem są ogólnie znane. One teraz uległy trochę redefinicji, niekoniecznie optymalnej, ale w chwili, o której mówimy, w latach, o które państwo pytacie, to są silne, mocne relacje Rosji i Izraela i wyobrażam sobie, że Rosja nie życzyła sobie, tak jak Stany Zjednoczone…

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Być podsłuchiwana przez kogokolwiek innego.

Biegły Krzysztof Dyki:

Na przykład.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czy w takim razie numery z prefiksem izraelskim również nie mogą być podsłuchiwane przy pomocy tego Pegasusa?

Biegły Krzysztof Dyki:

Numery z prefiksem izraelskim w Izraelu mogły być podsłuchiwane. Nie słyszałem o przypadku, co nie znaczy, że nie miał miejsca. Osobiście nie znam przypadku inwigilacji Pegasusem klienta…

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

…przez innego klienta aniżeli Izrael.

Biegły Krzysztof Dyki:

Tak, ofiary, która jest obywatelem Izraela, przez klienta, który pochodzi z innego kraju.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dobrze. To jakie jeszcze narodowości nie mogły być podsłuchiwane, idąc tym tokiem myślenia? Czyli mamy obywateli rosyjskich, czyli numery z prefiksem, numery z prefiksem izraelskim. Jakie jeszcze prefiksy nie mogły być?

Biegły Krzysztof Dyki:

Ja powiem, nie wiem, czy nie mogły być. Na pewno ciężko w statystyce, jeżeli spojrzymy na ofiary, to ciężko znaleźć oczywiście ofiary w Izraelu, ciężko znaleźć ofiary w Rosji i ciężko znaleźć ofiary w Stanach Zjednoczonych. Numery z prefiksem amerykańskim były co do zasady zablokowane, ale uwaga, niektórzy klienci nabywali niestandardową konfigurację, płacąc więcej niż Polska, nawet w tej sumie, o której nie wiedziałem, 60 mln, o których dzisiaj usłyszałem, pierwszy raz o nich słyszę, nie wiedziałem, kilka razy więcej płacili inni i niektórzy klienci mieli możliwość infekcji numerów, również tych… również amerykańskich, ale to były wyjątkowe transakcje o bardzo wysokich kwotach. Tak.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

A kto to weryfikował, jakie numery były infekowane?

Biegły Krzysztof Dyki:

To w chwili sprzedaży… nie było dwóch klientów, którzy mieli tę samą postać operowania Pegasusem. Nie ma czegoś takiego jak jeden Pegasus.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dobrze. Cofam w takim razie pytanie, to zapytam inaczej. Czy w standardowej wersji, w tej standardowej konfiguracji Pegasusa w Polsce weryfikowano osoby, które były infekowane?

Biegły Krzysztof Dyki:

Tu bym poprosił o podpowiedź, kto miał weryfikować.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

No właśnie, kto miał weryfikować? Jeżeli były na przykład takie obostrzenia jak zakaz infekowania numerów o danym prefiksie, to kto to weryfikował?

Biegły Krzysztof Dyki:

Już. Przede wszystkim to wynikało z konfiguracji technicznej narzędzia dostarczanego klientowi. Klient mógł zrobić to, na co pozwalała mu konfiguracja techniczna Pegasusa. Po drugie, jeżeli nie kontrolował sieci anonimizującej, to z końca tej sieci dopiero przebiegał atak. Więc po drugie, jeszcze tam blokada.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czyli w standardowej konfiguracji atak, chce pan powiedzieć, przechodził przez tę ostatnią część tego całego…

Biegły Krzysztof Dyki:

W każdej konfiguracji przechodził przez ostatnią część. W każdej.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czyli nie przez serwery w Polsce, a serwery pod kontrolą NSO Group.

Biegły Krzysztof Dyki:

Nigdy… W tych wersjach oprogramowania, które widziałem, we wszystkich nich atak nie pochodził przez serwer posiadany przez klienta. On raczej służy jako macierz, to jest zwykły serwer, on…

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czyli tak jak w przypadku Polski, na tym serwerze gromadzimy dane…

Biegły Krzysztof Dyki:

Tak, w archiwum.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

…które sobie my bezpośrednio przez operatora infekujemy z tych urządzeń. Tu trzymamy dane. Natomiast infekcja urządzeń, nawet tych wbijanych fizycznie przez operatora w Polsce, następuje przez serwery, które nie są w naszym posiadaniu.

Biegły Krzysztof Dyki:

Tak, następuje z nieznanego miejsca w standardowej konfiguracji infekcja. Nie następuje z serwera posiadanego przez klienta. To jest takie bardziej archiwum serwer… zresztą oprogramowanie i przede wszystkim urządzenia są standardowe. To nie jest nic wybitnego, normalny serwer. I ona, i wtedy… U każdego klienta infekcja nie następowała z tego serwera posiadanego przy stacjach operatorskich, tylko następowała w standardowej konfiguracji z miejsca, którego nie zna klient.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czyli przez serwery poza granicami Polski.

Biegły Krzysztof Dyki:

Prawdopodobnie tak, chociaż raz przypadkowo pewnie mogłoby się złożyć, że na przykład inny klient, z innego kraju akurat by nieświadomie atakował z Polski.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

My skupiamy się na naszym tym przypadku.

Biegły Krzysztof Dyki:

Tak, tak… Nie, to jeżeli polski klient, to na pewno atak nie pochodził z Polski, tak.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

To jest oczywiście szokująca informacja, ponieważ do tej pory zapewniano nas wszystkich, że stosowanie systemu Pegasus, niejednokrotnie wypowiadali się poprzednicy, koordynatorzy służb specjalnych, że była to w pełni bezpieczna czynność operacyjna, którą podejmowano. Ja uważam i taka jest moja opinia na tym etapie, a jeszcze nie… dobrze nie rozpoczęliśmy kwestii dotyczącej legalności stosowania tego systemu, ale jednak uważam, że mało to ma wspólnego z normami prawnymi, o które opiera się dzisiaj kontrola operacyjna w Polsce.

Czy pan jako biegły sądowy, który niejednokrotnie pewnie wydawał opinię w danym temacie, będzie potrafił odnieść się do takiej mianowicie kwestii? Kontrola operacyjna zarządzona jest na 3 miesiące. Od dnia 1 lipca do określonego dnia za 3 miesiące kończyć ma swoją pracę funkcjonariusz operacyjny prowadzący kontrolę operacyjną. Czy ten system dawał nam możliwość zaciągania historycznych danych, to znaczy sprzed kontroli operacyjnej, tej zarządzonej przez sąd?

Biegły Krzysztof Dyki:

W standardowej konfiguracji tak.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

W standardowej konfiguracji operator zaciągał dane historyczne?

Biegły Krzysztof Dyki:

Nie twierdzę tak, twierdzę, że miał techniczną możliwość.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

OK. A co do kamery, co do włączenia i tych możliwości, tutaj już mamy jasność, że nie jest prawdą, że nie można było włączyć kamery czy głośnika. Tutaj mamy… wszyscy się zgadzamy, technicznie była pełna możliwość…

Biegły Krzysztof Dyki:

Technicznie, tak.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

…a w tej standardowej konfiguracji Pegasusa na pewno była.

Biegły Krzysztof Dyki:

Tak.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Ta standardowa konfiguracja jest tą najniższą możliwą konfiguracją…

Biegły Krzysztof Dyki:

Umożliwia.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

…czyli wszystkie kolejne naturalnie musiały również posiadać takie możliwości.

My tutaj nie kwestionujemy potrzeby, konieczności wręcz posiadania przez polskie służby systemów typu Pegasus. Dzisiaj Pegasusa już nie ma, ale oczywiście wiemy, że służby muszą mieć możliwości walki z przestępczością.

Biegły Krzysztof Dyki:

Tak.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Ale jeżeli słyszymy, że nie mogliśmy inwigilować obywateli posługujących się prefiksem rosyjskim, a mieliśmy walczyć z najcięższymi gatunkowo przestępcami, to kłóci się trochę z tym, co słyszeliśmy do tej pory.

Czy pan posiadając wiedzę na tym etapie, już dostępną medialnie, ale także z dokumentacji i z pana doświadczenia, czy jest pan w stanie powiedzieć, czy system Pegasus stosowany w Polsce był stosowany legalnie w oparciu o normy prawne? Czy on był stosowany legalnie?

Biegły Krzysztof Dyki:

Przyznam, że nie posiadam wystarczającej wiedzy ani umocowania merytorycznego do odpowiedzi na tak postawione pytanie.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

OK. Ale czy pan… Dobrze, to inaczej zadam pytanie. Czy pan, gdyby był pan szefem służby, w taki sposób zakupiłby system Pegasus?

Biegły Krzysztof Dyki:

Nie wiem, w jaki zakupiono. Jeżeli zakupiono w standardowej konfiguracji, jeżeli nie miałbym kontroli nad siecią anonimizującą, to osobiście bym takiego narzędzia nie zakupił.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

A czy zakupiłby pan system w sposób jawny, to znaczy z jawnych środków, nie kupując go ze środków funduszu operacyjnego?

Biegły Krzysztof Dyki:

Wszystkie transakcje w tej klasy przy środkach ściśle tajnych, które ja widziałem, to odbywały się wszystkie 100% z funduszu operacyjnego i nigdy nie było z tym problemu. Zawsze to był fundusz operacyjny.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Nie, nie, bo tutaj próbują też nam poprzednicy wmówić, że zakup w taki sposób złożony, to znaczy właśnie z części środków Funduszu Sprawiedliwości, plus ta część operacyjna dołożona, plus później jeszcze wydatki, jest całkowicie legalnym zakupem. Otóż nie jest, ponieważ systemy do inwigilacji na potrzeby pracy służb operacyjnych, służb specjalnych w Polsce powinny być dokonywane z funduszu operacyjnego po to, żeby właśnie nie narazić na niebezpieczeństwo wypłynięcia takich informacji.

Jeszcze jedno pytanie. Ponieważ my tutaj cały czas mówimy o tym, co możliwe jest dla systemu Pegasus, ale zapominamy o jednym, że na końcu przy standardowej konfiguracji mamy do czynienia z informacjami ściśle tajnymi obejmującymi osoby, wobec których stosowano system Pegasus, czyli osoby inwigilowane i w takiej sytuacji istnieje duże prawdopodobieństwo, a na pewno nie zachowano wszelkich możliwości, żeby ta informacja była w dalszym ciągu ściśle tajna. Narażono na niebezpieczeństwo wypływu tych informacji poza granicę Polski, do obcych służb.

Biegły Krzysztof Dyki:

Jeżeli klient nie ma kontroli nad siecią anonimizującą i infrastrukturą systemu Pegasus, to nie jest w stanie zapewnić bezpieczeństwa tych danych.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dobrze. Na tym etapie dziękuję.

Biegły Krzysztof Dyki:

Dziękuję.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo proszę, teraz pani Joanna Kluzik-Rostkowska. Bardzo proszę.

Poseł Joanna Kluzik-Rostkowska (KO):

Panie Krzysztofie, panie biegły, chciałam uporządkować pewne rzeczy, biorąc pod uwagę dwie rzeczy. Po pierwsze, pana wywiad dla Defence24 i to, o czym rozmawialiśmy przed

chwilą. Jeśli dobrze rozumiem, bo bohaterów mamy trzech: mamy firmę NSO, mamy klienta, czyli CBA i później ewentualnie inne służby, i mamy ofiary. Ja tu używam nomenklatury pana. Jeśli dobrze zrozumiałam to, co pan mówił w tamtym wywiadzie, to nie ma możliwości, żeby klient, czyli CBA, zainfekowało smartfona bez pośrednictwa NSO.

Biegły Krzysztof Dyki:

W standardowej konfiguracji, nie wiem, w jakiej nabyło CBA, ale w standardowej konfiguracji, jeżeli nie zapewniono kontroli nad infrastrukturą Pegasusa i siecią anonimizującą, tak, to prawda.

