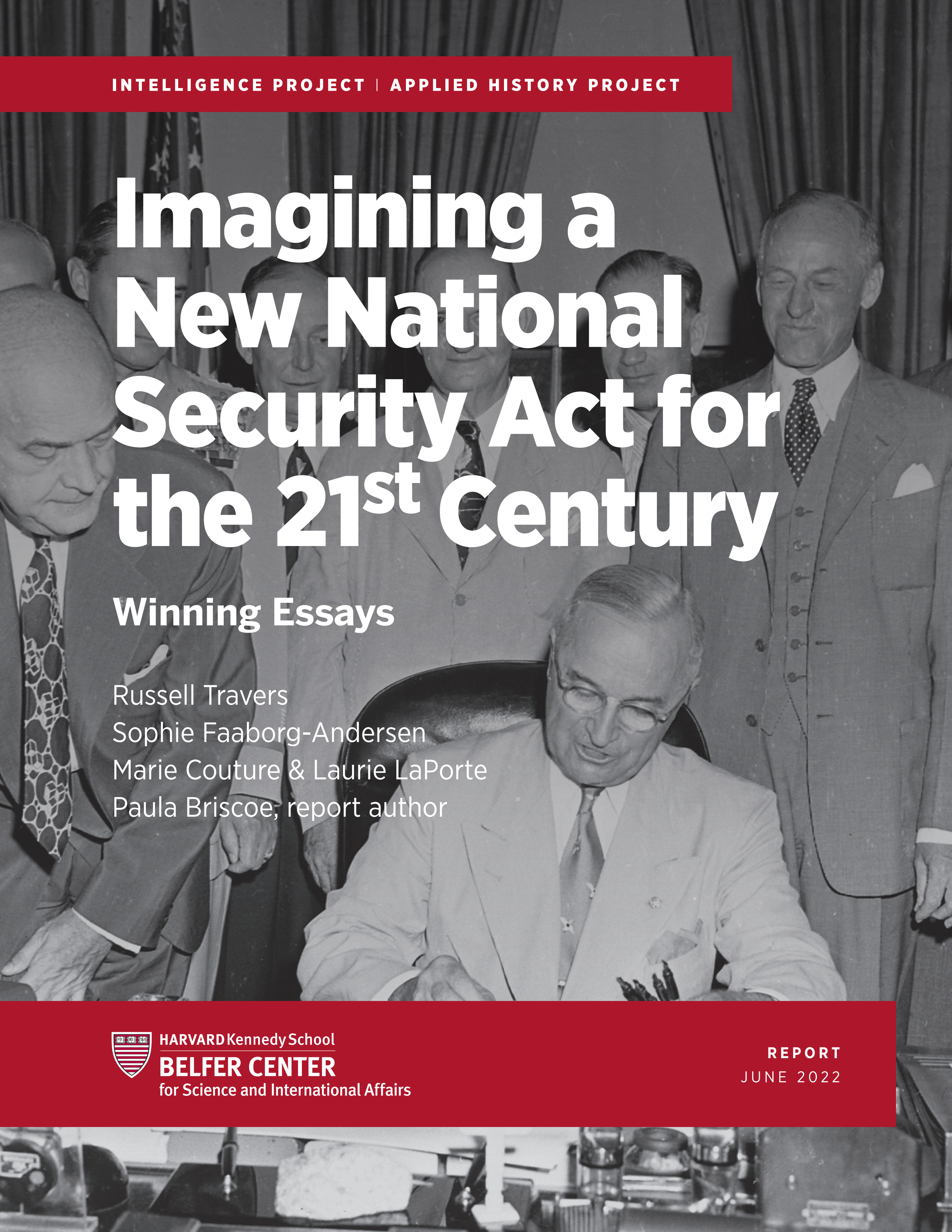
INTELLIGENCE PROJECT | APPLIED HISTORY PROJECT



