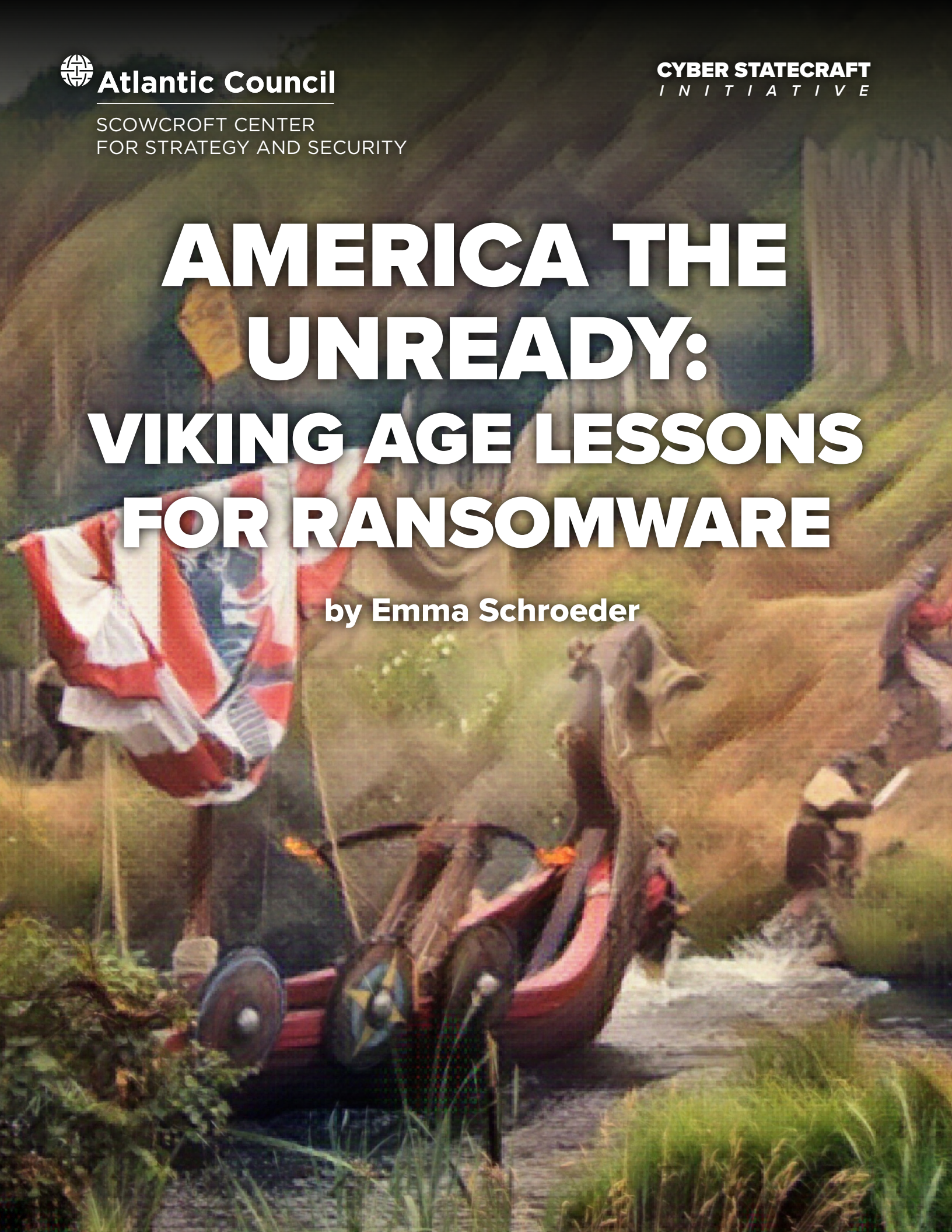
Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

CYBER STATECRAFT
INITIATIVE

AMERICA THE UNREADY: VIKING AGE LESSONS FOR RANSOMWARE

by Emma Schroeder



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.*

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

CYBER STATECRAFT
INITIATIVE

AMERICA THE UNREADY: VIKING AGE LESSONS FOR RANSOMWARE

by Emma Schroeder

ISBN-13: 978-1-61977-219-9

Cover: Flickr/DocChewbacca (https://www.flickr.com/photos/st3f4n/4794763792/)

March 2022

Table of Contents

Executive Summary

The ways in which humans have wrought or threatened violence upon one another for profit have evolved remarkably little in their basic form, from medieval Viking raids through to the ransomware gangs of today. Though ransomware itself is not a new problem, its sweeping impact demands innovative responses from governments and companies alike. Seeking more creative solutions, the US government and its allies and partners can look to the past for lessons learned and battles won and lost.

The Vikings, much like ransomware groups, took advantage of capable but fragmented targets, capitalizing on moments of weakness to strike without mercy. Their victims, threatened with destruction and ruin, made their venture profitable with capitulations of precious metals and food—the danegeld—which prompted the Vikings to leave, and to target new victims in turn.

