Biuletyn OPINIE FAE
nr 6/2014

Andrzej KOZŁOWSKI

Cyberwojownicy Kremla

Rosja, jako państwo z imperialnymi ambicjami, dostrzega szanse i zagrożenia związane ze wzrostem znaczenia cyberprzestrzeni dla bezpieczeństwa kraju. Nie ogranicza się tylko i wyłącznie do działań obronnych, często wykorzystując swoich hakerów do ofensywnych akcji wymierzonych w swoich wrogów – tak zewnętrznych, jak i wewnętrznych.

Rosyjskie bezpieczeństwo cybernetyczne

Gwałtowna informatyzacja całego świata, która nastąpiła na początku lat 90. ub. wieku wraz z upowszechnieniem internetu doprowadziła do sytuacji, w której coraz więcej ludzi, przedsiębiorstw oraz usług rządowych zostało przeniesionych do świata wirtualnego, włączając w to obsługę kluczowych obiektów infrastruktury państwowej. Fakt ten niesie ze sobą implikacje dla bezpieczeństwa państwa, jak też stwarza nowe możliwości prowadzenia działalności o charakterze ofensywnym, nastawionym na wyrządzenie szkód potencjalnemu przeciwnikowi. Rosja nie jest tutaj wyjątkiem. Wprawdzie jej instytucjonalne struktury działalności w cyberprzestrzeni nie są tak rozwinięte, jak np. w Stanach Zjednoczonych, to jednak FR jest jednym z państw, których zdolności przeprowadzenia cyberataków są w powszechnej opinii uważane za największe. Rosja jest postrzegana przez ekspertów jako członek tzw. „cybernetycznej triady", wespół z Chinami i Stanami Zjednoczonymi. To właśnie te kraje dyktują zasady w cyberprzestrzeni. Przy czym Pekin i Moskwa kładą większy nacisk na działania ofensywne, wymierzone w szczególności w Waszyngton.

Rosjanie, co ciekawe nie traktują cyberprzestrzeni jako oddzielnego strategicznego teatru działań wojennych – obok powietrza, morza, lądu czy przestrzeni kosmicznej. Zamiast słowa „cyberprzestrzeń" używają sformułowania „przestrzeń informacyjna". Dla Rosji jej cyber zdolności są nowym narzędziem dla działań w ramach wojny informacyjnej (wywiadu, kontrwywiadu, dezinformacji, propagandy), wojny elektronicznej, zakłócania komunikacji i nawigacji, wywierania presji psychologicznej oraz niszczenia zasobów informatycznych przeciwnika.

Rosjanie nie posiadają osobnego dowództwa na kształt amerykańskiego Cyber Command, chociaż planują powołanie takiego ośrodka w najbliższej przyszłości. Ich doktryna opiera się na trzech głównych dokumentach: „Doktrynie bezpieczeństwa informacyjnego" z 2000 roku, konwencji „O międzynarodowym bezpieczeństwie informacyjnym" oraz „Kompleksowym spojrzeniu na aktywność sił zbrojnych Federacji Rosyjskiej w przestrzeni informacyjnej" z 2011 roku. Pierwsza z nich definiuje interes narodowy Rosji w sferze informacji, mówi o zagrożeniach i szansach, które towarzyszą rozwojowi technologicznemu. Druga jest szeregiem rosyjskich propozycji odnośnie

kontroli sfery informacyjnej, wliczając w to takie kontrowersyjne pomysły jak możliwość odcięcia społeczeństwa od internetu. Dokument przygotowany przez Ministerstwo Obrony liczy zaledwie kilka stron i w dużej mierze jest kopią rozwiązań zawartych w strategii Stanów Zjednoczonych. Skupia się na trzech głównych punktach: monitorowaniu cyberprzestrzeni w celu zlokalizowania zagrożenia, przeciwdziałaniu jego rozprzestrzenianiu, a następnie jego eliminacji. Rosjanie roszczą sobie też prawo do konwencjonalnej odpowiedzi w przypadku zmasowanego ataku w cyberprzestrzeni, jednak nie jest to innowacyjna koncepcja, została wprowadzona już wcześniej przez Amerykanów. Na pierwszy rzut oka zaskakujący jest brak jakiejkolwiek wzmianki o akcjach ofensywnych przeprowadzanych w cyberprzestrzeni. Jednakże za taką działalność odpowiedzialni są hakerzy powiązani z Federalną Służbą Bezpieczeństwa, a dokument został przygotowany przez Ministerstwo Obrony i dotyka spraw istotnych dla wojska.

