Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

REPORT

Securing Transformation

DECEMBER 2019

TREY HERR AND SAFA SHAHWAN
WITH PAWEŁ PAWŁOWSKI

The Polish-US 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 commitment to clever solutions to the next generation's pressing cyber problems. This hundred-year relationship has been shaped by new developments and old challenges. Poland has transformed itself, building on its tradition of cryptography and emerging as a leader in both cybersecurity and statecraft, as well as developing common Western norms and policies to address threats from Russia, only now manifested in the cyber domain. The challenge is to develop common policies to unlock the digital potential of societies while also combating cyber threats, acting within shared traditions of freedom of expression and the rule of law.

Over the course of 2018 and 2019, the Atlantic Council and PKO Bank Polski have begun to strengthen the pillars of the relationship and drive cross-national engagement through a series of purposeful convenings, bringing together US and Polish cybersecurity and policy experts. The products of these efforts in 2019 were a large conference in Warsaw in January and a closed-door workshop in Washington, DC, in April. Together, these events have catalyzed the formation of a new community between the two nations, and the Atlantic Council partnership with PKO Bank Polski will seek to motivate and strengthen this community in the years to come.

Poland has a dynamic economy, having seen its gross domestic product (GDP) increase more than 150 percent since 1989, with strong technical literacy and a vibrant start-up community. Despite significant security challenges in the region, Poland appears poised to capitalize on the second wave of a digital revolution, with an intensity matched by few peers. The expression of this innovative intensity can be found through policy discussions, business initiatives, and the profile of a country on the rise.

A New Initiative for Poland: A Future Global Leader in Securing the 4th Industrial Revolution

In January, under the leadership of Zbigniew Jagiełło of PKO Bank Polski and Damon Wilson of the Atlantic Council, the city of Warsaw played host to a major conference, "A New Initiative for Poland: A

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.

Future Global Leader in Securing the 4th Industrial Revolution." This high-level conference was part of the larger partnership between the Atlantic Council and PKO Bank Polski, with the aim of deepening US-Polish transatlantic ties and developing cybersecurity as a key pillar in the relationship. The event was an expression of the intense partnership emerging between Poland—a pivotal hub for technology and security leadership in the Three Seas Region—and the United States.

The conference explored cybersecurity issues that underpin Poland's ongoing digital transformation in three tracks—policy, innovation, and private-sector leadership. Convening transatlantic cyber, innovation, defense, and foreign policy experts, the event featured Atlantic Council board directors and other prominent Americans in the cybersecurity and innovation realms. The Warsaw conference highlighted Poland's significant potential to become a global leader in cybersecurity, and emphasized the leading role of the Polish private sector in creating innovative cybersecurity solutions—positioning the country to be a powerhouse on cyber issues in Europe while bolstering Poland's cybersecurity expertise, especially in the policy and strategy spaces.

Across two days of public discussions with high-level Polish and US government, industry, and academic experts, this burgeoning cybersecurity community grappled with some of the most pressing problems facing technology policy today. The conference opened with remarks by **Polish Prime Minister Mateusz Morawiecki**, followed by a keynote from **General Keith Alexander**, former director of the National Security Agency (NSA), on the role of Poland in cryptography during World War II and its impacts on the establishment of the NSA in 1952. The Enigma code was broken by three Polish mathematicians—Jerzy Rozycki, Henryk Zygalski, and Marian Rejewski—through mathematical brilliance and perseverance, which curtailed WWII and saved countless lives. Cyber networks and the cryptology that goes with them are based on mathematics, and Poland is a center of mathematical prowess.

Today, the rapidly changing nature of technology seems to be an intractable problem for the cyber community—how can so many new and groundbreaking technologies be handled effectively? The exponential changes and growth in information and technology confirm that this is the greatest time in history, providing opportunity for governments and private companies to cooperate and achieve common defense and collective security. In this case, Poland is a nation of importance to both the United States and Europe, providing a foundation of stability in Central and Eastern Europe, and collective cybersecurity for the transatlantic alliance as a key pillar of NATO's Eastern Flank.