The Viking Age persisted in Anglo-Saxon England and the Kingdom of Wessex for hundreds of years, but was not without its moments of victory and respite. The reign of Alfred the Great created a sea change in the kingdom's dealings with the Viking raiders, a period of coordinated response through political, military, and social reforms. To counter the persistent threat from the Viking invaders, Alfred championed reforms building on the idea of collective resilience and defense—just as the United States must today to counter the rising tide of ransomware. First, the US government must restructure incentives to align, as closely as possible, the concerned stakeholders toward collective, not individual, resilience. Second, the US government must work alongside the private sector and civil society to improve the capability and preparedness of a larger proportion of the population. Third, the US government and private sector must streamline the mechanism through which they detect, share information about, and respond to ransomware attacks. At the heart of these reforms was a king's ability to respond to a persistent problem with an equal measure of persistence—something his descendants failed to do, to their ruin.

Cyberspace brings much that is challenging and novel, but the history of extortion in human society is an unfortunately consistent line reaching back more than a millennium. The domain of cyberspace is characterized by constant activity and exchange, where there will likely never be an entirely safe harbor. To combat ransomware, the United States, its allies, and its partners will need to take to heart the lessons of history—both its lessons and its failures.

Introduction

Sitting at the computer, at the daily grind or just browsing social media, security sits well at the back of the mind. There are much more immediate concerns, anxious apparitions much more likely to end in disaster, even when confronted by the recurrent public ransomware incidents that seem to force themselves into the news cycle with tenacious persistence. Ransomware attacks against hospitals and medical centers, like the University of Vermont Medical Center, have impeded medical treatment and access to necessary health records.[1] The Kaseya ransomware incident may be the largest ransomware attack in history, hitting targets as diverse as Swedish grocery stores and New Zealand schools.[2] The Colonial Pipeline ransomware incident led to the shutdown of the largest oil pipeline in the United States for nearly five days.[3] And, this is not to mention the multitude of ransomware incidents that fly clear of front-page news—incidents that have increased in frequency by 57 percent since 2020.[4] The landscape of cybersecurity is beset by a rash of ransomware assaults—financial crimes and extortion with, at times, brutal consequences.

1 Stacy Weiner, "The Growing Threat of Ransomware Attacks on Hospitals," Association of American Medical Colleges, July 20, 2021, https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals.

2 Gerrit De Vynck, Aaron Gregg, and Rachel Lerman, "Ransomware Attack Struck between 800 and 1,500 Businesses, Says Company at Center of Hack," *Washington Post*, July 6, 2021, https://www.washingtonpost.com/business/2021/07/06/kaseya-ransomware-attack-victims/.

3 Nicole Acevedo, "Colonial Pipeline Returns to 'Normal Operations' Following Shutdown," NBC News, May 15, 2021, https://www.nbcnews.com/news/us-news/colonial-pipeline-returns-normal-operations-following-shutdown-n1267494.

4 "Breaking Down the Ransomware Trends in 2021," Cyware Social, May 18, 2021, https://cyware.com/news/breaking-down-the-ransomware-trends-in-2021-e25a6a4c.

Though it seems to enter notice in fits and starts, ransomware is a persistent problem in US society. It is an economic drain on the population, draining wealth and disrupting operation of crucial services. But, it has also become a tool by which to exact strategic gains, both through long-term wealth extraction and through the use of ransomware to obfuscate the true intention of a cyber operation.[5] This second motive was demonstrated clearly in the NotPetya cyberattack exacted by Russia against Ukraine in 2016. Companies throughout Ukraine that thought themselves the victims of ransomware discovered, instead, that their attacker's intent had been degradation and disruption. Russia's role as a safe haven for ransomware groups is a strategic calculation. These gangs extract millions of dollars from the economies of Russian adversaries, enacting strategic costs without requiring direct Russian operation.[6] Ransomware wielded as a strategic tool is just beginning to see its full potential.

Yet, much of the US population still does not see this threat as imminent. After all, what is one more attack that quickly fades from the headlines? What is one small company? Especially when not perched precariously, exposed to the ocean itself. The smell of burning is barely a faint trace on the wind—we are far inland, far from the source of danger, far upriver.

But, the adversary has longships.

The Adversary's Longships

Worn timbers creak against the ceaselessly beating waves as the heft of a long wooden ship steadily advances, the men inside bristling in anticipation of the upcoming raid. A small armada of Viking longships follows closely, travels up the very same extensive system of rivers that supports local interchange of goods and information, deep into enemy lands. Though many are experienced, having left Scandinavia to go aviking, they do not need excessive size or strength when they have the incentive and the ability to strike wherever value and vulnerability coalesce. Their target for the day is a local monastery; these raiders have no compunction about attacking what their targets consider sacred, nor would they eschew the opportunity to attack during a holiday when defenses are lowered.[7]

The Vikings in these longships have yet to encounter much resistance. Forces whose remit is to challenge and repel these Norse marauders exist, but they are small and scattered at the will of local nobility. They may arrive only after damage is done, in time to do little more than staunch the bleeding. The Vikings seem to move at will across the coasts and interior waterways, halting their attacks to return home only when satiated with their bounty. What option seems left for these defenders, then, but to accede in the face of such a vividly demonstrated show of force and pay the price for peace?

