KOMENTARZ MIĘDZYNARODOWY PUŁASKIEGO
PULASKI POLICY PAPERS
www.pulaski.pl ISSN 2080-8852 2/2011

Bezpieczeństwo teleinformatyczne wyzwaniem dla Polski

Autor

Marcin Terlikowski

Rewolucja teleinformatyczna przyniosła głębokie konsekwencje dla wszystkich sfer życia. Umożliwiła powstanie całkowicie nowych form biznesu, zmieniła warunki działalności wielu tradycyjnych branż gospodarki, wpłynęła na sposoby nawiązywania i utrzymywania relacji międzyludzkich i spędzania wolnego czasu, a także wyznaczyła niektóre kierunki rozwoju kultury masowej. Przekształciła także środowisko bezpieczeństwa państw, generując nowego rodzaju zagrożenia, związane przede wszystkim z uzależnieniem społeczeństw od wielu różnych systemów teleinformatycznych. Zagrożenia te są wciąż słabo rozpoznane i przeanalizowane, a jednocześnie podlegają ciągłej ewolucji.

Marcin Terlikowski w swym artykule zastanawia się nad bezpieczeństwem teleinformatycznym Polski. „Ze względu na swoje zaangażowanie międzynarodowe, nie tylko wojskowe, polskie systemy teleinformatyczne mogą – i są – celem różnego rodzaju ataków; rozwija się też szara strefa cyberprzestępczości. W ostatnich latach dużo zrobiono dla zabezpieczenia polskiej cyberprzestrzeni, m.in. dzięki wysiłkom Agencji Bezpieczeństwa Wewnętrznego oraz środowisk informatycznych. Niemniej jednak wciąż potrzeba wielu działań".

Gorąco zachęcam do lektury najnowszego numeru „Komentarza Międzynarodowego Pułaskiego"!

Dominik Jankowski
Redaktor Naczelny „Komentarza Międzynarodowego Pułaskiego"

Marcin Terlikowski

Marcin Terlikowski
Analityk w Polskim Instytucie Stosunków Międzynarodowych, obszar badań: Wspólna Polityka Bezpieczeństwa i Obrony UE, europejski sektor obronny i rynek wyposażenia obronnego, bezpieczeństwo teleinformatyczne i wojna informacyjna. Autor kilkudziesięciu artykułów naukowych, analiz i raportów dotyczących m.in. misji WPBiO, rozwoju zdolności wojskowych na potrzeby UE, problemów przemysłu obronnego w Europie.
Współredaktor książki nt. znaczenia bezpieczeństwa teleinformatycznego dla nowoczesnego państwa („Bezpieczeństwo teleinformatyczne państwa", Warszawa 2009).
Od 2007 r. doktorant w Szkole Głównej Handlowej, przygotowywana rozprawa doktorska na temat polityki ekonomicznej państw UE wobec sektora obronnego.

Rewolucja teleinformatyczna przyniosła głębokie konsekwencje dla wszystkich sfer życia. Umożliwiła powstanie całkowicie nowych form biznesu, zmieniła warunki działalności wielu tradycyjnych branż gospodarki, wpłynęła na sposoby nawiązywania i utrzymywania relacji międzyludzkich i spędzania wolnego czasu, a także wyznaczyła niektóre kierunki rozwoju kultury masowej. Przekształciła także środowisko bezpieczeństwa państw, generując nowego rodzaju zagrożenia, związane przede wszystkim z uzależnieniem społeczeństw od wielu różnych systemów teleinformatycznych. Zagrożenia te są wciąż słabo rozpoznane i przeanalizowane, a jednocześnie podlegają ciągłej ewolucji.

