
**FAE Policy Paper**
**nr 13/2015**

**Andrzej KOZŁOWSKI**

# Aktywność Korei Płn. w cyberprzestrzeni

***Korea Płn. jest jednym z najbardziej nieprzewidywalnych elementów systemu międzynarodowego, negatywnie wpływając na system bezpieczeństwa w Azji poprzez militarne groźby i powtarzające się prowokacje. Podobna sytuacja ma również miejsce w środowisku wirtualnym, gdzie północnokoreańscy hakerzy przeprowadzają atak za atakiem przeciwko swoim rywalom, a sławę zyskali ostatnią operacją wymierzoną w Sony. Dlatego też słusznie KRL-D określana jest mianem głównego „państwa zbójeckiego w środowisku wirtualnym". Stopień zaawansowania przeprowadzanych operacji może dziwić, biorąc pod uwagę zacofanie państwa oraz przestarzałe siły zbrojne.***

Określenie zdolności przeprowadzania ataków cyfrowych Korei Północnej stanowi poważny problem. Ocena zdolności cyberataku i cyberobrony każdego państwa jest niezwykle problematyczna, ze względu na brak jasnych granic pomiędzy sektorem prywatnym i publicznym, sferą cywilną i militarną, wielością agencji odpowiedzialnych za ten obszar polityki bezpieczeństwa oraz samą naturę cyberprzestrzeni. Powoduje, to że proces ten jest niezwykle trudny nawet w przypadku tak otwartego i transparentnego państwa jak Stany Zjednoczone. W odniesieniu do jednego z najbardziej zamkniętych, odciętych od świata reżimów na świecie, zadanie to wydaje się wręcz niemożliwe.

## Ataki w środowisku wirtualnym – idealna broń dla KRL-D

Zainteresowanie Korei Północnej rozwojem zdolności działania w cyberprzestrzeni nie powinno nikogo dziwić. Tego typu operacje stają się coraz bardziej atrakcyjne dla praktycznie wszystkich aktorów stosunków międzynarodowych: największych i najpotężniejszych mocarstw, jak Stany Zjednoczone, Chiny, Rosja czy państwa europejskie; państw, których konwencjonalne siły są zdecydowanie słabsze (jak Kuba, Iran czy właśnie Korea Północna), aż po organizacje niepaństwowe, jak np. ruch Anonymous czy różnorodne grupy cyberprzestępcze. Atrakcyjność działania w cyberprzestrzeni wynika z niskich kosztów przeprowadzenia ataku, wysokiego prawdopodobieństwa sukcesu, braku transparentności prawnej oraz problemu z namierzeniem sprawcy ataku, co skutecznie utrudnia działania odwetowe. Kolejnym powodem, dla którego środowisko wirtualne jest popularne wśród słabszych podmiotów jest fakt, że promuje działania asymetryczne. Przy wykorzystaniu

zaawansowanych programów komputerów można spowodować poważne skutki, przy zdecydowanie mniejszym nakładzie sił i środków, niż przy użyciu konwencjonalnych metod. Wystarczy utalentowana jednostka ludzka, z dostępem do dobrej klasy sprzętu komputerowego, a konsekwencje jej działania mogą być przerażające.

Korea Północna ze swoją archaiczną gospodarką nie może rywalizować ze zdecydowanie bardziej rozwiniętym sąsiadem na południu czy ze Stanami Zjednoczonymi pod względem zbrojeń konwencjonalnych. Dlatego musi bazować na broni, która możne relatywnie tanim kosztem spowodować znaczne szkody, jak np. broń masowego rażenia czy właśnie cyberataki. Przy czym broń chemiczna, biologiczna i atomowa są straszakiem, który może zostać użyty w ostateczności – w obronie reżimu i dla jego przetrwania. Operacje w cyberprzestrzeni pozwalają na dokonywanie zniszczeń u swoich przeciwników bez większych konsekwencji.