This is a familiar position, repeated and transformed over thousands of years. The cyber domain is not unlike a vastly more complex and interconnected system of rivers, constructed—not by nature, but by men—in order to facilitate the exchange of information and ideas, and thereby prioritize interconnectedness over security.[8] In this interconnected environment, vulnerabilities abound. The Vikings of an earlier era, ruthless and without compunction, are found today in the ransomware gangs whose raiding across the digital ecosystem has provoked no end of hand wringing, but little systematic defense.

Cybersecurity in the private sector is an uneven patchwork. Defenders, even those who are well resourced, cannot prevent every incursion. Ransomware gangs, who benefit from the accessibility of their tools and the

5 Simon Handler, "The Strategic Intelligence Value of Ransomware," Lawfare, December 15, 2021, https://www.lawfareblog.com/strategic-intelligence-value-ransomware; Jenny Jun, "Could Ransomware Become a Geopolitical Weapon? Game Theory says Yes," *Politico*, July, 8, 2021, https://www.politico.com/news/magazine/2021/07/08/ransomware-game-theory-geopolitics-cyber-attack-498625; Jenny Jun, "The Political Economy of Ransomware," War on the Rocks, June 2, 2021, https://warontherocks.com/2021/06/the-political-economy-of-ransomware/.

6 Simon Handler, Emma Schroeder, and Trey Herr, Countering ransomware: Lessons from aircraft hijacking, Atlantic Council, August 26, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/countering-ransomware-lessons-from-aircraft-hijacking/?_thumbnail_id=427566.

7 "The Viking Raid on Lindisfarne," English Heritage, last visited February 11, 2022, https://www.english-heritage.org.uk/visit/places/lindisfarne-priory/History/viking-raid/; "The Anglo-Saxon Chronicle: Ninth Century," Yale Law School, Avalon Project, https://avalon.law.yale.edu/medieval/ang09.asp; Benjamin Merkle, *The White Horse King: The Life of Alfred the Great* (Edinburgh, UK: Thomas Nelson, 2009), 90; Matthew Firth and Erin Sebo, "Kingship and Maritime Power in 10th-Century England," *International Journal of Nautical Archaeology* 49, 2, 2020, 329–340, https://www.tandfonline.com/doi/full/10.1111/1095-9270.12421.

8 Craig Timberg, "Net of Insecurity: A Flaw in the Design," *Washington Post*, May 30, 2015, https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.

simplicity of their tactics, are able to pinpoint where value meets vulnerability.[9] Ransomware gangs leverage any potential advantage, seeing increased value in targeting hospitals where risk may incentivize rapid payment, as well as increased vulnerability in holiday staffing lulls.[10] Many companies, possibly as many as three-quarters of those affected, don't even report incidents of ransomware, let alone receive governmental aid.[11] More than half of those affected choose, in the face of such a visceral threat to their business, to pay the demanded ransom.[12]

You Never Get Rid of the Dane

"If once you have paid him the Dane-geld, you never get rid of the Dane." These words, taken from a twentieth-century poem by Rudyard Kipling, are only the latest in a line of historical castigation of Anglo-Saxon King Aethelred the Unready—or, as his epithet is more correctly but less commonly translated, the Ill-Counselled. This unfortunate epithet was partially founded on his payment of danegelds—the Vikings' demanded ransom—five times.[13] Kipling, and history, have perhaps been unkind to Aethelred; this same attitude against the danegeld is not applied to the various "greats" who did the same, like Charlemagne and Alfred. It is in connection with Aethelred that danegelds became solidified as a "byword for futile appeasement."[14] In a similar way, paying ransomware groups in return for decryption tools is perceived by some as both personally and systemically dangerous. The charge laid against danegelds by Kipling is that they are ineffective at preventing further attack. Once the danegeld is paid, there is no guarantee that the Viking band will decamp without causing further damage, or that the same or new Viking bands won't see that payment as proof of the profitability of raids in that kingdom.

In modern-day ransomware cases, targets similarly have no guarantee that paying the demanded ransom will ensure the complete return of all data. On average, ransomware victims who pay their raiders see only 65 percent of their data restored, and only 8 percent of victims see a successful full restoration.[15] In effect, this means that paying the ransom does not solve, but compounds, the problem. The victim has to pay up, recover time lost to the attackers, and still must slowly and painstakingly rebuild their data while remaining a target for future assaults. The cyber criminals may also choose to employ double extortion, threatening the release of exfiltrated sensitive data on top of the data encryption.[16]

One of the principal arguments against paying ransomware operators is that the money used to save one company often enables further, and possibly more effective, ransomware attacks against other victims.[17] The money plays a double role, enriching the ransomware group itself and signaling to other criminal groups the potential profit they could make through ransomware, even from that same target.[18] In fact, a 2021 report found that "80% of organizations that previously paid ransom demands confirmed they were exposed to a second attack."[19]

This difference in the historical perception of danegelds hinges on their precise intended use. The payer of the danegelds likely did not view them as a full solution; instead, they were viewed as a short-term necessity.[20] For those without the ability to head off attacks directly, danegelds

9 P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford, UK: Oxford University Press, 2014), https://ebookcentral.proquest.com/lib/kcl/detail.action?docID=4505491.

