STANISŁAW KOZIEJ Łatwiej dokonać cyberataku, niż się przed nim bronić – mówi szef BBN w rozmowie z Agatonem Kozińskim

Nie jesteśmy gotowi na cyberwojnę

1 września 1939 r. Polska okazała się nieprzygotowana do wojny. Dziś ważną areną konfliktu są sieci informatyczne. Jak byśmy sobie poradzili, gdyby 1 września 2012 r. wybuchła cyberwojna?
Pytanie jest o tyle zasadne, że jedną z najistotniejszych cech cyberwojny jest to, że może ona wybuchnąć nagle, bez widocznych zewnętrznie przygotowań. W związku z tym nawet pytanie o jutro ma strategiczny sens. Ale odpowiedź nie jest łatwa – wymaga nieco szerzej refleksji.

Zamieniam się w słuch.
Charakter konfliktów uległ ogromnej zmianie od czasów II wojny światowej. Przestrzeń wirtualna i zasoby informatyczne stanowią obecnie jeden z istotniejszych elementów naszego życia, a rozwój technologii związanych z eksploatacją sieci coraz częściej wykorzystywany jest do wrogich działań poprzez atakowanie infrastruktury krytycznej państw lub dokonywanie cyberataków mających na celu wykrycie i zniszczenie danych. Przykładem jest chociażby atak z wykorzystaniem zaawansowanej broni cybernetycznej na elektrownie atomowe w Iranie. Przyszłe konflikty prawdopodobnie będą się toczyć również w cyberprzestrzeni jako naturalnym obszarze walki zbrojnej. Już obecnie niektóre z państw deklarują, że cyberataki traktowane będą na równi z naruszeniem suwerenności kraju i obywateli.

Trochę ucieka Pan od pytania. Pytałem, jak Polska jest przygotowana na odparcie takich cyberataków.
Zdajemy sobie sprawę z wagi i złożoności zagrożeń występujących w cyberprzestrzeni, dlatego też sukcesywnie budowany jest zintegrowany system bezpieczeństwa uwzględniający bezpieczeństwo zasobów informatycznych. Biorąc pod uwagę przypadki podejmowania wrogich działań także przez podmioty państwowe, należy w najbliższej przyszłości uwzględnić konieczność rozpoczęcia budowy także ofensywnych zdolności cybernetycznych jako wsparcia działań konwencjonalnych. Przygotowanie Polski na potencjalny cyberatak jest stale analizowane, a mechanizmy ochronne są doskonalone.

Jak mogłyby wyglądać takie ofensywne zdolności cybernetyczne? Mielibyśmy mieć przygotowane np. wirusy komputerowe, za pomocą których infekowalibyśmy sieci informatyczne innego państwa?
Powiedzmy na początku, że budowa zdolności ofensywnych to bardzo wrażliwy temat i żaden kraj nie jest skłonny o nim konkretnie opowiadać. To problem o wiele trudniejszy niż rozmowa o własnym, konwencjonalnym potencjale uderzeniowym. Bo tak naprawdę środki ofensywne stosowane w cyberprzestrzeni są co do swej istoty inne niż klasyczne środki uderzeniowe. Proszę zauważyć, że sama rozmowa o nich już jest jakąś ofensywą w infosferze. A działania w cyberprzestrzeni są integralną, nieodłączną częścią działań w szerszym środowisku, jakim jest infosfera, wręcz przeplatają się z innymi operacjami informacyjnymi. Dlatego gdy mówimy o ofensywie czy kontrofensywie w razie cyberwojny, musimy mieć na uwadze zintegrowane operacje destrukcyjne w stosunku do przeciwnika prowadzone za pomocą środków zarówno o charakterze cybertechnicznym, jak i czysto informacyjnym, np. dezinformowanie przy wykorzystaniu mediów, ale także środków oddziaływania kinetycznego, np. przy pomocy sił specjalnych.

