PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NR 82 (3216), 19 LISTOPADA 2026 © PISM

BIULETYN

Od atrybucji do kosztów. Sankcje UE wobec działań hybrydowych Rosji

Elżbieta Kaca

16 listopada UE rozszerzyła sankcje wobec Rosji, co jest odpowiedzią na rosnącą skalę zagrożeń poniżej progu otwartego konfliktu zbrojnego, wymierzonych w państwa członkowskie. Sankcje mogą podnosić koszty prowadzenia takich operacji i wzmacniać efekt odstraszania, jednak ich skuteczność pozostaje ograniczona m.in. przez problemy z atrybucją działań oraz niewielki wpływ na zagraniczne podmioty.

Ewolucja. Rosja wykorzystuje wobec państw UE szeroki katalog działań hybrydowych, m.in. cyberataki, dezinformację, operacje wpływu, ingerencję w procesy demokratyczne oraz sabotaż, w tym infrastruktury krytycznej. Nasilenie takich aktywności po 2014 r., a szczególnie po pełnoskalowej agresji na Ukrainę w 2022 r., skłoniło UE do rozwijania nowych instrumentów reagowania, w tym sankcji. Obejmują one przede wszystkim zamrożenie aktywów, a w przypadku osób fizycznych także zakaz wjazdu do UE.

Pierwszym instrumentem był ustanowiony w 2019 r. system sankcji dotyczący cyberataków. Pozwala on nakładać restrykcje na osoby i podmioty odpowiedzialne za cyberataki lub ich próby wymierzone m.in. w infrastrukturę krytyczną, instytucje publiczne czy procesy wyborcze. Warunkiem jego zastosowania jest udowodnienie związku sprawców z konkretną operacją. Do tej pory objęto nim 27 osób i 7 podmiotów powiązanych z rosyjskimi cyberatakami (zob. tabela).

Przełomem było przyjęcie w 2024 r. odrębnego systemu sankcji za rosyjskie działania destabilizacyjne, m.in. za cyberataki, sabotaż, ingerencję w procesy demokratyczne, zagraniczną manipulację informacyjną i ingerencję (FIMI) oraz instrumentalizację migracji. Oprócz zamrażania aktywów i zakazu wjazdu do UE możliwe są także zakazy transakcji dotyczących statków, samolotów, nieruchomości, portów, infrastruktury cyfrowej czy zagranicznych dostawców usług kryptowalutowych wykorzystywanych w działaniach destabilizacyjnych. UE może również zakazać działalności mediom uczestniczącym w operacjach wpływu. Dotychczas restrykcjami objęto 111 osób i 21 podmiotów (zob. tabela). Równolegle UE stosuje sankcje wobec osób i organizacji uczestniczących w rosyjskich kampaniach dezinformacyjnych związanych z wojną przeciwko Ukrainie.

Stosowanie sankcji w praktyce. W latach 2020–2026 UE stopniowo rozszerzała listę osób i podmiotów podlegających sankcjom za cyberataki. Unijny system obejmował m.in. rosyjski wywiad wojskowy i jego oficerów zaangażowanych w próbę włamania do Organizacji ds. Zakazu Broni Chemicznej (OPCW) w Holandii, atak NotPetya (seria cyberataków w 2017 r., która wywołała duże globalne straty gospodarcze), cyberatak na Bundestag czy ataki na instytucje państwowe Estonii. W kolejnych latach restrykcje objęły także członków grup hakerskich, np. Callisto, Armageddon, Wizard Spider, Z-Pentest i NoName057(16), odpowiedzialnych za cyberataki m.in. na sektor zdrowia, finansowy, obronny czy wodociągowy w UE. Sankcjami objęto również firmy hostingowe i twórców złośliwego oprogramowania wspierających rosyjskie operacje cybernetyczne.

