Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

CYBER STATECRAFT
INITIATIVE

COLLECTIVE CYBERSECURITY FOR THE THREE SEAS

Safa Shahwan Edwards, Simon Handler,
Trey Herr, Adam Marczyński, and Jakub Teska

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

CYBER STATECRAFT
INITIATIVE

COLLECTIVE CYBERSECURITY FOR THE THREE SEAS

Safa Shahwan Edwards, Simon Handler,
Trey Herr, Adam Marczyński, and Jakub Teska

ISBN-13: 978-1-61977-184-0

Cover: Earth viewed from space at night with lights and connections from cities. Source: iStock/imaginima

June 2021

Atlantic Council, 1030 15th Street NW, 12th Floor, Washington, DC 20005

SCOWCROFT CENTER FOR STRATEGY AND SECURITY

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

CYBER STATECRAFT INITIATIVE

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

SUPPORTED BY

This report was produced as part of the Cyber Statecraft Initiative's work focused on cloud computing in partnership with PKO Bank Polski.

PKO Bank Polski

ABOUT PKO BANK POLSKI

Headquartered in Warsaw, Poland, **PKO Bank Polski** is the largest bank in Poland and is at the forefront of securing digital transformation in Central and Eastern Europe through policy, innovation, and private sector leadership. To that end, the company has invested in building the Polish National Cloud, leveraging transatlantic collaboration to bolster Poland's cybersecurity.

Table of Contents

Executive Summary

Around the world, societies' dependence on technology is increasing. In Central and Eastern Europe's Three Seas region, twelve countries have joined together to invest in critical infrastructure projects and increase interconnectivity on energy, infrastructure, and digitization efforts along the way. As the Three Seas Initiative Investment Fund makes investments that offer increased efficiencies and boost the region's economic potential, these large infrastructure projects also present new sources of risk in a challenging security environment. To strengthen the resilience of these technical investments and better bind together the defensive cybersecurity operations of these societies, Three Seas member states should establish a regional hub for cybersecurity together with key private sector partners. This hub could function as a shared platform for collective security against adversaries targeting critical infrastructure and ever more popular cloud services.

Introduction

Countries in the Three Seas region of Central and Eastern Europe are increasing their dependence on technology and investing heavily in critical infrastructure. While these investments offer increased efficiencies and bolster the region's economic potential, they also present new sources of risk in an already challenging security environment. Threat actors' interest in the Three Seas region has been characterized by a recent history of bold offensive cyber operations targeting both military and civilian infrastructure. Regional owners and operators of critical infrastructure are benefitting from concerted investment efforts led by the Three Seas Initiative, but fully capturing those benefits requires similarly concerted investments to improve security.

To protect their investments and create more resilient societies, governments of the Three Seas should collaborate with one another and with private industry to establish a regional hub for cybersecurity. This hub should leverage existing digital transformation efforts and the widening adoption of common cloud services to provide a basis for collective cybersecurity across the Three Seas region. The cybersecurity center should further convene stakeholders to reinforce regional collaboration, integration, and protection of regional infrastructure projects for years to come. Three Seas has created the opportunity for technologically advanced members like Poland and Estonia to shape investments that protect the whole of the Three Seas community and provide a shared platform for collective security against adversaries targeting critical infrastructure.

Three Seas Initiative

The Three Seas Initiative is an international project established by Croatian President Kolinda Grabar-Kitarović and Polish President Andrzej Duda to address the European infrastructure gap highlighted in 2014 by General James L. Jones, former national security advisor to US President Barack Obama and executive chairman emeritus of the Atlantic Council. Established in 2015, the Three Seas Initiative seeks to increase interconnectivity on energy, infrastructure, and digitization efforts in Central and Eastern Europe.[1] The initiative is comprised of twelve states, running north to south from the Baltic to the Adriatic and Black Seas: Austria, Bulgaria, Croatia, Czechia, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia, and Slovenia. The initiative's motives for funding and coordinating the development of cooperative infrastructure, energy, and digitalization projects are threefold. First, this effort helps realize the market potential of the region, which boasts a population of 110 million and a gross domestic product growth rate that amounts to a sizeable portion of the European Union's.[2] Second, the initiative increases regional integration through the development of shared regulations and infrastructure. Third, it strengthens the transatlantic community through economic prosperity and cooperation, maintaining Europe's position as a reliable security and economic partner of the United States while decreasing dependence on foreign energy imports.[3]