Bezpieczeństwo (w) cyberprzestrzeni

Bezpieczeństwo teleinformatyczne najczęściej jest definiowane jako zachowanie dostępu do informacji, jej integralności (pewności, że nie została zmieniona bez wiedzy i zgody użytkownika) oraz poufności (pewności, że nie zostanie przejęta prze nieuprawnionego użytkownika). W uproszczeniu, można zatem stwierdzić, że warunkiem bezpieczeństwa jest prawidłowe funkcjonowanie systemów teleinformatycznych – bezawaryjne, pod pełną kontrolą użytkowników i bez niepowołanej ingerencji z zewnątrz. W takim ujęciu zagrożeniami będą wszelkie działania, zaniechania lub zdarzenia losowe, prowadzące do zakłóceń pracy systemów teleinformatycznych. Jednak trzeba przy tym zaznaczyć, bezpieczeństwo teleinformatyczne obejmuje nie tylko bezpieczeństwo samych systemów (bezpieczeństwo „cyberprzestrzeni"), włącznie z ich zabezpieczeniem przed uszkodzeniami fizycznymi, lecz także bezpieczeństwo ich użytkowników (bezpieczeństwo „w cyberprzestrzeni"). W tym drugim wymiarze zagadnienia techniczne są tylko jednym z szeregu problemów – pracujący prawidłowo system może bowiem generować zagrożenia dla jego użytkowników, ze względu na treści, które są w nim przetwarzane i udostępniane.
Lista zagrożeń bezpieczeństwa teleinformatycznego obejmuje przede wszystkim działania celowe: tworzenie i rozprzestrzenianie złośliwego oprogramowania (działając automatycznie, modyfikuje ono funkcjonowanie zainfekowanych nim systemów bez wiedzy i zgody użytkowników, co potocznie, choć nie do końca poprawnie, określane jest terminem „wirus komputerowy") oraz zdalne, nieuprawnione manipulacje w obcych systemach (potocznie – „ataki internetowe", np. ataki paraliżujące pracę wybranych za cel systemów lub ataki służące wykradaniu danych, włącznie z oszustwami internetowymi).
Z wąskiej perspektywy bezpieczeństwo teleinformatyczne dotyczy technicznych parametrów pracy poszczególnych systemów i nie uwzględnia szerszego kontekstu ich funkcjonowania – ekonomicznego, społecznego, politycznego itp. W dobie ekspansji cyberprzestrzeni takie ujęcie jest jednak niepełne – inne jest bowiem znaczenie prawidłowego funkcjonowania komputera wykorzystywanego w gospodarstwie domowym lub małej sieci pracującej w przedsiębiorstwie, a inne – rozległych systemów sterujących np. dostarczaniem elektryczności czy gazu. Z tego powodu generalizowanie zagrożeń i przenoszenie doświadczeń zebranych z małych systemów na skalę państwa jest częściowo błędne i może sprzyjać niewłaściwej ocenie zagrożeń.
Istotą bezpieczeństwa teleinformatycznego państwa są następstwa występowania zakłóceń w pracy systemów, związane wprost ze stopniem uzależnienia życia społeczno-gospodarczego od komputerów i sieci elektronicznych. Dla państwa bezpieczeństwo cyberprzestrzeni ogranicza się do tych systemów, których dysfunkcja może spowodować negatywne i szeroko odczuwalne w społeczeństwie skutki. Przedmiotem szczególnej uwagi państwa będą sieci sterujące infrastrukturą krytyczną kraju, tj. przede wszystkim sieci wykorzystywane w przesyle mediów, przemyśle, sektorze finansowym, siłach zbrojnych

Fundacja im. Kazimierza Pulaskiego | Casimir Pulaski Foundation
ul. Oleandrów 6, 00-629 Warszawa, tel. +48 22 658 04 01, office@pulaski.pl

oraz sieci telekomunikacyjne organów administracji publicznej oraz służb. Destabilizacja wszystkich tych systemów, w skrajnym scenariuszu, mogłaby doprowadzić do bardzo poważnych konsekwencji – paraliżu normalnego funkcjonowania całego kraju (zakłócenia dostaw elektryczności lub gazu, łączności służb ratowniczych i porządkowych, elektronicznych rozliczeń sektora bankowego), a nawet wystąpienia szkód materialnych (katastrofy techniczne w przemyśle i transporcie oraz skażenia). Ze względu na lawinowy wzrost liczby usług realizowanych przez Internet, także paraliż tej sieci miałby odczuwalne skutki dla życia społeczno-gospodarczego, choć nie byłyby one tak poważne, jak w przypadku systemów związanych z infrastrukturą krytyczną.
Z drugiej strony systemy użytkowników indywidualnych, nawet większych przedsiębiorstw, nie powinny być przedmiotem szczególnej uwagi państwa i jego służb – zwiększenie liczby sieci podlegających specjalnej ochronie osłabiałoby bowiem zdolność do sprawnego przeciwdziałania najpoważniejszym zagrożeniom. Nie znaczy to oczywiście, że państwo nie powinno działać na rzecz zwiększenia stopnia bezpieczeństwa tych systemów, np. poprzez regulacje prawne czy kampanie informacyjne.