The opening spotlight discussed superiority, conflict, cooperation, and competition in cyberspace, examining how policy practitioners from the two countries should think about the domain of cyberspace in its entirety—war, peace, and everything in between. The conversation held between **Thomas Bossert**, former assistant to the president for homeland security and counterterrorism, retired **Lieutenant General William Mayville**, the former deputy commander of US Cyber Command, and **H.E. Tomasz Zdzikot**, deputy minister and secretary of state of the Ministry of National Defense of the Republic of Poland, delved into how to unify government and private-sector identification of threats and efforts on cybersecurity. The three speakers identified key elements of strategy necessary to develop a holistic approach to addressing cybersecurity threats on a national level, drawing from the experiences of the United States and Poland in creating their individual cyber commands and cyber strategies, and integrating them with other elements of national power. They stressed the importance of sharing information on cyber incidents between the United States and allied states like Poland. Many malicious Russian capabilities and tactics are used first against Poland and neighboring countries like Ukraine before spreading around the world. Operational collaboration between the public sectors of these states should also be reinforced by public-to-private and private-to-private links, like the tight-knit security community in the Polish and US financial sectors. The discussion concluded that deepening these links would improve the security of all.

The morning spotlights were followed by a keynote from renowned cybersecurity guru **Bruce Schneier**, a fellow with the Belfer Center at Harvard University's John F. Kennedy School. He gave remarks on the role and importance of privacy amidst deepening interconnectivity, before transitioning to the first full panel of the day. Schneier's keynote highlighted the issue of supply-chain security, including the increasing prevalence of attacks. His speech drove discussion throughout the day on how public and private sectors could cooperate to mitigate risk in this domain, including fending off attacks on governments, the

Polish Prime Minister Mateusz Morawiecki delivers opening remarks at the inaugural joint conference between the Atlantic Council's Cyber Statecraft Initiative and PKO Bank Polski.

financial sector, and major information-technology (IT) service companies.

The subsequent panel discussed innovation and cybersecurity as strategic advantages in digital transformation, including how the ubiquity of cybersecurity threats creates both challenges and opportunities for governments and the private sector in working to secure society. **Emily Frye,** the director of cyber integration at MITRE, spoke with **Andrzej Dopierała**, president of Asseco Data Systems, about how to embrace and redefine innovation in policy approaches, technology, research, workforce training, and education to reverse reactionary approaches in the field of cybersecurity and fully unlock digitization's value for both the state and society. Joined by **Barry Pavel**, senior vice president and director of the Scowcroft Center for Strategy and Security at the Atlantic Council, the panel concluded that businesses and governments must embrace new technologies, define strategies that deliver on customer experience, and take a proactive security approach to respond to the current and future threat environment. Their discussion highlighted the importance of fine-tuning regulatory models to balance the demands of corporate governance with the public interest and public-sector objectives. This included the disclosure of vulnerabilities discovered by governments, with discussion highlighting the US Vulnerability Equities Process (VEP).

This panel was followed by a discussion about disinformation in social media as a threat to democratic institutions. Moderated by **Ambassador Daniel Fried**, distinguished fellow at the Atlantic Council and former US ambassador to Poland, it included: **Jakub**

Kalensky, senior fellow at the Atlantic Council; **Dr. Alina Polyakova**, David M. Rubenstein fellow at the Brookings Institution; **H.E. Marek Szczygieł**, ambassador at large for international cyber policy at the Ministry of Foreign Affairs of the Republic of Poland; and **Dr. Bolesław Piasecki**, expert for the security department at PKO Bank Polski. The discussion examined the 2016 presidential election in the United States and elections across Europe in 2017, to uncover lessons about how vulnerable governments and the general public remain to digital disinformation campaigns. The group's discussion evaluated how governments and the private sector collaborate to develop technical and policy solutions to strengthen the integrity of information and challenge the influence of those who seek to destabilize the democratic order. The group debated the extent to which technology giants like Microsoft, Google, and Facebook could self-regulate to assure the security and privacy of their customers.