In June 2019, the twelve states making up the initiative established the Three Seas Initiative Investment Fund to serve as an investment vehicle for regional infrastructure, energy, and digital projects. The initiative's fund receives contributions from all member states, sponsored by their respective banking institutions, as well as international financial institutions and the United States.[4]

Risks to the Region

The efforts of the Three Seas Initiative are complicated by the region's unique heritage and cyber threat landscape. Not only is the Three Seas region located in Russia's near abroad, it is also comprised of several post-Soviet (Estonia, Latvia, and Lithuania) and former Soviet (Poland, Hungary, Romania, Bulgaria, and Czechia) satellite states that have experienced aggression in the cyber domain firsthand. While the region has developed the political will to invest in infrastructure that will decrease European reliance on foreign energy imports, it is this same infrastructure that may leave the region vulnerable to cyberattacks, just as threat actors have targeted the critical infrastructure of other countries.[5]

Cloud computing creates opportunities to better manage the risk associated with these regional threats while adding new risks of its own. Leveraging common security teams and insights on secure hardware and software gleaned from a global customer base, companies like Amazon, Microsoft, and Google are already offering services to member states in the region. While the cloud is no security panacea, it can provide a common technology base to share threat information and coordinate responses to new vulnerabilities at substantially greater speed and scale. Cloud computing can enable Three Seas members to invest in new technologies while earmarking resources to secure their critical infrastructure. Governments of the Three Seas region must collaborate with one another and private industry to build resilience in these technologies and increasingly digitized regional commerce. This collaboration can be facilitated by a regional hub—a security center for the cloud and for Three Seas digital projects—reinforcing regional collaboration and integration and protecting the region's infrastructure for years to come.

Vision in Brief

The Three Seas region is bursting with infrastructure investment opportunities and potential. In a list of the most attractive countries in the world for infrastructure investment, a 2019 ranking included seven members of the initiative—Austria (number eleven), Poland (nineteen), Czechia (twenty-three), Slovakia (twenty-four), Hungary (twenty-eight), Romania (thirty-nine), and Bulgaria (forty-one).[6] Relative political stability, strong market potential, and favorable policies have led to significant investments in areas such as aviation, green energy, and telecommunications. To promote cohesion, interconnection, and future investment, the Three Seas Initiative has channeled

1 David Wemer, "The Three Seas Initiative Explained," *New Atlanticist* (blog), Atlantic Council, February 11, 2019, www.atlanticcouncil.org/blogs/new-atlanticist/the-three-seas-initiative-explained-2/.

2 SpotData, *Perspectives for Infrastructural Investments in the Three Seas Region*, 2019, https://3siif.eu/wp/wp-content/uploads/2019/11/SpotData_Report_Three-Seas-region.pdf.

3 EuroStat, "From Where Do We Import Energy and How Dependent Are We?" 2020, https://ec.europa.eu/eurostat/cache/infographs/energy/bloc-2c.html.

4 US Department of State, "Deputy Secretary Biegun's Remarks at the Three Seas Initiative Virtual Ministerial," December 1, 2020, https://2017-2021.state.gov/deputy-secretary-bieguns-remarks-at-the-three-seas-initiative-virtual-ministerial/index.html.

5 Steve Ranger, "Russian Cyberattacks an 'Urgent Threat' to National Security," ZDNet, July 21, 2020, https://www.zdnet.com/article/russian-cyberattacks-an-urgent-threat-to-national-security/.

6 "Europe: Brimming with Opportunities," CMS, 2019, https://cms.law/en/zaf/publication/bridging-continents-infrastructure-index-2019/europe-brimming-with-opportunities.

its focus into forty-eight interconnection projects, broken into three primary categories: energy, digital, and transport.[7]

While digital innovation is just one dimension of infrastructure interconnection, transformation in this area can open opportunities for the other areas of infrastructure development. By 2022, there will be an estimated 365 million users and two billion devices connected to the internet in Central and Eastern Europe.[8] The adoption of cloud computing services stands to facilitate innovation and development across various critical infrastructure sectors.

