Cyberbezpieczeństwo w Arabii Saudyjskiej

Autor: dr Aleksander Olech
Wsparcie analityczne: Karolina Siekierka

11.08.2021

Artykuł w skrócie:

- Arabia Saudyjska ma największy rynek teleinformatyczny na Bliskim Wschodzie, a kraj cały czas się rozwija.

- W 2020 roku Arabia Saudyjska zanotowała ponad 22,5 mln takich ataków, a każdy z nich kosztował państwo 6,5 mln dolarów.

- W marcu 2021 roku Ministerstwo Edukacji Arabii Saudyjskiej i Krajowy Urząd ds. Cyberbezpieczeństwa podpisały porozumienie w sprawie uruchomienia wspólnych programów szkoleniowych i badawczych w dziedzinie cyberbezpieczeństwa.

- Od czasu pierwszego cyberataku na Saudi Aramco, Arabia Saudyjska wprowadziła serię rozwiązań mających na celu ograniczenie występowania ataków cybernetycznych.

Wyzwania i rywalizacja w kontekście miliardowych inwestycji

Arabia Saudyjska przechodzi ewolucję wewnątrzpaństwową koncentrującą się na rozwijaniu cyberprzestrzeni, a proces ten został przyspieszony przez pandemię COVID-19 oraz drastyczny spadek cen ropy. **Już w 2016 roku w ramach strategii *Saudi Vision 2030* podkreślono, że Królestwo Arabii Saudyjskiej (KSA) zamierza zmniejszyć zależność od ropy naftowej, zdywersyfikować swoją gospodarkę oraz rozwinąć sektory usług publicznych, takie jak sektor zdrowia, edukacji, infrastruktury, rekreacji czy turystyki.** U podstaw tej inicjatywy leży skupienie się na technologii, transformacji cyfrowej i rozwoju infrastruktury cyfrowej. Zasadniczo w samej strategii nie są poruszane kwestie cyberprzestrzeni ani cyberterroryzmu[1], wskazane są jednak kierunki zmian.

Na początku pandemii koronawirusa, w pierwszym kwartale 2020 roku, w krajach na Bliskim Wschodzie odnotowano wzrost ataków złośliwego oprogramowania o 22% i spamu o 36%. Był to szczególnie trudny okres dla firm w Arabii Saudyjskiej, które były w trakcie konwersji na pracę zdalną[2]. Infrastruktura teleinformatyczna w sektorze publicznym i prywatnym jest stale zagrożona incydentami cybernetycznymi ze względu na strategiczną pozycję Arabii Saudyjskiej w regionie. Te cyberataki mają poważny wpływ na gospodarkę na poziomie finansowym, operacyjnym i taktycznym, co może potencjalnie osłabić zaufanie obywateli do

[1] Kingdom of Saudi Arabia, *Saudi Vision 2030,* Government of Saudi Arabia, Riyadh 2016.
[2] A. Buller, *Saudi Arabia sees cyber security boom as coronavirus bites*, Computer Weekly, 17.09.2020, dostęp: 16.07.2021.

usług rządowych oraz do samej władzy[3]. To z kolei może wpłynąć na stabilność polityczną kraju oraz prowadzić do kolejnych ataków podejmowanych przez cyberprzestępców z państw sąsiadujących.