10 "Up to 1,500 Businesses Compromised by Latest Ransomware Attack, Kaseya CEO Says," CBS News, July 6, 2021, https://www.cbsnews.com/news/ransomware-attack-hackers-70-million-demand-1500-businesses/.

11 Garrit De Vynck, "Many Ransomware Attacks Go Unreported. The FBI and Congress Want to Change That," *Washington Post*, July 27, 2021, https://www.washingtonpost.com/technology/2021/07/27/fbi-congress-ransomware-laws/.

12 "Over Half of Ransomware Victims Pay the Ransom, but Only a Quarter See Their Full Data Returned," Kaspersky, press release, March 30, 2021, https://www.kaspersky.com/about/press-releases/2021_over-half-of-ransomware-victims-pay-the-ransom-but-only-a-quarter-see-their-full-data-returned.

13 "Danegeld," New World Encyclopedia, https://www.newworldencyclopedia.org/entry/Danegeld

14 Theodore M. Andersson, "The Viking Policy of Ethelred the Unready," *Scandinavian Studies* 59, 3, 1987, 284–295, http://www.jstor.org/stable/40918864.

15 "The State of Ransomware 2021," Sophos, April, 2021, https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx.

16 Brianna Leddy, "Double Extraction Ransomware," Darktrace, May 19, 2021, https://www.darktrace.com/en/blog/double-extortion-ransomware/.

17 Chris Strohm and Alyza Sebenius, "Wray Warns Companies Against Paying Ransom for Cyberattacks," Bloomberg, June 10, 2021, https://www.bloomberg.com/news/articles/2021-06-10/wray-warns-companies-against-paying-ransom-for-hacking-attacks.

18 Danny Palmer, "Ransomware: Don't Pay Up, It Just Shows Cyber Criminals That Attacks Work, Warns Home Secretary," ZDNet, May 11, 2021, https://www.zdnet.com/article/ransomware-dont-pay-the-ransom-it-just-encourage-cyber-criminals-that-attacks-work-warns-home-secretary/.

19 Nicole Sganga and Musadiq Bidar, "80% of Ransomware Victims Suffer Repeat Attacks, According to New Report," CBS News, June 17, 2021, https://www.cbsnews.com/news/ransomware-victims-suffer-repeat-attacks-new-report/.

20 Einar Joranson, "The Danegeld in France," Augustana Library Publications, 1923, https://babel.hathitrust.org/cgi/pt?id=mdp.39015049769246&view=1up&seq=5, 205.

provided a temporary respite from plunder and devastation, as well as time to strengthen defenders' means of resistance. Aethelred the Unready came to power in a land that had been plagued by Viking attacks for almost two centuries, and he was able to effectuate improvements. For example, he applied sufficient pressure upon the court of the king of Normandy to close its harbors to Viking fleets.[21] But, the Unready King, cast by medieval scholars as a slugabed, didn't have the inclination nor the political capital necessary to rouse a beleaguered country and actively combat the Viking armies, especially when paying the danegeld was always an option.[22] He was unable to use what time the danegelds bought him to rally his country to resistance.

The payment of modern-day ransoms, in cryptocurrency instead of precious metal, should not be viewed as a solution or a success, but neither is simply banning their payment. They are a tool to be used only when the targeted entity does not have the time or resources necessary to avoid serious, irreversible damage—and even then must be accompanied by parallel efforts to shore up defenses and improve detection and remediation capabilities. We should not repeat the mistakes of one of England's most censured kings and expect better results. Instead, let us look to his ancestor for counsel on how to repel the contemporary Vikings.[23]

What to Do with the Time That Is Given Us

Alfred the Great, despite his moniker, had his own share of failures and disasters when it came to the Vikings. The most prominent of these was the months-long period Alfred spent in the marshes of Somerset after losing his throne to the Viking leader Guthrum.[24] Once Alfred regained his throne, however, he set out to learn from his mistakes. He pursued a reorganization of the incentive structure of the nobility, revitalized and grew the kingdom's defense program, and developed a network of internal security chokepoints.

Lesson One: Altering Incentives

One of Alfred's most important political changes was the appointment of new noblemen and members of his inner council. Traditionally, Anglo-Saxon kings were chosen by a select council from among the nobility, usually the late king's first-born son. The tradition meant that, in a matter of honor, the king owed his throne to the nobility. Additionally, those nobles with "bookland"—land held in perpetuity by charter—had vested local interests that rated above the needs of the kingdom.[25] After regaining the throne, Alfred installed new noblemen to that council who now owed their station directly to him.[26] By tying the prosperity of the nobility to his rule, Alfred incentivized the nobles to support him and invest collectively in a stable vision for the kingdom.