Digital transformation opens the door for startups and large enterprises alike to access new technology, information, and customers. Critical infrastructure sectors, and states' economic and national security more broadly, will increasingly depend on cloud computing as a standard information technology (IT) practice. But investment in cloud computing technology and infrastructure in the Three Seas is hardly a distant goal—major service providers are pouring resources into regional infrastructure. Microsoft, for instance, announced a billion-dollar investment plan for digital transformation in Poland, including the establishment of a data center region in the country.[9] Google, for its part, cited Poland's growth potential as reason for its decision to invest as much as $2 billion in a Warsaw cloud services data center.[10]

The Three Seas Digital Highway project, proposed by Poland, may build off these high-profile investments in the country by enabling improved data transfer across Three Seas countries with new fiber-optic and 5G telecommunications infrastructure. Other digital project proposals include the digitalization toward interoperability of the energy sector across the Three Seas. Digital investment and integration across member states is increasingly part of core development plans and will be a central pillar of economic growth where these technologies are secure and their users well-defended.

Why Security for Cloud and Three Seas?

Heavy investment in Three Seas digital infrastructure requires proportionate dedication to security. From a business angle, it is critical to both protect existing investments—from state-sponsored threats and otherwise—and drive future growth. Malicious threat actors have long sought to exert influence, sow unrest, and divide countries within the Three Seas region, leaning on cyber operations to target critical infrastructure sectors. For example, since 2015, state-sponsored hackers have conducted various cyber-espionage and reconnaissance campaigns targeting Baltic energy networks.[11] As critical infrastructure operators shift toward cloud computing, they also open new avenues for attack. To counter the common threat actors, protect investments, and secure future business opportunities, the Three Seas would benefit from a regional security center for public and private sector partners to convene to share threat intelligence and collaborate on defense.

A strong value proposition from the center could attract important players involved in cybersecurity efforts across the region. Regional investments in infrastructure are broad in scope and increasingly leverage information and operational technologies. As cloud adoption grows in the region, tightly linking these investments to rigorous security best practices will bolster the security of states and businesses across the Three Seas.

Experts discussed the notion of a cyber alliance at the 2019 Atlantic Council and PKO Bank Polski Cyber Strategy Conference in Warsaw.[12] By organizing around collective security, a Three Seas center would offer states the infrastructure and opportunity to form what would manifest as a formal collaboration among nations and the private sector for cybersecurity against common

7 The Three Seas Initiative, *The Three Seas Initiative: Priority Interconnection Projects*, 2018, http://three-seas.eu/wp-content/uploads/2018/09/LIST-OF-PRIORITY-INTERCONNECTION-PROJECTS-2018.pdf.

8 "Central and Eastern European Data Center Markets - Investment Analysis and Growth Opportunities 2020-2025 - ResearchAndMarkets.com - Research and Markets," *Business Wire*, June 5, 2020, https://www.businesswire.com/news/home/20200605005238/en/Central-Eastern-European-Data-Center-Markets--.

9 "Microsoft Announces a $1 Billion Digital Transformation Plan for Poland, Including Access to Local Cloud Services with First Datacenter Region," Microsoft News Centre Europe, May 5, 2020, https://news.microsoft.com/europe/2020/05/05/microsoft-announces-a-1-billion-digital-transformation-plan-for-poland-including-access-to-local-cloud-services-with-first-datacenter-region/.

10 Rich Duprey, "Google Investing $2 Billion in Cloud Infrastructure Center in Poland," The Motley Fool, June 24, 2020, https://www.fool.com/investing/2020/06/24/google-investing-2-billion-in-cloud-infrastructure.aspx.

11 Stephen Jewkes and Oleg Vukmanovic, "Suspected Russia-Backed Hackers Target Baltic Energy Networks," Internet News, Thomson Reuters, May 11, 2017, https://www.reuters.com/article/us-baltics-cyber-insight/suspected-russia-backed-hackers-target-baltic-energy-networks-idUSKBN1871W5.

12 Atlantic Council, "Marek Zagórski - The Role of Technology and Innovation in a Changing International Environment," via YouTube, January 17, 2019, https://www.youtube.com/watch?v=GUo32US7U7Y&t=18s.

threats. This sort of institutional model is missing in much of the West, but long sought as a forum for strengthening trust through regular engagement and cooperation, exchanging data, and improving interoperability. This vision could serve as a model for like-minded states in other regions to effectively collaborate to strengthen ties in cyberspace.

Regional cybersecurity cannot be a responsibility borne entirely by firms whose infrastructure crisscrosses the continent, nor by a handful of states alone. Involving all, or at least most, of the Three Seas states at a national level is vital to addressing regional critical infrastructure protection and deriving maximum value from the Three Seas investment fund. Swift information sharing, common cybersecurity investment, broad cybersecurity skill building, and widely available security awareness and education will enable the digital transformation of the Three Seas region. The Three Seas Cybersecurity Center would be a mechanism to enable that cooperation among states and close alignment between the private and public sectors.