Imagining a New National Security Act for the 21st Century

Winning Essays

Russell Travers
Sophie Faaborg-Andersen
Marie Couture & Laurie LaPorte
Paula Briscoe, report author

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

REPORT
JUNE 2022

Intelligence Project | Applied History Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

belfercenter.org/project/intelligence-project
belfercenter.org/project/applied-history-project

Statements and views expressed in this report are solely those of the author(s) and do not imply endorsement by Harvard University, Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

INTELLIGENCE PROJECT | APPLIED HISTORY PROJECT

Imagining a New National Security Act for the 21st Century

Winning Essays

Russell Travers
Sophie Faaborg-Andersen
Marie Couture & Laurie LaPorte
Paula Briscoe, report author

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

REPORT
JUNE 2022

President Truman at his desk in the Oval Office signing the National Security Act Amendments of 1949. Abbie Rowe/U.S. National Archives and Records Administration

Table of Contents

Essays

About the National Security Act Essay Contest

The National Security Act Essay Contest, "Imagining a New National Security Act for the 21st Century," and an associated day-long symposium, were designed to generate new ideas for improving the intelligence and national security community in the US based on the dynamic security environment we face in the 21st century. The essay prompt offered a variety of hypothetical scenarios where intelligence failure contributed to catastrophic failure and posed the question: what you would change now to improve the intelligence and national security posture of the US? The winning essays were selected from approximately 75 applicants and rated by a team of judges drawn from the Belfer Center Intelligence Project Senior Fellow cadre. An Intelligence Project conference on 11 May brought together intelligence historians, the essay finalists, and senior intelligence professionals to discuss the challenges and opportunities for intelligence reform.

Introduction

Seventy-five years ago, the US Congress passed the National Security Act of 1947 to address the shortcomings in national security that had been identified in the run up to and during WWII. At the beginning of the nuclear age, and with the Soviet Union looming as the primary challenger to the US and democratic countries, the Congress established institutions including the National Security Council and the Central Intelligence Agency to meet the national security needs of the 20th century. Given that much has changed in the world since 1947, the Intelligence Project decided to put the question of our national security posture for the 21st century out to the public in the form of an essay contest. The Intelligence Project in conjunction with the Applied History Project then held a one day symposium on the topic, featuring the winning papers.

About the Authors

Paula Briscoe, PhD, is a Senior National Intelligence Service Officer with the Office of the Director of National Intelligence with over two decades of experience in the U.S. Intelligence Community, and ran the essay competition in her capacity as a 2021-2022 Recanati-Kaplan Fellow. Russell Travers, first-place winner, is retired from government after four decades of service including serving as the Acting Director of the National Counterterrorism Center at the Office of the Director of National Intelligence and three senior tours on the national Security Council. Sophie Faaborg-Andersen is a Masters of Public Policy student at Harvard Kennedy School of Government. Marie Couture and Laurie LaPorte, third-place winners, are both national security experts.

About the Intelligence Project

The Intelligence Project seeks to build a new generation of intelligence practitioners prepared to serve in a rapidly changing world and to help future policymakers and intelligence consumers understand how best to interact with intelligence to gain a decision advantage. Building on multi-disciplinary research being conducted at the Belfer Center, from history to human rights and cyber technologies, the Intelligence Project links intelligence agencies with Belfer researchers, Faculty, and Kennedy School students, to enrich their education and impact public policy.

About the Applied History Project

The mission of Harvard's Applied History Project is to revitalize applied history by promoting the production and use of historical reasoning to clarify public and private challenges and choices. The Project sponsors the Applied History Working Group of faculty members across Harvard University to organize discussions with scholars and practitioners; supports historians and policymakers in producing Applied History; develops courses in Applied History; funds the Ernest May Fellowships in History and Policy for pre- and post-doctoral students; and holds Applied History Seminars open to the Harvard Community and the public. Harvard's project is one of the leaders among a rapidly expanding network of universities and think tanks that are furthering the discipline of Applied History by clarifying predicaments and choices to inform better decisions.

