Biuletyn OPINIE FAE
nr 7/2016

Andrzej KOZŁOWSKI

NATO wobec wyzwań i zagrożeń w cyberprzestrzeni

Sojusz Północnoatlantycki – najpotężniejsza w dziejach świata organizacja militarna musiał w latach 90. XX wieku, po dekompozycji swojego głównego rywala, zmierzyć się z szeregiem nowych wyzwań dla bezpieczeństwa. Jednym z nich były zagrożenia z cyberprzestrzeni, początkowo bagatelizowane, z czasem stały się istotnym tematem dyskusji. Czy NATO jest gotowe zmierzyć się z tym problemem i jakie zastosowanie ma w tym obszarze, będący kamieniem węgielnym organizacji, artykuł V?

Lata 90. XX wieku

W latach 90. XX wieku działania w cyberprzestrzeni nie były rozpatrywane na forum NATO. Zmieniło się to dopiero w 1999 roku pod wpływem wojny w Kosowie. Obok kampanii lotniczej wymierzonej w serbskie wojska i infrastrukturę położoną na terytorium Jugosławii toczyła się potyczka w cyberprzestrzeni z wykorzystaniem takich narzędzi jak ataki *Denial Distribitud of Service* (DDoS), *e-mail bombing* i inne. Głównym celem tych działań prowadzonych przez serbskich hakerów było zmniejszenie poparcia opinii publicznej na Zachodzie dla prowadzonej kampanii wojskowej. Działania te zostały wsparte przez chińskich hakerów, którzy zaangażowali się w operacje po zbombardowaniu ambasady Chin w Belgradzie. Konflikt ten unaocznił decydentom z NATO znaczenie cyberprzestrzeni, ale nie doprowadził do diametralnych zmian. Powołano tylko Grupę Roboczą ds. Operacji Informacyjnych. Wyniki jej pracy w niewielkim jednak stopniu wpłynęły na kierunek rozwoju Sojuszu w tym obszarze.

XXI wiek

Pierwsze kroki ukierunkowane na zabezpieczenie cyberprzestrzeni zostały podjęte przez NATO na szczycie w Pradze w 2002 roku, pod silnym wpływem Amerykanów. Apelowali o to zarówno prezydent George W. Bush, jak i sekretarz obrony Donald Rumsfeld. Wtedy do życia powołano zespół techniczny reagowania na incydenty komputerowe (NATO *Computer Incident Response Capability* – NCIRC), którego celem było wykrywanie

i neutralizowanie złośliwego oprogramowania w sieciach i systemach NATO. Jego funkcje i charakter pracy zbliżone były do zespołów CERT. Na tym samym szczycie wdrożono również „Program obrony w cyberprzestrzeni" (*The Cyber Defense Program*), wszechstronny plan ukierunkowany na usprawnienie zdolności Sojuszu do obrony przeciwko cyberatakom. Temat cyberzagrożeń został również poruszony w 2006 roku na szczycie w Rydze, gdzie uznano go za jedną z form zagrożeń asymetrycznych. Zobowiązano się do poprawy ochrony systemów odpowiedzialnych za przesyłanie informacji. Należy jednak zauważyć, że w tamtym czasie nie przywiązywano większej uwagi do zagrożeń teleinformatycznych, które pozostawały w cieniu wojny z terroryzmem.

Zmiana nastąpiła dopiero w 2007 roku wraz ze zmasowanymi, trwającymi kilkanaście dni, atakami DDoS na Estonię. Choć straty powstałe na ich skutek nie były tak poważne, jak początkowo podawano, to jednak osiągnięto efekt psychologiczny, a media na całym świecie obiegła informacja o sparaliżowaniu państwa atakami cybernetycznymi. Przywódcy tego bałtyckiego kraju rozważali nawet powołanie się na artykuł V, ale ze względu na brak wypracowanych procedur postępowania i sprzeciw niektórych członków Sojuszu, z tego pomysłu szybko zrezygnowano. Nie oznacza to jednak, że NATO nie wsparło w żaden sposób Estonii. Państwa członkowskie przesłały swoje zespoły CERT oraz ekspertów od bezpieczeństwa teleinformatycznego, użyczono również serwery. W większości przypadków była to pomoc techniczna, ale w tamtym okresie okazała się niezbędna, przyczyniając się do zwalczenia zagrożeń.