Haker - terrorysta czy złodziej?

Z perspektywy państwa, drugim czynnikiem decydującym o stopniu zagrożenia bezpieczeństwa teleinformatycznego jest źródło (sprawca) zagrożeń i motywacja za nim stojąca. Pierwszymi zidentyfikowanymi podmiotami, które dokonywały zdalnych, nieuprawnionych manipulacji w sieciach komputerowych byli „hakerzy" – osoby, dla których pokonanie zabezpieczeń obcych systemów było rodzajem rozrywki intelektualnej. Zagrożenie ze strony hakerów jest relatywnie małe – ich motywacją jest włamanie do systemu samo w sobie, a nie jego niszczenie (są jednak osoby, które po włamaniu jednak niszczą system, np. usuwając dane); poza tym obecnie wydaje się to być działalność o bardzo małej skali nasilenia.
Za zagrożeniami może też jednak stać motywacja polityczna. Już w latach dziewięćdziesiątych notowano ataki będące formą elektronicznego protestu, np. w 1999 r., w czasie nalotów NATO na Serbię, zaatakowano witryny internetowe Sojuszu, umieszczając na nich treści proserbskie i antyamerykańskie (na gruncie studiów nad bezpieczeństwem, w USA działalność taką określono terminem „haktywizm" jako aktywność polityczną hakerów). Zagrożenia generowane przez haktywizm są poważniejsze niż w przypadku hakerów, jednak wciąż ograniczają się w zasadzie wyłącznie do niszczenia witryn WWW lub paraliżowania pracy serwerów pocztowych. Nie grożą zatem państwu jako całości, a co najwyżej poszczególnym instytucjom i ich mniej istotnym systemom.
Pojawienie się ataków elektronicznych motywowanych politycznie stało się jednak pewną cezurą w myśleniu o bezpieczeństwie teleinformatycznym państwa. Status cyberprzestrzeni jako nowej areny potencjalnego konfliktu politycznego, angażującego państwa, a także podmioty pozapaństwowe oraz systemy elektroniczne w funkcji broni, został bowiem powszechnie uznany (wcześniej jedynie w wojskowości istniała doktryna walki informacyjnej; dotyczyła one jednak raczej tylko sił zbrojnych i czasu wojny).
W obszarze zagrożeń motywowanych politycznie poważnym zagrożeniem jest cyberterroryzmu, tj. przeprowadzanie ataków terrorystycznych wyłącznie z użyciem systemów teleinformatycznych. W sprzyjających warunkach zorganizowane ugrupowania terrorystyczne, dysponujące odpowiednimi zasobami finansowymi i osobowymi, mogłyby zaatakować systemy sterujące infrastrukturą krytyczną kraju i, manipulując ich funkcjonowaniem, byłyby w stanie wywołać co najmniej paraliż funkcjonowania państwa (np. poprzez wyłącznie dostaw energii elektrycznej), a nawet doprowadzić do poważnych zniszczeń materialnych (np. wywołując katastrofy techniczne i ekologiczne), czy strat w ludziach (np. powodując wypadki w elektronicznie sterowanym transporcie kolejowym).