Zainteresowanie Korei Północnej zdolnościami w cyberprzestrzeni zostało potwierdzone przez głównodowodzącego siłami amerykańskimi na półwyspie koreańskim generała armii Jamesa Thurmanna. Ostrzegał on przed rosnącym zainteresowaniem północnokoreańskiego reżimu działaniami w cyberprzestrzeni. Wskazywał na rosnącą liczbę specjalnie wyszkolonych hakerów do przeprowadzania zaawansowanych cyberataków przeciwko różnym celom. Wystąpienie tak prominentnej i doświadczonej osoby rozwija wszystkie wątpliwości odnośnie rozwoju cyberzdolności KRL-D i jej chęci do ich zademonstrowania.

## Budowa cyberpotencjału

Korea Północna rozpoczęła pracę nad zdolnościami walki elektronicznej w latach 70. ub. wieku, w celu poprawy swojego asymetrycznego potencjału przeciwko sąsiadowi z południa. Rozwój tego sektora nabrał dynamiki dopiero po pierwszej wojnie w Zatoce Perskiej, na początku lat 90. XX w., kiedy USA zademonstrowały, jaką przewagę można osiągnąć na polu bitwy dzięki zastosowaniu komputerów i innych zaawansowanych technologii, umożliwiających dostęp do danych w czasie rzeczywistym. Wnioski do których doszli północnokoreańscy stratedzy, były podobne do tych, które zostały opracowane przez ich chińskich kolegów. Odpowiedzią na nową koncepcję amerykańskiego działania miała być wojna informacyjna stanowiąca jeden z elementów szeroko pojętej wojny radioelektronicznej.

Warto podkreślić, że północnokoreańskie podejście do operacji w cyberprzestrzeni w tym okresie nie odstawało od światowych standardów, wytyczanych przez główne mocarstwa. Powolna zmiana zaczęła następować pod koniec XX w., wraz z utworzeniem Jednostki 121 w strukturze Biura Rozpoznania Sztabu Generalnego.

Niezwykle ciężko jest oszacować liczebność północnokoreańskich jednostek operujących w środowisku wirtualnym. Raporty próbujące tego dokonać są mało precyzyjne, podając przedział od setek do dziesiątek tysięcy hakerów. Określenie liczby cyberwojowników Kima jest niezwykle trudne, ale możliwe jest zidentyfikowanie struktur odpowiedzialnych za prowadzenie operacji w środowisku wirtualnym. Jednostki Korei Północnej w cyberprzestrzeni skupione są w trzech grupach. Grupa Dochodzeniowa Partii Centralnej odpowiedzialna jest za trening oraz edukację techniczną i informatyczną. 204 jednostka Departamentu Operacyjnego prowadzi operacje o charakterze psychologicznym. Kręgosłupem operacji w środowisku wirtualnym jest Biuro Rozpoznania Sztabu Generalnego, podległe bezpośrednio głównodowodzącemu armii północnokoreańskiej Kim Dzong Unowi. Przełomowy dla rozwoju tej struktury był rok 2009, kiedy to w jej skład włączano konglomerat różnorodnych służb specjalnych i wywiadowczych, wcześniej operujących w ramach wielu instytucji rządowych.

Szczególnie znana jest działalność Jednostki 121, odpowiedzialnej za ataki na systemy Korei Południowej (Operacja „Seul w ciemnościach") oraz oddział znany pod nazwą Laboratorium 110 sprzedający pod przykrywką wadliwy, zarażony złośliwym oprogramowanie sprzęt komputerowy. Do szerokiego spektrum działalności Jednostki 121 zalicza się infiltrację sieci komputerowych, operacje szpiegowskie w środowisku wirtualnym oraz tworzenie, a następnie umieszczanie złośliwego oprogramowania we wrogich sieciach. Ponownie, określenie dokładnej liczby hakerów w tej elitarnej jednostce jest niemożliwe. Jedne źródło mówią o 300-osobowym personelu, inne o tysięcznym, a niektórzy autorzy podają, że w skład tej formacji wchodzi ponad 3000 osób. Niezależenie od faktycznej ilości północnokoreańskich hakerów, ich liczba będzie stale się zwiększała, ponieważ liderzy tego kraju widzą w cyberprzestrzeni środowisko, w którym faktycznie mogą spowodować znaczące straty wśród swoich przeciwników.