There are few direct lessons to be pulled from the restructuring of an eleventh-century kingdom, but the essential lesson of this story lives in how the incentives of a political power structure were altered to support collective security. Opposing today's digital Vikings demands coordinated expenditure and similar incredible effort. Policymakers need to understand and work to alter, where possible, the incentives of the private sector, especially those of the most consequential or frequently targeted industries. Defending against the scourge of ransomware attacks requires continual effort to harden "cybersecurity defenses by conducting an assessment of your platforms, systems, networks, devices, applications and services as well as applying multiple-layered security defenses."[27] It is in the interest of the US government, the general public, and private companies themselves for vendors to develop products

21 Eric John, "War and Society in The Tenth Century: the Maldon Campaign," *Transactions of the Royal Historical Society* 27, 1977, 173–195, https://www.cambridge.org/core/journals/transactions-of-the-royal-historical-society/article/abs/war-and-society-in-the-tenth-century-the-maldon-campaign/7C81A88B2DE4BFB53C6455CEAF718C86.

22 Andersson, "The Viking Policy of Ethelred the Unready"; Joranson, "The Danegeld in France."

23 Despite their popularity in contemporary media, the Vikings were a very real people with very real victims. It is too easy to read the tragedies of the past as a heroic saga. But, those people—men, women, and children—who were killed, sold into slavery, or starved to death as a result of Viking raids deserve more empathy than the false picture of "Vikings" our culture has created. These are figures of the past, not to be loved or hated but, rather, to be understood.

24 "The Anglo-Saxon Chronicle: Ninth Century"; Merkle, *The White Horse King,* 90; Michael Carr, "Alfred the Great Strikes Back," *Military History* 6, 2001, 62–69, https://www.proquest.com/magazines/alfred-great-strikes-back/docview/212652338/se-2?accountid=11862.

25 David Pratt, *The Political Thought of King Alfred the Great* (Cambridge, UK: Cambridge University Press, 2007), https://ebookcentral.proquest.com/lib/kcl/detail.action?docID=311224, 20.

26 Alfred P. Smyth, *King Alfred the Great* (Oxford, UK: Oxford University Press, 1995), 447.

27 Yuen Pin Yeap, "Why Ransomware Costs Businesses Much More Than Money," *Forbes*, April 30, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/04/30/why-ransomware-costs-businesses-much-more-than-money/?sh=47f8350971c6.

that are more secure by design. To that end, the government and customers should seek to shape vendor incentives. Meaningful progress on this front would include, as the Cyber Statecraft Initiative wrote in its recent Broken Trust Report, the establishment of a Cybersecurity and Infrastructure Security Agency (CISA) security team with directed funds dedicated to improving the integrity of critical and widely used open-source projects and packages, as well as the adoption of a Software Bill of Materials to improve transparency into software supply chains.[28] Private companies operate on market incentives, and expecting each individual company to develop and fund the necessary innovations in cybersecurity on a continuous basis is extremely unrealistic. Government-led efforts, like those highlighted, would raise the baseline of security by targeting widespread dependencies and points of potential propagation.

Though ransomware events themselves can be extremely injurious, effective and proactive defense is also costly. Therefore, in order to increase collective security, governments must continue to provide guidance, like CISA's Ransomware Guide, and make available increased resources to help private-sector companies improve their defenses.[29] This guidance shouldn't be an imposition by the government, but the result of stakeholder collaboration, such as that proposed in the CISA Joint Cyber Defense Collaborative.[30] This must be paired with an incentive structure that pushes companies toward preparation over payment. Helpful recommendations from the Institute for Science and Technology's Ransomware Task Force include compiling centralized and clear ransomware guidance, as well as dedicating government resources for victims of ransomware attack who choose not to make the demanded payment.[31] Such open and nonpunitive measures would help create the resilience necessary for private entities to eschew ransomware payments without risking the future of their own enterprises, an essential step in aligning incentives toward the collective good of denying resources to ransomware groups.

Lesson Two: Raising Competencies

Alfred's restructuring was not reserved reserved to political maneuvers, but included military reforms that affected all classes of society. The first of these was the reorganization and revitalization of the fyrd service—which constituted the military duty of freemen.[32] Alfred is credited with two major innovations to this service. First, he made the fyrd a permanent body, so that instead of relying on his nobles to levy their forces in response to crises, the kingdom would have a standing force prepared for Viking attack at any time. This innovation meant that men who once would have only sporadically seen military service now engaged in training or campaigns regularly, and were further equipped with horses. These changes meant that Alfred could pursue the enemy in the field without creating new points of vulnerability. While the fyrd did not have the experience and skill of a Viking army, these changes gave Alfred a moderately more professional, and far more mobile, force to harass lightning Viking raids and make their incursions costlier.[33]

Those on offensive duty were not leaving their homes and lands defenseless, however. Alfred also introduced service rotation, so that the half of the forces not currently on rotation were responsible for the protection of their own land and that which belonged to their close neighbors.[34] These forces had the advantage of familiarity with local territory; fyrd members from an attacked locality could provide vital information as to terrain and resources.

Cybersecurity ought to be cast as a "whole of nation" problem, as the cyber domain is principally composed of civilian activities that support much of the international economy. Ransomware impacts societies, from the individual to large corporations to government entities. As in Alfred's time, security needs to be a fixed priority and proactive, not just a response to crisis, because cyberspace is characterized by a state of constant "contact, action, hostility, and change."[35] The scale and ubiquity of this threat mean that a larger percentage of the population must, therefore,

28 Trey Herr, et al., *Broken Trust: Lessons from Sunburst, Atlantic Council*, March 29, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst/.

