CYBER STATECRAFT INITIATIVE

DFRLab

CYBER & INNOVATION POLICY INSTITUTE
U.S. NAVAL WAR COLLEGE

#ACcyber

ISSUE BRIEF

DECEMBER 2022

Wargaming to Find a Safe Port in a Cyber Storm

DANIEL GROBARCIK, WILLIAM LOOMIS, MICHAEL POZNANSKY, FRANK SMITH

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.

The mission of the **Digital Forensic Research Lab (DFRLab)** is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security.

EXECUTIVE SUMMARY

With the Maritime Transportation System increasingly reliant on cyberspace, how can cybersecurity be improved within key nodes of this critical infrastructure, particularly cargo ports? Given the close relationship between the cyber and maritime domains, wargaming provides a useful tool for examining the potential threats and opportunities. This includes the attack surfaces, prioritization challenges, and coordination advantages highlighted by the new maritime cyber wargame *Hacking Boundary*.

Critical infrastructure is rarely headline news—not until something goes very wrong—and the maritime transportation system (MTS) is no exception. The MTS, which is responsible for the safe transport of the majority of international trade, is vital to the global economy.[1] From backlogged cargo at port facilities during the COVID-19 pandemic to the Ever Given container ship blocking the Suez Canal, recent events have highlighted the vulnerability of maritime transportation, and how impactful disruptions to that system can be to everyday life.[2]

Broadly speaking, the MTS consists of all the waterways, vehicles, and ports that are used to move people and goods via water.[3] The volume of goods moved in this way is particularly striking, with most of the world's cargo carried by sea—between 70–90 percent, depending on how the cargo is counted. For the United States, the MTS contributes to nearly 25 percent of gross domestic

1 William Loomis et al., *Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity*, October 4, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/raising-the-colors-signaling-for-cooperation-on-maritime-cybersecurity/.

2 US Library of Congress, Congressional Research Service, *Supply Chain Bottlenecks at US Ports*, by John Frittelli and Liana Wong, IN11800 (2021), https://crsreports.congress.gov/product/pdf/IN/IN11800; Marc Jones, "Snarled-Up Ports Point to Worsening Global Supply Chain Woes – Report," *Reuters*, May 3, 2022, https://www.reuters.com/business/snarled-up-ports-point-worsening-global-supply-chain-woes-report-2022-05-03/; Vivian Yee and James Glanz, "How One of the World's Biggest Ships Jammed the Suez Canal," *New York Times*, July 17, 2021, https://www.nytimes.com/2021/07/17/world/middleeast/suez-canal-stuck-ship-ever-given.html.

3 US Department of Transportation, Maritime Administration, "Maritime Transportation System (MTS)," last updated January 8, 2021, https://www.maritime.dot.gov/outreach/maritime-transportation-system-mts/maritime-transportation-system-mts.

product, totaling around $5.4 trillion.[4] It is also essential to the US ability to project military power. Today, as for the past century, sealift—the use of cargo ships to deploy military assets—is responsible for transporting the vast majority of US military matériel around the world.[5]