Niemniej jednak, jak do tej pory nie odnotowano przypadków cyberterroryzmu – wydaje się bowiem, że stopień skomplikowania tego rodzaju ataków oraz niepewność ich rezultatów zniechęca organizacje nastawione na szybkie rezultaty do podejmowania prób tak niekonwencjonalnych działań.
Bardzo poważnym źródłem zagrożeń są też inne państwa, mające najłatwiejszy spośród wymienionych do tej pory podmiotów, dostęp do pieniędzy, sprzętu i osób potrzebnych do przeprowadzania ataków. W tym przypadku podstawowym problemem jest szpiegostwo elektroniczne. Wykorzystanie kanałów elektronicznych do przesyłania i przetwarzania informacji niejawnych powoduje, że wywiady wielu państw regularnie prowadzą operacje wywiadowcze w cyberprzestrzeni. Zwłaszcza państwa znajdujące się w stałym konflikcie ze społecznością międzynarodową mogą prowadzić tego rodzaju działania szpiegowskie na masową skalę. Z kolei rządy uwikłane w nierozwiązane konflikty regionalne mogą nawet uciekać się do aktów sabotażu elektronicznego, tj. destabilizowania lub niszczenia wybranych systemów.
Nie można wreszcie nie wspomnieć o motywacji ekonomicznej, stojącej za sprawcami ataków elektronicznych. Dynamiczny rozwój internetowych usług finansowych i handlowych pozwolił na rozkwit przestępczości wykorzystującej wyłącznie działania w cyberprzestrzeni. Poprzez różnego rodzaju oszustwa i kradzieże poufnych danych, cyberprzestępcy okradają swoje ofiary lub wyłudzają od nich pieniądze (inną powszechną formą cyberprzestępczości jest wysyłanie niechcianej korespondencji reklamowej, tzw. „spamu"). Relatywnie duża zyskowność cyberprzestępczości opiera się o niskie koszty i skalę działania – jeśli spośród kilkunastu milionów prób oszustwa, dokonywanych często przy użyciu zaledwie kilkunastu komputerów, powiedzie się choćby promil, to przestępcy są w stanie okraść tysiące indywidualnych osób i nieuczciwie zarobić setki tysięcy dolarów. Z perspektywy użytkownika indywidualnego, cyberprzestępczość jest chyba najpoważniejszym zagrożeniem. Cyberprzestępcy nie mają jednak ani potencjału, ani interesu, aby działać przeciwko państwu i jego instytucjom, z ich strony zagrożenie bezpieczeństwa państwa należy zatem ocenić jako względnie małe, choć zarazem ten rodzaj przestępczości należy stanowczo zwalczać.

Bezpieczeństwo teleinformatyczne A.D. 2011

Ostatnie trzy lata przyniosły szereg wydarzeń, które każą zredefiniować postrzeganie problematyki bezpieczeństwa teleinformatycznego państwa. Pierwszym z nich były ataki elektroniczne na Estonię w 2007 r., największy jak do tej pory przypadek tzw. „ataku DDoS", polegającego na celowym zalaniu urządzeń elektronicznych potokiem przypadkowych danych, powodującym ich przeciążenie i zablokowanie. Ataki wywołały paraliż estońskiego Internetu, który utrudnił funkcjonowanie setek tysięcy osób w całym kraju, choć nie wywołał szkód materialnych czy poważnych strat finansowych. Konsekwencje tych wydarzeń były jednak szerokie – ataki się sygnałem ostrzegawczym dla wielu rządów, obnażając słabość (lub brak) mechanizmów reagowania w odniesieniu do tak nietypowej sytuacji (brak, słabość lub złe umocowanie prawne rządowych zespołów komputerowego reagowania kryzysowego – CERT). Wkrótce po atakach Sojusz Północnoatlantycki, Unia Europejska oraz m.in. USA, Wielka Brytania, Francja czy Niemcy, utworzyły instytucje i procedury, które mają umożliwiać sprawną rekcję rządów (i organizacji międzynarodowych) w przypadku powtórzenia się estońskiego scenariusza (np. NATO, na szczycie w Bukareszcie w 2008 r., przyjęło specjalną strategię cyberbezpieczeństwa).
Ataki na Estonię ujawniły także inny, rosnący problem bezpieczeństwa cyberprzestrzeni – ogromną skalę działalności przestępczej. Były one możliwe dzięki specjalnym sieciom komputerów, liczącym setki tysięcy maszyn i wykorzystywanych na co dzień do popełniania

Fundacja im. Kazimierza Pulaskiego | Casimir Pulaski Foundation
ul. Oleandrów 6, 00-629 Warszawa, tel. +48 22 658 04 01, office@pulaski.pl

przestępstw (tzw. sieci „botnet", powstające głównie z komputerów należących do różnych użytkowników, zainfekowanych odpowiednimi złośliwymi programami). Ich powstanie to rezultat wykładniczego wzrostu aktywności przestępczości internetowej w ciągu ostatnich kilku lat. Obecnie można już wręcz mówić o globalnym w swym zasięgu czarnym rynku, na którym handluje się narzędziami do popełniania przestępstw elektronicznych (np. właśnie botnetami, a także wirusami czy wykrytymi lukami w zabezpieczeniach programów – tzw. explotami). Oferuje się także kompleksowe usługi w tym zakresie, np. kradzież danych. Rynek ten służy głównie zorganizowanym grupom cyberprzestępczym, które źródłem swych stałych zysków uczyniły np. oszustwa na klientach bankowości elektronicznej. Z tego rodzaju narzędzi i usług korzystać też mogą podmioty motywowane politycznie, zarówno niepaństwowe, jak i np. agencje rządowe.