Rosyjscy „cyberkozacy"

Rosyjscy hakerzy mają bardzo długą tradycję działalności w cyberprzestrzeni. Pierwszy akt cyberszpiegostwa został dokonany właśnie przez nich, kiedy w 1989 roku wykradli z sieci tajne dane Departamentu Stanu i amerykańskich firm, które sprzedali później KGB. Cechą specyficzną rosyjskiej społeczności internetowej jest istnienie dużej ilości grup niezależnych hakerów o patriotycznym nastawieniu, którzy od czasu do czasu współpracują z rządem. Działania większości z nich są prymitywne i ograniczają się do najprostszych ataków, jednakże zdarzają się też jednostki, które obrosły legendą w środowisku hakerskim, jak „Haker Piekło", który podejrzewany jest o kradzież wielu danych opozycji, czy też haker o pseudonimie SEVERA, który nazywany jest królem spamu. Z pewnością większość ich działań wspierana oraz koordynowana jest przez rosyjskie władze. Inną wyróżniającą cechą jest mnogość forów internetowych, gdzie początkujący hakerzy mogą znaleźć informacje oraz potrzebne programy do przeprowadzenia ataków w cyberprzestrzeni. Platformy te służą one również do koordynowana większych ataków.

Hakerzy w walce wewnętrznej

Od początku lat 90. i upowszechnienia się internetu w Rosji, dominuje w tym kraju podejście centralistyczne, polegające na poszerzaniu i pogłębianiu kontroli nad zasobami sieci. Federalna Służba Bezpieczeństwa (FSB) monitoruje pocztę elektroniczną i inne formy komunikacji przez program SORM. Zdaniem przedstawicieli tej służby pomaga to w przeciwdziałaniu terroryzmowi oraz umożliwia wykrywanie agentów obcych wywiadów. Mało kto wierzy w oficjalne komunikaty

przedstawicieli tej organizacji podejrzewając, że w ten sposób obserwowana jest działalność opozycji. W 1999 roku powstały specjalne agencje wyspecjalizowane w zwalczaniu działalności hakerskiej, takie jak Kompromat, Federalna Agencja Śledcza FLB czy Agencja Stringer.

Rosyjscy hakerzy prowadzą również ofensywne działania przeciwko opozycji poprzez ataki na jej strony oraz blogi prowadzone przez autorów nieprzychylnych Kremlowi. Pierwsza taka operacja miała miejsce w 2002 roku, kiedy unieszkodliwiono stronę prowadzoną przez czeczeńskich rebeliantów – Kavkaz.org. Akcja ta została przeprowadzona przez studentów z Tomska, a za jej koordynację odpowiedzialne było FSB.

Inne głośne ataki miały miejsce podczas wyborów parlamentarnych w Rosji w 2011 roku. Chcąc zapobiec pokazywaniu demonstracji antyrządowych oraz opisywaniu fałszerstw wyborczych, hakerzy zaatakowali strony internetowe nieprzychylnych im mediów, jak też blogi użytkowane przez działaczy opozycji. Również ich skrzynki poczty elektronicznej zostały splądrowane. Wraz z hakerami klasyczną działalność operacyjną prowadzili agenci FSB, którzy zastraszali opozycjonistów lub kazali pod groźbą kary zamknąć daną stronę internetową. Jednakże szerokie wykorzystanie mediów społecznościowych, głównie Twittera i Facebooka, spowodowało, że akcja hakerów nie zapobiegła publikacji niewygodnych informacji.

Kampania w cyberprzestrzeni nie polegała jedynie na atakach *sensu stricto*, ale również na szerzeniu dezinformacji. Doskonałym przykładem są tutaj operacje wymierzone w opozycję i jej lidera Aleksieja Nawalnego. Ich stopień zaawansowania i skuteczność stoją na różnym poziomie, od rozpowszechniania amatorskich zdjęć kompromitujących osoby krytykujące Kreml po publikację zhakowanych maili pokazujących, że np. organizacja Golos – odpowiedzialna za przestrzeganie wyborczych procedur – otrzymywała fundusze na swoją działalność z zagranicy. Inne działania obejmowały publikację rozmów telefonicznych jednego z liderów opozycji, w których to krytykuje swoich współpracowników, czy rozpowszechnianie informacji na temat nieprawdziwego wywiadu udzielonego w amerykańskich mediach. Wszystkie te operacje ukierunkowane są na uzyskanie propagandowego efektu w postaci przekonania, że opozycja utożsamiona jest z zewnętrznymi wrogami, a szczególnie ze służbami specjalnymi mocarstw zachodnich.