Pod wpływem doświadczeń z 2007 roku, na szczycie w Budapeszcie w 2008 roku, wprowadzono znaczne zmiany w polityce NATO w cyberprzestrzeni. W deklaracji końcowej podkreślono potrzebę ochrony kluczowych systemów informacyjnych, dzielenia się dobrymi praktykami oraz udzielania wzajemnej pomocy w przypadku ataków. W 2008 roku zadecydowano o powstaniu nowych instytucji: Rady NATO ds. Zarządzania Cyberobroną

(*The Cyber Defense Management Board – CDMB)* i Centrum Doskonalenia Obrony przed Cyberatakami *(Cooperative Cyber Defense Center of Excellence – CCDCOE)*[1].

Szczyt w 2010 roku przyniósł kolejne zmiany w rozwijaniu polityki cyberbezpieczeństwa przez NATO. Koncepcja strategiczna z 2010 roku oraz deklaracja ze szczytu z Lizbony z tego samego roku podkreślały konieczność kontynuowania działań zmierzających do usprawnienia cyberbezpieczeństwa, a szczególnie poprawy zdolności „wykrywania, oceny, ochrony, przeciwdziałania cyberatakom oraz przywracania systemów do funkcjonowania". Uznano również cyberprzestrzeń za kolejny obszar prowadzenia konfliktów zbrojnych oraz zintegrowano cyberobronę z procesem planowania obrony w NATO (*NATO's Defense Planning Process).* Był to krok ukierunkowany na całkowite zintegrowanie działań w cyberprzestrzeni ze wszystkimi konwencjonalnymi działaniami wojskowymi prowadzonymi przez NATO.

W 2011 roku zaadaptowano „Politykę cyberobrony" (*Cyber Defense Policy)* oraz wprowadzono jej plan realizacji. Celem obu dokumentów było zwiększenie politycznych i operacyjnych możliwości Sojuszu oraz zwiększenie pomocy dla jego członków. Głównymi elementami było:

- Uświadomienie decydentom, że zapewnienie cyberobrony jest niezbędne do wypełniania przez NATO misji zarządzania kryzysowego oraz obrony kolektywnej;
- Ochrona oraz zwalczanie zagrożeń dla krytycznych systemów NATO i państw członkowskich;
- Zaimplementowanie rozwiązań ukierunkowanych na wzmocnienie cyberobrony;
- Centralizacja ochrony sieci NATO;
- Wspomaganie państw członkowskich w osiągnięciu minimalnego, wymaganego poziomu cyberobrony gwarantującego zmniejszenie podatności infrastruktury krytycznej na ataki;

[1] Szerzej na ten temat w podrozdziale instytucje.

- Współpraca z organizacjami międzynarodowymi, sektorem prywatnym i przedstawicielami świata akademickiego

W celu implementacji tych postanowień, *CDMB* podpisała z przedstawicielami członków NATO protokół ustaleń. Coroczne raporty z postępów danych państw we wdrażaniu wyżej wymienionych zaleceń są przekładane Radzie Północnoatlantyckiej. Potwierdzeniem znaczenia cyberbezpieczeństwa dla NATO było również zwiększenie wydatków. W 2012 roku, na ten cel przeznaczono prawie 60 milionów euro, skupiając się na wzmocnieniu zdolności NCIRC poprzez zainstalowanie dodatkowych sensorów wykrywających zagrożenie dla sieci i serwerów NATO. Utworzono również zespół, którego zadaniem jest wyłącznie tworzenie ocen zagrożeń. W 2013 roku odbyło się pierwsze spotkanie ministrów obrony państw NATO poświęcone w całości zagadnieniom cyberbezpieczeństwa. Głównym wnioskiem osiągniętym przez polityków była decyzja o wzmocnieniu bezpieczeństwa wszystkich sieci Sojuszu. Był to dowód na to, że temat cyberbezpieczeństwa został potraktowany z taką samą powagą, jak inne zagrożenia.