Znacznie szerszy zakres miały sankcje nakładane od 2024 r. za rosyjskie działania destabilizacyjne. Objęły m.in. uczestników kampanii dezinformacyjnej „Doppelgänger" (Sobowtór), osoby związane z aktami wandalizmu i zastraszania w Estonii, kampaniami wywołującymi napięcia społeczne we Francji czy współpracujące z niemiecką skrajną prawicą wspierającą rosyjskie cele polityczne. Objęły także osoby odpowiedzialne za finansowanie wybranych

środowisk politycznych i kandydatów do Parlamentu Europejskiego. Restrykcje nałożono również w odpowiedzi na szerokie spektrum działań wywiadowczych, m.in. operację szpiegowską przeciwko niemieckiej Federalnej Służbie Wywiadowczej, werbunek sabotażystów (m.in. w celu podpalenia Muzeum Okupacji w Rydze przy użyciu koktajli Mołotowa), zakłócanie sygnału GPS nad Morzem Bałtyckim oraz wykorzystywanie statków rybackich do rozpoznawania infrastruktury krytycznej i obiektów wojskowych na Bałtyku i Morzu Północnym. W 2026 r. rozszerzono sankcje na propagandystów i uczestników rosyjskich operacji informacyjnych, w tym prezenterów telewizyjnych, dziennikarzy, blogerów, influencerów i artystów rozpowszechniających prorosyjskie narracje.

Znaczenie sankcji. Restrykcje służą przede wszystkim politycznemu przypisywaniu odpowiedzialności za działania hybrydowe. Wspólne wskazanie sprawców przez państwa UE wzmacnia ocenę zagrożeń i stanowi ważny sygnał polityczny. Zwiększa też w społeczeństwach świadomość skali rosyjskich działań destabilizacyjnych.

Sankcje mogą również podnosić koszty takich operacji, zwłaszcza jeśli prowadzą je podmioty utrzymujące relacje gospodarcze z UE. Zamrożenie aktywów, ograniczenie dostępu do usług finansowych czy utrudnienia handlowe zmniejszają możliwości ich działania. Przykładowo objęte sankcjami duże rosyjskie przedsiębiorstwa połowowe Norebo JSC i Murman Sea Food utraciły dostęp do ważnego rynku europejskiego, a Norebo JSC także możliwość połowów w norweskiej wyłącznej strefie ekonomicznej. Sankcje państw G7+, w tym UE, wobec istotnej rosyjskiej firmy hostingowej Media Land LLC i jej spółki ML.Cloud ograniczyły im dostęp do zachodnich klientów i infrastruktury. Nie pozbawiły ich jednak całkowicie zdolności działania, ponieważ mogły korzystać z zagranicznych pośredników.

Restrykcje bywają szczególnie dotkliwe dla obywateli UE zaangażowanych w rosyjskie operacje informacyjne. Utrudniają im prowadzenie działalności zarobkowej, dlatego część z nich zaskarżyła decyzje sankcyjne, wskazując m.in. na naruszenie wolności słowa. Przykładem są biznesmen i były oficer wojskowy Xavier Moreau (odwołanie odrzucone z przyczyn proceduralnych) oraz niemieccy blogerzy Thomas Röper i Alina Lipp (sprawy dotychczas nie rozstrzygnięto). Röper argumentował, że sankcje doprowadziły do utraty kanałów płatności, współpracy biznesowej oraz części dochodów ze sprzedaży książek i z darowizn. Dotychczasowe orzecznictwo Sądu UE nie podważa możliwości nakładania sankcji na uczestników operacji informacyjnych, ale koncentruje się głównie na ocenie jakości dowodów i proporcjonalności środków. Restrykcje uznawane są za zgodne z zasadą wolności wypowiedzi, ponieważ nie zakazują działalności medialnej, lecz utrudniają jej finansowanie.

Najważniejsze ograniczenia. Wyzwaniem są przede wszystkim stosunkowo niskie koszty prowadzenia operacji wpływu, cyberataków i kampanii dezinformacyjnych, a także ich zdecentralizowany charakter. Likwidacja jednej sieci lub kanału działania często prowadzi do szybkiego powstawania kolejnych struktur. Rosja wykorzystuje też zagranicznych pośredników, którzy nie posiadają aktywów ani istotnych interesów gospodarczych w UE, więc są w dużej mierze odporni na oddziaływanie restrykcji.

Dodatkowym problemem jest rozwój nowych technologii. Sztuczna inteligencja, kryptoaktywa oraz nowe platformy komunikacyjne ułatwiają finansowanie operacji wpływu i rozpowszechnianie treści dezinformacyjnych. Skuteczność restrykcji osłabiają również różnice w monitorowaniu i egzekwowaniu przepisów sankcyjnych przez państwa członkowskie oraz liczne sposoby obchodzenia restrykcji w internecie, m.in. poprzez alternatywne domeny, sieci VPN czy platformy IPTV.