Hakerzy a rosyjska polityka zagraniczna

W rosyjskich działaniach zewnętrznych w odniesieniu do cyberprzestrzeni można wyróżnić dwa główne elementy. Jedna to działalność dyplomatyczna, ukierunkowana na promowanie

własnego modelu cyberprzestrzeni na arenie międzynarodowej. Druga – nielegalna, opiera się na wykorzystaniu oddziałów hakerów do działań ofensywnych.

Z konieczności walki z opozycją i obawy o destabilizację obecnie panującego porządku politycznego wynika postawa władz Federacji Rosyjskiej na arenie międzynarodowej, dotycząca kwestii obiegu informacji w cyberprzestrzeni. Wbrew zaleceniom OECD, Rosja jest zwolenniczką kontroli danych przepływających w internecie i cenzury, wskazując na zagrożenie bezpieczeństwa narodowego kraju. Wraz z podobnie myślącymi krajami, których systemy polityczne dalekie są od demokracji, silnie lobbuje na forach organizacji międzynarodowych na rzecz wprowadzenia kontroli na zasobami internetu znajdującymi się w obrębie terytorium danego państwa oraz postuluje zwiększenie wpływów międzynarodowych organizacji na kształt i przyszłość sieci globalnej. Obecnie znajdują się one głównie w rękach prywatnych amerykańskich firm, co wzbudza obawę o wykorzystanie internetu przeciwko Rosji. Stąd też władze w Moskwie sprzeciwiają się wykorzystaniu technologii ICT w celu ingerowania w sprawy innych państw. W 2008 roku rosyjscy dyplomaci podczas obrad komisji rozbrojeniowej ONZ stwierdzili, że promowanie ideologii, wliczając w to demokratyczne inicjatywy, przez jedno państwo celem destabilizacji legalnie wybranego rządu Rosji będzie kwalifikowane jako akt agresji.

Takie stanowisko Federacji Rosyjskiej wobec wolności informacji w cyberprzestrzeni było przyczyną niepodpisania Konwencji Budapesztańskiej, dotyczącej zwalczania cyberprzestępczości. Zaniepokojenie rosyjskich władz wzbudził zapis mówiący o możliwości dostępu do danych znajdujących się na terytorium danego państwa przez państwa-strony Konwencji bez zgody owego państwa. Rosjanie obawiali się, że przepis ten będzie furtką do działalności obcych agencji wywiadu. Niepodpisanie przez Rosję Konwencji było w szczególności bolesne, biorąc pod uwagę fakt, że większość cyberprzestępców pochodzi z tego państwa.

Rosja uważana jest też za prekursorkę konfliktu w cyberprzestrzeni. W 2007 roku, kiedy w Estonii postanowiono o przeniesieniu z centrum Talinna pomnika poświęconego radzieckim żołnierzom, kraj padł ofiarą zmasowanego ataku cybernetycznego. Zablokowano strony administracji rządowej, głównych serwisów informacyjnych, wyłączona została bankowość elektroniczna. Władze estońskie oskarżały Kreml o tą akcję, wskazując, że większość ataków została zainicjowana na terenie Rosji. Jednakże nie przedstawiono przekonujących dowodów na udział Kremla w tej akcji. Większość ekspertów nie miała jednak wątpliwości, że to rosyjscy hakerzy stoją za pierwszą w historii próbą zaburzenia funkcjonowania nowoczesnego społeczeństwa przez atak hakerski. W 2009 roku

przedstawiciel prokremlowskiej młodzieżówki Nasi przyznał, że Rosja była autorem akcji zainicjowanej przeciwko Estonii. Atak cybernetyczny był jedynym możliwym sposobem ukarania tego kraju za antyrosyjski gest. Stanowił on również poligon dla zupełnie nowego rodzaju ofensywny wymierzonej w nowoczesne państwo. Rosja pokazała, że jest w stanie zaszkodzić państwu należącemu do NATO i Unii Europejskiej, nie ponosząc przy tym żadnych strat. Jednakże atak cybernetyczny miał znaczenie głównie propagandowe, ponieważ faktycznie nie przyniósł wielkich szkód dla Estonii. Uświadomiono sobie, że jeszcze nie jest możliwe poważne zakłócenie funkcjonowania państwa przy użyciu tylko i wyłącznie ataków cybernetycznych.