Instytucje prywatne oraz publiczne w Arabii Saudyjskiej zostały także postawione przed wyzwaniem organizacji pracy w trakcie pandemii COVID-19. Pojawiające się ryzyko utraty danych wrażliwych przesyłanych przez pracowników działających z domu spowodowało, że doszło do reorganizacji w obszarze IT w całym kraju. Przymusowa blokada w celu zatrzymania rozprzestrzeniania się wirusa spowodowała, że całość form komunikacyjnych została przeniesiona do internetu, normą stało się odbywanie spotkań za pośrednictwem internetowych komunikatorów, dokonywanie zakupów online i prowadzenie edukacji wirtualnej. Dotychczas w Arabii Saudyjskiej panowała kultura pracy w biurze i organizacji spotkań osobistych. Z uwagi na dynamiczną zmianę polityki działalności praktycznie wszystkich firm w kraju pojawiło się wzywanie szybkiego wdrożenia strategii, które umożliwiłyby pracownikom utrzymanie produktywności. Wiązało się to z przeniesieniem danych do chmur i udzieleniem dostępu do zdalnych zasobów IT przedsiębiorstw. Przez to należało zwiększyć poziom bezpieczeństwa w cyberprzestrzeni, inwestując w nowe technologie i implementując zabezpieczenia odporne na ataki zewnętrzne. Innym istotnym elementem było szkolenie pracowników[4], którzy mają dostęp do danych firmy, aby oni również stale analizowali pojawiające się zagrożenia oraz przestrzegali zasad bezpieczeństwa[5].

Ponad połowa dyrektorów ds. Informacji w Arabii Saudyjskiej postrzega zarządzanie bezpieczeństwem jako największe wyzwanie technologiczne, a inwestycje w cyberbezpieczeństwo uważa za kluczowy cel biznesowy. Ponadto potrzeba utrzymania cyberbezpieczeństwa stała się jednym z głównych wskaźników wydajności firm i transformacji cyfrowej w całym państwie, przez co wydatki na technologie i ochronę przed wyciekiem danych będą z każdym rokiem większe[6].

---

[3] A. Quadri, M. K. Khan, *Cybersecurity challenges of the Kingdom of Saudi Arabia: Past, Present and Future,* Global Foundation for Cyber Studies and Research, styczeń 2019, s. 7.
[4] A. Alzubaidi, *Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia*, Heliyon, tom 7, wydanie 1, 2021.
[5] A. Buller, *Saudi Arabia sees cyber security boom as coronavirus bites*, Computerweekly, 17.09.2020, dostęp: 16.07.2021.
[6] B. Wright, K. Allan, *Saudi CIOs consider security their toughest tech challenge, CIO, 25.08.2020,* https://www.cio.com/article/3445225/saudi-arabias-cybersecurity-concerns-increase-as-threats-evolve.html, dostęp: 18.07.2021.

Zagrożenia cyberterrorystyczne

Arabia Saudyjska zmagała się w 2015 roku z 160 000 atakami dziennie[7]. Z uwagi na jej pozycję międzynarodową i posiadane surowce jest dużo częściej atakowana niż inne państwa w regionie. Takie nasilenie zagrożeń powoduje utrudnienia w funkcjonowaniu zarówno sektora publicznego, jak i prywatnego. Cyberataki — o różnej skali i nasileniu — mogą powodować poważne szkody w gospodarce i negatywnie wpłynąć na stabilność społeczną i polityczną kraju. Ponadto cyberprzestępczość jest również jedną z głównych przyczyn ogromnych strat pieniężnych i wizerunkowych.

Ochrona cyberprzestrzeni stanowi obecnie jedno z najważniejszych wyzwań w zapewnianiu bezpieczeństwa i stabilności państw. Od 2006 roku można zaobserwować znaczny wzrost ataków na ich infrastrukturę krytyczną, pełniącą istotną rolę w ich funkcjonowaniu państwa i obywateli. Mogą one przybierać różne formy i są ukierunkowane m.in. na zdobycie wglądu, kradzież lub zniszczenie pilnie strzeżonych informacji oraz zakłócenie działalności plików czy systemów komputerowych poprzez wprowadzenie złośliwego oprogramowania. **Tylko w 2012 roku Królestwo straciło 693 mln dolarów, a z każdym rokiem ta suma jest wyższa[8]. W 2020 roku Arabia Saudyjska zanotowała ponad 22,5 mln takich ataków[9], każdy z nich kosztował państwo 6,5 mln dolarów[10], natomiast w pierwszym kwartale 2021 roku zarejestrowano ponad 7 mln cyberataków[11].** Amerykańskie Centrum Studiów Strategicznych i Międzynarodowych podaje, że spośród wszystkich ataków przeprowadzonych między majem 2006 a czerwcem 2020 roku 15 stanowiło znaczne zagrożenie dla bezpieczeństwa państwa. W sporządzonych w 2020 roku rankingach *Cybersecurity Exposure Index* dotyczących stopnia narażenia na cyberatak oraz *Cyber Risk Index* przewidującym