Poseł Joanna Kluzik-Rostkowska (KO):

Czyli tak naprawdę właściciel oprogramowania, czyli firma NSO, potencjalnie miała pełną kontrolę nad wszystkimi danymi, które przepływają od ofiary do klienta.

Biegły Krzysztof Dyki:

Jeżeli klient nie wykluczył takiego ryzyka, to tak.

Poseł Joanna Kluzik-Rostkowska (KO):

To jest o tyle interesujące, że z jednej strony oczywiście nas się przekonuje, że to wszystko było tutaj zamknięte, domknięte, nic nie wypływało. Z drugiej strony sam pan powiedział już chyba tutaj dzisiaj, że szef NSO w wywiadach publicznych mówił, że absolutnie panują nad tym, w jaki sposób te ich narzędzia są wykorzystywane, ponieważ jeżeli są wykorzystywane niezgodnie z intencjami, to po prostu natychmiast blokują tę możliwość. To zresztą spotkało Polskę również, tak? Więc rozumiem, że można zakładać, że tak poważna firma opiera się nie tylko na doniesieniach prasowych, tylko może mieć możliwość wglądu przez… we wszystko, co przepływa.

Biegły Krzysztof Dyki:

Rzeczywiście ówczesny prezes NSO udzielał takich wypowiedzi publicznych, gdzie zapewniał, że nie dochodziło do sytuacji, o które jest posądzana firma NSO i ich klienci, ponieważ oni zapewniali demokratyczny i bezpieczny charakter stosowania tego narzędzia i rzeczywiście padały stwierdzenia o tym, że klienci nieprawidłowo wykorzystujący to oprogramowanie byli pozbawiani tego oprogramowania, było ono wyłączane. Więc powstaje naturalne pytanie, w jaki sposób, jeżeli nie miałby nad tym kontroli.

Poseł Joanna Kluzik-Rostkowska (KO):

Tak, bo to trochę nam rysuje taki obraz, w którym nie możemy wykluczyć, że wszystko, co było pobierane od polskich ofiar dla klienta, miało również… znaczy, ponieważ przepływało przez NSO, to tam było gromadzone. W związku z tym tak naprawdę my nie tylko służbom izraelskim, być może jeszcze jakimś innym, daliśmy materiał gotowy, to jeszcze za niego zapłaciliśmy, tak?

Biegły Krzysztof Dyki:

To ciągle właśnie jest powrót do pytania do klienta, nad czym zapewniłeś bezpieczeństwo, bo nie wiemy, czy tak było, ale czy istniało takie ryzyko, jeżeli nie kontrolowaliśmy infrastruktury systemu. Tak, istniało.

Poseł Joanna Kluzik-Rostkowska (KO):

Proszę mi powiedzieć jeszcze coś takiego, bo to również pan dzisiaj już o tym mówił, że tak naprawdę NSO miało możliwość kontrolowania tego procesu. Nie mogło ingerować, jak rozumiem, konkretnie na przykład w SMS-y wewnątrz tego zapisu, ale mogło różne rzeczy do tych urządzeń transportować, tak?

Biegły Krzysztof Dyki:

Tak. Technicznie firma NSO swoim oprogramowaniem miała pełną kontrolę, mogła ingerować, w co tylko chce. Nie twierdzę, że to robiła, ale technicznie miała pełną kontrolę nad smartfonem.

Poseł Joanna Kluzik-Rostkowska (KO):

Przypuśćmy, ja wysyłam SMS i ktoś mi tam do tego coś dopisuje, albo coś mi z tego SMS-a kasuje.

Biegły Krzysztof Dyki:

Technicznie rzecz biorąc tak, nie twierdzę, że tak się działo, nie słyszałem o takich informacjach, ale technicznie ich oprogramowanie działa w taki sposób, który umożliwia całkowitą kontrolę nad treściami przechowywanymi i transmitowanymi przez smartfon. Natomiast klient w standardowej konfiguracji nie posiadał takiej możliwości.

Poseł Joanna Kluzik-Rostkowska (KO):

Tutaj chciałam nawiązać do tego, co pan mówił, o takim znaczeniu geopolitycznym, tak, bo to z jednej strony, ponieważ wiemy, że to co prawda narzędzie prywatnej firmy, ale pod całkowitą kontrolą rządu czy też służb Izraela, bo to jest taka duża pokusa, żeby w razie czego z różnych tego typu możliwości korzystać…

Ale zastanawia mnie jeszcze jedna rzecz. Przypuśćmy, jest ofiara, przechodzi informacja przez NSO do klienta i tam są jakieś treści wrażliwe z punktu widzenia Izraela. Czy również jest możliwe, żeby przez te kontrole ten fragment z tych treści po prostu wykasować?

Biegły Krzysztof Dyki:

Technicznie i teoretycznie, hipotetycznie tak.

Poseł Joanna Kluzik-Rostkowska (KO):

Czyli tutaj absolutnie wielkie narzędzie do takiej manipulacji. No i to jest podstawowe pytanie, właśnie czy przy braku akredytacji, sprawdzenia tego systemu, pośpiechu w jego zakupie, czy my po prostu nie naraziliśmy nasze bardzo wrażliwe dane na to, żeby one wyciekły.

Ostatnie moje pytanie w tej serii. Wiemy, że firma NSO się rozpada. Wiemy, że spora część pracowników firmy w tej chwili siedzi w Emiratach i tam założyła kolejną firmę.

Biegły Krzysztof Dyki:

Tak.

Poseł Joanna Kluzik-Rostkowska (KO):

Czy możemy być zaniepokojeni faktem, że jeżeli duża grupa pracowników NSO przeniosła się tam, to czy również te bardzo wrażliwe dane mogły przenieść się razem z nimi, mówiąc kolokwialnie?

Biegły Krzysztof Dyki:

Nie zakładam sytuacji, nie mam wiedzy o sytuacji pozyskania jakichkolwiek danych, natomiast ta grupa ludzi, która rzeczywiście do Emiratów i nie tylko się przeniosła, jest też nowa firma byłego prezesa NSO, to są osoby techniczne. Te osoby, o których rozmawiamy, to są inżynierowie głównie. To nie są osoby… to nie są analitycy posiadający informacje. Bo wiadomo, jeżeli mamy jakieś informacje obciążające, kompromitujące, które można w jakiś sposób wykorzystywać, rozgrywać, to nie są ci inżynierowie, to kto inny tym zawiaduje. Ci inżynierowie rzeczywiście tak…

Ryzyka, jakie ja widzę, są bardziej techniczne, czyli że już w krajach takich jak Emiraty Arabskie jest pierwsze narzędzie działające i jest pytanie takie, co my robimy, nawet nie jako Polska, tylko jako Europa, ja się bardziej tego obawiam, bo jeżeli tam ci ludzie robią już pierwsze narzędzie, są działające takie narzędzia, to po pierwsze, czy my mamy takie, a po drugie, czy mamy coś do obrony przed tym, tego bardziej się obawiam.

Jeżeli chodzi o możliwość pozyskania materiałów, to oczywiście takie materiały może pozyskać każdy ten, kto ma dostęp cały czas do tej sieci anonimizującej, to jest kluczowe. Wszelkie ryzyka, o których możemy rozmawiać, są w obszarze tej sieci, bo ona nie tylko odpowiada za transmisję danych, ale z niej też następuje, z sieci anonimizującej następuje atak na smartfon osoby inwigilowanej. Z ostatniego punktu, z ostatniego serwera sieci anonimizującej następuje atak i te dane też są wysyłane w pierwszej kolejności ze smartfonu ofiary do sieci anonimizującej. Nawet jeżeli NSO będzie chciało mieć kopię dla siebie, to i tak pierwsze dane ze smartfonu ofiary zawsze idą do sieci anonimizującej.

Te próbki, które ja badałem, o tym świadczyły, że to nie szło nigdy wprost do NSO. Nie. Idą do sieci anonimizującej. Gdzie one dalej idą, nie wiem.

Poseł Joanna Kluzik-Rostkowska (KO):

A czyja była ta sieć, którą pan badał?

Biegły Krzysztof Dyki:

Słucham?

Poseł Joanna Kluzik-Rostkowska (KO):

Kto był właścicielem tej sieci?

Biegły Krzysztof Dyki:

Sieci nigdy nie badałem. Ona mnie nigdy nie interesowała. Mnie interesował sposób działania programu. Nie badałem właściwości sieciowych, sieci anonimizujących. Oczywiście widziałem jakieś próbkowanie sieciowe, tak. Zwykłe serwery w różnych miejscach, wykupowane za kryptowaluty. Przeważnie to, co zauważyłem, że te serwery… kiedyś to był jeszcze jakiś Amazon, później już raczej takie miejsca, nieduże firmy, które akceptują kryptowaluty. To to zauważyłem, że wspólną cechą sieci anonimizującej, do której wychodziły dane ze smartfonów było to, że gdy sprawdzałem, gdzie są te serwery, to one znajdowały się u operatorów, u firm, które świadczyły normalnie istniejących, najczęściej legalnych, nie zawsze, bo to czasami też były dziwne firmy sieciowe, ale przeważnie legalne, które… wspólnym mianownikiem ich było to, że akceptowały kryptowaluty. Natomiast dalej już nie drążyłem. Mnie bardziej interesowała ta magia znajdująca się wewnątrz urządzenia. Nie mam pojęcia, co się działo, gdzie to szło dalej z sieci anonimizującej.

Poseł Joanna Kluzik-Rostkowska (KO):

Ale rozumiem, że biorąc pod uwagę scenariusze czarne, nie możemy wykluczyć, że z tych pobieranych, wrażliwych informacji od ofiary, one po prostu gdzieś mogły wyciekać i być wykorzystywane przez innych. Jak rozumiem, tutaj rację ma Biden, mówiąc: koniec obcych, tylko nasze, tak?

Biegły Krzysztof Dyki:

Tak, z tego, rzeczywiście… głównie z tego względu, aż został wydany dekret, co jest najwyższej rangi w Stanach Zjednoczonych dyspozycją. W tym obszarze, o którym rozmawiamy, nie ma wyższej dyspozycji, i ten dekret jest publicznie dostępny, można się z nim zapoznać. Wszystko… Bo właśnie pani pytanie dotyka istoty problemu, czyli możliwych zagrożeń. Stany Zjednoczone mówią w tej treści tego dokumentu tak: „wszystko, co może stwarzać zagrożenia". Oni nie badają, czy stwarza. Wszystko, co może.

Poseł Joanna Kluzik-Rostkowska (KO):

Potencjał…

Biegły Krzysztof Dyki:

Koniec, wykluczone. W tej chwili już Stany też nie posiadają Pegasusa. Oni kupili, co ciekawe, Stany Zjednoczone, z informacji posiadanych przeze mnie wynika, że oni zakupili Pegasusa i bardzo sprytnie, bo wyłącznie na potrzeby badań. Oni go nie stosowali, czyli chcieli przebadać, co istnieje.

Poseł Joanną Kluzik-Rostkowska (KO):

Żeby zrobić swoje, lepsze.

Biegły Krzysztof Dyki:

Tak, porównać do tego, co mają. Zainteresowały ich te exploity, tak. Stany Zjednoczone nie stosowały tego narzędzia. Kupiły je, bodajże FBI, o ile się nie mylę, kupiły całą infrastrukturę, i to jest ta różnica, żeby zbadać, jak to dokładnie działa, co to robi. Nie stosowały tego narzędzia.

Poseł Joanna Kluzik-Rostkowska (KO):

Na marginesie, te kontakty polityczne, przyjaźń polityczna pomiędzy Stanami Zjednoczonymi a Izraelem jest duża, tak. Czyli w zasadzie można byłoby myśleć, że łatwiej

o takie zaufanie, ale jednak taki interes państwowy, partykularny jest tutaj absolutnie najważniejszy.