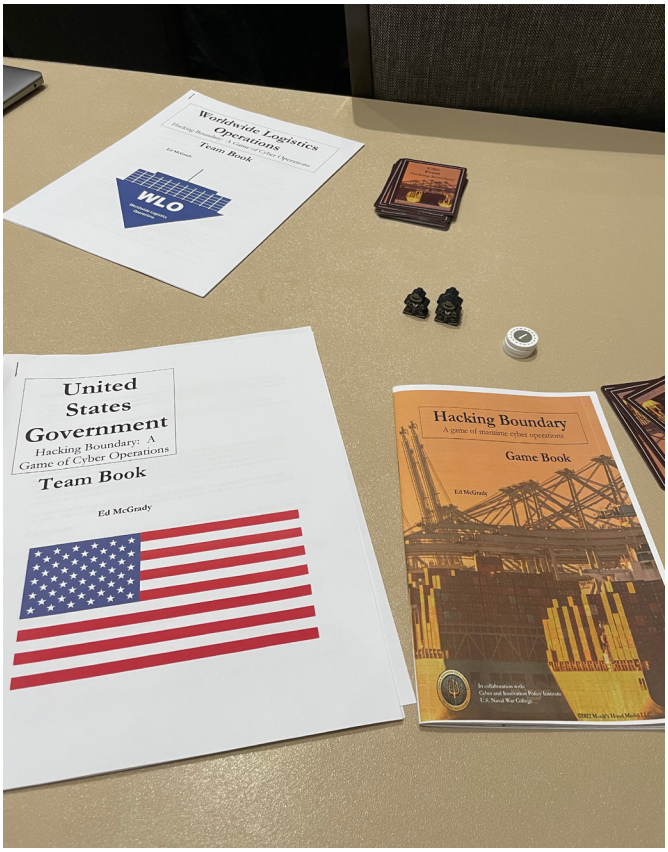
Unfortunately, this critical infrastructure is under threat. Along with natural disasters and human errors, cyberattacks are increasingly threatening the MTS. In 2017, a destructive and rapidly propagating piece of malware known as NotPetya spread from Ukraine around the world.[6] One of the many NotPetya victims was Maersk, the world's largest shipping company. This single cyber incident cost the shipping giant approximately $300 million,[7] and the price would have been much higher, were it not for a single uninfected server in Ghana. During another cyber incident just last year, foreign government-backed hackers were suspected of breaching information systems at the Port of Houston, further demonstrating that maritime transportation is firmly in the crosshairs.[8] NotPetya, the Port of Houston, and other cyberattacks against various kinds of critical infrastructure—including the ransomware attack on Colonial Pipeline in 2021—provide an ominous glimpse into the threat environment.

LEARNING THROUGH GAMING

Global and national security depend on understanding and mitigating threats to the MTS. The US government has taken some steps in this direction, including the *National Maritime Cybersecurity Plan* released in December 2020. More needs to be done, however, and one approach is to study what's necessary through cyber wargaming, a useful tool for examining the complex and confusing problems involved with cyber and physical threats to critical infrastructure.

Working with Ed McGrady, the Cyber & Innovation Policy Institute (CIPI) at the US Naval War College in Newport, Rhode Island, hosted government officials, military service members, students, and academics to play *Hacking Boundary: A Game of Maritime Cyber Operations*.[9] This war game addresses a hypothetical cyberattack against a major US port facility, and the first iteration of the game was played at the CIPI Summer Workshop on Maritime Cybersecurity in June 2022.

The second iteration of the game, conducted in partnership with the Atlantic Council's Cyber Statecraft Initiative, was held at the Industrial Control Systems Village at the DefCon Hacking Conference in August 2022 in Las Vegas, Nevada. This iteration featured participants from across the maritime ecosystem, including active duty US Navy and Coast Guard personnel, penetration testers, private sector operators, and many more.



Picture from game play in Las Vegas.

This brief describes *Hacking Boundary*, along with several strategic and policy implications illuminated by repeated game play. The core takeaways include: (1) understanding the large attack surfaces of port facilities and the lead times that may be required to attack them; (2) the difficulties of prioritizing how and when to spend scarce resources; and (3) understanding that the tensions between competition and coordination, if navigated wisely, may offer defenders marginal—but valuable—advantages when providing maritime cybersecurity.

4 William Loomis et al., *Introduction: Cooperation on Maritime Cybersecurity*, October 27, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-introduction/.

5 Jason Ileto, "Cyber at Sea: Protecting Strategic Sealift in the Age of Strategic Competition," Modern War Institute, May 10, 2022, https://mwi.usma.edu/cyber-at-sea-protecting-strategic-sealift-in-the-age-of-strategic-competition/; See also https://www.maritime.dot.gov/national-security/strategic-sealift/strategic-sealift.

6 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

7 Nina Kollars, Sam J. Tangredi, and Chris C. Demchak, "The Cyber Maritime Environment: A Shared Critical Infrastructure and Trump's Maritime Cyber Security Plan," *War on the Rocks*, February 4, 2021, https://warontherocks.com/2021/02/the-cyber-maritime-environment-a-shared-critical-infrastructure-and-trumps-maritime-cyber-security-plan/.