Jeszcze bardziej zaawansowany był atak skierowany przeciwko Gruzji w 2008 roku, który rozpoczął się na krótko przed wkroczeniem do akcji rosyjskich sił konwencjonalnych. Podobnie jak w przypadku Estonii, ofiarą działalności hakerów padły strony administracji rządowej, gdzie umieszczono zdjęcia porównujące gruzińskiego prezydenta Micheila Saakaszwiliego do Hiltera, oraz główne serwisy informacyjne. W aspekcie cybernetycznym konfliktu z 2008 roku bardzo interesujące są dwie rzeczy. Pierwszą jest udostępnienie przez profesjonalnych hakerów możliwości udziału w ataku cybernetycznym dla każdego Rosjanina, podłączonego do internetu. Na specjalnym forum zamieszczono instrukcję, w jaki sposób dokonać ataku na gruzińskie strony. Ponadto bardzo aktywni w internecie byli rosyjscy blogerzy, którzy promowali rosyjską wersję wydarzeń. Drugim istotnym aspektem jest fakt, że konflikt z 2008 roku był pierwszym w dziejach świata, który toczył się w czterech wymiarach, poza tradycyjnymi: lądem, morzem i powietrzem, doszła do tego jeszcze cyberprzestrzeń. Działania w niej były zaplanowane i skoordynowane z wkroczeniem konwencjonalnych sił rosyjskich do Gruzji. Głównym celem hakerów w tej wojnie była dezinformacja przeciwnika oraz odcięcie rządu Saakaszwiliego od świata. Rosja, blokując strony administracji państwowej oraz główne serwisy informacyjne chciała przedstawiać światu Gruzję i jej prezydenta jako niebezpiecznego podżegacza i ludobójcę, zabierając możliwość obrony. Był to przykład zastosowania propagandy przy użyciu środków z XXI wieku oraz przejaw wojny informacyjnej, która coraz częściej toczyć się będzie w cyberprzestrzeni. Paraliż stron rządowych miał też pokazać, że rząd Saakaszwiliego nie funkcjonuje i nie jest w stanie sprawować władzy nad własnym krajem. Rosjanie w ataku wymierzonym przeciwko Gruzji wyciągnęli wnioski z 2007 z Estonii, jednak po raz kolejny ich akcja nie spotkała się z całkowitym sukcesem. W osiągnięciu zamierzonego celu przeszkodziło przeniesie stron administracji gruzińskiej na serwery amerykańskie, polskie oraz estońskie. Potyczki w cyberprzestrzeni z Gruzją nie skończyły się wraz porozumieniem

pokojowym Sarkozy – Miedwiediew, ale trwały z mniejszą intensywnością aż do wyborów parlamentarnych w 2012 roku.

Również Kirigistan padł ofiarą rosyjskich hakerów w 2009 roku, kiedy w tym kraju toczyła się dyskusja na temat likwidacji amerykańskiej bazy w Manas. Prawdopodobnie operacja została przeprowadzona przez organizację cyberprzestępców Russian Business Network, która została oddelegowana do tego zadania przez rosyjski rząd. Prezydent W. Putin zamierzał pozbyć się amerykańskich sił zbrojnych z Azji Centralnej, a zmasowany atak cybernetyczny miał być skutecznym narzędziem do osiągnięcia pożądanego celu. Mimo początkowej zgody władz Kirgistanu na usunięcie infrastruktury Stanów Zjednoczonych ze swojego terytorium, Amerykanie wyasygnowali dodatkowe pieniądze i tym samym wywarli wpływ na zmianę decyzji. Z technicznego punktu widzenia nie można przypisać tych trzech wielkich kampanii w cyberprzestrzeni Rosjanom, ale jeśli wziąć pod uwagę polityczną motywację, stojące za nimi centrum decyzyjne tych operacji musiało znajdować się w Rosji.

Umiejętności rosyjskich hakerów rosną, o czym może świadczyć pierwszy udany w dziejach Ameryki atak cybernetyczny na jej infrastrukturę w 2011 roku (zniszczono pompę wodną w stanie Illinos). Wprawdzie nie udało się zebrać wystarczającej liczby dowodów, żeby wskazać sprawców, to jednak większość ekspertów wskazywała, że ślady wiodą do Rosji. Rosjanie nie ograniczają się tylko do ataków w świecie wirtualnym, ale prowadzą również zaawansowane operacje cyberszpiegowskie na kierunkach atrakcyjnych z punktu widzenia ich gospodarki i interesów strategicznych. Ostatnio opublikowany raport amerykańskiej firmy CrowdStrike zajmującej się bezpieczeństwem w Internecie wskazuje rosyjską grupę tzw. energetycznych niedźwiedzi, jako niezwykle aktywne ugrupowanie szpiegowskie ukierunkowane na nielegalne pozyskiwanie informacji o działalności zachodnich koncernów energetycznych. Biorąc pod uwagę, że ropa i gaz są kluczowe dla rozwoju Rosji, nie może to nikogo dziwić.