Biegły Krzysztof Dyki:

W tej kategorii narzędzi nie ma zaufania. W tej kategorii narzędzi nawet ta więź bardzo silna Izraela ze Stanami Zjednoczonymi, bardziej geopolityczna niż wynikająca z emocji, bardziej z biznesu i geopolityki w mojej ocenie, ale rzeczywiście bardzo silna, co widać obecnie chociażby w regionie Izraela, ta więź jest bardzo mocna, to jednak ona… Stany Zjednoczone mają taką politykę, że oni nie zaufają, nie użyją takiej broni u siebie. Oni muszą mieć swoją broń. Nie, to Stany wykluczają taką sytuację. Oni nie korzystają z tej klasy narzędzi innej produkcji. Skupują, badają, płacą, ale nie stosują od tej produkcji.

Poseł Joanna Kluzik-Rostkowska (KO):

Rozsądne. Dziękuję bardzo w tej części.

Biegły Krzysztof Dyki:

Dziękuję bardzo.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo dziękuję.

Pan poseł Witold Zembaczyński.

Poseł Witold Zembaczyński (KO):

Dziękuję, wielce szanowna pani przewodnicząca.

Wysoka Komisjo, państwo doradcy, eksperci oraz proszę biegłego, ja bym chciał jeszcze więcej wyjaśnień w sprawie kwestii wyłączenia z możliwości infekowania kart SIM o określonych prefiksach. Co zatem z tym walorem Pegasusa, jakim miało być użycie kontrwywiadowcze? Jeżeli nie możemy naszych głównych przeciwników, Rosjan, Białorusinów, kogokolwiek tam zabraniano w tej umowie licencyjnej, przy użyciu tego urządzenia inwigilować, to jakie jest jego zastosowanie stricte kontrwywiadowcze? Czy… Proszę powiedzieć, czy intencją NSO tworzenia tego narzędzia było stricte wykorzystanie cywilne, antykorupcyjne, polegające na kontroli operacyjnej w różnych sprawach, stricte kryminalnych, czy głównym walorem, nie wiem, w ich na przykład katalogu reklamowym było to, co daje tę przewagę w walce z obcymi wywiadami?

Biegły Krzysztof Dyki:

NSO trochę ewoluowało, jeżeli chodzi o medialne przeznaczenie tego programu. Najpierw to były czynności kryminalne, później widząc, że się robi coraz trudniej wokół, powstaje szum medialny wokół tego narzędzia, poszli bardziej w kierunku terroryzmu, że to jest narzędzie do… przeciwdziałające, zwalczające terroryzm. To brzmi lepiej, to się lepiej adoptuje, lepiej się sprzedaje. Więc ta polityka medialna, handlowa, sprzedażowa NSO była wprost proporcjonalna do sezonu, do prognozy pogody. Co pasuje.

Poseł Witold Zembaczyński (KO):

Co się zmieniało.

Biegły Krzysztof Dyki:

Co się zmieniało. A tak jeżeli przychodzimy do pytania tak naprawdę już jak to się odbywało w rzeczywistości, a nie medialnych deklaracji, to nie miało wielkiego znaczenia, kto do czego tego potrzebował. To po prostu miało zwalczać przestępczość, koniec, kropka. Jakiego typu, średnio to interesowało NSO. Byleby to było legalne, byleby organ państwa to kupował. Nie sprzedawano tego prywatnym firmom. To jest bardzo ważne, chwalebne i zbawienne, że nie sprzedawano tego jakimkolwiek firmom.

Poseł Witold Zembaczyński (KO):

Tylko rządom.

Biegły Krzysztof Dyki:

Tylko rządom, tylko uprawnionym, zweryfikowanym organom, ale przeznaczenie i kto do czego, już nie zadawali pytań.

Poseł Witold Zembaczyński (KO):

To jakbyśmy się tak znaleźli w 2017 r., to zakup przez CBA Pegasusa de facto był podyktowany potrzebami wykrywania przestępstw kryminalnych. Tak de facto, tutaj, na miejscu, takich przestępstw kryminalnych, korupcyjnych, popełnianych przez osoby posługujące się polską kartą SIM.

Biegły Krzysztof Dyki:

To jest pytanie… Z informacji medialnych wiem, że centralne biuro zakupiło Pegasusa. Jeżeli inne służby zakupiły bądź wykorzystały… wykorzystywały to narzędzie, to już jest pytanie, tak, czy go stosowały. Najprościej by było sprawdzić, czy jeżeli inne służby korzystały z tego narzędzia, to wystarczy wziąć materiał dowodowy, porównać, czy były pozyskiwane dane ze smartfonów o numerach abonenckich z rosyjskim prefiksem. To będzie bardziej już…

Poseł Witold Zembaczyński (KO):

Gdzie Komisja może ustalić te dane, proszę powiedzieć.

Biegły Krzysztof Dyki:

U samego… Aha, u klienta, który nabył, i u klientów, którzy stosowali to oprogramowanie.

Poseł Witold Zembaczyński (KO):

Czyli w naszym przypadku jest to stricte CBA, tak?

Biegły Krzysztof Dyki:

Nie wiem, kto… Wiem, kto nabył z informacji medialnych – CBA, ale nie wiem, czy i kto jeszcze tego używał, tego nie wiem. Być może albo biuro wspomagało inne służby w legalnych operacjach, albo może… Trudno mi jest sobie wyobrazić, żeby inna służba uzyskała dostęp. Teoretycznie jest to możliwe za pomocą stacji operatora. Jeżeli nabyto więcej niż jedną stację operatora i ta stacja znajdowała się poza biurem, to byłoby zastanawiające, ale zakładam jednak, że to był jeden klient, jeden operator, że to było CBA.

Poseł Witold Zembaczyński (KO):

Proszę biegłego, czy krzyżowe zakażenia były możliwe w wypadku polskich abonentów, czyli osób, które są już dzisiaj powszechnie znane i uznawane za ofiary Pegasusa? Czy było możliwe krzyżowe infekowanie systemów operacyjnych w pierwszej wersji Pegasusa, a potem przy użyciu exploitów, tych bramek, poprzez aplikację?

Biegły Krzysztof Dyki:

Tak. Pegasus umożliwiał tzw. krzyżową infekcję, czyli on sam w momencie przejmowania kontroli nad smartfonem, przynajmniej te komponenty, które ja badałem, one obsługiwały tzw. mówimy o nich wyjątki techniczne, obsługiwały, technicznym językiem mówiąc, wyjątki, które dotyczyły próby infekcji telefonu, smartfonu już kontrolowanego przez kogoś i on to… Pegasus to umożliwiał. Czyli…

Poseł Witold Zembaczyński (KO):

Na przykład Galileo czy jakikolwiek tam inny system?

Biegły Krzysztof Dyki:

Nie, to ja mówię cały czas o…

Poseł Witold Zembaczyński (KO):

O równoległym zakażeniu Pegasusem, dwoma licencjami.

Biegły Krzysztof Dyki:

Pegasusem, tak dwoma lub więcej, tak. Umożliwiał to i obsługiwał.

Poseł Witold Zembaczyński (KO):

A taka sytuacja nie powodowała w istocie pewnego ryzyka procesowego wynikającego z konieczności gromadzenia dowodów, że mogą te dowody być zmanipulowane w wyniku zakażenia krzyżowego?

Biegły Krzysztof Dyki:

Nie, bo w modelu, w którym standardowo działał Pegasus, on nie umożliwiał operatorowi ingerencji w pozyskiwany materiał w chwili jego pozyskiwania. Operator nie miał wpływu na to. Operator wydaje polecenie…

Poseł Witold Zembaczyński (KO):

Mieścił się w pamięci operacyjnej, tak?

Biegły Krzysztof Dyki:

Mieścił się w pamięci operacyjnej i badał tylko, czy nie ma próby kolejnej infekcji, którą przejmował i obsługiwał równolegle drugiego na przykład klienta, który nie wie, że ta ofiara już jest zainfekowana i wysyła te same dane, które chce pozyskać, w tej samej postaci do tylu operatorów i różnych klientów i ilu atakowało ten smartfon.

Poseł Witold Zembaczyński (KO):

Proszę biegłego, czy polskie służby w tamtym czasie, CBA, były w stanie używać Pegasusa do tego, żeby stwierdzić, czy jakiś konkretny polski abonent jest zainfekowany, na przykład z zagranicy Pegasusem?

Biegły Krzysztof Dyki:

Nie miało takiej możliwości. Nie.

Poseł Witold Zembaczyński (KO):

Dobrze. A czy może biegły nam też opowiedzieć po kolei, jak w etapach rozwijało się to oprogramowanie? Czyli mamy rok 2017, CBA kupuje Pegasusa, który obsługuje na tamten czas systemy operacyjne, poprzez te zero-day, przełamuje albo właściwie dostaje się przez te luki, ale jeszcze w systemie operacyjnym telefonu Androida i iOS do urządzenia, rozpoczyna infekcję, jest potrzebne kliknięcie w jakiś link aktywacyjny. Potem co się dzieje? Jak zmienia się moduł funkcjonowania tego oprogramowania? Mam na myśli przejście… Co jest powodem i kiedy jest ten moment, kiedy infekcja z kliknięcia przychodzi na zero-click i co się dzieje, że infekcja z zero-day w oprogramowaniu przychodzi na exploita w aplikacji?

Biegły Krzysztof Dyki:

Czyli mamy tak – te dwa rodzaje infekcji, jeden, który wymaga interakcji z użytkownikiem, jest jakaś socjotechnika prowokująca go do kliknięcia…

Poseł Witold Zembaczyński (KO):

Profilowanie, wiemy, tak.

Biegły Krzysztof Dyki:

…i drugi, który nie wymaga interakcji. Co ciekawe, mitem tu jest to, że oprogramowanie iPhone, iOS, w oprogramowaniu smartfonów iPhone jest to bezpieczniejsze, bo jeżeli, co nie jest chyba w ogóle wiadome w przestrzeni publicznej, międzynarodowej, to ciekawostka wynikająca z moich analiz jest taka, że statystycznie ja widziałem, analizując te próbki, ja widziałem znacznie większą skuteczność Pegasusa wobec iPhone'ów niż wobec na przykład androidów. To jest bardzo ciekawe.

Poseł Witold Zembaczyński (KO):

A to proszę wyjaśnić, czy to zależy od nawyków użytkownika.

Biegły Krzysztof Dyki:

Nie.

Poseł Witold Zembaczyński (KO):

Czy od podatności?

Biegły Krzysztof Dyki:

To zależy… NSO z niewiadomego dla mnie powodu skupia się… skupiało się na iPhone'ach. Z niewiadomego dla mnie powodu skupia statystycznie więcej exploitów, posiadali tych, niewymagających kliknięcia, więcej exploitów, tych zero-day, zero-click, o które pan słusznie pyta. To, co nie jest wiadome w przestrzeni publicznej,

a co ja tu zeznaję pod odpowiedzialnością karną, to większą skuteczność bez klikania mają na urządzeniach iPhone. Więc to mnie też zawsze zastanawia, że jest takie przeświadczenie, że iPhone jest bezpieczniejszy. Pegasus…

Poseł Witold Zembaczyński (KO):

A jeśli chodzi o wykrywalność infekcji czy tam…

Biegły Krzysztof Dyki:

Wykrywalność była w obu przypadkach, czy Android, iPhone, czy inny smartfon taka sama, czyli zerowa.

Poseł Witold Zembaczyński (KO):

No, ale przecież mamy słynne raporty, między innymi przygotowane przez Citizen Lab…

Biegły Krzysztof Dyki:

Tak.

Poseł Witold Zembaczyński (KO):

…które dowodzą, że na poziomie kodu binarnego była możliwość dojścia do schematu zakażenia przy użyciu iOS, a przy wypadku Androida poprzez otwarte źródła instalacji aplikacji było to niemożliwe. Czy biegły podtrzymuje te…

Biegły Krzysztof Dyki:

Myślałem, że chodzi o… Jeżeli mówimy o Citizen Labie, mówiąc o wykrywalności zerowej, to mówię o zdolności smartfonu do wykrycia.

Poseł Witold Zembaczyński (KO):

Do wykrycia infekcji.

Biegły Krzysztof Dyki:

A jeżeli mówimy po infekcji…

Poseł Witold Zembaczyński (KO):

Tak, post factum.

Poseł Marcin Bosacki (KO):

Przez użytkownika.