8 Olafimihan Oshin, "Major US Port Target of Attempted Cyber Attack," *The Hill*, September 24, 2021, https://thehill.com/homenews/state-watch/573749-major-us-port-target-of-attempted-cyber-attack/.

9 The game was developed and run by Ed McGrady at the Center for a New American Security.

SCENARIO AND PLAYERS

Imagine a major US port facility, modeled on the Port Elizabeth Intermodal Complex of New York and New Jersey, in the year 2027. The facility includes a terminal along the water. Within the terminal are the yard, gantry cranes, cargo containers, scales, semitrucks, inspection sites, gates, and administrative offices needed to load, offload, process, and move 1.8 million twenty-foot equivalent units (TEUs) annually, or approximately 43 million tonnes of cargo. Connecting all of this equipment, and the people operating it, are local area networks, Wi-Fi, radios, phones, and wires, forming a complex web of near constant communication.

Picture of the Hacking Boundary game board.

When an ultra large container ship carrying 21,000 TEUs enters port, all of this information and operational technology is put to work. Positioning systems and radio communication with pilot ships helps steer the container ship into a berth; cargo data files are digitally sent to the port authority; local security contractors screen the cargo; and access control handles the hundreds of trucks required to move the cargo. Work that was once handled by thousands of people is now performed by computers, scanners, remote closed-circuit television cameras, and routers working both autonomously and with human support. Underpinned by cyberspace, this daily routine unfolds at a massive scale and pace.

During the wargame, teams of defenders and attackers face off in this cyber-physical environment. On the defending team, the maritime shipping industry is represented by a fictitious private firm called Worldwide Logistics Operations (WLO), which leases the container terminal. WLO runs the information technology (IT) infrastructure for the terminal. It also cooperates with local authorities and the federal government, played by another team of defenders. The attackers are broken into four groups, each representing different kinds of advanced persistent threats (APTs) with their own background, expertise, and modus operandi. These attackers range from independent cyber criminals to mercenaries to groups with ties to foreign intelligence organizations. Overseeing the contest between the attackers and the defenders is a game master, who helps construct and control the game narrative and, in the process, judges the outcome of each team's moves.

GAME PLAY

This game is played over multiple turns, with each turn representing a month in the real world. At the start of each turn, the attacking and defending teams both draw random event cards. Possible events range from good news (e.g., receiving an unexpectedly large budget) to bad news (e.g., a power outage or having members of your team poached by the competition). These events are intended to represent some of the unpredictable realities faced by both parties in the real world. With a random event card in hand, each team plans their course of action.

The defending team's objective is to prevent port terminal intrusions and establish resilient systems that fail gracefully, minimizing potential disruption or damage. Given a limited budget, represented in the game as coins, the team must make choices that involve difficult trade-offs. For example, defenders could prioritize security training and upgraded hardware but, as a consequence, they may have insufficient resources to conduct penetration testing to identify other potential vulnerabilities. Or, they could choose to conduct penetration testing, but then lack resources to fix the vulnerabilities they find. It is also important to safeguard port facility physical security against theft and illicit access to critical systems. The networked nature of cyber and physical systems means that neglecting one could expose the other to risk.

The objective of the attacking teams is to secure a profit at the expense of the port and the WLO. Attackers start the game with a set budget. They can earn additional coins by completing missions ranging from exfiltrating data to causing physical damage. To complete a mission successfully, an attacking team must allocate limited resources to hiring the right people for the job, which included technical experts to defeat defensive measures. For simplicity, the categories of expertise in this game are: social, physical, network, malware, operating system, applications, electronics, and cryptography. Attackers must also acquire the capabilities needed to accomplish their mission, such as tailored malware or radio-frequency identification scanners. This wargame emphasizes the full breadth of the cyber kill chain, including preplanning and lateral movement over time.[10] Attackers may also take cyber actions that do not have immediate effects, laying the foundation for success later in the game.

The respective plans of attackers and defenders—and the logic behind them—interact via the game master, who determines the likelihood of success or failure. Outcomes are determined through discussion, with each team arguing their case about defensive measures taken at the port terminal, the complexity of the attack, and the personnel and capabilities dedicated to the job. This part of the game is where the collective expertise of each team really shines. Based on these discussions, the game master assesses the probability of an attack succeeding.