Generał porucznik Bae Deukshin z armii Korei Południowej ocenił, że reżim Kima przywiązuje ogromną uwagę do rozwoju jednostek hakerów i w przyszłości będą one w stanie

przeprowadzić ataki w cyberprzestrzeni zdolne do zadania poważnych strat w skali kraju i zakłócenia funkcjonowania społeczeństwa. Słowa generała znajdują potwierdzenie w raportach firm prywatnego sektora, zajmujących się bezpieczeństwem w sieci. Wskazują one na rosnące z roku na rok zaawansowanie operacji przeprowadzanych przez północnokoreańskich hakerów.

Znaczenie rozbudowy zdolności operowania w środowisku wirtualnym jest silnie zaakcentowane w procesie edukowania obywateli. Osoby, którym udało się uciec z Korei Północnej donoszą, że reżim od najmłodszych lat wyszukuje utalentowane dzieci, szczególnie zwracając uwagę na ich wyniki z matematyki. Najlepsi dwunastolatkowie zapisywani są na 6-letni program do elitarnej szkoły w Phenianie. Osoby, które podczas tego okresu osiągną najlepsze rezultaty, wysyłane są do jednego z trzech najlepszych uniwersytetów w kraju. Przez 5 lat zdobywają wiedzę z zakresu programowania, automatyki, rozpoznania elektronicznego i sposobów prowadzenia szkodliwej działalności w cyberprzestrzeni. Najlepsi absolwenci mogą dołączyć do Komórki Rozpoznania Sztabu Generalnego Koreańskiej Armii Ludowej lub też udać się zagranicę w celu poprawy swoich umiejętności i przetestowania doświadczenia w praktyce.

Nie można również zapominać o znacznym udziale państw trzecich w budowie potencjału Korei Północnej w środowisku wirtualnym. W szczególności dwa państwa – Rosja i Chiny – chętnie dzielą się wiedzą ze swoimi sojusznikami z Phenianu. Umożliwia im to przetestowanie skuteczności stworzonych rozwiązań poprzez atakowanie sieci Stanów Zjednoczonych, Japonii czy Korei Południowej rękami hakerów Kima, samemu odcinając się od jakiegokolwiek zaangażowania. Chiny dodatkowo dostarczają hardware i software stronie północnokoreańskiej, przez co ich wpływ na rozwój cyberzdolności jest nie do przecenienia.

## Zdolności ofensywne

Amerykański kongresman Steve Chabot na posiedzeniu podkomisji ds. Azji i Pacyfiku Izby Reprezentantów zeznał, że rosnące zdolności Korei Północnej w dziedzinie wykorzystania cyberprzestrzeni do działań ofensywnych stanowią największe zagrożenie wywołania poważnego konfliktu w regionie Azji.

Przeprowadzone ataki cyfrowe na serwery Korei Południowej, Stanów Zjednoczonych i Japonii, które z dużą dozą prawdopodobieństwa przypisać można hakerom Kima,

potwierdzają słowa amerykańskiego polityka. Jedną z najbardziej zaawansowanych kampanii była „operacja Troy", która rozpoczęła się w 2009 roku serią skoordynowanych ataków typu DDoS (*Denial Distributed of Service*), trwających sześć dni, przeciwko południowokoreańskim i amerykańskim witrynom. Zablokowane zostały strony Białego Domu, Pentagonu, Ministerstwa Obrony, Ministerstwa Bezpieczeństwa i Administracji, Zgromadzenia Narodowego oraz Narodowej Służby Wywiadu. Kolejne ataki wymierzone były w strony internetowe największych banków Korei Południowej, nowojorską giełdę oraz główny portal południowokoreański – Naver. W 2010 roku ataki te były kontynuowane, a ich ofiarą padły strony administracji rządowej Korei Południowej.