W 2014 roku na szczycie w Walii przyjęto „Wzmocnioną politykę cyberobrony" (*Enhanced Cyber Defense Policy)*, w której stwierdzono, że NATO uznaje istniejące normy prawa międzynarodowego za obowiązujące w świecie wirtualnym. Podkreślono również, że cyberataki mogą powodować zniszczenia podobne do działań konwencjonalnych i dlatego, w ich kontekście, może zostać przywołany artykuł V Traktatu Waszyngtońskiego. Zaadaptowany dokument podkreślił, że NATO odpowiada przede wszystkim za obronę własnych sieci, a państwa członkowskie odpowiedzialne są za ochronę własnych systemów teleinformatycznych. Zainicjowano również projekt Programu Partnerstwa z Sektorem Przemysłu Cybernetycznego (*NATO Industry Cyber Partnership),* który był pierwszą inicjatywą nawiązania współpracy z sektorem prywatnym. Głównym zadaniem było zwiększenie cyberobrony łańcucha dostaw sprzętu i oprogramowania komputerowego, wymiana informacji i dobrych praktyk oraz przeprowadzania wzajemnych szkoleń.

NATO przeprowadza wiele różnorodnych ćwiczeń, starając się jak najlepiej przygotować do wyzwań współczesnego pola walki. Dotyczy to również operacji w środowisku wirtualnym. Do najbardziej znanych należą *Cyber Coalition* i *Locked Shields*. W ramach ich scenariusza dwie drużyny symulują konflikt w cyberprzestrzeni, przy czym często posługują się ogólnie dostępnym narzędziami, a nie przygotowanymi wcześniej specjalnymi cyberbroniami. Ćwiczenia mają pomóc NATO w sprawdzeniu doktryn, strategii oraz mechanizmu reagowania w sytuacjach kryzysowych. Służą również wzmacnianiu współpracy pomiędzy członkami Sojuszu. Należy tu podkreślić, że przygotowywane są one w oparciu o doświadczenia estońskie. W przyszłych ćwiczeniach wojsk konwencjonalnych: marynarki, wojsk lądowych czy sił powietrznych, NATO powinno uwzględnić również czynnik cyberbezpieczeństwa i ryzyko cyberataku. Prowadzone w ostatnich latach operacje wojskowe na Ukrainie, Gruzji czy izraelska operacja *Orchard* pokazały sposób integracji działań konwencjonalnych i w zakresie cyberprzestrzeni.

Cyberbezpieczeństwo stało się również istotnym elementem koncepcji *Smart Defense*. Pierwszym z nich był projekt zatytułowany „Wielonarodowy rozwój zdolności cyberobronnych" (*The Multinational Cyber Defense Capability Development),* ukierunkowany na usprawnienie środków wymiany informacji technicznych oraz promowania świadomości zagrożeń. Drugi z nich to „Platforma wymiany informacji o zagrożeniach w cyberprzestrzeni (*The Malware Information Sharing Platform),* umożliwiająca państwom członkowskim wymianę informacji o technicznej charakterystyce złośliwych programów, bez konieczności podawania szczegółów odnośnie przeprowadzonych za ich pomocą ataków. Trzeci projekt polega na zwiększeniu nakładów na edukację w szkołach NATO oraz CCDCOE.

Wyżej wymienione inicjatywy są potrzebne, ponieważ NATO coraz częściej pada ofiarą hakerów. W 2013 roku odnotowano 2,500 incydentów, większość z nich była niegroźna i ograniczała się do ataków typu DDoS. W 2014 roku, w czasie aneksji Krymu strona natowska została czasowo wyłączona z powodu działań hakerów. Udało się im

również spenetrować sieci poczty elektronicznej CCD COE, nie zawierały one jednak poufnych informacji. Biorąc pod uwagę napiętą sytuacją międzynarodową, a w szczególności złe relacje z Rosją – jednym z najaktywniejszych graczy w cyberprzestrzeni – liczba i poziom zaawansowania operacji będą tylko rosnąć.

Instytucje

Zespół techniczny reagowania na incydenty komputerowe *(Computer Incident Response Capability* – NCIRC) – instytucja ta zajmuje się wykrywaniem i zwalczaniem złośliwego oprogramowania oraz informowaniem o nowych rodzajach zagrożeń, które napotkano w sieciach NATO.