Acknowledgments

We are grateful to the many essay authors from around the world and many walks of life who took time to pen thoughtful entries. There were many great ideas, and we wish to continue the conversation. We would also like to thank our panelists and speakers, particularly: James Clapper, Sue Gordon, Ellen McCarthy, Michael Warner, James Wirth, Sarah Castro, Michael Miner, Paula Briscoe, and Graham Allison. Special thanks to Maria Robson Morrow, Maya Cotton, Raleigh Brown, and the Belfer Communications team for your invaluable support without which this event would never have happened.

Call for Papers: Imagining a New U.S. National Security Act for the 21st century

The following is the call for papers that the Belfer Center disseminated on December 16, 2021, to launch the essay contest.

Imagine if you woke up tomorrow to news of:

A massive cyber-attack that irreparably damaged financial markets and shut down critical infrastructure, or

A significant conventional defeat due to strategic surprise like happened at Pearl Harbor, or

The release of a manufactured pathogen that marks the beginning of a new global pandemic.

Each of the scenarios above, and others, could be caused in part by a catastrophic intelligence failure. Drawing on the lessons of World War II and in the context of the impending Cold War, the United States Congress passed the National Security Act of 1947 to address institutional challenges and to set favorable conditions for U.S. intelligence and national security. Now, nearly a quarter of the way through the 21st century, the National Security Act of 1947 remains the bedrock of the U.S. national security enterprise, but in a world in which the threats and challenges have dramatically changed. We pose an overarching question: If you were starting from scratch, what might a National Security Act for the next 75 years contain to address current shortcomings and to improve intelligence capabilities, structures, and organizations to meet requirements in the years ahead?

The Intelligence and Applied History Projects at Harvard's Belfer Center invite submissions for an essay contest on imagining a new U.S. National Security Act for the 21st century. Essays should consider the rise of China, technological advances, globalization, changes in U.S. relative power, redefinition of national security to include economic and cyber issues, espionage at scale, compression of decision time, and climate change—among other trends you deem important—and how these factors might drive a paradigm shift for U.S. intelligence and national security in general.

As you examine this question and possible approaches to a reformed national intelligence enterprise, we invite you to provide a framework for new legislation along with ideas for what the United States should prioritize. The best papers should address the national interests at stake and the most pressing challenges your construct is designed to address. What institutions, mechanisms, legal requirements, or other factors would you choose to create, merge, alter, or abolish and why? What efficiencies, benefits, and synergies are part of the big picture objective? Finally, what are the foreseeable impediments to your proposed changes and what is driving them?

The contest was open to the general public and papers were limited to 2,500 words.

The winning papers received cash prizes of $5,000, $2,500, and $1,000, and the authors presented at the May 11, 2022, symposium hosted at the Harvard Kennedy School.

Please read on for the winning papers.

Imagining A National Security Act For The 21st Century

Russell Travers

First-place winner

“[T]he basic deficiency of the current national security system is that parochial departmental and agency interests, reinforced by Congress, paralyze interagency cooperation, even as the variety, speed and complexity of emerging security issues prevent the White House from effectively controlling the system.”

Project on National Security Reform (PNSR) 2006

Inadequacies in the National Security Act of 1947 (NSA47) have been apparent for decades.[1] Unfortunately, effective remedies remain elusive. Clinton Administration Directives tinkered at the margins but were too timid. The Intelligence Reform and Terrorism Prevention Act (IRTPA) attempted to “fix” intelligence but was ultimately watered down, adding bureaucracy while leaving existing authorities largely intact. And the PNSR envisioned a grandiose overhaul of government and never gained traction. These efforts stemmed from a recognition that security is increasingly defined by more than the capabilities to fight big wars. That reality continues.