Kolejnym istotnym wydarzeniem były ujawniane sukcesywnie od 2008 r. akty masowego szpiegostwa elektronicznego w USA, Niemczech, Francji i Norwegii. Niezidentyfikowani sprawcy (spekulowano o chińskich źródłach ataku), nie wykryci przez dłuższy okres, uzyskali dostęp do różnych sieci rządowych, z których udało im się skopiować dane zawierające miliony stron dokumentów. Choć, jak podkreślały pokrzywdzone rządy, nie było wśród nich informacji niejawnych, to doszło do jednego z największych w historii wycieków informacji. Ataki te uwidoczniły głównie cechę charakterystyczną elektronicznego procesu przetwarzania informacji, tj. fakt, że jednorazowe uzyskanie dostępu do systemu pozwala na wykradzenie bardzo dużej ilości danych przetwarzanych w tym systemie. Szpiegostwo, kojarzące się dawniej z mikrodrukiem czy szyfrogramami, zyskało tym samym charakter masowy.

Następstwa dla postrzegania problematyki bezpieczeństwa cyberprzestrzeni dwóch wydarzeń z ostatnich tygodni 2010 r. (afery Stuxnet i Wikileaks) nie są jeszcze w pełni jasne. Pojawienie się wirusa Stuxnet, specjaliści uznali przez za pierwszy w historii przypadek programu stworzonego w celu uszkodzenia precyzyjnie określonego systemu elektronicznego – program celował bowiem wyłącznie w systemy sterujące specyficznymi maszynami przemysłowymi. Co jednak najistotniejsze, w opinii ekspertów Stuxnet powstał w wyniku pracy całego zespołu programistów, którzy mieli dostęp do różnorodnych narzędzi elektronicznych oraz poufnych informacji (np. architektury systemu, który miał być zniszczony). Motywacja jego twórców nie jest znana – media sugerowały, że zadaniem Stuxneta było sparaliżowanie programu jądrowego Iranu, jednak brakuje na to przekonywujących dowodów. Pojawiły się też opinie, że jest to swoisty demonstrator technologii lub test instrumentu, który w niedalekiej przyszłości posłużyć może do prowadzenia wojny elektronicznej. Niezależnie od spekulacji, przypadek Stuxneta pokazuje, że środki finansowe i odpowiednie zasoby ludzkie już obecnie pozwalają tworzyć bardzo destrukcyjne, a zarazem selektywnie działające programy, w praktyce będące rodzajem elektronicznej broni. Nie ma powodów, aby odrzucić założenie, że tego rodzaju ataki mogą pojawić się również w przyszłości.

Z kolei w przypadku afery Wikileaks kluczowe wyzwanie to potencjał manipulacji opinii publicznej dzięki dysponowaniu tak wielką liczbą poufnych informacji. Choć jak do tej pory z nielegalnie ujawnionych depesz Departamentu Stanu USA nie wynikają sensacyjne treści, to nie można zapomnieć, że w innym potencjalnym wycieku informacje mogłyby być ujawniane selektywnie lub wśród prawdziwych przecieków mogłyby się pojawić informacje fikcyjne. Takie działania pozwoliłyby na manipulowanie opinią publiczną, a w skrajnym przypadku także rządami. Wikileaks ilustruje zatem aspekt bezpieczeństwa „w cyberprzestrzeni" – prawidłowe działanie systemów nie oznacza, że nie jest przetwarzana w nich informacja selektywnie dobrana lub nawet fikcyjna, której zadaniem jest stymulowanie określonych poglądów czy zachowań. Ten wymiar bezpieczeństwa teleinformatycznego, istotny także dla państwa, pozostaje jednak bardzo słabo zanalizowany.