Rada NATO ds. Zarządzania Cyberobroną (*The Cyber Defense Management Board* – CDMB) – instytucja ta jest odpowiedzialna za koordynowanie cyberobrony NATO, ocenianie zdolności do walki z cyberatakami oraz zarządzanie ryzkiem w sieciach. Organ ten wspiera również państwa członkowskie w pracach nad wzmocnieniem narodowych systemów cyberbezpieczeństwa.

Centrum Doskonalenia Obrony przed Cyberatakami *(Cooperative Cyber Defense Center of Excellence* – CCDCOE*)* – pełni rolę natowskiego think-tanku, którego zadaniem jest prowadzenie interdyscyplinarnych badań nad cyberbezpieczeństwem oraz przeprowadzanie ćwiczeń oraz kursów dokształcających w tym obszarze.

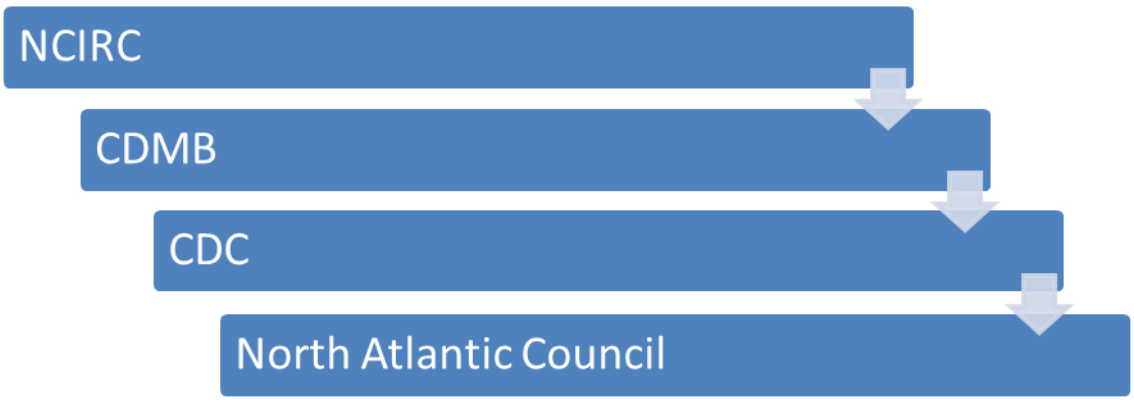
***Rapid Reaction Team* (RRT)** – powołane w celu pomocy technicznej przy atakach i przywracaniu systemów teleinformatycznych do ponownego funkcjonowania. Zespoły te przeznaczone są do wsparcia zaatakowanego członka NATO. Odgrywają również ważną rolę polityczną, udowadniając, że NATO jest solidarne z zaatakowanym krajem i zamierza przyjść mu z pomocą. W przypadku rozmieszczenia RRT pojawią się jednak praktyczne problemy wynikające z błyskawicznego tempa prowadzenia operacji w cyberprzestrzeni. Wysłanie RRT w trakcie cyberataku wymaga od nich zapoznania się z zaatakowanymi systemami, charakterystyką cyberataków, a następnie podjęcie natychmiastowych działań. Zadanie to jest

bardzo trudne do wykonania, biorąc pod uwagę, że musi zostać zrealizowane w bardzo krótkim czasie.

Komitet Cyberobrony *(Cyber Defense Committe* – CDC) – ogólne zarządzanie polityką bezpieczeństwa NATO w cyberprzestrzeni oraz kierowanie i sprawdzanie procesu wdrażania przez państwa rekomendacji zawartych w *Cyber Defense Policy*.

W ramach NATO ustalono następującą hierarchię informowania o zagrożeniu. Wpierw zostaje ono wykryte przez NCIRC, następnie – jeżeli uznano, że incydent ten może mieć znaczenie polityczne – informacje o nim przekazywane są do CDMB oraz CDC i na końcu do Rady Północnoatlantyckiej. Nie opisano wprawdzie, co następuje potem, ale prawdopodobnie procedura zbliżona jest do tej dotyczącej każdego innego zagrożenia (schemat 1).