Znacznym ograniczeniem pozostają też trudności z identyfikacją sprawców i zgromadzeniem odpowiedniego materiału dowodowego. Przypisanie odpowiedzialności za cyberataki, operacje wpływu czy działania sabotażowe często trwa latami i wymaga wykazania związku między konkretną operacją a odpowiedzialnymi za nią osobami lub podmiotami. Proces ten utrudniają ograniczona wymiana informacji niejawnych między państwami członkowskimi oraz niewystarczające zasoby przeznaczone na monitorowanie finansowej strony działań hybrydowych, w tym przepływów związanych z kryptowalutami. W konsekwencji sankcje są zazwyczaj nakładane z opóźnieniem, co zmniejsza ich efekt odstraszający.

Wnioski. Unijna polityka sankcyjna ewoluowała od reagowania na pojedyncze cyberataki do odpowiedzi na całe spektrum rosyjskich działań hybrydowych. Choć sankcje nie są narzędziem zdolnym samodzielnie powstrzymać operacje destabilizacyjne, odgrywają ważną rolę w przypisywaniu odpowiedzialności, budowaniu świadomości zagrożeń i częściowym zwiększaniu kosztów rosyjskich działań.

W przyszłości większe znaczenie może mieć ograniczanie źródeł finansowania operacji wpływu poprzez obejmowanie sankcjami całych sieci powiązań finansowych, w tym w sferze kryptowalut. Skuteczność restrykcji mogłoby zwiększyć także szersze ich nakładanie na infrastrukturę technologiczną wspierającą działania hybrydowe, w tym firmy hostingowe, operatorów domen, sieci reklamowe i dostawców usług cyfrowych. Istotne będą również szybsza identyfikacja sprawców, zamrażanie aktywów kluczowych pośredników w państwach trzecich, łączenie sankcji z postępowaniami karnymi oraz ściślejsza współpraca z USA, Wielką Brytanią i pozostałymi państwami G7. W takim ujęciu sankcje stałyby się elementem strategii przeciwdziałania zagrożeniom hybrydowym.

Analiza przygotowana we współpracy z Weroniką Moroz.

Tabela

Osoby i podmioty objęte sankcjami UE za cyberataki i działania destabilizacyjne Rosji w latach 2020–2026

System sankcji za destabilizacyjne działania Rosji			
Data	**Osoby**	**Podmioty**	**Charakterystyka pakietu**
16 grudnia 2024 r.	1. Artiom Siergiejewicz Kuriejew 2. Nikołaj Aleksandrowicz Tupikin 3. Sofija Awramowna Zacharowa 4. Andriej Władimirowicz Awierjanow 5. Tinatin Giwijewna Kandelaki 6. Władimir Władimirowicz Sergijenko 7. Denis Aleksandrowicz Smolaninow 8. Wołodimir Lipczenko 9. Jurij Sizow 10. Wisa Nochajewicz Mizajew 11. Olga Aleksiejewna Bielawcewa 12. Timofiej Wiaczesławowicz Bordaczew 13. Harouna Douamba 14. Antolii Prizenko 15. Alesja Miłoradowicz 16. Oleg Siergiejewicz Jeriemienko	1. Jednostka GRU nr 29155 ФКУ „Войсковая часть 29155” (Moskwa) 2. Groupe Panafricain pour le Commerce et l’Investissement GPCI (Lome) 3. African Initiative (Moskwa)	Jednostka i oficerowie rosyjskich służb specjalnych i sił zbrojnych; osoby i podmioty zaangażowane w operacje wpływu i dezinformację w UE i Afryce.
20 maja 2025 r	17. Alik Jurjewicz Chuczbarow (obywatelstwo: rosyjskie, estońskie) 18. Ilja Siergiejewicz Boczarow 19. Jelena Kołbasnikowa 20. Hüseyin Dogru 21. Julia Siergiejewna Prochowa 22. Rostisław Tiesluk 23. Alina Lipp (obywatelstwo niemieckie) 24. Wiktor Władimirowicz Miedwiedczuk 25. Artem Pawłowicz Marczewśkyj 26. Natalja Sudlenkowa 27. Iurie Neculiti 28. Ivan Neculiti 29. Andriej Charkowskij 30. Antolij Jurjewicz Abramow 31. Rusłan Wasiljewicz Niestierienko 32. Wiktor Aleksandrowicz Łukowienko 33. Oleg Anatolijowycz Wołoszyn 34. Justin Blaise Tagouh (obywatelstwo: rosyjskie, estońskie) 35. Michaił Michajłowicz Prudnikow 36. Sylvain Afoua (obywatelstwo: francuskie, togijskie) 37. Thomas Röper (obywatelstwo niemieckie)	4. AFA Media (Stambuł) 5. Voice of Europe (Praga) 6. Norebo JSC (Murmańsk) 7. Murman Sea Food (Murmańsk) 8. Przedsiębiorstwo unitarne Main Radio Frequency Center (Moskwa) 9. Stark Industries Solutions Ltd. (Londyn)	Propagandyści, blogerzy, firmy medialne, przedsiębiorstwa połowowe wykorzystywane do działań rozpoznawczych, podmioty prowadzące operacje wpływu w Europie i Afryce oraz osoby związane z kanałem Voice of Europe i kampaniami dezinformacyjnymi.