Biegły Krzysztof Dyki:

…czyli informatyka śledcza, użytkownika, badamy smartfon, podobnie to wygląda na iPhonie i na Androidzie.

Poseł Witold Zembaczyński (KO):

To dlaczego właśnie Citizen Lab otwierał tę ścieżkę wyłącznie dla telefonów z użyciem systemu operacyjnego iOS? Jeżeli chodzi o wykrycie infekcji post factum, nie z poziomu użytkownika urządzenia, tylko z poziomu laboratoryjnego.

Biegły Krzysztof Dyki:

Przyznam, że nawet nie wiedziałem tej analizy, czy one… Citizen Lab oczywiście znam, ale nie wiedziałem, że one też głównie dotyczyły iOS.

Poseł Witold Zembaczyński (KO):

To tam był taki argument, że Android uniemożliwia wykrycie post factum na poziomie laboratoryjnym…

Biegły Krzysztof Dyki:

Umożliwia.

Poseł Witold Zembaczyński (KO):

Czyli według biegłego umożliwia.

Biegły Krzysztof Dyki:

Umożliwia, tylko wymaga większej pracy ręcznej. W przypadku iPhone'a wykrycie jest dlatego możliwe, że iPhone ma bardzo mocno nałożone ograniczenia, izolację uprawnienia i w przypadku ataku Pegasus ma trudniej…

Poseł Witold Zembaczyński (KO):

Chodzi o… (*niezrozumiałe*)

Biegły Krzysztof Dyki:

…trudniej Pegasusowi się wymazuje ślady, ale w obu przypadkach jest możliwe udowodnienie obecności Pegasusa. Z tym że w ostatnich latach, szczególnie właśnie po tej aferze medialnej, NSO i nie tylko NSO bardzo mocno zainwestowało, właśnie dzięki też analizom Citizen Lab, Recorded Future i innym analizom, zainwestowało bardzo mocno w niewykrywalność, czyli w wymazywanie śladów. Wcześniej to było…

Poseł Witold Zembaczyński (KO):

No właśnie.

Biegły Krzysztof Dyki:

Czyli teraz jest znacznie ciężej post factum stwierdzić, czy był Pegasus. Czyli te analizy Citizen Labu obróciły się przeciwko Citizen Labowi.

Poseł Witold Zembaczyński (KO):

Właśnie o to chciałem biegłego dopytać, bo mam tutaj takie pytanie z nr 21, nie mylić się z oczkiem… Dlaczego NSO reklamowało właśnie Pegasusa jako niewykrywalne narzędzie, a de facto pozostawał ten ślad w oprogramowaniu zarówno jednego i drugiego systemu operacyjnego, który to umożliwiał? Czy to był tylko chwyt marketingowy, czy chodziło o fakt niewykrywalności z poziomu użytkownika?

Biegły Krzysztof Dyki:

Ta niewykrywalność Pegasusa jest… Możemy ją porównać obrazowo, metaforycznie do niewykrywalności amerykańskich myśliwców. Ona jest, jest faktem, ale jeżeli wlatują i jest konfrontacja na przykład z Rosją, to się okazuje…

Poseł Witold Zembaczyński (KO):

…że je widać.

Biegły Krzysztof Dyki:

…że to działa, ale nie tak jak się reklamuje. Więc to jest ta niewykrywalność Pegasusa. Rzeczywiście on bardzo mocno usuwa ślady swojego działania, natomiast rzeczywiście na iOS jest nieco trudniej usunąć te ślady niż na Androidzie, ale w obu przypadkach one zostają. To jest pytanie o to, jak wiele dni poświęcimy na analizę – dni, nie godzin – na analizę smartfonu. Jeżeli chcemy w kilka godzin, to możemy nic nie znaleźć. W kilka dni może być ciężko, a w kilkanaście możemy odnaleźć, ale prawie nikt nie robi tyle analizy.

Poseł Witold Zembaczyński (KO):

Czy Polska posiada możliwości techniczne analizy, współczesnej analizy również użycia takiej cyberbroni?

Biegły Krzysztof Dyki:

Polska posiada ekspertów zdolnych do takiej analizy. W żadnej z istniejących instytucji państwowych nie ma takiej jednostki, ale kompetencje techniczne są aż w nadmiarze w Polsce.

Poseł Witold Zembaczyński (KO):

Rozumiem.

Biegły Krzysztof Dyki:

Przepraszam. Taki przykład grupa Dragon Sector i firma NEWAG, udowodnili to, pomimo tego, że to nie był Pegasus.

Poseł Witold Zembaczyński (KO):

Ale to poprzez tę odwróconą inżynierię.

Biegły Krzysztof Dyki:

Tak, dokładnie, odwróconą inżynierię. Czyli takie kompetencje wystarczają w zupełności do tego, nie żeby zrobić Pegasusa, ale żeby zlecić to, o czym pan mówi, czyli te

same osoby byłyby w stanie, lub im podobne, te same lub im podobne byłyby w stanie stwierdzić – tu był Pegasus.

Poseł Witold Zembaczyński (KO):

Dobrze. Proszę świadka, jeszcze proszę powiedzieć, czy w tamtym czasie, kiedy pojawiło się na rynku oprogramowanie typu Pegasus, polskie środowisko prawne, pytam też świadka, jako osobę doświadczoną w służbach specjalnych, było przystosowane do funkcjonowania tego typu narzędzia pracy, techniki operacyjnej.

Biegły Krzysztof Dyki:

Tak, tu byśmy pewnie rozpoczęli debatę trochę akademicką, przy której nie jestem godzien, nie mam takich kompetencji. Wiem, że są te wątpliwości co do interpretacji. Sam od lat prowadzę, w zasadzie nie ja, do mnie raczej dzwonią koledzy z różnych miejsc, debatując na ten temat, różne są opinie. Na pewno wymaga nasz system prawny doprecyzowania tej kwestii, wobec tej klasy narzędzi, tak jak zrobiono to czy w Stanach Zjednoczonych, czy w Niemczech. Bardzo szybko, prosto i binarnie, zero-jedynkowo po prostu to dopuszczono.

Poseł Witold Zembaczyński (KO):

Dziękuję za tę odpowiedź.

Biegły Krzysztof Dyki:

Dziękuję.

Poseł Witold Zembaczyński (KO):

Proszę powiedzieć, proszę biegłego, zważywszy na pana doświadczenie jako właśnie biegłego sądowego, czy zatem możemy powiedzieć, że wykorzystanie Pegasusa przez CBA nosiło znamiona przestępstwa z art. 130 Kodeksu karnego. Ja na tym etapie przesłuchania zadaję to pytanie, między innymi z uwagi na to, że ten artykuł odnosi się do szpiegostwa, a już tutaj padły te informacje, że nie można wykluczyć, że informacje z podsłuchów Pegasusem były dostępne dla obcych wywiadów, co najmniej wywiadu izraelskiego, to oczywiście będziemy ustalać. Natomiast czy tutaj w kontekście wiedzy jako biegły może się pan wypowiedzieć? Chodzi o art. 130, czyli kwestia szpiegostwa na rzecz obcego wywiadu.

Biegły Krzysztof Dyki:

Znam ten artykuł, oczywiście, i też inne, o których można by tutaj debatować w kontekście zaistniałej sytuacji. W mojej ocenie nie ma dzisiaj dowodów świadczących o wypełnieniu znamion takiego czynu, ale jednocześnie chciałbym podkreślić, że tu absolutnie też nie jestem radcą prawnym.

Poseł Witold Zembaczyński (KO):

To jest kwestia do ustalenia, która nam odpowie na pytanie…

Biegły Krzysztof Dyki:

Tak.

Poseł Witold Zembaczyński (KO):

…kiedy przeanalizujemy proces infekcji, szyfrowania i umowy. Bardzo dziękuję.

Czy jako biegły może pan powiedzieć, czy wykorzystując Pegasusa, CBA mogło popełnić przestępstwo z art. 234 Kodeksu karnego, mówiącym o fałszywym oskarżaniu innej osoby, co jest oczywiście przestępstwem zagrożonym karą pozbawienia wolności do lat 5? To w nawiązaniu do zmanipulowanych wiadomości z telefonu Krzysztofa Brejzy.

Biegły Krzysztof Dyki:

Tylko w sytuacji udowodnienia takiej manipulacji.

Poseł Witold Zembaczyński (KO):

Jaka jest droga, z wiedzy biegłego sądowego, do udowodnienia takiej sytuacji?

Biegły Krzysztof Dyki:

Badanie z zakresu informatyki śledczej, które musiałoby wykazać, że funkcjonariusz danej służby, osoba oskarżona albo po pozyskaniu materiału dowodowego dokonała jego nieuprawnionej, tym samym bezprawnej modyfikacji, albo druga sytuacja – stworzyła taki materiał dowodowy. Tylko w takiej sytuacji.

Poseł Witold Zembaczyński (KO):

No właśnie, tutaj mamy też pytanie o kwestię odpowiedzialności z art. 235 Kodeksu karnego, mówiącym o tym, że tworzenie fałszywych dowodów, to właściwie w korelacji z poprzednim artykułem, jest przestępstwem zagrożonym do lat 5 i to jest również ta materia, którą Komisja będzie na bieżąco ustalać, między innymi w oparciu o naprowadzenie, które tutaj z zeznania biegłego uzyskaliśmy.

Można tutaj rozwijać również kolejne pytanie, czy nie popełniono tutaj przestępstwa również z art. 236 Kodeksu karnego, mówiącym, że zatajenie dowodów niewinności danej osoby jest przestępstwem zagrożonym karą pozbawienia wolności, więc jak widać, środowisko prawne było nieprzygotowane na wprowadzenie Pegasusa do użycia. Stąd moje pytanie: Czy z wiedzy świadka jako biegłego NSO w kontaktach tych międzynarodowych kładło nacisk na swoich klientów w aspekcie przygotowania środowiska prawnego, legalizmu, czy jest prawdopodobieństwo, że Beata Szydło, na przykład jako premier, która dokonywała tej pierwszej słownej umowy z premierem Izraela, musiała – czy wynika to z wiedzy biegłego w oparciu o inne doświadczenia, inne kazusy – gwarantować to, że środowisko prawne w danym kraju, otoczenie prawne jest przygotowane do tego, żeby nabywca mógł używać legalnie Pegasusa, bo przecież czymś te obostrzenia musiały być licencyjne, umowne?

Biegły Krzysztof Dyki:

To jest problem… to jest dobre pytanie, ponieważ to jest problem tej kategorii ogólnie. Narzędzia nie dotyczą tylko NSO, producenci tej kategorii narzędzi w celu maksymalizacji swoich zysków, działalności biznesowej do tego są powołani, stworzeni. Rzeczywiście jest taka tendencja u nich na skupieniu się na technologii, skupieniu się na działalności gospodarczej, na generowaniu i maksymalizacji zysków. Troska o ład prawny w danym kraju nie jest ich priorytetem.

Poseł Witold Zembaczyński (KO):

To nie był priorytet.

Biegły Krzysztof Dyki:

To nie jest priorytet, nie mówię, że nie ma znaczenia, natomiast prywatna firma ma zarabiać.

Poseł Witold Zembaczyński (KO):

Ale nie wiemy, czy takie pytania przy tych negocjacjach standardowo z dostawcą takiej cyberbroni się pojawiają?

Biegły Krzysztof Dyki:

Nie słyszałem o takich pytaniach. Próbuję sobie przypomnieć treści umów, które widziałem, polskiej nie widziałem i tam chyba nie było nawet też takich zapisów.

Poseł Witold Zembaczyński (KO):

Nie było.

Biegły Krzysztof Dyki:

Zgodnie… bardziej ogólnie gdzieś widziałem, że „użycie zgodne z prawem”, ale to koniec.

Poseł Witold Zembaczyński (KO):

Proszę biegłego, my również badamy inne systemy zajmujące się zbieraniem danych. Między innymi napotkaliśmy takie oprogramowanie zakupione przez polską prokuraturę o nazwie Hermes, służące do zaawansowanej analizy danych w Internecie. Czy biegły coś na temat tego oprogramowania wie więcej poza tym, co Komisja w trakcie przesłuchań gdzieś dopytywała?