Wszystkie omówione wyżej aspekty bezpieczeństwa teleinformatycznego w równym stopniu dotyczą Polski i powinny być brane pod uwagę w procesach formułowania myśli strategicznej i głównych założeń polityki bezpieczeństwa kraju. Ze względu na swoje zaangażowanie międzynarodowe, nie tylko wojskowe, polskie systemy teleinformatyczne mogą – i są – celem różnego rodzaju ataków; rozwija się też szara strefa cyberprzestępczości. W ostatnich latach dużo zrobiono dla zabezpieczenia polskiej cyberprzestrzeni, m.in. dzięki wysiłkom Agencji Bezpieczeństwa Wewnętrznego oraz środowisk informatycznych. Niemniej jednak wciąż potrzeba wielu działań – upowszechnienia i uporządkowania wiedzy nt. bezpieczeństwa teleinformatycznego, dokonania spójnej analizy znaczenia różnych aspektów tej problematyki dla bezpieczeństwa narodowego, opracowania spójnego modelu działań na rzecz podniesienia bezpieczeństwa wszystkich kluczowych dla kraju systemów, zwiększenia współpracy z sektorem prywatnym, a także – stworzenia i przećwiczenia schematów działań , jasno określających kompetencje instytucji i służb państwowych w sytuacjach kryzysowych.

Fundacja im. Kazimierza Pulaskiego | Casimir Pulaski Foundation
ul. Oleandrów 6, 00-629 Warszawa, tel. +48 22 658 04 01, office@pulaski.pl

Fundacja im. Kazimierza Pułaskiego

jest niezależnym, apolitycznym think tankiem specjalizującym się w polityce zagranicznej, którego misją jest propagowanie wolności, sprawiedliwości i demokracji oraz wspieranie działań mających na celu umacnianie społeczeństwa obywatelskiego. Fundacja prowadzi swoją działalność zarówno w Polsce jak i za granicą ze szczególnym uwzględnieniem Europy Środkowej i Wschodniej, jak i Ameryki Północnej.

Fundacja mogła powstać dzięki przemianom politycznym, które nastąpiły w Polsce po 1989 roku. Ideały generała Kazimierza Pułaskiego (wolność, sprawiedliwość i demokracja) stanowią inspirację dla wszelkich inicjatyw podejmowanych przez Fundację. Działania Fundacji obejmują m.in.: prowadzenie badań naukowych, opracowywanie publikacji i analiz, przygotowywanie seminariów oraz konferencji, edukowanie i wspieranie liderów www.instytutprzywodztwa.pl

Fundacja jest organizatorem Warszawskiego Regionalnego Kongresu Organizacji Pozarządowych www.warsawcongress.pl, Akademii Młodych Dyplomatów www.akademia.diplomacy.pl oraz wydawcą Platformy Komunikacyjnej dla Organizacji Pozarządowych www.non-gov.org

Fundacja przyznaje Nagrodę im. Kazimierza Pułaskiego „Rycerz Wolności" dla wybitnych postaci zasłużonych w promowaniu demokracji. Nagrodę dotychczas otrzymał profesor **Władysław Bartoszewski,** profesor **Norman Davies**, **Alaksandar Milinkiewicz**, lider demokratycznej opozycji na Białorusi, prezydenci **Lech Wałęsa**, **Aleksander Kwaśniewski**, **Valdas Adamkus** oraz wysoki przedstawiciel ds. wspólnej polityki zagranicznej i bezpieczeństwa **Javier Solana**.

Fundacja Pułaskiego jest jedną z dwóch polskich organizacji pozarządowych posiadających status organizacji partnerskiej Rady Europy. Więcej o Fundacji na www.pulaski.pl

Komentarz Międzynarodowy Pułaskiego

to pogłębione analizy istotnych dla Polski zagadnień z zakresu polityki międzynarodowej, gospodarki światowej bądź bieżących wydarzeń w polskiej polityce. Dokument publikowany jest w dwóch wersjach językowych, polskiej i angielskiej. Osoby chcące publikować swoje oryginalne prace w Komentarzu proszone są o kontakt z Redaktorem Naczelnym p. **Dominikiem Jankowskim** djankowski@pulaski.pl Żeby regularnie otrzymywać kolejne numery KMP należy podać swój e-mail na stronie www.pulaski.pl

Fundacja im. Kazimierza Pulaskiego | Casimir Pulaski Foundation
ul. Oleandrów 6, 00-629 Warszawa, tel. +48 22 658 04 01, office@pulaski.pl