[1] This paper draws on a 43-year Intelligence Community career – including three senior NSC tours, and some of my writings: “Waking up on Another September 12th: Implications for Intelligence Reform” (Intelligence and National Security 2015); “Addressing our Whole of Government Deficit” (Just Security 2020); and a 2020 Urgent Concern memo to Congress alleging the Executive Branch was not abiding by the IRTPA.

2021 Epitomized the Challenge

Last year began with the January 6th insurrection. Ten days after President Biden's inauguration a coup occurred in Burma. Throughout 2021, the USG grappled with Afghanistan – the withdrawal decision/evacuation/aftermath, Southwest border migration, Shia militia attacks in Syria and Iraq, Iranian nuclear negotiations, Houthi UAV attacks from Yemen, international/domestic terrorism, Ethiopia, Colonial pipeline and other cyber attacks, global disinformation, China/Hong Kong/Taiwan issues, North Korean missile launches, Haitian President's assassination, billion dollar weather events and climate change, record deaths from opioids/synthetics abetted by transnational organized crime, Russia/Ukraine, foreign malign influence, global backsliding of democracy, the worst pandemic in 100 years. And more.

Such wide-ranging issues typify the 21st century security environment. Generally, they are not primarily military in nature. They rarely fall within the purview of a single Department or Agency (D/A). They often straddle the foreign/domestic divide. They implicate D/As not typically considered part of the national security architecture. And because globalization has afforded individual transnational threat actors the wherewithal to cause strategic effects, the potential for surprise is high. By extension, Intelligence needs to "do the world."

Such issues invariably occupy Deputies', if not Principals' attention – on multiple occasions, often contemporaneously, and involve Seniors busy running large organizations. And political implications dictate involvement by the same D/A seniors as policy decisions are being implemented. Bandwidth and time constraints are significant challenges.

NSA47 was fit for its time. Security was primarily viewed in foreign, military terms, heavily USSR-focused; the Act integrated parts of the Defense establishment, augmented existing defense intelligence with the CIA, and created the NSC. Now, we need to further government-wide integration, building on what exists and adapting to the challenges of the 21st century. While the constellation of organizations and authorities must change, transitions are tricky. Executive Branch operations would be significantly impaired while orchestrating a major government-wide transformation. But the status quo is untenable; history has demonstrated that we either don't identify problems in advance, or we react slowly/ineffectively. This paper suggests a phased approach: near-term modifications to existing structures to see us through the next decade, while also developing a consensus longer term vision addressing authorities, intelligence, public/private engagement, and professional education.

Near-Term Fixes

In the near term we will largely rely on existing structures – D/As and a small interagency apparatus. But changes at the margins could help. For instance, while conventional wisdom maintains that the NSC staff is too large, the security environment, history, and empirical data suggest the conventional wisdom is wrong. We tried shrinking the staff at the end of the Obama Administration, and the Trump Administration further minimized NSC involvement by moving issues out of the White House – under the premise that D/As would self-organize to address problems. They both failed.

The academic retort to proposals to grow the NSC staff is that focus should be limited to "strategic" issues – in essence, geopolitical chess. Certainly important, but in a globalized world, where tactical problems implicating multiple D/As can have out-sized effects, what does "strategic" mean? Russia/Ukraine? Sure. Iranian nuclear negotiations? Of course. But what about watchlisting (inadequacies led to 9/11) … balancing sharing/protecting sensitive information (shortcomings led to Wikileaks and Snowden) … Pandemic planning failures in testing, surveillance, and stockpiling of PPE (downgrading the NSC Senior Director focusing on pandemics undermined COVID efforts) … the Chinese purchase of mining rights to cobalt in DROC (a Great Power Competition failure)? If not by the NSC, where are such interagency issues addressed?