W marcu 2011 roku 40 południowokoreańskich stron internetowych, powiązanych z rządem, wojskiem oraz infrastrukturą krytyczną, jak również witryny amerykańskich wojsk stacjonujących na Półwyspie Koreańskim – stały się celem serii dziesięciu ataków, bliźniaczo podobnych do tych z 2009 roku. Była to wskazówka, że za obiema operacjami stały te same jednostki. Analiza technik ataków dokonana przez ekspertów z branży prywatnej stwierdziła wysoki poziom zaawansowania technicznego oraz zaplanowanie operacji ściśle pod konkretny cel. Złośliwe oprogramowanie miało również 10 dniowy termin użytkowania, a po jego wygaśnięciu wymazywało dane z twardych dysków, na których się znajdowało, zdecydowanie utrudniając wykrycie autorów ataku. Pokazuje to, że operacja ta nie mogła zostać przeprowadzona przez zwykłych amatorów i wymagała zaangażowania profesjonalnych, pracujących dla wojska hakerów.

Mimo, iż kampania cyberataków była zaplanowana i przeprowadzona w doskonały sposób, eksperci analizujący ją doszli do wniosku, że stanowiła rekonesans zdolności obronnych Korei Południowej a dokładnie badała ile czasu potrzeba na wykrycie ataku, zminimalizowanie strat zadanych przez nie, skutecznego przeciwdziałania użytemu złośliwemu oprogramowaniu i programowaniu zwrotnemu, pozwalającym na ustalenie szczegółów działania danego produktu. Napastnik posiadający taką wiedzę może w przyszłości wyprowadzić zdecydowanie skuteczniejsze uderzenie, a biorąc pod uwagę fakt, że operacje w cyberprzestrzeni miałyby również odegrać niezwykle istotną rolę w potencjalnym, konwencjonalnym ataku Korei Północnej, ryzyko to zdecydowanie wzrasta. W pierwszej fazie takiego konfliktu, północnokoreańscy hakerzy mieliby przeprowadzić zmasowane, zsynchronizowane cyberataki na wybrane elementy infrastruktury krytycznej,

agencje rządowe oraz główne centra dowódcze, paraliżując życie w Korei Południowej, a następnie przeprowadzić uderzenie kinetyczne, nie wyłączając użycia ładunków jądrowych.

Dotychczas takie apokaliptyczne scenariusze pozostają w fazie planowania, a Korea Północna kontynuuje kampanie cyberataków na różne instytucje w Korei Południowej. W 2012 roku celem ataku były najpopularniejsze gazety, ich bazy danych zostały zniszczone, a strony internetowe zablokowane. Rok później 20 marca w operacji „Seul w ciemności" banki oraz trzy stacje telewizyjne odnotowały poważne straty wynikające z unieszkodliwienia tysięcy komputerów poprzez skasowanie tzw. *Master Boot Record* (głównego rekordu startowego).

Rokroczne, coraz bardziej zaawansowane i skoordynowane cyber operacje pozwalają na wyciągnięcie wniosków, że większość z nich była politycznie umotywowana, a grupy jej dokonujące otrzymywały znaczne wsparcie finansowe. Dlatego też mimo problemów z atrybucją ataku w cyberprzestrzeni, można jednoznacznie stwierdzić, że to Korea Północna ponosi za nie odpowiedzialność. Co więcej, za tymi operacjami stoi prawdopodobnie jedna konkretna grupa hakerów, co pozwala domniemywać o scentralizowanej jednostce, charakterystycznej dla sił zbrojnych reżimu Kima.

Poza operacjami *strice* ofensywnymi Korea Północna wykorzystuje swoje zdolności w środowisku wirtualnym do szpiegowania i zbierania informacji. Penetracja sieci południowokoreańskich sieci pozwala na zapoznanie się z planami rządu. W kręgach szczególnego zainteresowania leżą wszystkie dane powiązane z operacjami wojskowymi, bezpieczeństwem oraz strategicznym rozwojem Korei Południowej. Znalezienie oraz zrozumienie niedostatków w obronie przeciwnika jest kluczowe przy planowaniu potencjalnego ataku. Biorąc pod uwagę stopień usieciowienia południowokoreańskiego państwa, który w tej kategorii lokuje się w światowej czołówce, nie może dziwić, że hakerzy Kim Dzong Una wybrali sobie ten rodzaj aktywności. Trzeba zauważyć, że im więcej urządzeń podłączonych do internetu, tym większe prawdopodobieństwo, że któreś z nich nie jest odpowiednio zabezpieczone i dlatego podatne na atak.