[7] Arabian Business, *160,000 cyberattacks a day in Saudi Arabia*, https://www.arabianbusiness.com/160-000-cyberattacks-day-in-saudi-arabia-630120.html, dostęp: 20.07.2021.
[8] A. Quadri, M. K. Khan, *Cybersecurity challenges of the Kingdom of Saudi Arabia: Past, Present and Future*, Global Foundation for Cyber Studies and Research, styczeń 2019, s. 7.
[9] T. Nasarallah, *Saudi Arabia: over 7 million cyberattacks foiled in 3 months*, Gulf News, https://gulfnews.com/photos/lifestyle/photos-fashion-abayas-by-safia-hussain-showcased-in-riyadh-1.1611420228808?slide=6, dostęp: 16.07.2021.
[10] C. Kelly, *IBM: Cyber breaches cost enterprises in the UAE and KSA over $6.5m per attack in 2020*, ITP, https://www.itp.net/news/93473-ibm-cyber-breaches-cost-enterprises-in-the-uae-and-ksa-over-65m-per-attack-in-2020, dostęp: 16.07.2021.
[11] T. Nasarallah, op. cit.

możliwość jego doświadczenia, Arabia Saudyjska zajęła odpowiednio 31.[12] i 25.-26. miejsce w skali globalnej[13].

Ataki na cyberprzestrzeń Arabii Saudyjskiej

Jeden z najgroźniejszych ataków na cyberprzestrzeń państwa miał miejsce w sierpniu 2012 roku, kiedy do wewnętrznej sieci komunikacyjnej państwowego koncernu naftowego Saudi Aramco wprowadzono wirus *Shamoon*. Jego celem było wstrzymanie produkcji ropy i gazu oraz osłabienie największego przedsiębiorstwa rynku energetycznego w regionie Bliskiego Wschodu. Wskutek tego zdarzenia uszkodzono ponad 30 tys. komputerów, usunięto wszystkie dane znajdujące się na ich dyskach i zastąpiono obrazem płonącej amerykańskiej flagi. W celu zatrzymania rozprowadzania wirusa Saudi Aramco było zmuszone przerwać pracę i zablokować zarówno pocztę e-mail wszystkich pracowników, jak i dostęp do internetu. Wstrzymało to działalność przedsiębiorstwa na dwa tygodnie i przyniosło ogromne straty finansowe. W czasie trwającej pięć miesięcy blokady internetu zespół ds. bezpieczeństwa cybernetycznego prowadził działania mające na celu implementację nowych rozwiązań w celu utrzymania cyberbezpieczeństwa. Atak stanowił zagrożenie nie tylko dla samej Arabii Saudyjskiej, ale także dla państw Zachodu, w szczególności uzależnionych od dostaw ropy naftowej Stanów Zjednoczonych. Pomimo braku dowodów wywiad amerykański oskarżył o atak największego rywala Arabii Saudyjskiej w regionie, Islamską Republikę Iranu.