The successful first day of the conference closed with a panel discussion moderated by **Lieutenant Colonel Robert Kośla**, director of cybersecurity for the Polish Ministry of Digital Affairs, featured: **Adam Marciniak**, vice president with PKO Bank Polski; **Paweł Jakubik**, director of digital transformation in cloud with Microsoft; **H.E. Karol Okoński**, secretary of state for the Ministry of Digital Affairs of the Republic of Poland and the government plenipotentiary for cybersecurity; and **Fred Streefland**, regional chief security officer (CSO) for Palo Alto Networks, on cloud computing and cybersecurity. A rapidly maturing area of enterprise-IT management and security, cloud computing represents a confluence of massively scaled engineering, evolving consumer demand, and novel security challenges. The group looked to address the differences between implemented security systems in the cloud and more traditional structures, and how to safely and effectively implement cloud technologies in public administration and private entities. A keystone in the discussion was how to evaluate the risks of using public cloud technologies—a pressing issue in the United States and Poland, as both governments move to more effectively secure cloud-services hosting and ever more sensitive and impactful information. There was a remarkable distinction in views of the importance of policies around technological sovereignty and their impact on cybersecurity, with European panelists taking a surprisingly dim view of allowing citizens' data to be processed, let alone stored, outside of their countries. The group debated the role of local governments in regulating cloud-services providers—an issue that will see further discussion at future gatherings—as well as the degree of public trust in cloud providers owned, wholly or partially, by the state. In the United States and parts of Europe, this state ownership and its potential for abuse are widely discussed, whereas in Poland it is nearly a moot point.

The second day of the Warsaw conference opened with a high-level survey of recent threats and technology trends by **Christopher Porter** (who, at the time, was a non-resident senior fellow at the Atlantic Council and chief intelligence strategist with FireEye, and is now the US national intelligence officer for cyber) and **Kenneth Geers**, non-resident senior fellow with the Atlantic Council. **Porter** discussed the global effects of the spread of damaging cyberattacks, including malware like "NotPetya," and efforts by states to grapple with the effects of emerging technologies like artificial intelligence, which threaten to upend conventional assumptions about speed and adaptation in cybersecurity. **Geers** focused on regional trends, highlighting the spreading importance of social media and the role of Russia as an adversary to Poland and its neighbors in multiple dimensions. Their discussion of global trends was followed by a series of spotlights by: **H.E. Marek Zagórski**, Polish minister of digital affairs, on the crucial role of technology and innovation in a changing international environment; **Emily Frye**, director of cyber integration at MITRE, on strategies and policies that can better protect national critical infrastructure; and **Sebastian Bay**, senior expert of the Technical and Scientific Development Branch of NATO Strategic Communications Center of Excellence on how to counter the misuse of social media. The group discussed machine learning and the potential for machine-learning models to be poisoned during the learning-and-training process. This led to several comments highlighting the importance of protecting data associated with these models.

The final public panel of the event focused on best practices in cybersecurity, including a discussion among: **Fred Streefland; Kenneth Geers; Piotr Kalbarczyk**, director of the cybersecurity department for PKO Bank Polski; **Merle Maigre**, executive vice president for government relations at CybExer Technologies; and **Paula Januszkiewicz**, founder and chief executive officer of CQURE. Taking a wide-ranging view, the group discussed different forms of public-private collaboration, the importance of organizations

CYBER STATECRAFT INITIATIVE
A NEW INITIATIVE FOR POLAND:
A FUTURE GLOBAL LEADER IN SECURING THE 4TH INDUSTRIAL REVOLUTION
JANUARY 16-17, 2019
WARSAW, POLAND
JANUARY 16-17, 2019 / WARSAW, POLAND
Bank Polski
Atlantic Council

General Keith Alexander (ret.), former Director of the National Security Agency, delivers a keynote address at the inaugural joint conference between the Atlantic Council's Cyber Statecraft Initiative and PKO Bank Polski.

understanding their own technology infrastructures, and rapid patching amidst a continually shifting threat landscape. The panel provided recommendations for the cybersecurity and policy communities, touching on the need to think and act like a malicious actor, developing a culture in which *everyone* in an organization is responsible for cybersecurity, and how the creation of dynamic opportunities for employees to be trained in cyber hygiene and cyber-crisis management can help them better internalize best practices. This was particularly true of technology vendors, including those in the Internet of Things (IoT) marketplace, whose security and design decisions will continue to have effects not only on their customers directly, but on whomever their customers' technology can be abused to target.

Thinking like a malicious actor, adopting an adversarial mindset, is particularly important in structuring the public-private collaboration models that PKO and other financial institutions must adopt to work effectively with law enforcement. Attackers will seek to exploit policy seams and jurisdictional boundaries in addition to technical flaws, making it important for collaboration to cover not just basic information, but also mature expectations about how groups will operate together and where their respective activities overlap. The final panel leveraged this attacker mindset to discuss attribution, and highlighted the lack of clarity in international law and norms that would support collective attribution and clear consequences for malicious action. The influence these difficulties have on the policy community was compared to major challenges faced in commercial security, such as cyber insurance, where ambiguity around state attribution has created potential for confusion undermining a growing market.