Schemat 1



Artykuł V Traktatu Waszyngtońskiego

Głównym fundamentem NATO jest artykuł V Traktatu Waszyngtońskiego, mówiący o wspólnej obronie przed zagrożeniami[2]. Ataki z 2007 roku na Estonię uwydatniły konieczność wypracowania sposobów jego zastosowania w przypadku zagrożeń z cyberprzestrzeni. O możliwości zastosowania artykułu V mówiła Strategiczna Koncepcja NATO z 2010 roku. Przełomowy okazał się tutaj szczyt NATO z 2014 w Walii. W jego tekście końcowym znalazło się bezpośrednie odniesienie do możliwości zastosowania artykułu V w odpowiedzi na ataki cybernetyczne. Rada Północnoatlantycka postanowi o tym, analizując każdy przypadek oddzielnie. Można przypuszczać, że na jej decyzje może wpłynąć szereg czynników:

- zasięg – czy celem ataku jest jedno państwo i jak wiele jego sektorów zostało zaatakowanych;
- czas trwania – czy cyberatak trwał kilkanaście godziny czy może był długą, uporczywą, liczoną w miesiącach operacją;
- skutki – czy atak doprowadził do zniszczeń fizycznych i śmierci ludzi;
- atrybucja – istotne jest też, czy sprawcą ataku był aktor państwowy czy niepaństwowy i skąd został zainicjowany atak. Co do zasady, NATO zajmuje się tylko aktami, za którymi stały podmioty państwowe.

Przyjęte kryteria powodują, że powołanie się na artykuł V jest mało prawdopodobne. Po pierwsze, w dotychczasowej historii cyberataków nie odnotowano żadnego, który jednocześnie spełniałby kryterium zasięgu, czasu trwania oraz skutków. Ponadto,

[2] Artykuł V: „Strony zgadzają się, że zbrojna napaść na jedną lub więcej z nich w Europie lub Ameryce Północnej będzie uznana za napaść przeciwko nim wszystkim i dlatego zgadzają się, że jeżeli taka zbrojna napaść nastąpi, to każda z nich, w ramach wykonywania prawa do indywidualnej lub zbiorowej samoobrony, uznanego na mocy artykułu 51 Karty Narodów Zjednoczonych, udzieli pomocy Stronie lub Stronom napadniętym, podejmując niezwłocznie, samodzielnie, jak i w porozumieniu z innymi Stronami, działania jakie uzna za konieczne, łącznie z użyciem siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego." (Traktat północnoatlantycki, http://www.stosunki.pl/sites/default/files/images/Traktat%20P%C3%B3%C5%82nocnoatlantycki.pdf , 27.04.2016)

w środowisku wirtualnym, zawsze bardzo trudnym i czasochłonnym procesem jest stwierdzenie tożsamości atakującego i wykazanie jego powiązania z rządem danego państwa. Istnieje niewiele przypadków, w których udało się tego dokonać. Jednym z nich jest raport prywatnej firmy *Madiant* o chińskiej jednostce szpiegowskiej 61398. Jednak, jego przygotowanie trwało ponad dwa lata i w przypadku rozważania zastosowania artykułu V, jest to zdecydowanie zbyt długi czas. Niemniej jednak deklaracja ze szczytu była istotna i mogła działać jako czynnik odstraszający potencjalnego agresora.

Bardzo ważnym, w kontekście cyberzagrożeń, jest artykuł IV[3]. W sytuacji, kiedy państwo znajduje się w początkowej fazie cyberataku zainicjowanego przez przeciwnika, skorzystanie z artykułu V jest bardzo trudne politycznie, dlatego lepszym wyjściem wydaje się odwołanie do artykułu IV, zdecydowanie mniej kontrowersyjnego, ale użytecznego w odpieraniu ataków cybernetycznych. Szybka reakcja innych państw w postaci wsparcia zespołów CERT, natowski RRT czy użyczenia serwerów pozwoli na przygotowanie się i odparcie kolejnych faz cyberataków, które będą prawdopodobnie o wiele bardziej zaawansowane.