Kolejny atak na Saudi Aramco, tym razem przy użyciu zaktualizowanego wirusa *Shamoon 2*, miał miejsce w sierpniu 2017 roku i wstrzymał pracę przedsiębiorstwa na 48 godzin. Znacznie krótsza przerwa w prowadzeniu działalności wynikała z podjętej po 2012 roku decyzji przedsiębiorstwa o stałym gromadzeniu kopii zapasowych. Jak podaje ***The New York Times*, celem cyberataku było wywołanie eksplozji oraz ogólny sabotaż systemu[14]. Nie potwierdzono, kto odpowiada za atak, jednak także w tym przypadku oskarżony został Iran.**

[12] J. Frisby, *Cybersecurity Index (CEI) 2020*, PasswordManagers.co, https://passwordmanagers.co/cybersecurity-exposure-index/, dostęp: 16.07.2021.
[13] NordVPN, *Cyber Risk Index*, 2020, https://s1.nordcdn.com/nord/misc/0.13.0/vpn/brand/NordVPN-cyber-risk-index-2020.pdf, dostęp: 16.07.2021.
[14] N. Perlroth, C. Krauss, *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try*., The New York Times, https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html, dostęp: 16.07.2021.

W grudniu 2019 roku saudyjskie organy państwowe wykryły cyberatak planowany na infrastrukturę krytyczną Arabii Saudyjskiej. Do jego przeprowadzenia miało zostać wykorzystane złośliwe oprogramowanie *Dustman*, trwale usuwające dane przechowywane na dyskach. Nie poinformowano, które organy państwa miały być celem, natomiast pozostawienie przez hakerów licznych śladów w sieci sugeruje jego pospieszną organizację. Co istotne, miał on miejsce podczas eskalacji napięcia na linii irańsko-amerykańskiej. Jak podaje *CyberScoop,* ze względu na ówczesną sytuację polityczną oraz na podstawie podobieństwa sposobu przeprowadzenia ataków oraz pozostawionych śladów uznaje się, że stoją za nim irańscy hakerzy[15].

Arabia Saudyjska, jej organy państwowe oraz przedsiębiorstwa nie są celem wyłącznie ataków skutkujących usunięciem lub blokadą danych. W maju 2020 roku KSA padło ofiarą nieudanej kampanii szpiegowskiej prowadzonej przez irański podmiot *Chafer APT*. Miała ona być wymierzona w saudyjską infrastrukturę krytyczną, w szczególności w przechowujące znaczną liczbę danych osobowych sektory telekomunikacyjny i turystyczny oraz w administrację rządową, celem m.in. zebrania danych na temat szpiegów i danych uwierzytelniających[16].

Oprócz powyższych, współczesne trendy w Arabii Saudyjskiej wskazują, że cyberterroryści wykorzystują media społecznościowe jako alternatywę, aby zakłócić komunikację pomiędzy obywatelami oraz utrudnić działalność gospodarczą poprzez penetrację kanałów komunikacyjnych użytkowników. Dodatkowo wykorzystują sieć do rekrutacji członków, pozyskiwania funduszy czy prowadzenia ataków dezinformacyjnych na Arabię Saudyjską. **Aż 30,2 mln obywateli (91% ludności) posiada dostęp do sieci, a 25 mln ma konto w serwisie społecznościowym. Obecnie najczęściej rozpracowywane przez terrorystów media to WhatsApp, YouTube, Facebook, Instagram i Twitter[17].**

[15] S. Lyngaas, *Saudi cyber authority uncover new data-wiping malware, and experts suspect Iran is behind it*, CyberScoop, https://www.cyberscoop.com/saudi-arabia-iran-cyberattack-soleimani/, dostęp: 17.07.2021.
[16] B. Rusu, *Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia*, Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf, dostęp: 17.07.2021.
[17] Skillzme, *Saudi Arabia Social Media Statistics 2018*, https://skillzme.com/ksa-social-media-statistics-2018, dostęp: 17.07.2021.