In reality, a more robust NSC is required – laser focused on identifying security issues, teeing them up for senior consideration. This wouldn't be a mini-State Department or Defense Policy shop, and an "honest broker"

National Security Advisor mustn't countenance staff "micromanagement" of D/As. But we do need adequate capacity to set the table for senior-level interagency conversations. Reasonable people could differ on what that means numerically,[2] but it certainly requires more Senior Directors to survey the security landscape and bring together the interagency to address security challenges. The NSC staff must also address an age-old problem - getting discussion/decision papers drafted/circulated sufficiently in advance to facilitate informed Senior discussions.

Even with a more robust NSC staff, this complicated world requires greater integration below the White House level. A successful model exists. The National Counterterrorism Center (NCTC), created after 9/11 – initially under Executive Order, is an "interagency joint venture", staffed by various D/As to work counterterrorism. NCTC has unique authorities allowing it to straddle foreign/domestic and access most relevant information. The Center is not "operational", thereby not impinging on equities of D/As (which retain analysts to support operational missions). But by bringing intelligence analysts and data together from across the Federal government and doing work on behalf of the entire government (while promoting information sharing), it ideally eliminates wasteful redundancy of ½ dozen CT organizations producing similar reports. Moreover, NCTC has a "whole-of-government" planning function; it supports the NSC bringing all elements of state power to bear and conducts net assessments.

While other "centers" exist, none have the authorities or analytic capacity of NCTC. We should consider where else this robust model makes sense. One candidate would be Transnational Organized Crime, a threat killing far more Americans than terrorism. Among other things, this Center would be charged with maintaining an authoritative database of TOC actors to address a major hole in border security – mirroring post-9/11counterterrorism improvements.

[2] Seasoned NSC alums with an understanding of the security environment should conduct a zero-based review.

Other specific near-term fixes could begin addressing intelligence shortfalls within existing authorities:

Data Processing: Machine learning and artificial intelligence will remain suboptimized until we make it easier for machines to assist analysts. Unstructured data is a particular problem because of Department-specific approaches to indexing and reporting. The ODNI should work with the IC to adopt a common future reporting format, with common indexing standards. It would eventually pay huge dividends in generating new knowledge.

Open Source: Exploiting the open internet poses challenges. What limits to scraping, ingesting, and processing open-source information strike the right balance - uncovering plots like 6 January, but not chilling free speech and invading privacy? What guard rails are required? Similarly, what open-source data (particularly "ad tech" and "collateral telemetry data") is appropriate for purchase by the Government? The advocacy community and Congress must be engaged; codification and oversight are required.

Developing a Longer-Term Vision:

Even these incremental changes would stress the Executive Branch. Unfortunately, while they would meaningfully improve national security processes without requiring major statutory change, they would be insufficient. Former Defense Secretary Robert Gates has characterized our "whole-of-government" efforts as largely "smoke and mirrors".[3] I agree. We need to consider more extensive changes in Executive Branch authorities, the Intelligence Community, public/private interaction, and professional education, to better posture ourselves for a 21st Century security environment

However, with our complicated government, we must be deliberate, and practical. The government needs to function while we consider change and build consensus. That suggests some sort of commission-like effort; this could be orchestrated by an FFRDC, or an independent purpose-built group, but it needs to involve current and former Executive and Legislative branch officials, as well as private sector thinkers, steeped in the practical aspects of how Government works. Along with big picture organizational and authorities' issues, second and third order implications need study: personnel, training, acquisition, data processing/privacy etc. And the study effort needs to accept that we can't just flip a switch; it took decades to fashion/implement Goldwater Nichols to better integrate DoD. This would be vastly more complicated; a detailed, phased, decade-long+ transition plan would be required.

[3] Robert Gates, "The Overmilitarization of American Foreign Policy", www.foreignaffairs.com, July/August 2020

In broad strokes, the following issues should be addressed:

Executive Branch Authorities. We need to examine potentially significant changes in the authorities construct between/among D/As.