Do najbardziej znanych aktów cyberszpiegostwa KRL-D należy operacja „Kimsuky" od nazwy konta na *dropboxie*. Była ona wymierzona przeciwko 11 południowokoreańskim (głównie wojskowe *think-thanki*) i dwóm chińskim instytucjom. Hakerzy stosowali wiele znanych i typowych dla tego operacji metod i narzędzi, jak np. *keyloggery* (urządzenie

rejestrujące klawisze naciskane przez użytkowników). Po raz kolejny grupa stojąca za tą operacją pochodzi prawdopodobnie z Korei Północnej. Wskazuje na to kilka następujących faktów:

- wszystkie cele w Korei Południowej zajmowały się sprawami bezpieczeństwa i obronności, brały również udział w tworzeniu strategii oraz poruszały sprawy regionalne ( np. Ministerstwo ds. Unifikacji),
- uzyskanie danych odnośnie działalności wyżej wymienionych instytucji leżało w interesie władz Korei Północnej, pozwalając na poznanie planów strategicznych swojego głównego rywala,
- adresy IP, z których wyprowadzano ataki wskazują na chińskie prowincje ulokowane przy granicy z Koreą Północną.

Operacje dokonywane przez hakerów Kima w samym tylko 2013 roku kosztowały rząd w Seulu ponad 700 milionów USD. Naprawienie szkód wyrządzonych przez ataki DDoS wymagało dodatkowych 60 milionów USD. Wyraźnie widać, że kampania w środowisku wirtualnym wymierzona w Koreę Południową przynosi znaczne straty finansowe temu państwu, a rosnący potencjał głównego przeciwnika pozwala prognozować, że będą one tylko wzrastać. Poważne są też straty wizerunkowe, których nie można wyrazić w postaci ciągu cyfr. Rzutują one negatywnie na obraz efektywności rządu południowokoreańskiego, który jawi się jako nieskuteczny i niezdolny do obrony sektora publicznego i prywatnego przed rosnącą aktywnością hakerów Kima.

W 2014 roku hakerzy północnokoreańscy dokonali rzeczy bez precedensu: grożąc cyberatakami, które miałyby mieć porównywalną skalę do zamachów terrorystycznych z 11 września, zmusiły Sony Pictures do odwołania wprowadzenia filmu „The Interview", opowiadającego historię fikcyjnego zamachu na przywódcę Korei Północnej. Pierwszy raz w historii groźba ataku w środowisku wirtualnym zmusiła kogoś do spełnienia żądań wysuwanych przez konkretną grupę. FBI oskarżyło reżim Kima o tę akcję, a prezydent Obama nałożył nowe sankcje. Według osób, które zbiegły z najbardziej opresyjnego państwa na świecie, były to tylko kolejne ćwiczenia, poprzedzające prawdziwe uderzenie przeciwko sektorowi energetycznemu i innym elementom infrastruktury krytycznej Stanów Zjednoczonych i Korei Południowej.

## Obrona

Wydawać by się mogło, że tak słabo rozwinięty kraj jak Korea Północna nie może posiadać odpowiednio rozwiniętej cyberobrony. Okazuje się jednak, że zaatakowanie reżimu Kim Dzong Una w środowisku wirtualnym jest niezwykle trudne. Wynika to z faktu, że Korea Północna należy do grona państw z najmniejszą ilością użytkowników internetu na świecie, gdzie dostęp do sieci globalnej jest ściśle reglamentowany. W Korei Północnej działają też tylko trzy przedsiębiorstwa oferujące usługi internetowe. Sytuacja taka powoduje, że ciężko jest przeniknąć do systemów komputerowych reżimu Kim Dzong Una, ponieważ znalezienie słabego punktu stanowi prawdziwie wyzwanie.