26 czerwca 2025 r.	38. Nathalie Yamb		Influencerka w mediach społecznościowych. Od 2019 r. otwarcie wspiera Rosję, powtarza jej narracje i atakuje Francję oraz Zachód, by osłabić ich wpływy w Afryce. Ma również szczególne powiązania z AFRIC, organizacją łączoną z rosyjskimi prywatnymi firmami wojskowymi.
15 lipca 2025 r.	39. Andriej Jurjewicz Romanczenko 40. Władimir Najdienow 41. Dmitri Buimistru 42. Veaceslav Valico 43. Simeon Boikov 44. Witalij Kulikow 45. Jurij Iłłarionowicz Łastoczkin 46. Jewgienij Szewczenko 47. Aleksiej Nikołajewicz Szawrow	10. Federalne przedsiębiorstwo państwowe „Sieć Radiowo-Telewizyjna Rosji" (RTRS) (Moskwa) 11. Wydzielony ośrodek walki radioelektronicznej Floty Bałtyckiej (obwód królewiecki) 12. BRICS Journalist Association 13. Center for Geopolitical Expertise (Moskwa) 14. Foundation to Battle Injustice 15. Tiger Web	Osoby i podmioty odpowiedzialne za dezinformację, manipulację informacyjną oraz zakłócanie sygnałów nawigacyjnych GNSS w Europie.
15 grudnia 2025 r.	48. John Mark Dougan 49. Andriej Andriejewicz Suszencow 50. Dmitrij Wiaczesławowicz Susłow 51. Fiodor Aleksandrowicz Łukjanow 52. Iwan Nikołajewicz Timofiejew 53.Andriej Gieorgijewicz Bystrickij 54. Władisław Jewgienjewicz Borowkow 55. Dienis Igoriewicz Denisienko 56. Dmitrij Jurjewicz Gołoszubow 57. Jacques Baud 58. Xavier Moreau (obywatelstwo francuskie) 59. Diana Witaljewna Panczenko	16. 142. Samodzielny Batalion Walki Radioelektronicznej (Kumaczewo) 17. Międzynarodowy Ruch Rusofilów	Osoby i podmioty odpowiedzialne za działania hybrydowe, w tym kampanie dezinformacyjne, propagandę prorosyjską oraz cyberataki wymierzone w państwa UE, NATO i Ukrainę.
29 stycznia 2026 r.	60. Dmitrij Wiktorowicz Gubernijew 61. Jekatierina Siergiejewna Andriejewa 62. Marija Eduardowna Sittiel 63. Pawieł Aleksandrowicz Zarubin 64. Roman Wasiljewicz Czumakow 65. Siergiej Władimirowicz Połunin		Propagandyści, w tym prezenterzy rosyjskiej telewizji i artyści
16 marca 2026 r.	66. Siergiej Aleksandrowicz Kluczenkow 67. Ernest Gedrevich Mackevicius (obywatelstwo: litewskie, rosyjskie) 68. Graham Williams Phillips 69. Adrien Bocquet (obywatelstwo: francuskie, rosyjskie)		Propagandyści