Biegły Krzysztof Dyki:

Ja kojarzę kiedyś wywiad, nie pamiętam, gdzie, ale to było kilka lat temu, w którym pytano mnie dokładnie na tę okoliczność. I jeżeli dobrze pamiętam – nie pamiętam tej sytuacji, ale pamiętam, że wtedy dokładnie się wypowiadałem na ten temat – to chodziło prawdopodobnie o oprogramowanie analityczne.

Poseł Witold Zembaczyński (KO):

Tak.

Biegły Krzysztof Dyki:

To gdzieś w mediach, pamiętam, pomylono kwestię właśnie oprogramowania szpiegowskiego z oprogramowaniem do informatyki śledczej i oprogramowaniem analitycznym. Natomiast to tylko bardzo słabo, przez mgłę pamiętam, zwracam uwagę.

Poseł Witold Zembaczyński (KO):

A gdzie jest ta granica, proszę powiedzieć między tą analizą kryminalistyczną a np. takim programem Hermes, który dokonuje zaawansowanej analizy, również przy użyciu otwartych źródeł, ale potrafi te dane w jakiś sposób restrukturyzować, zagregować i przedstawić w sposób niedostępny dla innych tego typu urządzeń? Czy to już jest forma inwigilacji według biegłego?

Biegły Krzysztof Dyki:

Nie. Mamy trzy kategorie oprogramowania, które są w zainteresowaniu państwa, organów państwa i służb specjalnych. Pierwsza kategoria, ta najcięższa, to jest oprogramowanie klasy Pegasus do inwigilacji elektronicznej.

Poseł Witold Zembaczyński (KO):

To jest waga najcięższa? To jest super heavyweight, tak?

Biegły Krzysztof Dyki:

Najcięższa, absolutnie tak. Nieco lżejsza kategoria wagowa to jest oprogramowanie informatyki śledczej…

Poseł Witold Zembaczyński (KO):

(*niezrozumiałe*)

Biegły Krzysztof Dyki:

…w wyniku którego pozyskujemy dowody, podłączamy urządzenia, analizujemy, czyli np. w wyniku zatrzymania czynności, przeważnie procesowych, śledczych zabezpieczamy urządzenia i badamy to na okoliczność istnienia informacji, które mogą być dowodami… To jest informatyka śledcza. I to jest ta druga kategoria.

Trzecia, najlżejsza, to jest znowu jeszcze inna kategoria oprogramowania bardzo często stosowanego w obszarach państwa. Mam wrażenie, że o to chodziło w prokuraturze. To jest oprogramowanie do analityki i otwartego wywiadu, analizy otwartych źródeł informacji i analityki tych informacji. Czyli tak, znajdują się w nich często różne roboty przetwarzające masowo otwarte źródła informacji, które syntezują, tak jak pan mówi, te informacje, przedstawiają wyniki w postaci…

Poseł Witold Zembaczyński (KO):

To jest profilowanie osobowości?

Biegły Krzysztof Dyki:

Nie, to nie jest… to jest profilowanie…

Poseł Witold Zembaczyński (KO):

Ale na przykład użytkownika…

Biegły Krzysztof Dyki:

To jest zebranie informacji o danej osobie prawnej lub fizycznej, czyli o człowieku lub firmie, instytucji, organizacji. I to są systemy, które zbierają na podstawie białego wywiadu, czyli analizy otwartych źródeł informacji, informacje o danej osobie, ale podkreślam, na podstawie otwartych źródeł informacji. To jest istotne. Nie ma szpiegowania,

nie ma przełamywania zabezpieczeń, nie ma analizy naszych urządzeń, nie ma zgody sądu, bo nie jest wymagana. Co ciekawe, w tej właśnie kategorii rozwiązań, które służą do białego wywiadu, analizy otwartych źródeł informacji, ostatnio… w ostatnich latach obumiera ten rynek, ponieważ regulacje prawne, szczególnie europejskie, de facto zabiły te produkty i technologie. Uniemożliwiają automatyczną analizę. Czyli z jednej strony korporacje amerykańskie co miesiąc, można powiedzieć, już naprawdę co miesiąc wprowadzają bardzo duże restrykcje. Z drugiej strony Unia Europejska wprowadza bardzo duże restrykcje i te narzędzia stają się… nie chcę powiedzieć nielegalne, ale niemożliwe do wykorzystania w aktualnym porządku prawnym.

Poseł Witold Zembaczyński (KO):

Ale chodzi ogólnie o kwestie profilowania w Internecie, tak, czy…

Biegły Krzysztof Dyki:

Zbierania informacji, bo to nie… chyba że przez to rozumiemy profilowanie, zbierania informacji o osobie, osobach lub powiązaniach.

Poseł Witold Zembaczyński (KO):

Tak, analiza wpisów, kont społecznościowych, aktywności itd. Rozumiem.

Biegły Krzysztof Dyki:

Tak, są takie narzędzia. Tak.

Poseł Witold Zembaczyński (KO):

Ale oczywiście co do mocy Pegasusa to porównanie…

Biegły Krzysztof Dyki:

Kompletnie żadnego nie ma, w związku, żadnego.

Poseł Witold Zembaczyński (KO):

Kompletnie nie ma.

To może jeszcze ostatnie pytanie, bo tutaj już mam presję czasową. Proszę powiedzieć, czy Pegasus na przykład dawał takie możliwości, oprócz tych przestępstw, o które ja pytałem, czyli zbieranie fałszywych dowodów czy zatajanie czyjejś niewinności, hipotetycznie, czy też dawał na przykład możliwości wyczyszczenia komuś konta bankowego.

Biegły Krzysztof Dyki:

Pegasus…

Poseł Witold Zembaczyński (KO):

Czy to się tyczyło tylko komunikatorów, Signal, WhatsApp?

Biegły Krzysztof Dyki:

Nie, nie tylko, bo również przeglądarki i inne aplikacje, ale…

Poseł Witold Zembaczyński (KO):

Ale czy na przykład według biegłego wiedzy była możliwość ingerowania w inne aplikacje, na przykład w aplikacje, nie wiem, odnośnie zdrowia, mamy takie publiczne usługi, czy bankowe aplikacje, randkowe, wszystkie jedno jakie, inne niż służące do klasycznej komunikacji?

Biegły Krzysztof Dyki:

Nie… Pegasus nie umożliwiał wykonywania operacji w imieniu użytkownika na żadnej z aplikacji, pomimo posiadania takiego potencjału technologicznego, nie umożliwiał takiej funkcjonalności użytkownikowi.

Poseł Witold Zembaczyński (KO):

Czyli tak mówiąc kolokwialnie, dla zwykłego Kowalskiego, mam nadzieję, że nie Janusza, który to ogląda, czyli Pegasus to był taki skaner, taki czytnik zawartości, jakby to nazwać?

Biegły Krzysztof Dyki:

Pegasus służył, tak, do pobierania danych ze smartfonu osoby inwigilowanej. Natomiast rzeczywiście dochodziło do takich sytuacji, znam takie sytuacje i nie mówię o Polsce,

gdzie ktoś uzyskiwał zgodę na zakres A, a przeglądał sobie konto, operacje, tak, oczywiście tak, ale nie wykonywał operacji, tylko przeglądał coś.

Poseł Witold Zembaczyński (KO):

Czyli konto można było przejrzeć?

Biegły Krzysztof Dyki:

Tak, całe, oczywiście.

Poseł Witold Zembaczyński (KO):

OK, konto, czyli wszystko, każda jedna aplikacja była możliwa do otwarcia, do spenetrowania.

Biegły Krzysztof Dyki:

Nie, nie, Pegasus… Pegasus, jeżeli jesteśmy przy tym konkretnym narzędziu, o nim mówimy, to to konkretne narzędzie nie umożliwiało uruchomiania aplikacji, natomiast umożliwiało wgląd w to, co robi użytkownik. Jeżeli otworzę swój smartfon, to operator mógł widzieć, co ja robię. Jeżeli wchodzę na konto, to on to widzi…

Poseł Witold Zembaczyński (KO):

Na żywo.

Biegły Krzysztof Dyki:

…i jeżeli ja pobieram wyciągi, a pobieram na swoim smartfonie i zapisuję, to również operator je widzi, wszystko, co ja zapisuję, to on też to widzi. I czy to pochodzi z aplikacji bankowej, z kryptogiełd, walut – to nie ma znaczenia, operator to widzi.

Poseł Witold Zembaczyński (KO):

A w jaki sposób się to… ta transmisja tego obrazu… czy to były zrzuty w formie PDF-u, czy…

Biegły Krzysztof Dyki:

Nie, zrzuty w formie grafik, w formie najczęściej JPG, różne formaty.

Poseł Witold Zembaczyński (KO):

JPG, tak?

Biegły Krzysztof Dyki:

Tak, w formie bitmap.

Poseł Witold Zembaczyński (KO):

A dźwięk w formie zapisu MP3, czy…

Biegły Krzysztof Dyki:

Dźwięk był ostatecznie MP3, tam były jakieś próby stosowania innych algorytmów, ale chyba ostatecznie, z tego, co pamiętam, stanęło – przynajmniej te moduły, które ja widziałem – na MP3, bo on jest najłatwiej otwieralny. Najbardziej kompatybilny format, bo są lepsze algorytmy, ale ostatecznie dla operatora… dla operatora, nie wiem, co by nie było, bo nie widziałem stacji operatorskiej, ale zakładam, że to było MP3.

Poseł Witold Zembaczyński (KO):

Dobrze. Ja już chciałem zakończyć, jeszcze tylko ostatnią taką konkluzją. Bo była mowa i często to się pojawia w przestrzeni publicznej, że Pegasus był narzędziem inwigilacji totalnej. Teraz proszę odpowiedzieć, czy to stwierdzenie odnosi się do tego, że miał możliwość np. włączania mikrofonu i nasłuchiwania otoczenia, w związku z tym jest to narzędzie inwigilacji totalnej, ponieważ nie jesteśmy w stanie wyłącznie skoncentrować się na figurancie, ale możemy nasłuchiwać otoczenia. Czy… z czego to potoczne określenie jako inwigilacji totalnej przyklejone do Pegasusa się brało? Chcę, żeby to wyjaśnił po prostu biegły, ekspert i nam opowiedział.

Biegły Krzysztof Dyki:

Ono mi się kojarzy trochę z II wojną światową, tam padały te hasła, wojna totalna, ze strony Niemiec. Natomiast nie wiem, autorem… co autor miał na myśli tych słów „inwigilacja totalna".

Poseł Witold Zembaczyński (KO):

Chodzi o moc Pegasusa, on jest wszechmogący, może włączyć kamerę, mikrofon, odczytać twoje maile, zobaczyć twojego Telegrama. Ale to słowo „totalna", czy można je połączyć np. z tym modułem obsługującym mikrofon, więc nasłuchiwanie otoczenia?

Biegły Krzysztof Dyki:

Ja będę trochę bardziej skromny, wierzę, że wszechmogący jest tylko Bóg, więc myślę, że Pegasus był bardzo mocny, jest najmocniejszy na pewno tak, ale nie wszechmogący, nie totalny. Miał ograniczenia, dalej ma ograniczenia, nie zawsze jest w stanie zainfekować bez interakcji z naszej strony, więc na pewno jest to dzisiaj również najlepsze publicznie dostępne narzędzie, publicznie w sensie dla rządów. Jest to najlepsze ciągle publicznie dostępne narzędzie, najmocniejsze, ale czy wszechmogące i totalne, mi się to kojarzy z pewnymi emocjami, które są mi obce.

Poseł Witold Zembaczyński (KO):

Bardzo dziękuję.

Biegły Krzysztof Dyki:

Dziękuję bardzo.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję.

Pan przewodniczący Bosacki, proszę uprzejmie.

Poseł Marcin Bosacki (KO):

Dziękuję bardzo, pani przewodnicząca.