Wiadomo, że najlepszą obroną jest atak. Ale czy jesteśmy w stanie odeprzeć uderzenia cybernetyczne innych krajów?
Biuro Bezpieczeństwa Narodowego w będącym już na ukończeniu Strategicznym Przeglądzie Bezpieczeństwa Narodowego uwzględnia również zagrożenia dla cyberbezpieczeństwa. Także z inicjatywy BBN nastąpiła nowelizacja ustaw o stanach nadzwyczajnych, która wprowadziła do obiegu prawnego kategorię cyberprzestrzeni. W jej rezultacie powinna następować stopniowa aktualizacja pod tym kątem właściwych planów operacyjnych. Mimo tych wszystkich działań nie ulega wątpliwości, że nie jesteśmy jeszcze przygotowani na odparcie cyberagresji na dużą skalę, gdyby taka nastąpiła. W razie cyberwojny ponieślibyśmy duże straty. Nawet mniejsze operacje cyberwojenne lub akty cyberdywersji byłyby bardzo niebezpieczne. Ale też trzeba pamiętać, że dziś nikt na świecie nie ma pewnej, gwarantowanej obrony przed agresją w cyberprzestrzeni. Trzeba raczej mówić o minimalizacji strat. Ale to nie jest coś zaskakującego. To jest ogólna zasada sztuki wojennej. Atak dzięki możliwości zaskoczenia jest zawsze łatwiejszy, obrona jest o wiele trudniejszą dziedziną sztuki wojennej. Od czasów najdawniejszych nic się tutaj nie zmieniło: zawsze prościej i łatwiej było rzucić kamieniem, niż się przed nim osłonić.

Dziennik „Kommiersant" donosi, że rosyjski wywiad testuje sposoby manipulowania rzeczywistością za pomocą portali społecznościowych. Niewykluczone, że te testy obejmą też Polskę. Jak sobie radzić z takimi – potencjalnymi na szczęście – zagrożeniami?
Tego rodzaju działania stanowią jeden z elementów coraz bardziej intensywnej i niemal codziennej walki informacyjnej. Już starochiński filozof i teoretyk wojen Sun-Tzu podkreślał ogromną rolę manipulacji. Dzisiaj te klasyczne reguły zyskują większe możliwości wcielenia ich w życie dzięki rewolucji informacyjnej. W zmaganiach w infosferze czysto defensywne środki są wyjątkowo mało efektywne. Bierna obrona przed manipulacją, podstępem, fortelem, dezinformacją na niewiele się zda. Ochrona cyberprzestrzeni musi więc obejmować nie tylko obronę przed istniejącymi lub potencjalnymi zagrożeniami, ale także zdolności ofensywne: potrzebne czy to w taktycznym kontrataku lub większej kontrofensywie, czy też w strategicznych działaniach uprzedzających, prewencyjnych. Dodajmy do tego, że mówimy nie tylko o zmaganiach między wyspecjalizowanymi siłami i środkami dwóch przeciwstawnych stron. Rewolucja informacyjna włącza w nie całe społeczeństwa. Z tego względu wobec wykorzystywania internetu i portali społecznościowych do cyberszpiegostwa, przestępstw ekonomicznych, kradzieży tożsamości czy właśnie manipulacji opinią publiczną szczególnego znaczenia nabiera jak najszersza edukacja o bezpieczeństwie informacyjnym.

Jak wygląda system zabezpieczeń na wypadek cyberataków na Polskę? Kto odpowiada za cyberbezpieczeństwo kraju: wojsko czy policja?
I wojsko, i policja, i wszystkie służby. Ale nie tylko. Tak naprawdę wszystkie struktury państwa – publiczne i niepubliczne – muszą być w to zaangażowane. Muszą działać w swoim interesie i działać w imię bezpieczeństwa państwa. Cyberbezpieczeństwo, podobnie jak nowoczesne bezpieczeństwo w ogóle, musi być działaniem kompleksowym, zintegrowanym. W świecie wirtualnym widzimy lustrzane odbicie tych wszystkich wyzwań, potrzeb i problemów bezpieczeństwa, które występują w realu. A dzisiaj podstawowym wyzwaniem wobec bezpieczeństwa jest konieczność zintegrowanego doń podejścia. Mówię o konieczności, bo niestety w praktyce dopiero takie podejście zaczynamy kształtować. Jesteśmy na początku drogi. Wierzę, że Strategiczny Przegląd Bezpieczeństwa Narodowego, który na polecenie prezydenta prowadzimy, będzie momentem przełomowym. Także w podejściu do cyberbezpieczeństwa. Bo dziś mamy na tym polu działania raczej rozproszone, resortowe, agencyjne, instytucjonalne.

Jak ten system działa w praktyce? Kto tak naprawdę odpowiada za cyberbezpieczeństwo w Polsce?
Oczywiście za całość odpowiada władza wykonawcza. To przede wszystkim kompetencje rządu. Realizowane są głównie przez ministra spraw wewnętrznych, ministra obrony narodowej, szefa Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu oraz dyrektora Rządowego Centrum Bezpieczeństwa. Należy też pamiętać, że Polska posiada ogólnokrajowe systemy przeciwdziałania atakom, które stanowią sektorowe punkty kontaktowe systemu. Z punktu widzenia wzmacniania zdolności sojuszniczych i procesu dostosowywania instytucjonalnego w zakresie cyberobrony ważnym jest przystąpienie w ubiegłym roku Polski do Centrum Obrony Cybernetycznej NATO w Tallinie. Ale powtórzę raz jeszcze kwestię, moim zdaniem, najważniejszą – potrzebna jest integracja zarządzania bezpieczeństwem w cyberprzestrzeni, stopniowe scalanie różnych działań różnych instytucji wokół jednego strategicznego planu i programu.