Strategia cyberbezpieczeństwa

Z uwagi na współczesne wyzwania dla cyberbezpieczeństwa, **Dekretem królewskim z dnia 31 października 2017 roku ustanowiono Krajowy Urząd ds. Cyberbezpieczeństwa (*National Cybersecurity Authority*, NCA), którego głównym zadaniem jest zwiększanie bezpieczeństwa cybernetycznego państwa poprzez przygotowywanie wewnętrznych analiz i rozwiązań prawnych. W skład urzędu wchodzą: szef Prezydium Bezpieczeństwa Państwa**[18], szef *General Intelligence Presidency* (GIP, służba wywiadu Arabii Saudyjskiej), wiceminister spraw wewnętrznych oraz zastępca ministra obrony[19]. NCA pełni zarówno funkcje regulacyjne, jak i operacyjne, związane z cyberbezpieczeństwem, a także ściśle współpracuje z podmiotami publicznymi i prywatnymi w celu poprawy stanu cyberbezpieczeństwa kraju, ochrony jego interesów, bezpieczeństwa narodowego, infrastruktury krytycznej, usług rządowych oraz budowania środowiska cyberprzestrzeni na rzecz implementacji strategii 2030[20].

NCA opracowało strategiczną wizję cyberbezpieczeństwa, która odzwierciedla cele Arabii Saudyjskiej, tworząc w cyberprzestrzeni warunki do utrzymania bezpieczeństwa i zaufania do władz oraz wzrostu technologicznego. Priorytetowe cele do 2030 roku obejmują 6 aspektów[21]:

- ujednolicenie cyberbezpieczeństwa w całym kraju — zapewnienie wysokiego poziomu koordynacji i dostosowania wytycznych we wszystkich podległych podmiotach; ważne jest przyjęcie kompleksowego krajowego podejścia do cyberbezpieczeństwa poprzez integrację, określenie ról i obowiązków podmiotów na poziomie krajowym w celu opracowania i wdrożenia regulacji i polityk oraz zgodność z krajowymi normami;
- zarządzanie ryzykiem — identyfikacja zaatakowanych elementów w cyberprzestrzeni oraz określenie szkód; następnie weryfikacja najwłaściwszych metod eliminacji zagrożenia w celu ograniczenia negatywnych skutków;

[18] Prezydium Bezpieczeństwa Państwa (eng: *Presidency of State Security*) to saudyjski organ bezpieczeństwa powstały w 2017 roku przez utworzenie nadzoru na symultanicznymi działaniami krajowych służb antyterrorystycznych i wywiadowczych.
[19] Saudi Gazette, *King orders setting up of National Cyber Security Authority*, https://saudigazette.com.sa/article/520782/SAUDI-ARABIA/King-orders-setting-up-of-National-Cyber-Security-Authority, dostęp: 17.07.2021.
[20] National Cybersecurity Authority, *Essential Cybersecurity Controls*, 2018, s. 6-10.
[21] National Cybersecurity Authority, *National Cybersecurity Strategy (Overview)*, Kingdom of Saudi Arabia, grudzień 2020, s. 14-29.

- optymalne funkcjonowanie w środowisku cyberprzestrzeni — wprowadzenie kompleksowych kontroli, norm krajowych i systemu monitorowania zgodności, które zapewnią ochronę środowiska cyberbezpieczeństwa, w tym podnoszenie poziomu społecznej świadomości na temat cyberzagrożeń;
- dynamiczna obrona — wzmacnianie i ciągły rozwój krajowych zdolności w zakresie obrony przed cyberzagrożeniami; wykrywanie, przeciwdziałanie, reagowanie oraz reorganizacja po atakach;
- partnerstwo międzynarodowe — cyberbezpieczeństwo wymaga stabilnych partnerstw lokalnych i międzynarodowych, wzmocnionych zaawansowanymi mechanizmami wymiany informacji, pozwala to na udoskonalenie systemów i wymianę najlepszych praktyk; w celu osiągnięcia wymaganego poziomu bezpieczeństwa należy dążyć do wzmocnienia partnerstwa zagranicznego;
- rozwój w cyberprzestrzeni — należy dążyć do zwiększania zdolności krajowych w dziedzinie cyberbezpieczeństwa, a jednym z głównych kierunków są inwestycje w programy edukacyjne i szkoleniowe oraz w przemysł i badania.