Podsumowanie

NATO odpowiedziało na zagrożenia w cyberprzestrzeni, rozwijając politykę bezpieczeństwa w świecie wirtualnym. Ma ona charakter głównie obronny, ukierunkowany na ochronę sieci i systemów teleinformatycznych oraz intensyfikację wymiany informacji o zagrożeniu i zwiększeniu nakładów na edukację. Te trzy główne cele nie odbiegają znacznie od światowych standardów cyberbezpieczeństwa i powtarzają się w wielu strategiach i koncepcjach innych państw i organizacji. W żadnym z dokumentów nie wspomniano o możliwości przeprowadzania operacji ofensywnych.

[3] Artykuł IV: „Strony będą się konsultowały, ilekroć zdaniem którejkolwiek z nich zagrożona będzie integralność terytorialna, niezależność polityczna lub bezpieczeństwo którejkolwiek ze Stron"
(Traktat północnoatlantycki, http://www.stosunki.pl/sites/default/files/images/Traktat%20P%C3%B3%C5%82nocnoatlantycki.pdf , 27.04.2016)

NATO jednak cały czas ma wiele problemów w świecie wirtualnym, m.in. liczba systemów i sieci Sojuszu jest na tyle duża, że ochrona ich wszystkich jest bardzo trudna. Należałoby wybrać krytyczne systemy, których zabezpieczenie jest najważniejsze. Drugim problemem są różnice w poziomie cyberbezpieczeństwa poszczególnych państw, jedne z nich – jak Estonia – przywiązują olbrzymią wagę do tego problemu, inne go lekceważą. Brak odpowiednich zabezpieczeń w krajach członkowskich może zagrażać sieciom i systemom Sojuszu. Scenariusz, w którym hakerzy atakują najsłabsze ogniwo, a potem wykorzystują zdobyte informacje do kontynuowania operacji wymierzonej w sieci i systemy NATO, jest bardzo prawdopodobny i występował już w przeszłości.

W przyszłości NATO powinno opracować własną strategię cyberbezpieczeństwa, w której zdefiniowana zostanie rola NATO w cyberprzestrzeni wraz z najważniejszymi celami. Warto, żeby znalazło się w niej odniesienie do artykułu V i IV, z wyraźnym podkreśleniem, że NATO może odpowiedzieć konwencjonalnie na cyberatak. Z pewnością należy również przedyskutować sposoby reakcji Sojuszu na takie zagrożenia, które nie kwalifikują się do przywołania artykułu V. Celem jest tutaj stworzenie przekonania u podmiotów atakujących, że Sojusz ma możliwość i wolę odpowiedzi na cyberataki.

Ponadto należy naciskać na wprowadzenie przez państwa członkowskie minimalnych standardów cyberbezpieczeństwa. Obecnie państwa NATO zobowiązane są wydawać co najmniej 2 proc. PKB rocznie, przeznaczając je na obronność. Podobne zobowiązanie, nieograniczające się jednak tylko do finansowania, można odnieść do cyberbezpieczeństwa, które powinno być traktowane jako niezbędny element każdej operacji NATO. Sojusz musi również rozważyć współpracę z partnerami międzynarodowymi, w szczególności tymi podzielającymi wspólne wartości, jak Unia Europejska, Japonia, Izrael czy Australia. Należałoby również rozszerzyć kwestię współpracy z sektorem prywatnym. Dotychczasowa inicjatywa NATO ma wiele do zrobienia w zakresie cyberobrony i nadchodzący szczyt w Warszawie stanowi dobrą okazję do podjęcia odpowiednich decyzji w tym obszarze.

Tezy przedstawiane w serii „Biuletyn OPINIE" Fundacji Amicus Europae nie zawsze odzwierciedlają jej oficjalne stanowisko !

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 7/2016

NATO wobec wyzwań i zagrożeń w cyberprzestrzeni

Autor: Andrzej Kozłowski

Ekspert Zespołu Analiz Fundacji *Amicus Europae* , Fundacji Pułaskiego oraz Instytutu Kościuszki.
Członek redakcji pisma „Stosunki Międzynarodowe". Doktorant Wydziału Studiów Międzynarodowych i Politologicznych UŁ.
W kręgu jego zainteresowań znajdują się cyberbezpieczeństwo, region Kaukazu Południowego oraz polityka 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.