Chance is incorporated by rolling dice. For example, an attack with a 50 percent probability of success means that the attacking team must roll an eleven or higher on a twenty-sided die. More difficult attacks require a higher roll to succeed; easier attacks can succeed with a lower roll. The dice rolls determine if the attacker successfully completes all or part of their chosen mission.

Successful missions pay off in coins, building a unique narrative for the game. However, there is also the risk of discovery, modeled in the game as another roll of the dice by the team for "forensic points." Depending on the complexity of the move, attacking teams incur higher or lower forensic points. Too much bravado or sloppy tradecraft risks teams being discovered by defenders and having all of their coins seized by the authorities. As is sometimes the case in real life, a bit of bad luck can mean the difference between striking it rich or losing it all.

When the success, failure, and payoff of all the teams' actions have been decided, the next turn of the game begins with another round of event cards, planning, and outcome adjudication. Typically, each turn takes about an hour. There is no constraint on how many turns can be played, with consideration that higher stakes missions take longer to accom-

10 Lockheed Martin, "Cyber Kill Chain," June 29, 2022, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

plish. Whenever the game ends, a victor is determined just for fun. Defender success is measured by number of attacks successfully repelled vice attempted intrusions into the port or related networks. For attackers, success depends on the number of missions accomplished, their coin haul, and not getting caught.

GAME TAKEAWAYS FROM NEWPORT AND LAS VEGAS

Observations from only a few iterations of this game, with different players, do not constitute authoritative evidence. Even so, preliminary takeaways contain potentially important insights for maritime cyber and broader cybersecurity challenges facing critical infrastructure.

Attack Surfaces and Lead Times

Large and varied attack surfaces challenge defenders and provide attackers with numerous opportunities for exploitation. This wargame only captured some of the complexities of real-world maritime infrastructure. Nevertheless, it illustrated the importance of interrelationships and dependencies in a cyber-physical system. Subject matter experts who played the game showed how hypothetical attackers might probe several points of entry that intersected with even this simplified version of a cargo port. The attempted exploits were both physical (e.g., breaking and entering or conducting reconnaissance at a local pub frequented by port security) and cyber (e.g., phishing, injecting malware via flash drives, or hacking shipboard systems using a Raspberry Pi). The various attack options illustrate the myriad vulnerabilities of these complex facilities.

Put another way, no port is an island. Accidents and attacks outside the facility, such as disrupting a pump station or a nearby rail line, could still impact maritime operations by, for example, paralyzing road traffic around the cargo terminal. These interdependencies highlight the need to broaden the conceptual and operational boundaries of maritime cybersecurity as currently and traditionally conceived. In the wargame, defenders overlooked these external relationships, to their detriment.

While the multitude of attack options seemed to afford the attackers with endless choices, carrying out the attacks in this complicated environment took time. Successful attacks often required long lead times for planning and execution. In the game, as in real life, the cyber kill chain had multiple links spread out over time and, in some cases, over physical space. For example, some attacking teams probed physical security at the port early on, in an attempt to gather useful intelligence. Later, they exfiltrated data through lateral moves within the target network, exploiting access gained through phishing.

Both the large attack surfaces and the long lead times reaffirmed a well-known argument in cybersecurity that nevertheless bears repeating: defending a network is a lengthy and dynamic process, comprised of many different steps. Several attacks crossed multiple systems, spanning three or four moves in the game before a full picture of the offensive operation became apparent. The dramatic image of hackers running a rogue ship aground distracts from much of the preparatory, and seemingly mundane, work that would go into such an attack (e.g., orchestrating a phishing campaign against the cleaning company subcontracted to service the port bathrooms).

> **Key Takeaway**—Maritime infrastructure consists of complex systems, which provide numerous opportunities for exploitation but also complicated kill chains.

Prioritization and Resilience

The sheer number and variety of vulnerabilities to exploit and defend during game play posed serious challenges for players about how to allocate their scarce resources. Effective prioritization was a deciding factor for both attackers and defenders.