29 "Ransomware Guide," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/stopransomware/ransomware-guide.

30 "Joint Cyber Defense Collaborative," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/jcdc.

31 "Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force," Institute for Security and Technology, April 29, 2021, 25 and 43, https://securityandtechnology.org/ransomwaretaskforce/report/.

32 Stephen Pollington, *The English Warrior: From Earliest Times to 1066* (Little Downham, UK: Anglo-Saxon Books, 1996), 85; Hollister C. Warren, *Anglo-Saxon Military Institutions on the Eve of the Norman Conquest* (New York: Oxford University Press, 1962), 59–60.

33 "The Anglo-Saxon Chronicle: Ninth Century"; Pratt, *The Political Thought of King Alfred the Great*, 95.

34 Pratt, *The Political Thought of King Alfred the Great*, 95; Pollington, *The English Warrior,* 86.

35 Richard J. Harknett and Michael P. Fischerkeller, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, 3, 2017, 381–393, http://doi.org/cp9b.

practice cyber-literate or hygienic behaviors.[36] A common distribution method for ransomware attacks is phishing, a social-engineering attack in which emails disguised as legitimate messages either solicit personal information, like passwords, or deploy malware.[37] It is an effective means of deploying ransomware, as most people display a basic level of trust in their daily email interactions and miss the small clues that point to an email's inauthenticity. End users are, therefore, one of the largest points of vulnerability, but also of potential improvement in cybersecurity.[38] Focusing efforts on this key knowledge gap will be essential—not only sharing cyber best practices, but communicating clearly that we are collectively the first line of cyber defense.

Unlike in Alfred's time, the population engaged in cybersecurity efforts need not be segmented into active and reserve divisions, nor is this necessary to preserve local connections. In fact, it strengthens them. Cyber-literate individuals and in-house information-technology (IT) professionals should have the advantage of familiarity with, and responsiveness to, their local networks and patterns of behavior, allowing them to notice out-of-place emails or changes in network activity.[39] This combination of centralized organization and training with decentralized security should raise the baseline of cyber safety and make it that much more difficult for attackers to execute harmful operations. Attackers and defenders in any domain will be locked in a constant competitive evolution; therefore, cyber competence cannot be merely learned by rote. More central to the practice of cybersecurity is the ability to learn, to recognize problems and seek out solutions proactively.

The United States has a workforce problem: not enough people are engaged in cyber-defense efforts.[40] This is true in terms of both pure quantity and of diversity. According to the Aspen Institute, only 4 percent of cybersecurity workers self-identify as Hispanic, 9 percent as Black, and 24 percent as women.[41] Cybersecurity, like all fields, benefits from "a richer set of voices and perspectives, in the analysis, at the keyboard, and in the boardroom."[42] Ongoing efforts across government and the private sector to expand and diversify the cyber workforce, such as CISA's Cybersecurity Education and Training Assistance Program and the Department of Defense's Cybersecurity Education Diversity Initiative must be built upon by seeking lessons from civil-society organizations whose focus is cyber-workforce growth and diversity.[43] What is really needed, says Kurt John, chief cybersecurity officer of Siemens USA, "is a mindset change for how we recruit that taps into the full range of talent across society and enables us to address the needs of industry."[44] But, proactive countermeasures could potentially go even further. A model similar to the Estonian Defence League's Cyber Defence could be established within the United States.[45] This group, as Monica Ruiz of Microsoft's Digital Diplomacy suggested, could be housed within the National Guard and consist of "cyber-security experts across sectors who are willing and able to contribute time and resources on a defensive, voluntary, and situation-dependent basis."[46] We largely hold a shared fate in the cyber domain and, as such, should step up to create a shared mission and shared responsibility.

Lesson Three: Detection and Response

The third of Alfred's major reforms was to order large-scale military construction, a network of fortified settlements across his territory called the burh system.[47] These burhs were placed such that no settlement would be more than a day's ride from one of these protected locations. News

36 SL Russell and SC Jackson, "Operating in the Dark: Cyber Decision-Making from First Principles," *Journal of Information Warfare* 17, 1, 2018, 1–15, https://www.jstor.org/stable/26504126; I. A. Magomedov, H. A. Murzaev, and A. L. Zolkin, "Cyber Literacy as One of the Main Discipline Necessary in Modern Time," International Conference on Economic and Social Trends for Sustainability of Modern Society, October 2020, https://www.europeanproceedings.com/article/10.15405/epsbs.2020.10.03.117; Chris Brook, "What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More," Data Insider, October 6, 2020, https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more; Arun Vishwanath, et al., "Cyber Hygiene: The Concept, Its Measure, and Its Initial Tests," *Decision Support Systems* 128, 2020, https://www.sciencedirect.com/science/article/pii/S0167923619301897.

37 "Phishing Attacks," Imperva, https://www.imperva.com/learn/application-security/phishing-attack-scam/.

38 Ashley A. Cain, Morgan E. Edwards, and Jeremiah D. Still, "An Exploratory Study of Cyber Hygiene Behaviors and Knowledge," *Journal of Information Security and Applications* 42, 2018, 36–45.