W razie cyberwojny ponieślibyśmy duże straty. Nawet mniejsze akty cyberdywersji byłyby niebezpieczne. Możemy jedynie próbować minimalizować wielkość strat

Bardzo groźne byłoby uderzenie na sieci informatyczne polskich instytucji finansowych – zablokowanie wirtualnego obiegu pieniędzy między bankami mogłoby kompletnie sparaliżować Polskę. Jak jesteśmy przed tym zabezpieczeni?
Należy pamiętać, że większość instytucji finansowych to przedsiębiorstwa prywatne, tak więc trudno jest określić stopień przygotowania poszczególnych podmiotów na tego typu zdarzenia. Niepokojąca jest także ogólna niechęć niektórych podmiotów do ujawniania informacji o naruszeniach bezpieczeństwa w ich sieci. O skali ujawnionych ataków możemy dowiedzieć się z raportów CERT Polska opracowanych na podstawie zgłoszonych naruszeń przestrzeni wirtualnej, natomiast ochrona zasobów własnych i ponoszenie nakładów na doskonalenie systemów ochronnych leży w kompetencjach samych podmiotów gospodarczych. W przypadku małych i średnich przedsiębiorstw wygospodarowanie środków na zabezpieczenie sieci, w połączeniu ze zbyt niską świadomością o potencjalnych zagrożeniach stanowią newralgiczny element całości infrastruktury, który może zostać wykorzystany przy planowaniu cyberataków na wielką skalę. Jednak sektor bankowy wydaje się jednym z najlepiej przygotowanych w tym zakresie.

Jak Pan przed chwilą zauważył, duża część newralgicznych instytucji w kraju, na przykład banki, znajduje się w rękach prywatnych. W jaki sposób państwo dba o ich bezpieczeństwo w internecie? Czy to w ogóle rola państwa?
Z atakami na zasoby informatyczne banków mamy do czynienia od wielu lat. Stopień informatyzacji tego sektora jest bardzo wysoki, dlatego też jest to obszar wyjątkowo atrakcyjny dla cyberprzestępców. Chociażby na początku tego roku mieliśmy do czynienia z dużym atakiem hakerskim w Izraelu, gdzie skradziono i upubliczniono tysiące danych z kart kredytowych. Wzrasta też liczba skutecznych ataków na duże przedsiębiorstwa handlowe i korporacje. Niektóre z państw zapowiadają, że cyberataki także na zasoby gospodarcze będą traktowane jako naruszenie suwerenności kraju i obywateli. Jednak jak dotychczas rola państwa – będącego gwarantem bezpieczeństwa ekonomicznego – polega w głównej mierze na zapewnieniu właściwych podstaw prawnych i mechanizmów efektywnego ścigania sprawców przestępstw w cyberprzestrzeni, a także dążeniu do rozszerzania współpracy w sferze ochrony przed atakami na sektor prywatny. Biorąc pod uwagę elementy infrastruktury krytycznej będące własnością prywatnych kontrahentów, a mających często strategiczne znaczenie dla bezpieczeństwa kraju, współpraca na tej płaszczyźnie stanowi kluczowy element skuteczności zintegrowanego systemu bezpieczeństwa. To wszystko też pokazuje konieczność integracji spraw cyberbezpieczeństwa.

Jest to możliwe?
Wierzę, że tak. Dlatego chciałbym zakończyć apelem o zrozumienie dla idei wdrażania zintegrowanego podejścia do spraw bezpieczeństwa narodowego w ogóle, a w tym stosownie także do spraw cyberbezpieczeństwa. Myślę, że właściwą do wdrażania tej idei instytucją na szczeblu rządowym, wokół której mogłoby następować ponadresortowe spinanie i koordynowanie spraw cyberbezpieczeństwa, mogłoby być podległe bezpośrednio premierowi Rządowe Centrum Bezpieczeństwa o poszerzonych w stosunku do dzisiejszych kompetencjach.

Rozmawiał Agaton Koziński

prof. Stanisław Koziej, generał brygady w stanie spoczynku, były wiceminister obrony, obecnie szef Biura Bezpieczeństwa Narodowego