What Is in a Three Seas Cybersecurity Center?

At a high level, a regional cybersecurity center for the Three Seas could improve cybersecurity, cooperation, and protection of regional infrastructure investments funded by the Three Seas Initiative. This regional cybersecurity center would provide cybersecurity guidance for an array of stakeholders (from governments to corporations, researchers, and civil society organizations) and build trust and support among these varied groups.

The center's functions could be broken down into five areas: operational security, information-sharing, international cooperation, skills and competencies, and standardization. First, the center would focus on securing and protecting regional critical infrastructure and Three Seas Fund investments. Second, the center would serve as an information hub, creating a network of organizations that gathers, analyzes, and circulates information about ongoing cyber incidents, threat actors, and response methodologies. Third, the center would collaborate and coordinate with national incident response teams, international cybersecurity centers, regulators, and civil society organizations to best manage risks across the Three Seas cybersecurity ecosystem. Fourth, the center would concentrate talent from across borders and advance the competencies needed to protect core infrastructure and organizations. Fifth, and finally, the center would support the standardization of cybersecurity taxonomy, incident response protocol, certifications, and best practices across the Three Seas region.

FUNCTION	VALUE
Operational Security	Protect regional critical infrastructure and Three Seas Fund investments.
Information-Sharing	Create a network that gathers, analyzes, and circulates information and best practices regarding stakeholder organizations, Three Seas Initiative programs and investments, and threat actors.
International Cooperation	Collaborate and coordinate with national incident response teams, international cybersecurity centers (e.g., the NATO Cooperative Cyber Defence Centre of Excellence), regulators, and civil society organizations to best manage risks across the cybersecurity ecosystem.
Skills and Competencies	Concentrate and advance cyber workforce skills and competencies needed to protect regional infrastructure and organizations.
Standardization	Standardize cybersecurity taxonomy, incident response protocol, certifications, and best practices across the region.

Membership

The creation of such a center would help mitigate the risks and vulnerabilities associated with the adoption of new technical infrastructure and services across the Three Seas region. As these risks and vulnerabilities impact a broad array of organizations, the center could provide immediate value by convening governments, private industry, and civil society to collaborate and secure Three Seas critical infrastructure. Government entities would be provided an outlet to collaborate with companies that operate and steward the infrastructure they fund. Involving these states would

provide the center with a clear mission and help motivate the participation of other entities.

The center would also create a non-adversarial platform for firms to work closely with governments, regulators, and industry peers to develop best practices on infrastructure protection and build links across the cyber ecosystem, reinforcing trust across stakeholder groups. Tools, infrastructure, and data are at the disposal of the private sector, so it is necessary for governments to have a forum to convene with relevant transnational corporations and security experts. Technology giants such as Microsoft and Google are just as important stakeholders as governments and should be accompanied by regional and local cloud service providers. Broadening beyond major cloud providers, the center would also establish an open marketplace for cybersecurity vendors and specialized services companies offering capabilities to Three Seas members from both the public and private sectors. These small and medium-sized firms could contribute to all interested parties, helping extend cybersecurity offerings from cloud service providers with a range of specialized third-party security products.

Nongovernmental organizations would also play an important role. These organizations already serve as important information exchange hubs. Entities like FIRST help coordinate incident and vulnerability response and provide educational resources on secure technology operations and deployment best practices. Potential members like the Cloud Security Forum, ISACA, CIS, (ISC)[2], and the Cloud Native Computing Foundation already have local chapters in the Three Seas region and would be well positioned to support the center's development.

Center Functions and Services

Bearing in mind the rapid development of cloud computing and the sudden digital transformation sparked by the COVID-19 pandemic,[13] the cybersecurity center should focus on offering cloud services and protecting the increasingly digitized critical infrastructure across the Three Seas region. The shortage of technical talent with sufficient expertise in these domains lends urgency to the center's mission, balancing both operational security and incident response with workforce skill building and standards harmonization. This section addresses some of the specific challenges of the move to cloud and where the center could play a role in facilitating secure adoption and operation.

Digital transformation and automation have become a top priority for many organizations. As organizational processes become digitized and automated, challenges with infrastructure and limited computing resources will become more acute. Some local authorities, such as the Polish Financial Supervision Authority, have released guidance on public and hybrid clouds, allowing supervised entities to process customer data and store them in a public cloud.[14] This streamlines contacts among customers, employees, and equipment suppliers and accelerates the shift to cloud.