Dodatkowo operacje ofensywne utrudnia stosowanie systemów operacyjnych „Czerwona Gwiazda" opartych na bazie systemu Linux. Powoduje to, że z penetracją północnokoreańskich sieci problem mają nawet elitarni hakerzy z jednostki *Tailored Access Operation*, należącej do NSA. Ponadto najważniejsze instytucje w KRL-D używają sieci wewnętrznej, znanej pod nazwą „Jasna Gwiazda", która ulokowana jest na serwerze w Chinach, całkowicie odciętym od sieci globalnej. Zresztą nawet operacja zakończona sukcesem raczej nie przyniesie większych skutków, ponieważ tylko niewielka liczba procesów jest w Korei Płn. skomputeryzowana. Problem ten był szczególnie widoczny podczas ataku na Sony, gdzie rozważano różne opcje odwetu na jego sprawcach. Szybko jednak wykluczono cyberatak, z góry uznając, że nie będzie on skuteczny.

## Podsumowanie

Korea Północna zaliczana jest do grupy najbardziej nieprzewidywalnych i agresywnych państw na kuli ziemskiej, z najbardziej opresyjnym reżimem totalitarnym, a jej władze postrzegane są jako garstka szalonych fanatyków, dążących do wywołania wojny ze swoim sąsiadem i Stanami Zjednoczonymi. To zacofane pod wieloma względami państwo stworzyło jedne z najlepszych oddziałów do walki w cyberprzestrzeni, które od kilku lat testują swoje umiejętności głównie na serwerach południowego sąsiada, corocznie powodując wielomilionowe straty.

Część oficerów południowokoreańskich uważa zdolności Phenianu za jedne z największych na świecie, umiejscawiając je w pierwszej światowej piątce. Opinie te wyolbrzymiają zagrożenie ze strony reżimu Kima, ale nie oznaczają, że jego hakerzy powinni

być lekceważeni. Cyberataki umożliwiają Korei Północnej wyrządzenie szkód po stronie wroga, bez narażania się na ryzyko odwetu. Wynika to z faktu, że Korea Północna nie stanowi atrakcyjnego celu w środowisku wirtualnym, a inny rodzaj działań odwetowych mógłby prowadzić do stopniowej eskalacji napięcia. Wyjątkiem była tutaj reakcja Stanów Zjednoczonych na przełomowy w historii cyberataków atak na Sony, które odpowiedziały nałożeniem dodatkowych sankcji ekonomicznych. Był to jednak symboliczny gest, ponieważ gospodarka Korei Północnej i tak jest od dawna izolowana na świecie.

Z całą pewnością można stwierdzić, że reżim Kima będzie rozwijał zdolności prowadzenia operacji w cyberprzestrzeni, widząc w tym skuteczne narzędzie atakowania swoich przeciwników. Część ekspertów uważa, że może to doprowadzić do poważnego konfliktu na skalę regionalną lub nawet światową z zaangażowaniem Stanów Zjednoczonych i Chin. Wydaje się to jednak mało prawdopodobne. Korea Północna nie przekroczy progu ataku, który mógłby spotkać się z konwencjonalną odpowiedzią ze strony swoich przeciwników. Mimo częstego postrzegania reżimu Kima jako szalonego, jego działalność jest racjonalna i pozwala na realizację interesu narodowego, którym jest przetrwanie reżimu, a w tym zdolności jego hakerów z pewnością się przydadzą.

*Tezy przedstawiane w serii „Policy Papers" 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

**FAE Policy Paper nr 13/2015**

**Aktywność Korei Północnej w cyberprzestrzeni**

**Autor: Andrzej Kozłowski**

Ekspert Fundacji *Amicus Europae* oraz Instytutu Kościuszki. Członek redakcji pisma „Stosunki Międzynarodowe".
Doktorant na Wydziale Studiów Międzynarodowych i Politologicznych UŁ.
Specjalizuje się w tematyce cyberbezpieczeństwa, regionu Kaukazu Południowego oraz polityki bezpieczeństwa i zagranicznej 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.