Throughout the rest of the conference's second day, the Atlantic Council and PKO Bank Polski hosted a series of breakout sessions on digital forensic research, cybersecurity education, and how technologies can enable public services for citizens. Looking at forensics, the Atlantic Council's Digital Forensic Research Lab (DFRLab) hosted a working session on tracking events in governance, technology, and security, and where they intersect. DFRLab utilizes open-source research to identify, expose, and explain disinformation where and when it occurs, as part of its goal to build digital resilience worldwide. The lab showcased the power of open-source and digital forensic research to analyze disinformation campaigns and follow military developments in real time.

The session on cybersecurity education saw **Klara Jordan**, senior fellow with the Atlantic Council, moderate a discussion between **Victor Piotrowski**, lead program director at the National Science Foundation, and **Dr. Bolesław Piasecki,** expert for the security department at PKO Bank Polski. The session confronted a jobs crisis—an estimated 3.5 million unfilled positions across the global cybersecurity industry by 2021. Panelists argued that organizations must broaden their candidate pools to include multidisciplinary and non-technical individuals who understand the cyber-threat landscape and how to tackle challenges with national, international, and private-sector interests in mind. Of particular importance is prioritizing communications, analytical, and problem-solving skills to attract the multidisciplinary candidates that the industry and international community sorely need.

The conference's third breakout session, on technology as an enabler of public services, showed off new offerings from Polish entrepreneurs who deliver services to citizens with more effective delivery, higher quality, and better security. The session featured presentations from various Polish startups, including Cryptomage, Comarch Financial Services, Grey Wizard, Prebytes, and Startup Poland Foundation. The event underlined how technology is shaping new models of governance and society, as innovations such as artificial intelligence provide new ways to interact with the government and decentralize services. Looking across the various new ideas, it was clear that the security of technology will play a pivotal role in enabling new economic vitality and development.

Closing remarks for the conference were delivered by **Zagórski**, who discussed the need for deeper cooperation on technology development, deployment, and security across the transatlantic relationship. Referring to the ongoing debate about fifth-generation (5G) telecommunications, the speech sought to emphasize values common across all of Western civilization, and the need for states to seek out opportunities for cooperation over competition or misalignment.

The January 2019 Warsaw conference, "A New Initiative for Poland: A Future Global Leader in Securing the 4th Industrial Revolution," represented a unique convening of the intellectual and practitioner communities, stretching across organizational and political boundaries. A classic example of the Atlantic Council's ability to drive passionate engagement across diverse communities, the event would not have been possible without the vision and support of PKO Bank Polski and its leadership, especially Zbigniew Jagiełło and Adam Marciniak. But, this conference was not an isolated event. The shared community brought together there continues to engage with one another and, in so doing, deepens the US-Polish security relationship in important and meaningful ways.

Securing the 4th Industrial Revolution

To build on the success of Warsaw, the Atlantic Council and PKO Bank Polski gathered an even more select community of experts on the sidelines of the International Conference on Cyber Engagement in April 2019. The goal of the April 24 half-day workshop was to prompt new consideration of the fundamental questions of government digitization: why digitize, the steps to digitize, how to innovate and defend at scale, and how to collaborate to achieve goals.

A government may digitize, such as by adopting cloud-based technologies, for any of the following reasons, including

- as only one part of a larger goal of innovation in governance;

Pictured (left to right): Amb. Daniel Fried, Mr. Jakub Kalenský, Dr. Bolesław Piasecki, Dr. Alina Polyakova, and H.E. Marek Szczygieł, discussing the threat disinformation in social media poses to democratic institutions.

- because digitization has a direct and positive impact on the public;
- because digitization remains consistent with a government's core values of privacy and transparency;
- because digitization saves money; and
- because digitization can prepare a government to better take advantage of future technologies.

The workshop was built around two ninety-minute roundtables, the first of which tackled "what to do," while the second addressed "how to do it." Each roundtable focused on a specific instance of innovation as a way to refine the scope of the discussion and develop concrete steps for action. The first roundtable, **"Innovation and Defense at Scale,"** looked at the deployment of cloud technologies as a means to illustrate how countries can balance technological innovation with assuring citizens' safety and security. The second roundtable, **"Reimagining Collaboration in Cyberspace,"** used the financial sector as an example of how to address systemic risk by improving interagency and public-private collaboration.