39 "Benefits of an In-House Cybersecurity Tea," Cyber Policy, https://www.cyberpolicy.com/cybersecurity-education/benefits-of-an-in-house-cybersecurity-team.

40 *Building America's Skilled Technical Workforce* (Washington, DC: The National Academies Press, 2017), https://www.nap.edu/catalog/23472/building-americas-skilled-technical-workforce2.

41 "Diversity, Equity, and Inclusion in Cybersecurity," Aspen Institute, September 9, 2021, https://www.aspeninstitute.org/publications/dei-in-cybersecurity/.

42 *Cyber 9/12 Strategy Challenge*, *Atlantic Council*, https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/cyber-912/.

43 "Cybersecurity Education and Training Assistance Program," Federal Grants Wire, https://www.federalgrantswire.com/cybersecurity-education-and-training-assistance-program-cetap.html#.YTo1So5Kg2w; "Department of Defense and National Security Agency Announce New Cybersecurity Initiative Aiming to Close the Cybersecurity Talent Gap," National Security Agency, press release, October 15, 2020, https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2382623/department-of-defense-and-national-security-agency-announce-new-cybersecurity-i/.

44 Kurt John, *The 5×5—Minding the Cyber Talent Gap*, *Atlantic Council*, https://www.atlanticcouncil.org/content-series/the-5x5/minding-the-cyber-talent-gap/.

45 "The Estonian Defence League Act," Riigi Teataja, November 25, 2013, https://www.riigiteataja.ee/en/eli/525112013006/consolide.

46 Monica M. Ruiz, "Is Estonia's Approach to Cyber Defense Feasible in the United States?" War on the Rocks, January 9, 2018, https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/.

47 Pratt, *The Political Thought of King Alfred the Great*, 94; Pollington, *The English Warrior*, 97.

of a Viking incursion would be reported to the nearest burh, which could relay the information onward along the specially constructed roads in the direction the threat was moving, so as to "limit the advantage of highly mobile aggressive troops."[48] This notification system, while not instantaneous, made it more difficult for the Vikings to travel through Alfred's lands undetected, robbing them of their "major strategic advantages: surprise and mobility."[49] Alfred also, influenced by the Carolingians, built bridges across rivers near these fortifications to better control these crucial highways of attack.[50] Vikings who encountered a low bridge could be forced, depending on the design of their longship, to disembark and carry their ships around the impediment, creating opportunities for Anglo-Saxon forces to attack and halt their progress inland.

When the Vikings did reach their target and commence the attack, the nearest burh would call for aid along the chain of nearby burhs, and forces would convene to launch a counterattack. The system was staffed independently of the fyrd, though fyrd members could be called upon to swell the ranks of each burh in times of crisis, and the fyrd itself often used these fortified locations as meeting points.[51] A single burh under attack or with knowledge of an adversary's movements was not expected to stand alone, but was part of a network with set procedures to share information and request aid. These military construction efforts, in concert, created points of concentrated strength, as well as a system of threat detection, information sharing, and coordination.

Every point of potential vulnerability, whether in Alfred's kingdom of Wessex or the cyber domain, cannot be fortified against all potential harm; adversaries will seep through. Key to a successful defensive system is acceptance of this reality. With this acceptance comes a new mission more important than just prevention—detection. The burh system succeeded in changing the effective terrain of Wessex, creating internal security points in the place of near-complete freedom of movement. Applied to ransomware, this means being aware of both external points of potential vulnerability and internal security measures. Attacks will get through, so network awareness and internal chokepoints are as important, if not more so, as outer defenses. If we increase the scale, seeing an individual company or government entity as the Kingdom of Wessex, freedom of network access should be at or near only what is necessary for mission function. There should be "burhs" and "bridges" throughout internal networks that permit or deny access to commensurate privileges. The fewer employees with administrative access, the lower likelihood a phishing email will successfully infiltrate the network and spread.

Information sharing is the frequent buzzword of the cyber policy establishment—and for a reason. Underreporting is a massive impediment to understanding the true impact of cyber criminality.[52] In this fast-evolving space, every piece of intelligence could translate into defenders' success or failure. But, this information must be understandable and actionable in its delivery, which is often where formal information-sharing agreements break down—especially where there are large resource or capability asymmetries among the parties.[53] Information-sharing networks regarding ransomware must be straightforward, accessible on a sliding scale to all potential targets from individuals to large corporations, and established so that the benefit of engaging is very clear and information value is flowing multi-directionally between the private sector and government. As the ransomware task force proposes, there should be a standard format for ransomware reporting to streamline the reporting process and aid in data-aggregation efforts.[54] Like Alfred's burhs, this system of information exchange should be directly tied to requests for aid so that entities under extreme stress do not need to engage multiple agencies and sources in order to remediate their situation. CISA's Ransomware Guide instructs victims of ransomware to "consider requesting assistance from CISA; MS-ISAC; and local, state, or federal law enforcement (e.g., Federal Bureau of Investigation [FBI], U.S. Secret Service [USSS])."[55] Instead of this gamut of options, ransomware information sharing and response should be housed under a single agency with a clear mission. This does not mean that multiple entities cannot be involved, but that the interaction should be as streamlined as possible from the "victim" side. The FBI could serve as the central spoke of US ransomware response, collecting and disseminating information, as well as coordinating aid and response with other entities.