Cloud computing can offer an array of control and monitoring mechanisms designed to bolster security. These mechanisms allow customers to build infrastructure and assemble services in a controlled environment, while imposing security controls with the push of a button. Technologies such as Terraform and other "code as infrastructure" services allow for quick implementation of what would otherwise be large-scale physical changes, offering flexibility over traditional enterprise IT. This can improve an organization's security against both internal and external threats but also introduce new risks as organizations must understand the new tools and products they are using.

A regional cybersecurity center could help accelerate sensible cloud adoption in the Three Seas region, speeding up post-pandemic digital transformation by improving organizations' security literacy with cloud technologies and enabling them to take full advantage of these benefits while managing the associated risks. While the number of experts with knowledge and experience in cloud computing remains limited, a cybersecurity center has the potential to serve as a regional hub for experts on cloud technology and adoption.

Taking into account the regulatory requirements and environment across the Three Seas region, the cybersecurity center could map regulatory requirements (including the General Data Protection Regulation) that guide cybersecurity monitoring, secrets management, data security, and more for local regulators and partners. Cloud computing and infrastructure security should be the main focus of the cybersecurity center's services and activities to meet the rising demand for best practices, advisory services, and support in these areas. This focus would also help the cybersecurity center provide a coherent platform to enable the automation of cybersecurity data exchange; relationship building; and coordination among its customers, regional and national stakeholders, and Computer Emergency Response Teams.

13 Laura LaBerge, Clayton O'Toole, Jeremy Schneider, and Kate Smaje, "How COVID-19 Has Pushed Companies over the Technology Tipping Point—and Transformed Business Forever," McKinsey & Company, October 5, 2020, https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever#.

14 Urzad Komisji Nadzoru Finansowego, "Communication from the UKNF on Information Processing by Supervised Entities Using Public or Hybrid Cloud Computing Services," January 23, 2020, https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_Chmura_Obliczeniowa_EN_69242.pdf.

Obstacles

While this proposed regional cybersecurity center has great potential to catalyze cybersecurity, resilience cohesion, and interconnectivity in the Three Seas region, there are potential obstacles to its implementation and ultimate success. First, the center will have to address the challenge of developing a shared understanding of and priorities for cybersecurity and infrastructure across twelve countries with unique policy priorities, capabilities, cultures, and languages. Once consensus is eventually developed across stakeholders, the challenge remains to develop a joint educational curriculum, training modules, and shared best practices that account for the varying needs of users responsible for the management or configuration of the cloud and protection of infrastructure.

One area of opportunity that will require effort is the capacity for this regional hub to standardize cybersecurity taxonomy, incident response protocols, certifications, and best practices across a diverse set of stakeholders. While this challenge will require time to overcome, it could pay dividends in the future as Europe continues to grapple with corporations duplicating efforts by developing their own products and each country spearheading individual initiatives and establishing standards that struggle to travel well. This challenge of standardization is perhaps the most crucial as the Three Seas governments are investing billions of dollars in infrastructure and technologies that will cross national borders and will require a set of shared standards and practices that can best support this new level of interconnectivity.

Implementation

Given the obstacles, such as lack of standardization and shared understanding, that a cybersecurity center for the Three Seas might encounter, a thoughtful and pragmatic approach to implementation is required to build confidence early on and attract future investment and participation. Successful buy-in and execution are critical, especially considering the novelty of the project. The center would require a phased approach centered around building trust and cohesion among members. Phase one would prioritize operational security by establishing security-focused procedures and guidelines in operations, phase two would implement security response protocols that could be referenced in the event of a cyber incident, and phase three would shift focus to security planning. Through these three phases, the center could manage complexity while building the trust needed to meet its full potential.

Focusing on combined threat intelligence to meet operational security needs would be a logical first phase for the center. The Three Seas Cybersecurity Center could look to the Hague Security Delta as a model network of organizations, governments, and institutions dedicated to exchanging threat intelligence and collaborating over critical infrastructure protection.[15] As member organizations exchange information, they build trust and in turn grow more comfortable in their ability to execute complex tasks together—a mutually beneficial result for all parties.

Once organizations and states recognize the center as a useful and reliable source of shared knowledge, various forms of cooperation, such as joint incident response, become possible. Even states and organizations lacking experience or resources devoted to cybersecurity incident response stand to gain from collaborating with more established actors in the space. The forum would be beneficial to small and large critical infrastructure operators alike, be it from newfound experience, access to useful intelligence, or as a means of collaboration.