Oprócz powyższych, ze względu na wielkość saudyjskiej gospodarki Królestwo skoncentrowało się na tworzeniu struktur rządowych, które pozwoliłby wykorzystać potencjał państwa oraz przeciwdziałać pojawiającym się zagrożeniom. Tym samym **Arabia Saudyjska w 2019 roku utworzyła kolejne 3 organy powiązane z NCA. *Saudi Data and Artificial Intelligence Authority* (SDAIA), które jest odpowiedzialne za opracowywanie strategii przechowywania danych oraz rozwój sztucznej inteligencji i podległe jej *National Centre for Artificial Intelligence* oraz *Saudi Commission for Data and Artificial Intelligence*.** Takie działania są wyraźnym przejawem determinacji Królestwa w dążeniu do rozwijania swoich możliwości cyfrowych i budowania przyszłości opartej na sztucznej inteligencji i innowacjach. Według saudyjskich władz sztuczna inteligencja zwiększy produktywność, usprawni procesy decyzyjne we wszystkich sektorach, zapewni bardziej innowacyjne usługi świadczone obywatelom oraz pozwoli na rozwój przedsiębiorstw[22]. Warto także zaznaczyć, że Arabia Saudyjska stale aktualizuje Ustawę o cyberprzestępczości (ang. *Cyber Crime Law*) z 2007 roku.

[22] A. Gernonimo, *National Centre for AI to drive Saudi Arabia's digital future: minister*, TahawulTech, 01.09.2019.

Nowe rozdanie w cyberprzestrzeni

W marcu 2021 roku Ministerstwo Edukacji Arabii Saudyjskiej i Krajowy Urząd ds. Cyberbezpieczeństwa podpisały porozumienie w sprawie uruchomienia wspólnych programów szkoleniowych i badawczych w dziedzinie cyberbezpieczeństwa. Ma to duże znaczenie w zakresie inwestowania w inicjatywy na rzecz cyberbezpieczeństwa oraz jest częścią realizacji Strategii 2030. Ministerstwo Edukacji i NCA realizują już kilka wspólnych projektów dotyczących stypendiów dla badań na cyberprzestrzenią oraz rozwoju szkolnictwa wyższego w zakresie bezpieczeństwa cybernetycznego[23].

Od czasu pierwszego cyberataku na Saudi Aramco, Arabia Saudyjska wprowadziła serię rozwiązań mających na celu ograniczenie występowania ataków cybernetycznych. Jednym z nich jest decyzja rządu o podwojeniu budżetu na cyberbezpieczeństwo. **Jeszcze w 2012 roku wydatki te wzrosły z 7,8 mld do 15,4 mld dolarów[24], natomiast w 2020 roku osiągnęły kwotę 27,2 mld dolarów[25]. W 2014 roku powstało Narodowe Centrum Technologii Cyberbezpieczeństwa (ang. *National Center for Cybersecurity Technology*), instytucja naukowo-badawcza zajmująca się kwestiami zarządzania bezpieczeństwem, bezpieczeństwem sieci, oprogramowań i informacji.** Analizy opracowywane przez Centrum mają przygotować państwo do wprowadzania projektu „Wizja 2030".

Państwo współpracuje w zakresie cyberbezpieczeństwa zarówno z organizacjami międzynarodowymi (m.in. z ONZ, Ligą Państw Arabskich), jak i na podstawie umów bilateralnych (np. ze Stanami Zjednoczonymi, Wielką Brytanią, Zjednoczonymi Emiratami Arabskimi), jednak ze względu na napięcia w relacjach z Iranem oraz powiązany z nimi wzrost liczby cyberataków najbardziej aktywną działalność prowadzi w ramach Rady Współpracy Zatoki Perskiej, gdzie inicjuje rozmowy nt. rozszerzenia współpracy w zakresie bezpieczeństwa cybernetycznego. **Liczba aktorów, z którymi Arabia Saudyjska prowadzi współpracę, jest ograniczona, gdyż państwo postrzega kwestię cyberbezpieczeństwa jako**