48 John Baker and Stuart Brookes, *Beyond the Burghal Hidage: Anglo-Saxon Civil Defence in the Viking Age* (Leiden, Netherlands: BRILL, 2013), 139, https://ebookcentral.proquest.com/lib/kcl/reader.action?docID=1170060&ppg=157.

49 Richard Abels, *Alfred the Great: War, Kingship and Culture in Anglo-Saxon England*, (White Plains, NY: Taylor & Francis Group, 1998), 198, https://ebookcentral.proquest.com/lib/kcl/detail.action?docID=1569874.

50 Jeremy Haslam, "King Alfred and the Vikings: Strategies and Tactics 876-886 AD," *Anglo-Saxon Studies in Archaeology and History* 13, 2005, 121–153, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.628.1028&rep=rep1&type=pdf.

51 Pratt, *The Political Thought of King Alfred the Great*, 95.

52 Warwick Ashford, "Cyber Crime Widely Under-reported, Isaca Study Shows," *Computer Weekly*, June 4, 2019, https://www.computerweekly.com/news/252464401/Cyber-crime-widely-under-reported-Isaca-study-shows; "State of Cybersecurity 2020 Part 2: Threat Landscape and Security Practices," ISACA, https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoFmEAK.

53 Herr, et al., *Broken Trust*.

54 "Combating Ransomware: A Comprehensive Framework for Action," 46.

55 "Ransomware Guide," 12.

In Conclusion—History Does Not Repeat Itself, but It Sure Does Rhyme

The Anglo-Saxons did not know that they were living through what would be termed the Viking Age until it had well begun, and they certainly did not know how history would unfold. None of us can. But, we can learn from the parallels of times past. The Anglo-Saxons, and much of Northwestern Europe, faced a persistent threat in the Vikings—a threat that would fundamentally reshape the continent's political and social makeup. Many leaders chose, repeatedly, to pay whatever these Vikings demanded, and even occasionally hired them as mercenaries in their own internal conflicts.[56] The Vikings' basic economic model and operational structure mean that the lessons of one era may be applied, in part, to the other.

Ransomware is another of the complex and persistent problems that governments, corporations, and individuals face in the cyber domain, and to which these entities will respond in myriad, complex ways. There is no one correct answer that will result in a domain free of ransomware. Instead, we must draw counsel from the response to another complex, persistent problem centuries before. Just as Alfred the Great reorganized the incentive structure of his government to combat a Viking scourge, contemporary governments must work with the private sector to align their responses to these incidents to build toward collective resilience. Just as Alfred reformed military service, government and the private sector must invest in their own "front line of defense" against attack—the people. Finally, just as Alfred ordered the construction of internal fortification and communication, government and the private sector must orient security toward detection and rapid response and prevention and establish a coherent information-sharing and aid-request system.

But, among the best lessons from the Viking Age is found not in Alfred's reign, but in Aethelred's. The reforms of Alfred were largely undone by the time of his great-great-grandson's rule, perhaps because the threat no longer seemed worth the investment. Our steadfastness must match or exceed those of the persistent threats we face, or, like Aethelred, we will be left to reap the consequences. We have the collective ability to stave off the raids and inhibit the plundering, to keep the fires from spreading without restraint. Reform is crucial, and will mean nothing if we, too, are not persistent.

About the Author

Emma Schroeder is an assistant director with the Atlantic Council's Cyber Statecraft Initiative within the Scowcroft Center for Strategy and Security. Her focus in this role is on developing statecraft and strategy for cyberspace that is useful for both policymakers and practitioners. She is the managing editor for the Cyber Statecraft Initiative's ongoing Cyber Strategy Series, which presents new perspectives on the most pressing topics in cybersecurity strategy. This series is intended to challenge assumptions and spark productive debate, to contribute to a better understanding of how the United States and its allies and partners can and should operate in the cyber domain.

Schroeder is passionate about using fiction as a tool to build bridges, both to complex topics and to other communities. She is the lead author of The Cyber Moonshot, an ongoing series of short stories from the Cyber Statecraft Initiative designed to communicate core themes and concepts in cybersecurity.

56 Simon Coupland, "The Frankish Tribute Payments to the Vikings and their Consequences," Herausgegeben vom Deutschen Historischen Institut Paris, 1999, https://journals.ub.uni-heidelberg.de/index.php/fr/article/view/47294.

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
Stéphane Abrial
Todd Achilles
*Peter Ackerman
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
John Bonsell
*Rafic A. Bizri
Linden P. Blue
Adam Boehler
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
*Alan H. Fleischmann
*Michael Fisch
Jendayi E. Frazer
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
Frank Haun
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Maria Pica Karp
Andre Kelleners
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Mian M. Mansha
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Christian Marrone
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Dambisa F. Moyo
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
W. DeVier Pierson
*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
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
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
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 February 4, 2022

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