Lastly, the security planning phase of implementation would allow public and private sector organizations that have worked together and built trust to learn from their shared experiences around a set of best practices. Standardization of behavior and certification of solutions across the Three Seas is critical to maximizing efficiency and protecting critical infrastructure. The third phase of implementation should focus on selecting a set of standards and certifications that can be applied across the region.

Conclusion

The transatlantic security relationship rests on long-standing shared values and interests; in the digital age, it also is undergirded by technological entrepreneurism, clear-sighted cybersecurity policies, and a commitment to creating innovative solutions for both today's challenges and the next generation's pressing cyber issues. The Three Seas community is already home to passionate entrepreneurism as countries have banded together to invest in the critical infrastructure supporting the region's future. The challenge that the initiative faces is determining how to develop common policies to unlock the digital potential of societies while combating cyber threats and acting within the transatlantic shared traditions of freedom of expression and the rule of law.

The Three Seas Cybersecurity Center is a manifestation of both operational collaboration and strategic alignment. The center would be a decisive move toward collective security by a vital community against common foes. This paper offers a vision for that center and addresses short-term obstacles as well as steps toward implementation. Should it be realized, such a vision would rest on the outcome of continued cooperation and collective investment from the Three Seas community.

15 "About HSD," The Hague Security Delta, accessed May 14, 2021, https://www.thehaguesecuritydelta.com/about.

About the Authors

Safa Shahwan Edwards is the deputy director of the Atlantic Council's Cyber Statecraft Initiative within the Scowcroft Center for Strategy and Security. In this role, she manages the administration and external communications of the Initiative, as well as the Cyber 9/12 Strategy Challenge, the Initiative's global cyber policy and strategy competition.

Safa holds an MA in International Affairs with a concentration in Conflict Resolution from the George Washington University Elliott School of International Affairs and a BA in Political Science from Miami University of Ohio. Safa is of Bolivian and Jordanian heritage and speaks Spanish and Arabic.

Simon P. Handler is an assistant director of the Atlantic Council's Cyber Statecraft Initiative, within the Scowcroft Center for Strategy and Security. In this role, he manages a wide range of projects at the nexus of geopolitics and international security with cyberspace. Prior to joining the Atlantic Council, he served as a special assistant in the United States Senate, where he worked on foreign policy issues. During his time on the Hill, he was a congressional fellow with the Wilson Center's Congressional Cybersecurity Lab and Congressional Artificial Intelligence Lab and completed the East-West Center's Congressional Staff Program on Asia. He holds a BA in both International Relations & Global Studies, with a concentration in International Security, and Middle Eastern Languages & Cultures from the University of Texas at Austin.

Dr. Trey Herr is the director of the Cyber Statecraft Initiative under the Scowcroft Center for Strategy and Security at the Atlantic Council. His team works on cybersecurity and geopolitics including cloud computing, the security of the internet, supply chain policy, cyber effects on the battlefield, and growing a more capable cybersecurity policy workforce. Previously, he was a senior security strategist with Microsoft handling cloud computing and supply chain security policy as well as a fellow with the Belfer Cybersecurity Project at Harvard Kennedy School and a non-resident fellow with the Hoover Institution at Stanford University. He holds a PhD in Political Science and BS in Musical Theatre and Political Science.

Adam Marczyński is a seasoned security executive, serving as the CISO of the Polish National Cloud Operator (OChK) and the Vice President of Cloud for Health. Adam has 28 years of experience working for IT solutions providers and financial institutions, and has spent the past 14 years focusing on information security and cybersecurity.

In the past, Adam worked for regional and global IT companies, including Bull, Getronics, HP and has served in an array of roles including Europe BCP Manager, CEE Security Officer, Country Security Officer, as well as the CISO of BIK, the Polish Credit Information Bureau.

Adam holds professional certifications including CISA, CISM, CRISC, CISSP, CEH. He is also a lecturer at the Warsaw School of Economics, teaching courses in Information Security, Cloud Cybersecurity, Risk Management and Business Continuity.

Jakub Teska is the Director of the Cybersecurity Architecture and Services Bureau at PKO Bank Polski, where his team works on cloud security, cybersecurity architecture, customer security and security audits. He has carried out projects related to the digital banking security, cybersecurity monitoring, and identity management. He has worked for PKO Bank Polski for 14 years, focusing on Information Technology Security and Cybersecurity.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org