Ja nie mam ambicji pytania pana o wszystko i zapytam o to, co w mojej ocenie jest kluczowe dla pana dotychczasowych zeznań, czyli ustalenie, ile mogły wiedzieć… operator… przepraszam, nie operator, twórca systemu, czyli grupa NSO, i potencjalnie, bo nikt z nas nie wyklucza takich możliwości, służby obcego kraju, czyli izraelskie. Czyli to, przed czym zabezpieczył się w pewnym momencie rząd Stanów Zjednoczonych. Pan cały czas podkreśla, że kluczowe dla odpowiedzi, ile one mogły wiedzieć, jest to, kto kontrolował sieć anonimizującą, tak?

Biegły Krzysztof Dyki:

Tak.

Poseł Marcin Bosacki (KO):

Ponieważ to z niej, nie z biurka operatora w Polsce, tylko z niej, atakowano fizycznie tych, których poddawano inwigilacji Pegasusem.

Biegły Krzysztof Dyki:

Tak, operatorowi mogło wydawać się, że to ja klikam i ja to robię, ale ja wydawałem polecenie do sieci, która z końcówki ostatniej stacji swojej sieci infekowała smartfon osoby inwigilowanej, tak.

Poseł Marcin Bosacki (KO):

Czyli z punktu widzenia operatora, czyli polskiej służby, czyli CBA, kluczowe jest to, kto kontrolował sieć anonimizującą. Natomiast jak to wygląda z punktu widzenia twórcy systemu, czyli NSO? Czy on… Ile on widzi, gdyby się okazało, że sieć anonimizująca nie jest jego albo on nie jest jej właścicielem?

Biegły Krzysztof Dyki:

Jeżeli nabylibyśmy taki produkt, kontrolując całą infrastrukturę stanowiącą ten produkt, wszystkie jego moduły i wykonując dodatkowo jeszcze testy bezpieczeństwa, które potwierdzają, jak to działa, to NSO nie powinno mieć żadnego dostępu i żadnej wiedzy. Tylko to musimy potwierdzić, po pierwsze, posiadając pełen dostęp do infrastruktury, po drugie, wykonując na początku testy bezpieczeństwa i pod tym warunkiem jesteśmy w stanie się upewnić, że NSO nie ma do niczego dostępu.

Poseł Marcin Bosacki (KO):

OK, tylko dwie uwagi. Jedna o tych klauzulach, o których rozmawiamy już od pewnego czasu, czyli że pewnych telefonów z pewnych sieci w pewnych krajach zgodnie z licencją nie można… dany operator nie może kontrolować.

Biegły Krzysztof Dyki:

Przepraszam, drobna uwaga, to nie wynika z licencji. To wynika… sam nie wiem z czego, raczej z technicznej konfiguracji. Nie jest to zapisane w licencji. Przynajmniej w tych umowach, których ja widziałem.

Poseł Marcin Bosacki (KO):

Pozwolę się z panem nie zgodzić.

Biegły Krzysztof Dyki:

Dobrze, i być może tu było, OK.

Poseł Marcin Bosacki (KO):

Pozwolę się z panem nie zgodzić. No, ale dobrze, powiedzmy, że Izrael sobie zastrzega, że…

Biegły Krzysztof Dyki:

W umowie mógł.

Poseł Marcin Bosacki (KO):

Na przykład, że nie można telefonów, niekoniecznie w Rosji, w Stanach Zjednoczonych… po to, żeby nie zadrażniać stosunków ze Stanami Zjednoczonymi. To w jaki sposób oni są w stanie to wyegzekwować, jeśli nie mają wpływu na to, kogo się atakuje, jeśli nie mają wpływu na sieć anonimizującą?

Biegły Krzysztof Dyki:

Bardzo dobre pytanie. W takim przypadku nie byliby w stanie wyegzekwować.

Poseł Marcin Bosacki (KO):

Nie byliby w stanie.

Biegły Krzysztof Dyki:

W tych umowach, które ja widziałem, nie było zapisów w treści umowy. One wynikały właśnie z tego, o co pan pyta, z konfiguracji.

Poseł Marcin Bosacki (KO):

Ale oczywiście wie pan, ja wiem to tylko… to już nie jest żadna wiedza z dokumentów, tylko z doniesień medialnych, zresztą głównie amerykańskich, że Izrael, abstrahując już od tej sprawy głośnej Polski, Węgier przede wszystkim, gdzie były jakby zastrzeżenia co do tego, kogo inwigilowano, w jaki sposób, czy zgodnie z prawem i tak dalej, ale Izrael też… były kraje, to już powiedziałbym, spoza kręgu Zachodu, którym odbierano licencję na Pegasusa, którym odbierano, właśnie z tego powodu, że on przekroczył to i zasięg tych, których można inwigilować, co do których się umówił zatwierdzaną przez rząd Izraela… w umowie zatwierdzanej przez rząd Izraela z firmą NSO. To jednak rozumiem, że standardem było to, że oni wszystko widzą, tak.

Biegły Krzysztof Dyki:

Standardem…

Poseł Marcin Bosacki (KO):

Ja mówię o krajach Arabskich, mówię o Meksyku częściowo, tam wszędzie, gdzie Izrael kupował polityczne wpływy, sprzedając Pegasusa.

Biegły Krzysztof Dyki:

Standardem… W standardowej konfiguracji Izrael posiadał kontrolę nad siecią anonimizującą i tym samym kontrolował te podmioty… kontrolował zdolność klienta do ataków poszczególnych krajów.

Poseł Marcin Bosacki (KO):

I to, czy on ewentualnie łamie, czy nie łamie jakieś zapisy umów…

Biegły Krzysztof Dyki:

Tak, bo z jednej strony mógł teoretycznie, nie widziałem, ale mógł wystąpić zapis pozwalający klientowi na coś albo zakazujący klientowi czegoś. W tych umowach, które ja widziałem kilku, nie było takiego zapisu, ograniczenia były… bo badałem wtedy w jaki sposób… więc oni na przykład wykluczali numery amerykańskie i to wtedy było… wynikało z konfiguracji infrastruktury, a nie z umowy, ale możliwe, że niektórzy mieli wprost jakieś zapisy w umowach.

Poseł Marcin Bosacki (KO):

OK.

Biegły Krzysztof Dyki:

Te umowy nie były wszystkie identyczne.

Poseł Marcin Bosacki (KO):

Czyli jednym słowem, wtedy kiedy będziemy mieli wiedzę o tym, kto miał kontrolę nad siecią anonimizującą w wypadku polskiej transakcji Pegasusa, będziemy wiedzieli, ile potencjalnie wiedziały niepolskie służby.

Biegły Krzysztof Dyki:

Dokładnie tak.

Poseł Marcin Bosacki (KO):

Dziękuję bardzo.

Biegły Krzysztof Dyki:

Dziękuję bardzo.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo dziękuję.

Pan poseł Patryk Jaskulski.

Poseł Patryk Jaskulski (KO):

Dziękuję bardzo, pani przewodnicząca.

Wysoka Komisjo, panie biegły, ja mam teraz serię pytań, które przygotował ekspert pana posła Śliza, który jest dzisiaj nieobecny.

Pierwsze pytanie. Wydaje się oczywistym z tego, co pan mówił, że nie mieliśmy dostępu do całości kodu źródłowego. Jak ze swojego doświadczenia oceni pan, czy korzystając z inżynierii wstecznej, jest pan w stanie, mając na uwadze ograniczenia deasemblerów, dekompilatorów czy analizatorów protokołów, stwierdzić ze 100% pewnością, że Pegasus jest absolutnie bezpieczny i dane uzyskiwane z jego wykorzystaniem są tylko i wyłącznie w posiadaniu państwa polskiego?

Biegły Krzysztof Dyki:

Nie wiem, czy dobrze odczytuję pytanie. Technicznie wiem, o co chodzi.

Poseł Patryk Jaskulski (KO):

Innymi słowy, czy mając na uwadze te techniczne ograniczenia, czy ABW, czy dowolne inne podmioty mogły skutecznie zweryfikować ten system pod kątem bezpieczeństwa?

Biegły Krzysztof Dyki:

Oczywiście, że tak. Do tego mamy niezbędne, tak jak mówiłem, kompetencje, przykładowe kategorie narzędzi, nie tylko te narzędzia, ale te, które pan wskazał w pytaniu, deasemblery, dekompilatory i również innego typu narzędzia do inżynierii wstecznej.

Natomiast to pytanie idzie trochę za głęboko, bo najpierw ono się powinno zatrzymać na… nie na aż tak niskopoziomowej, czyli zaawansowanej, bo „niskopoziomowe" w inżynierii wstecznej oznacza „bardzo dokładne", tak zaawansowanej inżynierii wstecznej. Ale pierwsza analiza, która… gdybym ja ją wykonywał, bo rozumiem, że pytanie jest skierowane do mnie, personalnie, to ona nie dotyczyłaby aż tak zaawansowanej inżynierii wstecznej w pierwszym kroku.

W pierwszym kroku ja bym chciał zobaczyć architekturę tego, co nabywam. W drugim kroku zbadać tego działanie, bez tych narzędzi, o których pan wspomniał.

Czyli w drugim kroku badam działanie, w pierwszej kolejności… sieciowe. Badam, co robi sieć tych modułów, poszczególnych stacji operatora, jak się komunikują z serwerem fizycznym, później siecią anonimizującą, co je tworzy i tak dalej, jak przebiega infekcja i w drugą stronę transmisja zwrotna. Do tego nie potrzebuję żadnych narzędzi, o których… które pan wymienił. Do tego potrzebuję znajomości zagadnień sieciowych, narzędzi sieciowych, snifferów, analizatorów tego typu. Więc tu badam behawioralnie, czyli pod kątem zachowania się, działania, tak zwaną analizę dynamiczną robimy, behawioralną, jak to coś działa na razie na poziomie sieciowym. I dopiero gdy ustalamy, wiemy, że rozumiemy, to nam odpowiada lub nie, dopiero przechodzimy dalej do tych narzędzi już, o których pan powiedział. Czyli możemy zrobić sobie analizę kodu, jeżeli kodów źródłowych nie udostępni nam NSO, bo może odmówić, nie musi udostępniać, to wtedy możemy przejść do analizy oprogramowania na stację operatora, na serwerze naszym fizycznym, w sieci anonimizującej i ostatnia końcówka, na przykład implant za pomocą tych narzędzi, które pan powiedział.

Stuprocentowa pewność to jest daleko idące sformułowanie, bo stuprocentowej pewności nie ma nikt. NSO… przepraszam, Citizen Lab po wydaniu kilkudziesięciu milionów dolarów na swoje badania… Nawiasem mówiąc, zachęcam do sprawdzenia, kto je sponsorował, bo we wszystkich tych organizacjach, które badały NSO, sponsorowała to jedna osoba, to taka ciekawostka na marginesie.

Poseł Witold Zembaczyński (KO):

Można powiedzieć, kto?

Biegły Krzysztof Dyki:

George Soros. Wszystkie organizacje, które badały Pegasusa publicznie, dzięki którym… na które państwo się powołujecie, jest jedna osoba, która sponsoruje te organizacje. To nie jest nic złego, tylko ciekawostka. Nie dwie osoby, jedna. Ale to może dobrze, bo dzięki temu jest dużo większa wiedza o tym narzędziu. Kilkadziesiąt milionów dolarów poszło na badania Citizen Labu, który popełnił sporo poważnych błędów. Często… może nie często… zdarzało się, że klasyfikował Pegasusa błędnie, tak zwane fałszywe alerty. Zdarzało się, że klasyfikował standardowe oprogramowanie jako Pegasusa.