Ukraina

Konflikt, który wybuchł na Ukrainie, trwa również w cyberprzestrzeni. Ze względu na fakt, że cały czas nie został on zakończony, informacje na temat jego skali oraz charakteru różnią się w zależności od źródła. Z pewnością mamy do czynienia z wojną informacyjną w starym rosyjskim stylu, toczoną tym razem w cyberprzestrzeni. Przykładem jest tutaj działalność propagandowa wielu serwisów internetowych oraz *think-thanków* w Polsce i zagranicą, które deklarują swoją miłość do

W. Putina, widząc na Ukrainie hordy nazistów. Innym, też mało wyrafinowanym przykładem, jest kampania prorosyjskich komentarzach pod artykułami w zachodniej prasie dotyczącymi Ukrainy.

Przy jakimkolwiek konflikcie w cyberprzestrzeni nie może zabraknąć najprostszego rodzaju ataków typu DDoS (*Distributed Denial of Service* – rozproszona odmowa usługi). Tym razem strony internetowe dotknięte tego rodzaju operacją należały do różnych ministerstw w Rosji i na Ukrainie, rosyjskich banków, ale również czasowo wyłączona z użytkowania została witryna NATO. Bardziej zaawansowane metody wojny informacyjnej uwzględniały próby dyskredytacji zachodnich dyplomatów, poprzez ujawnienie ich prywatnych rozmów, w których kwestionują ustalenia, kto strzelał na Majdanie, czy też amerykańską krytykę działań Unii Europejskiej, co miało uderzać w sojuszniczą solidarność.

Kolejnym aspektem konfliktu między Rosją a Ukrainą w cyberprzestrzeni jest wykrycie w ukraińskich sieciach programu szpiegowskiego Snake, podobnego do osławionego Stuxnetu, który wymierzony był w irański program nuklearny. Daje on możliwość pełnego przejęcia kontroli nad zaatakowaną maszyną. Jego poziom zaawansowania wskazuje, że za jego stworzeniem musiało stać państwo, a w kodzie znaleziono poszlaki wskazujące na rosyjskie pochodzenie. Prawdopodobnie jednak nie tylko ten program odpowiada za szpiegowanie ukraińskich sieci. Od upadku ZSRR, Rosjanie starali się zinfiltrować polityczne, wojskowe oraz dyplomatyczne instytucje używając tradycyjnych środków, ale również korzystając z możliwości oferowanych przez internet. Ich działania były o tyle ułatwione, że wiele zabezpieczeń i systemów zostało zbudowanych przez rosyjskich ekspertów.

Do najbardziej zaawansowanych ataków doszło podczas aneksji Krymu. Ich celem były systemy komunikacji ukraińskich żołnierzy stacjonujących na półwyspie. Rosyjska operacja doprowadziła do chaosu informacyjnego i przekreśliła szanse na jakąkolwiek skoordynowaną odpowiedź. Przypuszczono również atak na sieć telefonii komórkowej, z której korzystają ukraińscy politycy, w celu utrudnienia komunikacji pomiędzy różnymi agendami rządowymi. Należy również wspomnieć, że podczas aneksji Krymu zerwano wszystkie połączenia z Ukrainą. Stało się to jednak nie w konsekwencji wyspecjalizowanego cyberataku, ale metodami rodem ze starożytności – poprzez fizyczne przecięcie kabla.

W wypadku Ukrainy, tocząca się w cyberprzestrzeni kampania różni się od tej z 2008 roku, która miała miejsce w Gruzji. Przede wszystkim wciąż nie doszło do zmasowanych ataków na strony administracji rządowej, tak jak podczas konfliktu na Kaukazie. Wynika to prawdopodobnie z innej

narracji i założeń polityki zagranicznej Rosji względem wydarzeń na Ukrainie, gdzie Moskwa nie chce widzieć siebie jako strony walczącej, ale pragnie występować jako niezależny, niezaangażowany w działania separatystów podmiot. Zmasowane ataki na strony administracji ukraińskiej były jasnym przejawem zaangażowania Rosji przeciwko rządowi ukraińskiemu. Oczywiście, jeśli dojdzie do najgorszego zakładanego scenariusza, czyli interwencji rosyjskich wojsk regularnych, ataki w cyberprzestrzeni ulegną zwielokrotnieniu i można spodziewać się powtórzenia sytuacji z Gruzji, a być może nawet jeszcze bardziej zaawansowanych i groźniejszych operacji.