21 kwietnia 2026 r.		18. Euromore (Bruksela) 19. Fundacja na rzecz Wsparcia i Ochrony Praw Rodaków Mieszkających za Granicą (Pravfond) (Moskwa)	Podmioty odpowiedzialne za destabilizację, w tym platforma medialna nagłaśniająca kremlowską propagandę.
15 czerwca 2026 r.	70. Marija Władimirowna Dudko 71. Alexandra Jost 72. Roman Jurjewicz Antonowskij 73. Pawieł Aleksiejewicz Astachow 74. Olga Adolfowna Kirij 75. Igor Walentinowicz Malcew 76. Marija Jurjewna Wołkonskaja 77. Anatolij Aleksandrowicz Kuziczew 78. Gieorgij Aleksandrowicz Szewkunow 79. Kirill Fedorov (obywatelstwo łotewskie)	20. Prezydencka Fundacja Inicjatyw Kulturalnych/PFKI (Moskwa)	Propagandyści.
13 lipca 2026 r.	80. Iwan Siergiejewicz Kasjanienko		Zastępca dowódcy Służby ds. Operacji Specjalnych (SSD), współorganizował działania jednostki związanej z Afganistanem, w tym wypłaty zachęcające do ataków na personel USA i koalicji międzynarodowej działającej w Afganistanie. Koordynował też działania związane z otruciem Siergieja Skripala i jego córki oraz zarządzał sieciami Grupy Wagnera w Afryce, a także wspólne z Iranem projekty wojskowo-techniczne.
24 września 2026 r.	81. Ksenija Władimirowna Fiodorowa		Rosyjska osoba publiczna związaną z mediami oraz była członkini kierownictwa stacji Russia Today (RT) we Francji. Pełniąc funkcję prezesa i dyrektora ds. informacji w RT France, brała udział w wdrażaniu i propagowaniu linii redakcyjnej tej stacji, w tym narracji prorosyjskich

16 listopada 2026 r.	82. Andriej Naumowicz Perła 83. Aleksiej Witaljewicz Uljanow 84. Wiktor Nikołajewicz Ostrieszko 85. Anastazja Olegowna Kazakowa 86. Władimir Igoriewicz Gołowaszyn 87. Aleksandr Pawłowicz Koczetow 88. Siergiej Wiaczesławowicz Tatti 89. Jelena Grigorjewa 90. Olga Aleksandrowna Połosina 91. Wiktoria Igoriewna Gordiejewa 92. Andriej Pietrowicz Manzolewskij 93. Michaił Alieksandrowicz Barajew 94. Aleksiej Władimirowicz Miedwiediew 95. Jan Giennadijewicz Nalimow 96. Jewgienija Wiraczewa 97. Gulnara Wilsurowna Androsowa 98. Igor Władimirowicz Bogatyriew 99. Władimir Wiktorowicz Kremlew 100. Siergiej Nikołajewicz Korsun 101. Armen Genrichowicz Asrjan 102. Ilja Władimirowicz Lipkind 103. Władimir Aleksandrowicz Troszyn 104. Aleksiej Andriejewicz Klimowskij 105. Alina Maratowna Gabdullina 106. Chay Bowes (obywatelstwo irlandzkie) 107. Aleksiej Stiepanow 108. Witalij Borisowicz Jelisiejew 109. Jurij Iwanowicz Podolaka 110. Daniił Wiktorowicz Biezsonow 111. Piotr Walentinowicz Marczenko	21. Social Design Agency LLC, SDA (Agencja Projektowania Społecznego LLC), znana również jako Agentstvo Sotsialnogo Proektirovania (ASP)	SDA to moskiewskie przedsiębiorstwo zajmujące się public relations i technologią polityczną, które realizuje zakrojone na szeroką skalę projekty manipulacji informacjami i ingerencji w informacje (finansowane, kierowane i nadzorowane przez rosyjską administrację prezydencką). Pracownicy SDA, dziennikarze, blogerzy.
System sankcji UE za cyberataki			
Data	**Osoby**	**Podmioty**	**Charakterystyka pakietu**
30 lipca 2020 r.	1. Aleksiej Walerjewicz Minin 2. Aleksiej Siergiejewicz Moreniec 3. Jewgienij Michajłowicz Sieriebriakow 4. Oleg Michajłowicz Sotnikow	1. The Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Rosyjskie cyberataki były wymierzone w organizacje międzynarodowe, infrastrukturę energetyczną oraz przedsiębiorstwa i instytucje publiczne. Obejmowały próby włamania do sieci OPCW, atak NotPetya powodujący masowe straty gospodarcze oraz operacje zakłócające funkcjonowanie ukraińskiej sieci energetycznej.