Więc nie ma czegoś takiego jak 100% pewności w tej dziedzinie, której dotyczy pytanie. Mówimy o pewnym prawdopodobieństwie, czyli jeżeli wydajemy kilkadziesiąt milionów dolarów i potrafimy się nieraz pomylić, to wiemy, że to nie jest profesja binarna, zero-jedynkowa. Tu nie… W tej materii inżynierii wstecznej nie operujemy pojęciem 100%. Nic nie jest pewne, ponieważ jeżeli… Czego najlepszym świadectwem jest Pegasus. Jeżeli zapytamy Apple'a, który wydaje miliardy dolarów rocznie na swój system operacyjny, albo Microsoft, który wydaje 4 mld dolarów rocznie tylko na cyberbezpieczeństwo: „Czy ty jesteś na 100% bezpieczny", to oni powiedzą: „Nie, bo w tej materii wiemy, że nie ma czegoś takiego jak 100%. My minimalizujemy ryzyka".

Wracając do istoty pytania, 100% nigdy nie mamy, ale my rozmawiamy o pewnej odwrotności. My ze 100% zagrożenia, 100% braku wiedzy minimalizujemy ten brak wiedzy, nabywamy coraz więcej… więc dochodzimy… powinniśmy dochodzić do poziomu, w którym mówimy: OK, to nam wystarcza, ja się… ja uznaję, że to jest bezpieczne i Krzysztof Dyki się podpisuję pod tym, nabywając, że ja uważam, że to jest bezpieczne. Wtedy specjalista, który powinien to wykonać, czy w służbie lub poza służbą powinien się podpisać: tak, ja uważam, że to jest bezpieczne w zakresie. Nikt się nigdy nie podpisze, że to jest na 100% bezpieczne. Nie, on… zbadałem ten zakres i podpisuję, że to jest według mnie bezpieczne. Tak to się powinno odbywać. Na pewno nie 100%, o które pan pyta.

Poseł Patryk Jaskulski (KO):

Dobrze. Kontynuujemy pytania pana doradcy i pana Pawła Śliza.

Panie biegły, mając na względzie, że mówimy o dostarczeniu narzędzi do uzyskiwania dostępu do systemów informatycznych, dwa pytania. Czy model, w którym mielibyśmy zarządzać platformą analizy technicznej narzędzi, oznaczałoby to, że CBA musiałoby stawiać takie serwery proxy i nimi zarządzać, czy nadal byłaby to infrastruktura NSO, którą tylko my byśmy współzarządzali?

Biegły Krzysztof Dyki:

Nie do końca jestem… rozumiem pytanie, nie do końca jego szczegóły. Postaram się odpowiedzieć pomimo tego, bo chyba wiem, co autor miał na myśli. Mamy dwie… Mamy dwie możliwe sytuacje, czyli stawiam się teraz w roli, jeżeli to na mnie spoczywa polecenie zakupu tego, wdrożenie i to ma być…

Poseł Patryk Jaskulski (KO):

Ja może rozwinę…

Biegły Krzysztof Dyki:

Dobrze, bardzo proszę.

Poseł Patryk Jaskulski (KO):

…bo mam rozwinięcie jeszcze tego pytania, jeżeli pan ma wątpliwości, ono nie jest wystarczające. Więc wydaje się zatem, że NSO stawiał, zarządzał i kontrolował elementy PATM, a ewentualnie tylko przekazywane były prawa admina do danej służby, ale nadal podać należy w wątpliwość, czy nie ma tam zastosowanego backdoora. Nawet analiza na przykład ABW czy CBA uwzględniać musi, że mówimy o podmiocie, który sprzedaje system z exploitami zero-day. Możemy zatem stwierdzić, ale nigdy nie znajdziemy tej podatności, więc sprawdzanie jest tak naprawdę iluzoryczne.

Biegły Krzysztof Dyki:

Zawiła hipoteza i teza. Częściowo się zgadzam, częściowo nie. Ponieważ tak, jeżeli mamy sieć anonimizującą, to wbrew pozorom nie jest lot w kosmos. To jest zbiór serwerów opartych na mniej lub bardziej standardowym oprogramowaniu, bo nikt tego nie pisze. Dzisiaj gotowe są komponenty. Najczęściej nawet na darmowym, otwartym oprogramowaniu, które stawiamy takie serwery, czyli mówiąc prościej, jesteśmy w stanie zbudować bardzo bezpieczną sieć anonimizującą bez zakupu jakiejkolwiek licencji. Jeżeli mamy kompetencje, doświadczenie, możemy to zrobić.

Ale wiem, do czego pytanie zmierza, więc odpowiedź jest następująca. Mamy dwie kategorie możliwości: pierwsze to zbudować sami taką sieć, drugą to powiedzieć – drogie NSO, dobrze, wiemy, że robicie to lepiej, więc oddajcie nam ją w dyspozycję. I teraz trzecie zagadnienie, o którym pan mówi, czyli że NSO posiada takie możliwości, że być może jest exploit i tym samym kontrola staje się iluzoryczna. W przypadku rozwiązań sieciowych nie interesują nas exploity, bo exploity zawsze mogą być na wszystko. My mówimy o czymś innym, my nie mówimy o tym, że czy jest ryzyko zaatakowania takiej sieci, bo oczywiście tutaj pan ekspert ma rację, w każdej chwili jest, również exploitem. Zagadnienie dotyczy czego innego – czy my mamy kontrolę nad tą częścią infrastruktury. Czy jest ryzyko jej zaatakowania? Zgadzam się z ekspertem – jest. Czy 100% bezpieczeństwa jest? Nie, nigdy nie jest, w żadnej sytuacji. Również mój smartfon nie jest w 100% bezpieczny. Czyli mówimy o kontroli nad infrastrukturą, również możliwości, również w zakresie, wyobrażam sobie, nie tylko funkcjonowania tej sieci, ale i bezpieczeństwa, czyli to, co mówiłem wcześniej, my nie dajemy 100% gwarancji, my minimalizujemy ryzyko. Czyli dopełniamy staranności, należytej staranności, zachowujemy bezpieczeństwo, kontrolujemy tę infrastrukturę, zgadzając się z tym, że zawsze może być jakiś exploit, który coś niedobrego zrobi na każdym urządzeniu na świecie, tak.

Poseł Patryk Jaskulski (KO):

Obiecuję, że to ostatnie takie bardzo techniczne pytanie od doradcy.

Biegły Krzysztof Dyki:

Nie ma problemu.

Poseł Patryk Jaskulski (KO):

Czy orientuje się pan, czy nasza instalacja była on-premise, czy z dostępem chmurowym, bo dane pozyskiwane, przechowywane były chyba lokalnie na jakimś serwerze, który znajdował się w Polsce? Czy wiemy o tym? A skoro zakładamy, że jest jakiś element infrastruktury przygotowany w Polsce, ile mógł trwać montaż, instalacja takiego systemu wraz z odpowiednim szkoleniem personelu?

Biegły Krzysztof Dyki:

Nie wiem, w jakim modelu zakupiła Polska, natomiast z tego, co mi wiadomo, standardowym modelem był fizyczny serwer u klienta. Czasami on występował w tym samym pokoju, w którym jest operator, czasami w innym pomieszczeniu. Oczywiście najlepiej, żeby to było jak najbliżej. Super, gdyby było w jednym. To jeżeli chodzi o to, ile trwał montaż. To jest zwykły… widziałem te parametry, nie polskie, ale one bardzo podobnie wyglądają, bo to jest zwykły serwer. Ten serwer, który posiadał klient, jest zwykłym, klasycznym, normalnym serwerem, możliwym do zakupienia w normalnych sklepach. Oczywiście oprogramowanie na nim instalowane było inne, ale sprzęt był klasyczny. Instalacja, jeżeli mamy przywiezione te komponenty, to jest kilka godzin. Sama instalacja, uruchomienie kilka godzin, później próbne testy, ale całość się zamyka… można w 2 dni to zrobić z kawą, herbatą, ciastkami, ale uruchomienie kilka godzin, montaż. Dziękuję bardzo.

Poseł Patryk Jaskulski (KO):

Dziękuję bardzo w imieniu pana Pawła Śliza.

Teraz kilka jeszcze takich moich pytań, już nie tak technicznych.

Biegły Krzysztof Dyki:

Bardzo proszę.

Poseł Patryk Jaskulski (KO):

Znając funkcjonalność Pegasusa, jego możliwości, to, że tak naprawdę ten program dawał możliwość pełnego dostępu do telefonu z możliwością wgrywania dowolnych treści, czy można postawić tezę, że osoba, która została zaatakowana takim Pegasusem, jest w pełni bezbronna?

Biegły Krzysztof Dyki:

Jeżeli mówimy o przeciętnym, normalnym użytkowniku, tak.

Poseł Patryk Jaskulski (KO):

Czyli rozumiem, że jeżeli służby dokonywały jakiegoś ataku i na przykład wgrywały jakieś zdjęcia na przykład, to ta osoba, która padła ofiarą takiego złamania, włamu przez Pegasusa, jest w pełni bezbronna i można jej przypiąć dowolną de facto łatkę.

Biegły Krzysztof Dyki:

Jeżeli zakładamy złą wolę operatora, to on nie musi infekować tej osoby, żeby… może spreparować sobie materiały i powiedzieć: to pochodzi od tej osoby. Pamiętajmy, proszę to, na co zwracałem uwagę, że Pegasus w standardowej konfiguracji nie umożliwiał wgrywania materiałów na smartfon ofiary, więc przy złej woli nawet operatora on w standardowej konfiguracji nie miał możliwości wysłania niczego na smartfon ofiary. Jeżeli ktoś ma złą wolę i jest nieuczciwym, niebezpiecznym człowiekiem, który nigdy nie powinien pracować w organach państwa, to może zrobić prostą rzecz – może po prostu na stacji operatorskiej wgrać ten plik i przenosząc go już na dalszą infrastrukturę służbową do pracy operacyjnej i procesowej, powiedzieć, że to jest z tej infrastruktury, co jest prawdą, bo będzie pochodzić ze stacji operatora.

Poseł Patryk Jaskulski (KO):

Jak dobrze wiemy, dochodziło do wycieków – wycieków w mediach, danych, informacji, SMS-ów, które pochodziły z użycia Pegasusa. Jak pan myśli, co było źródłem tych wycieków? Kto był… Czy to były służby? Czy to były… Kto to mógł być?

Biegły Krzysztof Dyki:

Ja osobiście nie wierzę, że to pochodziło ze służb, bo nie chciałbym żyć w kraju, w którym służby kolportują takie materiały, więc ja osobiście wierzę i chcę wierzyć, że to jednak nie pochodziło ze służb.

Poseł Patryk Jaskulski (KO):

Myślę, że na ten moment więcej pytań nie mam. Dziękuję.

Biegły Krzysztof Dyki:

Dziękuję bardzo.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo dziękuję.

Jeszcze jedno pytanie zgłosiła pani poseł Joanna Kluzik-Rostkowska i myślę, że będziemy już zmierzać ku końcowi. Bardzo proszę.

Poseł Joanna Kluzik-Rostkowska (KO):

Ja chciałam tak podsumować i podejść do tego od takiej strony pozytywnej. Przyjmijmy, że jest pan osobą odpowiedzialną za zakup Pegasusa w Polsce. Sam pan powiedział, że to jest tego typu instrument, gdzie nie ma mowy o żadnym zaufaniu, w związku z tym musimy minimalizować ryzyka i musimy brać pod uwagę czarne scenariusze. Na co pan najbardziej zwróciłby uwagę wtedy, kiedy by to od pana zależało? Czy na wyciek danych, szczelność, kontrolę? Jak zdefiniowałby pan te najbardziej wrażliwe obszary przy zakupie?

Biegły Krzysztof Dyki:

W pierwszej kolejności interesowałoby mnie to, czy ja chcę to narzędzie do pracy operacyjnej, czy również procesowej i to by zdeterminowało moje podejście. W przypadku narzędzia do… który miałby generować materiały wyłącznie operacyjne, co też często ma głęboki sens w służbach, a szczególnie jeżeli mówimy o wywiadzie i kontrwywiadzie, to byłby inny model działania nieco. Natomiast jeżeli mówimy, zakładam, że pytanie dotyczy jednak waloru procesowego i że rozmawiamy o materiałach, które nie mają mieć tylko wartości operacyjnej, ale również, a nawet przede wszystkim procesową…

Poseł Joanna Kluzik-Rostkowska (KO):

Dwa w jednym może.