Zakończenie

Działania Rosjan w cyberprzestrzeni są bardzo podobne do tych, dokonywanych przez Chiny, i wymierzone są przeciwko przeciwnikom tak zewnętrznym, jak i wewnętrznym. Przy czym Pekin w swoich działaniach stawia zdecydowanie na szpiegostwo przemysłowe, a mniej koncentruje się na aspekcie cyberwojny. Z pewnością akcje rosyjskich hakerów będą kontynuowane, ponieważ odgrywają one bardzo ważną rolę dla bezpieczeństwa wewnętrznego reżimu Władimira Putina, jak również w kontaktach z innymi państwami na arenie międzynarodowej. Mimo, iż dotychczasowe akcje wykonane przez rosyjskich hakerów nie zakończyły się sukcesem, nie wolno ich lekceważyć, ponieważ cały czas metody ich pracy są udoskonalane. Rosja, będąc świadoma niemożności zrównania się ze Stanami Zjednoczonymi w arsenale konwencjonalnym, będzie usprawniać swoje działania w cyberprzestrzeni, która ma charakter asymetryczny i daję nadzieje na zadanie poważnych szkód przeciwnikowi.

Polska powinna w szczególność obserwować działalność Rosji w środowisku wirtualnym, ponieważ po Majdanie znajduje się na liście potencjalnych rosyjskich celów. Wydarzenia z 2012 roku, kiedy to w ramach protestów przeciwko przyjęciu przez polski rząd ACTA przeprowadzono zmasowane ataki typy DDoS oraz inne operacje wymierzone w administrację państwową RP, obnażyły słabość jej cyberzabezpieczeń. W ciągu dwóch lat sytuacja ta nie uległa zmianie i w przypadku działalności rosyjskich hakerów należy spodziewać się dużych strat.

Kontakt

Fundacja Aleksandra Kwaśniewskiego „Amicus Europae”

Aleja Przyjaciół 8/5
00-565 Warszawa

Tel. +48 22 622 66 33
Tel. +48 22 622 66 03
Fax:+48 22 629 48 16

email: fundacja@fae.pl, www.fae.pl

Biuletyn OPINIE FAE nr 6/2014

Cyberwojownicy Kremla

Autor: Andrzej Kozłowski

Ekspert Fundacji Amicus Europae oraz Instytutu Kościuszki. Członek redakcji pisma „Stosunki Międzynarodowe”. Doktorant na Wydziale Studiów Międzynarodowych i Politologicznych UŁ. W kręgu jego zainteresowań znajdują się cyberbezpieczeństwo, region Kaukazu Południowego, polityka bezpieczeństwa i zagraniczna USA.

Nadrzędną misją **Fundacji AMICUS EUROPAE** jest popieranie integracji europejskiej, a także wspieranie procesów dialogu i pojednania, mających na celu rozwiązanie politycznych i regionalnych konfliktów w Europie.

Do najważniejszych celów Fundacji należą:

- Wspieranie wysiłków na rzecz budowy społeczeństwa obywatelskiego, państwa prawa i umocnienia wartości demokratycznych;
- Propagowanie dorobku politycznego i konstytucyjnego Rzeczypospolitej Polskiej;
- Propagowanie idei wspólnej Europy i upowszechnianie wiedzy o Unii Europejskiej;
- Rozwój Nowej Polityki Sąsiedztwa Unii Europejskiej, ze szczególnym uwzględnieniem Ukrainy i Białorusi;
- Wsparcie dla krajów aspirujących do członkostwa w organizacjach europejskich i euroatlantyckich;
- Promowanie współpracy ze Stanami Zjednoczonymi Ameryki, szczególnie w dziedzinie bezpieczeństwa międzynarodowego i rozwoju gospodarki światowej;
- Integracja mniejszości narodowych i religijnych w społeczności lokalne;
- Propagowanie wiedzy na temat wielonarodowej i kulturowej różnorodności oraz historii naszego kraju i regionu;
- Popularyzowanie idei olimpijskiej i sportu.