For their part, attackers had to invest in capabilities and staffing to effectively penetrate target systems and accomplish mission objectives. Missteps or bad luck could result in a failed mission, setting attackers back in terms of time and money. For defenders, early investments to bolster security tended to have a large impact on their ability to thwart attacks later in the game. Defenders also needed to retain resources—and acquire skills—to dynamically (re)allocate defensive capabilities and capacities, which were then distributed across physical and network infrastructure, as well as across shipboard and terminal information systems. With limited resources at their disposal, poorly chosen priorities or bad luck could leave defenders struggling to respond to even basic incidents. Lack of defensive planning, or a purely reactive posture, provided attackers with dangerous freedom of movement.

Here again, the wargame only captured some of the real-life complexity, underscoring the very real challenge and necessity of prioritization. While critical infrastructure is, by definition, "critical," some systems within it are more important than others, and some problems are easier to solve. Prioritizing investments where ease and importance overlap may seem obvious, but many of the tradeoffs are acute, presenting hard choices. As will be discussed, these choices are easier when public agencies and private firms share useful cyber intelligence. Each party may make different decisions about how to prioritize and allocate their respective resources, but both stand to benefit from pooling information about the threat environment.

Making the right investments and allocating the proper resources to defense is only half the battle. When attacked, organizations also need resilience, namely the "ability to adapt to changing conditions and prepare for, withstand, and

rapidly recover from disruption."[11] In this game, as in real life, no defense was perfect: financial data leaked; ransomware jumped from contractor to vendor; and even positioning and navigation systems were compromised. Adapting and responding to unfortunate incidents is difficult, but necessary for minimizing disruptions to the most important MTS administrative and operational functions.

There is little doubt that bolstering the resilience of maritime cybersecurity will remain a challenge. Best practices and high standards can help, such as the US Coast Guard's Navigation and *Vessel Inspection Circular 01-20* and the International Maritime Organization's guidance on cybersecurity.[12] Since so many different operators and information systems intersect at port facilities, best practices within and across sectors are significant to forming strong links between the diverse entities involved. By providing a platform for practical learning, wargames can help individuals and organizations synthesize risk, identify priorities, build resilience, and highlight the significant—but often unappreciated—role that these various relationships can play in cybersecurity.

Key Takeaway—The range of cyber physical vulnerabilities in the MTS mean that prioritization and resilience are core challenges when allocating scarce resources.

Competition and Coordination

Competition and coordination were reoccurring themes in this wargame, with significant policy implications. Attackers not only competed against defenders, but also against each other. Competition over scare resources, access points, and cyber exploits fueled tension among the APTs. In addition, some attacking teams were hurt by the actions, misfortunes, or errors of other team members. Attackers were both beneficiaries and potential victims of the difficulties of attribution in cyberspace, as some enterprising attackers tried to disguise their tracks by imitating others in false flag operations.

Instances of attacking teams directly targeting one another—as opposed to defenders—broke the binary concept of purely offensive and defensive roles in the game. These dynamics mirrored real life, helping dispel the notion that offensive and defensive moves in cyberspace inevitably aggregate to the attacker's advantage. Different attackers have different motives. While a criminal enterprise may hack a port to steal cargo information to sell for financial gain, a state or hybrid actor may attempt to cripple port automation for political reasons. These different, and sometimes competing, objectives limit attackers' incentives to cooperate with each other, let alone coordinate their actions. Leaked chat records from the Conti ransomware group highlight this discord inside real attacking teams, with interpersonal squabbles compounding conflicts between different APTs.[13]

Defenders suffered from conflicts of interest as well. The private firms that own and operate port facilities may not have the same incentives as government agencies to share information, especially if doing so invites scrutiny by regulators or law enforcement. These defenders also compete with each other for scarce cybersecurity talent and other resources.

While competition and conflict were evident among both defenders and attackers, *Hacking Boundary* indicates that defenders enjoy some advantages when it comes to institutionalizing cooperation, including a higher baseline level of trust. Honor among thieves may be harder to come by than even begrudging coordination between industry and government. Although defenders in the government, WLO, and terminal IT security teams had different incentives and threat perceptions, many still found ways to share information and coordinate action. On balance, this coordination gave defenders an edge in the game. Successful defenders established lines of communication sooner rather than later.