Biegły Krzysztof Dyki:

Dwa w jednym, tak. Czyli ten drugi wariant, bo procesowa musi wynikać z operacyjnej, bo operacyjne jest zastosowanie tego narzędzia i później materiał operacyjny staje się materiałem procesowym, uzyskując walor procesowy, to wiedząc, że chcę pozyskiwać takie… taki materiał, chciałbym po pierwsze, tak jak wspominałem, żeby on był legalny. Czyli chcę wiedzieć, że to, co kupuję, jest legalne.

Po drugie, chciałbym wiedzieć, że materiał, który pozyskuję, jest autentyczny. Nie ma wątpliwości co do jego autentyczności. Poprzez autentyczność rozumiem autentyczną postać, na przykład zdjęcia naszej rozmowy.

Po trzecie, chciałbym wiedzieć, czy jest to materiał dla mnie weryfikowalny, że osoba, która przedstawia mi taki materiał, mówi: „Krzysztof, słuchaj, zobacz, jest coś takiego", a ja mam wątpliwości i nie wiem, to chciałbym mieć możliwość zlecenia, powiedzenia: „OK, uruchamiamy weryfikację. Chcę uruchomić weryfikację, czy ten materiał pochodzi z urządzenia". To jest weryfikowalność osoby inwigilowanej.

W przypadku… Bardzo prostym przykładem jest kontrola operacyjna zwykła połączeń głosowych GSM, operatorów telekomunikacyjnych, którzy codziennie realizują bardzo duże liczby takich kontroli w naszym kraju, w innych krajach. Tam autentyczność uzyskujemy w sposób bardzo prosty. Po stronie operatora widzimy… mamy kopię, po stronie służby jest druga kopia, można autentyczność zweryfikować. Mamy systemy, które są zweryfikowane, zbadane, scertyfikowane, więc mamy autentyczność, mamy weryfikowalność. Wszystkie logi odkładają się po stronie operatorów, po stronie służby. Jest… Nie ma marginesu na nadużycia i chyba nigdy nie było poważnych nadużyć. Pomijamy ewentualnie stosowanie kilkudniowej kontroli bez zgody i zatwierdzenia później sądu. Natomiast w przypadku tego pytania interesowałoby mnie, czy to jest legalne, autentyczne, weryfikowalne i żeby to spełniało te atrybuty.

Podczas zakupu zleciłbym potwierdzenie tego przez jakąkolwiek osobę, czyli jeden podpis czyjś, tak, że to jest, spełnia te warunki, ponieważ… Nie da się tego zrobić, jeżeli nie mam pełnej kontroli nad systemem, to nie spełnia tych moich atrybutów, więc na potrzeby procesowe nie byłbym w stanie tego wykorzystać. Chyba że mam kontrolę nad infrastrukturą, zrobię testy, o których dzisiaj mówiłem, bezpieczeństwa, abstrahu-

jąc już od akredytacji, ale robię testy bezpieczeństwa, weryfikując to, co słusznie tutaj za pośrednictwem ekspert zapytał przed chwilą. Zlecam testy bezpieczeństwa infrastruktury, testy statyczne, testy dynamiczne, analizę behawioralną. Wiem, że to jest wykonane, to jest do zrobienia, to jest mierzalne, możemy to zmierzyć co do ilości dni, co do kosztów, są ludzie, albo ich mamy w służbach, albo zlecamy te testy na zewnątrz, bo mogę nie mieć kogoś w służbach, może mam kryzys kadrowy albo jest tyle pracy, że nie ma kiedy tak zwanej taczki załadować, to zlecam takie testy na zewnątrz. Wynajmuję osoby zaufane, może z jakiegoś NASK – Państwowego Instytutu Badawczego, może z innych jednostek albo biorę eksperta, ekspertów z rynku, którzy do mojej transakcji takiej wykonają mi i podpiszą się pod tym, że to tak działa, to jest bezpieczne. Albo jadę z nimi do Izraela, albo Izrael przyjeżdża tutaj, badamy to, prosimy o próbkę, albo na żywo to badamy. Ktoś się podpisuje pod tym, że tak, to jest weryfikowalne, to jest autentyczne, to jest bezpieczne. W przeciwnym przypadku miałbym fajne narzędzie, bardzo kuszące, potężne, ale o małej wartości biznesowej dla mnie, gdybym był po stronie klienta takiego jak CBA, to dla mnie biznesowa wartość byłaby mała, bo obawiałbym się kwestionowania waloru procesowego później, na poziomie sporu sądowego.

Poseł Joanna Kluzik-Rostkowska (KO):

Dziękuję bardzo.

Mam takie przypuszczenie, graniczące z pewnością, że gdybyśmy się trzymali tych wszystkich punktów, o których pan teraz mówił, tobyśmy po prostu Pegasusa w Polsce nie zakupili, tak, dlatego że nie mamy ani pełnej kontroli, ani nie mamy weryfikowalności.

Ostatnie pytanie. Czy spotkał się pan kiedyś z taką sytuacją, że ktoś, kto znał system Pegasus, ostrzegał, sugerował, oficera służb, który chciał taką kontrolę zlecić, żeby tego nie robił, bo właśnie będą takie konsekwencje, że nie można będzie np. tego użyć w kwestiach procesowych?

Biegły Krzysztof Dyki:

Nie pamiętam, czy to dotyczyło systemu Pegasus, ale takie debaty odbywały się i odbywają się w służbach od lat, tak. Nie chodzi chyba o samego Pegasusa, w ogóle o tej klasy narzędzia, a szczególnie przy braku tych walorów, o których mówię, to jeszcze głębsze są te debaty. Tak, one mają miejsce w służbach i to chyba wszystkich – słyszałem SKW, AW, CBŚ, KGP. Tak, to te debaty, wątpliwości, ta problematyka jest omawiana.

Poseł Joanna Kluzik-Rostkowska (KO):

Dziękuję bardzo.

Biegły Krzysztof Dyki:

Dziękuję bardzo.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo dziękuję.

Zmierzamy do końca, ale jeszcze na koniec, ponieważ my jako Komisja ponad miesiąc temu zwróciliśmy się do Prokuratury Krajowej o zabezpieczenie tych serwerów, narzędzi i systemu Pegasus znajdującego się w Centralnym Biurze Antykorupcyjnym i mam nadzieję, że ekspertyza wykonana przez biegłych da nam odpowiedź, myślę, na kluczowe pytanie, które warto, żeby opinia publiczna też usłyszała. Czy byliśmy właścicielami wszystkich części tego systemu, począwszy od tej pierwszej, czyli miejsca, gdzie operatorzy siedzieli i wbijali dany numer telefonu jako osobę, wobec której chcą zastosować kontrolę operacyjną, serwery, które znajdowały się na terenie, czy we władaniu naszych służb specjalnych, ale także tę sieć anonimizującą? I czy według pana ekspertyza wykonana w ramach tej czynności zleconej będzie nam mogła udzielić odpowiedzi na to pytanie?

Biegły Krzysztof Dyki:

W zakresie proporcjonalnym do profesjonalnego sformułowania treści pytań do biegłych, czyli tak, bo z ekspertyzami w tej kategorii w przedsięwzięciach jest tak, że wynik pracy

biegłych jest wprost proporcjonalny do jakości definicji zadań lub pytań do nich skierowanych. To jest kluczowe. Tak, jeżeli jest prawidłowo skierowane, jak najbardziej, tak.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dobrze. Tak że czekamy z niecierpliwością właśnie na tę ekspertyzę, którą wykonują biegli na zlecenie Prokuratury Krajowej na naszą prośbę.

Na końcu ostatnie pytanie, które nurtuje mnie od pewnego czasu. Czy CBA miało możliwość usuwania pozyskanych danych w 100%?

Biegły Krzysztof Dyki:

Z którego urządzenia?

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Rozumiem, że tego we władaniu, którego byli, czyli serwerów znajdujących się w CBA.

Biegły Krzysztof Dyki:

Aha, czyli na przykład serwera znajdującego się w fizycznym władaniu CBA i ze stacji operatorskich. Technicznie w jakimś zakresie, tak. W jakim? W takim, jakim mieli uprawnienia na tych stacjach. Czyli klient w zależności od posiadanych uprawnień… te uprawnienia mogą być niskie, wysokie, średnie – zakładam jednak, że wysokie, bo trudno mówić o innych – to może dokonywać tych… nie twierdzę, że dokonywał, ale na tak teoretycznie zadane pytanie, hipotetycznie, oczywiście takie, jakie klient ma uprawnienia, tak, może dokonywać modyfikacji danych zapisanych na dowolnym urządzeniu. Tak samo jak na smartfonie czy na komputerze.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

A o czym świadczyłby fakt, gdyby na przykład nie mógł czegoś takiego dokonać?

Biegły Krzysztof Dyki:

Jeżeli nie mógłby tego dokonać, to powstałoby pytanie, kto sprawował, kto posiadał uprawnienia administratora do fizycznych urządzeń posiadanych przez klienta. Wyobrażam sobie, gdybym ja to nabywał, to ja chcę posiadać te uprawnienia administratora i wtedy na tak zadane pytanie musiałbym odpowiedzieć: tak, mogę modyfikować, usuwać dane. Jeżeli nie posiadam uprawnień administratora jako klient, to trudno mi jest nawet sobie wyobrazić taką sytuację, bo powstałoby pytanie, kto posiada takie uprawnienia do serwera i do stacji operatorów.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Mam nadzieję, że na wszystkie pytania znajdziemy odpowiedzi i w wyniku pracy Komisji będziemy mogli przekazać również państwu.

Dziękuję w takim razie bardzo. Po sporządzeniu protokołu przesłuchania poinformujemy pana o terminie, w którym będzie pan mógł go podpisać. Na tym kończymy dzisiaj pierwszy punkt porządku dziennego. Bardzo dziękuję panu biegłemu za przybycie.

Biegły Krzysztof Dyki:

Dziękuję bardzo.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Przystępujemy teraz do rozpatrzenia punktu drugiego, czyli sprawy bieżące. Przystępujemy do rozpatrzenia wniosków dowodowych. Do Komisji wpłynęła prośba pana posła Patryka Jaskulskiego. Bardzo proszę w takim razie, jako pierwszy, o złożenie wniosku, którym zajmie się Komisja. Bardzo proszę o zgłoszenie doradcy.

Poseł Patryk Jaskulski (KO):

Bardzo dziękuję. Szanowna pani przewodnicząca, Wysoka Komisjo, chciałbym rekomendować na funkcję doradcy Komisji panią mecenas Joannę Martyniuk, która jest radcą prawnym, wpisaną na listę Okręgowej Izby Radców Prawnych w Szczecinie. Prowadzi swoją kancelarię prawną od lat, a w tym roku także kończy i planuje zdać doktorat na szkole doktorskiej na Uniwersytecie Zielonogórskim z zakresu nauk prawnych. Była też dziennikarką, niesamowicie bardzo kompetentna osoba. Uprzejmie proszę Wysoką Komisję o przegłosowanie pozytywne zaopiniowanie jej kandydatury na doradcę Komisji.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo dziękuję.

Przypominam, że Komisja po przyjęciu kandydatury na stałego doradcę zwraca się do Prezydium Sejmu o wyrażenie zgody na jej powołanie.

Teraz poddam pod głosowanie wniosek pana posła. Kto jest za przyjęciem kandydatury? Kto jest za? Kto jest przeciw? Kto się wstrzymał? Bardzo dziękuję.

Proszę o podanie wyników. 6 głosów za, 0 przeciw, 0 wstrzymujących się. Wniosek pana posła Patryka Jaskulskiego uzyskał większość.

W tej chwili Komisja wystąpi do Prezydium Sejmu z wnioskiem o powołanie pani Joanny Martyniuk-Plachy na stałego doradcę Komisji.

Czy są jeszcze jakieś wnioski, głosy w tej chwili? Nie słyszę, nie widzę. Zamykam w takim razie posiedzenie Komisji wobec wyczerpania punktu w porządku dziennego. Dziękuję państwu bardzo.