22 października 2020 r.	7. Dmitrij Siergiejewicz Badin 8. Igor Olegowicz Kostiukow	2. Główny Ośrodek Służb Specjalnych (GTsSS) Głównego Zarządu Sztabu Gene ralnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU)	Rosyjskie cyberataki były wymierzone w systemy informatyczne instytucji państwowych, w tym niemieckiego parlamentu, prowadząc do kradzieży poufnych danych i przejęcia kont e-mail polityków, w tym kanclerz Angeli Merkel.
24 czerwca 2024 r.	9. Rusłan Aleksandrowicz Pieretiatko 10. Andriej Stanisławowicz Koriniec 11. Ołeksandr Sklanko 12. Mykoła Czernych 13. Michaił Michajłowicz Carew 14. Maksim Siergiejewicz Gałoczkin		Rosyjskie cyberataki były wymierzone w infrastrukturę krytyczną, państwowe systemy informatyczne oraz instytucje odpowiedzialne za obronność, bezpieczeństwo i relacje zagraniczne państw UE i Ukrainy. Obejmowały phishing, ransomware i złośliwe oprogramowanie służące kradzieży wrażliwych danych oraz zakłócaniu usług, m.in. w sektorach zdrowia i bankowości.
27 stycznia 2025 r.	15. Nikołaj Aleksandrowicz Korczagin 16. Witalij Szewczenko 17. Jurij Fiodorowicz Denisow		Rosyjskie cyberataki były wymierzone w instytucje rządowe państw UE, w tym ministerstwa Estonii, oraz prowadziły do kradzieży poufnych dokumentów, danych zdrowotnych i innych wrażliwych informacji.
13 lipca 2026 r.	20. Witalij Nikołajewicz Kowal 21. Aleksandr Aleksandrowicz Wołosowik 22. Denis Olegowicz Diegtiarienko 23. Julija Władimirowna Pankratowa 24. Maksim Jewgienjewicz Woronin 25. Maksim Aleksandrowicz Gordijenko 26. Jewgienij Wiktorowicz Baaszew 27. Roman Aleksandrowicz Puntus	3. Media Land LLC (Sankt Petersburg) 4. ML. Cloud (Ryga) 5. Implus LLC (Federacja Rosyjska) 6. Z-Pentest (Federacja Rosyjska)	Przedmiotem rosyjskich cyberataków były przede wszystkim infrastruktura krytyczna (zwłaszcza sektory energetyczny i wodociągowy) oraz instytucje rządowe, finansowe i media w państwach UE, Ukrainie i innych krajach wspierających Ukrainę. Ataki obejmowały ransomware, phishing, DDoS i kradzież danych.
16 listopada 2026 r.		7. NoName057(16)	NoName057(16) jest prorosyjską grupą hakerską, która prowadziła ataki na usługi niezbędne do utrzymania podstawowej działalności społecznej i gospodarczej oraz krytycznych funkcji państwa w krajach członkowskich, w tym na portale rządowe, służby wywiadu wojskowego, partie polityczne i kandydatów w czasie procesów wyborczych, sektor energetyczny i przemysłowy, infrastrukturę transportową, instalacje wodociągowe, banki, instytucje finansowe i internetowe usługi płatnicze oraz krajowe urzędy pocztowe.

Źródło: Opracowanie własne na podstawie rozporządzenia Komisji Europejskiej, 2026.

Redakcja: Jacek Foks, Rafał Tarnogórski, Marcin Terlikowski, Justyna Szczudlik
Jędrzej Czerep, Anna Maria Dyner, Amanda Dziubińska, Mateusz Piotrowski, Daniel Szeligowski, Jolanta Szymańska, Damian Wnukowski, Szymon Zaręba, Tomasz Żornaczuk