Real-world coordination between maritime owners, operators, and government agencies is easier said than done. Nevertheless, the potential payoff is considerable and physical proximity may help. Anecdotal evidence from our wargame suggests that players in the roles of port operators and government representatives conversed more when seated together. Perhaps it is no coincidence that communication between similar organizations in the real world correlates to a significant federal presence—Coast Guard headquarters, Department of Homeland Security regional centers, Federal Bureau of Investigation field offices, and the like—close to port facilities. Cybersecurity is social as well as technical, and face-to-face interaction can make a difference. However these relationships develop, the policies that build them before the next major cyber incident could prove to be invaluable.

Key Takeaway—Real-world coordination, whether among attackers or defenders, is a key dynamic in any cyber operation, and is easier said than done.

11 "US Department of Homeland Security, Management Directorate, OCRSO, Sustainability and Environmental Programs, *Providing a roadmap for the Department in Operational Resilience and Readiness*, July 2018, https://www.dhs.gov/sites/default/files/publications/dhs_resilience_framework_july_2018_508.pdf."

12 US Department of Homeland Security, *United States Coast Guard, Navigation and Vessel Inspection Circular No. 01-20* (Washington, DC, 2002), Commandant Publication P16700.4, https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2020/NVIC_01-20_CyberRisk_dtd_2020-02-26.pdf?ver=2020-03-19-071814-023; International Maritime Organization, "Guidelines on Maritime Cyber Risk Management," MSC-FAL.1/Circ.3/Rev.1, June 14, 2021, https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf.

13 Gareth Corfield, "60,000 Conti Ransomware Gang Messages Leaked," *The Register*, February 28, 2022, https://www.theregister.com/2022/02/28/conti_ransomware_gang_chats_leaked/; Maria Henriquez, "Inside Conti Ransomware Group's Leaked Chat Logs," *Security Magazine*, April 6, 2022, https://www.securitymagazine.com/articles/97379-inside-conti-ransomware-groups-leaked-chat-logs.

CONCLUSIONS

Cyber wargaming has demonstrated the potential to demystify and clarify threats and opportunities involving critical maritime infrastructure. The game *Hacking Boundary* engages players with a challenging, but realistic scenario that reflects some of the serious risks facing the companies, crews, and government authorities operating port facilities around the country and around the world. The large attack surfaces, the importance of prioritization, and the implications of competition and coordination reinforce many well-established cybersecurity ideas. The relationship of these lessons to the maritime domain warrants further exploration.

The intersection between the maritime and cyber environments will likely grow in the years ahead. How these relationships and dependencies are conceptualized will likely determine our success or failure in protecting the MTS. The same goes for improving systemic resilience, including transportation by road, rail, and air – all of which increasingly rely on automation and networked information technology. Further iterations of this wargame and similar exercises stand to help by encouraging practitioners, academics, corporate executives, and government officials to think through potential threats and responses in order to secure these kinds of critical infrastructure.

ABOUT THE AUTHORS

Daniel Grobarcik is a research associate with the Cyber & Innovation Policy Institute at the U.S. Naval War College.

William Loomis is an associate director at the Atlantic Council's Cyber Statecraft Initiative, within the Digital Forensic Research Lab.

Michael Poznansky is an associate professor with the Cyber & Innovation Policy Institute at the U.S. Naval War College.

Frank Smith is a professor and director of the Cyber & Innovation Policy Institute at the U.S. Naval War College.

The ideas expressed here do not represent the US Naval War College, US Navy, Department of Defense, or US Government.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*C. Boyden Gray
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Todd Achilles
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
Linden P. Blue
Adam Boehler
John Bonsell
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
Richard R. Burt
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Mark T. Esper
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Jarosław Grzesiak
Murathan Günal
Frank Haun
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
Henry A. Kissinger
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Christian Marrone
Gerardo Mato
Erin McGrain
John M. McHugh
*Judith A. Miller
Dariusz Mioduski
Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
*Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Gregg Sherrill
Jeff Shockey
Ali Jehangir Siddiqui
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
*Gil Tenzer
*Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
*Al Williams
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of November 18, 2022