The sessions occasioned lively debate and dialogue among participants who represented a cross-section of academic, industry, and practitioner experience from the United States and Poland. The discussion was so rich that this paper includes the key takeaways of the conversation surrounding several of the most critical questions from each section in the summary below.

Session 1–Innovation and Defense at Scale

In developing a national strategy for cyberspace, two parallel, but linked, questions arise: how to innovate at scale and how to defend at scale. Some of the most successful adopters of digital technology have been small countries (e.g., Singapore and Estonia), whose size affords the agility necessary to adapt to the unforeseen challenges posed by digitization. Larger nations face a different sort of task. Integrating new technology into their sizeable government services requires a deliberate strategy, national buy-in, and significant investment in physical and organizational structures. Innovative ideas, developed ad hoc, are not enough to realize the potential of new technologies—instead, countries need to identify and develop consensus on the key principles and values they want to enshrine, and then develop and execute a strategy in line with those principles.

At the same time, large-scale digitization—by definition—increases the attack surface to which nations are exposed. Basic steps, such as implementing "secure by design" methodology, are necessary to boost defensibility in all networks. But, for government networks, even more is required. Digitization on the national scale demands that citizens give up more control of their data than ever before. If their trust is broken, digitization is bound to fail. A defensible digital strategy must secure information, deter adversaries, and build trust from the start.

The development of a cloud strategy requires close attention to these twin questions of scalability. Standardized government-wide approaches to cloud security, such as the US Federal Risk and Authorization Management Program (FedRAMP), if applied well, can expedite the speed and security with which agencies can migrate their operations to the cloud.

Session 2—Reimagining Collaboration in Cyberspace

Transforming how organizations collaborate on cyber issues is vital to ensuring that cyber policy can keep up with technological innovation. New organizational formats, such as Computer Emergency Response Teams (CERTs) and Information Sharing and Analysis Centers (ISACs), have done much to boost the advantages held by defenders, at relatively little cost.

The interconnectivity of modern digital society has created new dependencies, and addressing them requires collaboration among government agencies, between the public and private sectors, and among close allies. Since the early 1990s, the US government has promoted the use of a well-defined enterprise architecture that cuts costs, streamlines operations, and enhances interagency collaboration on mission operations. As illustrated by the launch of the US National Risk Management Center (NRMC), housed within the Department of Homeland Security, the United States has taken a step away from focusing on singular assets and toward addressing systemic risks, which must include closer collaboration with the private sector.

In the financial sector, organizations in the United States, such as the Financial Systemic Analysis & Resilience Center (FSARC), have brought together private-sector banks and government partners, such as the US Department of the Treasury and the US Department of Homeland Security. The role of these entities has become clearer in the years since their creation, but overlaps and inconsistencies remain. The heart of effective collaboration appears to be exercising these capabilities, working through points of organizational friction and uncertainty in order to build trust and shape expectations for shared response.

Conclusion

The conclusion of the April workshop sounded a warning note for those present—the pace of technological innovation is only quickening, and the ability to tackle ever more complex challenges will hinge on more rapid, deep, and effective collaboration. This message was rooted in conversations during the January conference in Warsaw, and remains a clarion call for the community that the Atlantic Council and PKO Bank Polski have begun to build in service of a deeper and more impactful US-Polish security relationship.

Looking forward, understanding the impact of new technologies will not diminish in importance. Both public and private defenders must collaborate to secure the technology base underlying the next era of economic growth and transformation. Cybersecurity presents an enduring set of challenges beyond questions of pure technology, the role of users, the strategy of industry, and the conduct of statecraft. These first two events in the Atlantic Council-PKO Bank Polski partnership forged the outlines of a community of interest between these two states, and deepened a shared sense of the importance of these challenges.

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 the role of the technology industry in geopolitics, cyber conflict, the security of the internet, cyber safety, 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.`

Safa Shahwan is the Assistant 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.

Paweł Pawłowski is the Vice President of the Cegielski Center for Analysis and the Supervisory Board Chairman of the Warsaw Institute. He is an Expert with the Industrial Development Agency at the Departmant of Strategic Analysis in Warsaw. Previously, Paweł worked in a financial sector for leading banks in Poland, including PKO Bank Polski. He holds an MA in Law from the University of Warsaw. Paweł is doing a PhD in the Institute of Theory of State and Law at the same university. His research concentrates on relations between disinformation and guarantees of freedom of speech in the European Union.

Atlantic Council Board of Directors

Atlantic Council

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