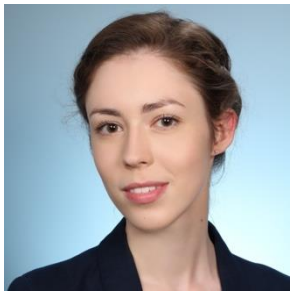
[23] Arab News, *Deal signed to boost cybersecurity education in Saudi Arabia,* https://www.arabnews.com/node/1830711/saudi-arabia, Homepage 24.03.2021, dostęp: 17.07.2021.
[24] S. Alshathry, *Cyber Attack on Saudi Aramco*, "International Journal of Management and Information Technology", 2017, t. 11, nr 5, s. 3039.
[25] *USSABC Economic Brief: Saudi Arabia's Emergence in Cyber Technology*, U.S.-Saudi Arabian Business Council, http://ussaudi.org/wp-content/uploads/2020/01/Economic-Brief-Saudi-Cybersecurity-Leadership.pdf, dostęp: 17.07.2021.

niewielką część swojej polityki zagranicznej[26], a kluczowe jest dla niej bezpieczeństwo wewnętrzne.

[26] *Saudi Arabia's Foreign Policy Priorities*, Chatham House, https://chathamhouse.soutron.net/Portal/DownloadImageFile.ashx?objectId=3483, dostęp: 17.07.2021.

O AUTORACH

Dr Aleksander Olech. Dyrektor Programu Bezpieczeństwa Europejskiego w Instytucie Nowej Europy. Doktor nauk o bezpieczeństwie. Specjalista z zakresu bezpieczeństwa i relacji międzynarodowych. Doświadczenie badawcze zdobywał m.in. na Université Jean Moulin III w Lyonie, Instytucie Stosunków Międzynarodowych w Pradze oraz Instytucie Wspierania Pokoju i Zarządzania Konfliktami w Wiedniu. Stypendysta OSCE & UNODA Peace and Security oraz Fundacji im. Kazimierza Pułaskiego. Jego główne zainteresowania badawcze to terroryzm, międzynarodowa współpraca na rzecz bezpieczeństwa w Europie Wschodniej oraz rola NATO i UE w środowisku zagrożeń hybrydowych.



Karolina Siekierka. Studentka drugiego stopnia na kierunku stosunki międzynarodowe specjalizacji Bezpieczeństwo i Studia Strategiczne Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego. Podczas studiów uczestniczyła w wymianach studenckich z Université Panthéon-Sorbonne (Paris 1) oraz Institut d'Etudes Politique de Paris (Sciences Po Paris). Jej zainteresowania badawcze obejmują prawo międzynarodowe, międzynarodowe stosunki polityczne oraz prawa człowieka. Zaangażowana w działalność organizacji studenckich na Uniwersytecie Warszawskim oraz Sciences Po.

NIW Narodowy Instytut Wolności Centrum Rozwoju Społeczeństwa Obywatelskiego

Sfinansowano przez Narodowy Instytut Wolności - Centrum Rozwoju Społeczeństwa Obywatelskiego ze środków Programu Rozwoju Organizacji Obywatelskich na lata 2018 – 2030

Program Rozwoju Organizacji Obywatelskich na lata 2018–2030 PROO

JEŻELI DOCENIASZ NASZĄ PRACĘ, DOŁĄCZ DO GRONA NASZYCH DARCZYŃCÓW!

Z otrzymanych funduszy sfinansujemy powstanie kolejnych publikacji.

Możliwość wsparcia to bezpośrednia wpłata na konto Instytutu Nowej Europy: 95 2530 0008 2090 1053 7214 0001 tytułem: „darowizna na cele statutowe".