- Gates suggests that the State Department be the lead Federal Agency overseas for other than wartime situations. Intuitively logical, but what are the implied implications? Could State tell DOD how to spend its appropriated funds? Or whether/how other D/As engage overseas? How would Congressional oversight change? What would be the required size, composition, and organization of the State Department to assume this role? Where would NSC responsibilities begin/end?

- Cyber defense authorities also require focus. My guess is that our very decentralized efforts will not stand the test of time. The threat is nimble, and we aren't. This study needs to recommend bare minimum centralized authorities and where they should reside - complicated by the fact that it's a shared public/private sector problem. Could the UK cyber-center model have some applicability?

- Finally, the "Management side" of OMB should be strengthened to address interagency issues receiving inadequate Deputies' attention. This would assist governance of lower profile security activities where shared D/A dependencies exist; Wikileaks remedial issues and some COVID-related shortcomings could have been addressed by a strengthened OMB.

IRTPA 2.0. The Intelligence portion of the study should envision an empowered DNI, specifically rewriting section 1018 of the IRTPA that rendered the DNI "herding cats". The loose confederation approach isn't up to the realities of the 21st century.

- **Streamlining Command and Control**. The Combat Support Agencies - NSA and NGA (and parts of DIA), should explicitly fall under the DNI; to protect the equities of DOD and its warfighting needs, the Deputy DNI should be statutorily established as a 4-star billet.

- **Increasing Effectiveness and Efficiency**. Differences between "national" intelligence and "defense" intelligence are less meaningful today; duplication among organizations is rampant and resources to address new threats are invariably difficult to find. DNI should oversee a single national analytic office (consolidating analysts from DIA and CIA), along with interagency Centers focused on transnational threats; together they would constitute the national hub of all-source intelligence. There are significant manpower savings to be had.

- **Achieving Balance within the Intel Cycle**: With direct programmatic control over all elements of the intelligence cycle, the DNI would be empowered to balance collection and analysis, and rationally allocate resources between/among threats. The necessary size of the ODNI staff to effectively perform this mission would need to be evaluated.

- **Improving Data Access**. Various legal/policy/privacy/security/operational constraints preclude any analyst or organization in the USG from accessing all relevant information pertinent to any specific threat category. We should identify/address the specific information sharing impediments or clearly articulate the risk associated with leaving them intact.

- **Ensuring Government-wide Intelligence Support**. Other D/As require ongoing intelligence support. Their intelligence requirements generally fall into the "situational awareness" and/or strategic analysis categories – largely drawing on product being generated by the national hub. However, the DNI would also be responsible for ensuring appropriate dissemination of particularly sensitive information.

- **Creating a Single Dissemination/Access Portal**. This enterprise would be stitched together by creating a single ODNI-sponsored dissemination portal, replacing many Departmental-specific architectures. Analysts could then easily find/access intelligence/knowledge from the entirety of the IC enterprise. "One-stop shopping" would become a reality.

- **Clarifying "Domestic Intelligence"**. With no legal definition of "domestic intelligence" and the IRTPA's use of the phrase "national intelligence", confusion exists as to the appropriate use of intelligence in support of homeland matters. As transnational threats grow and publicly available information increases in importance, treatment of U.S. Persons' information requires clarification and buy-in.

- **Guarding Against Politicization.** We have seen a recent Presidential attempt to politicize IC leadership; with a substantially empowered DNI, we need to take steps to ensure qualified, apolitical leadership. Something akin to the ABA vetting of Supreme Court judges is required for both "acting" and nominated IC leaders.

Whole-Of-Society. While improving "whole-of-government" performance is necessary, "whole-of-society" efforts are increasingly required for cyber threats, domestic and international terrorism prevention, disinformation, threat finance, economic espionage, and others. How do we routinize public/private relationships, at scale? There are 501(C)3 exemplars – the National Cyber Forensics Training Alliance and the Global Internet Forum Combatting Terrorism, that can serve as models. They somewhat improved transparency and information sharing but are relatively small efforts. We need to be thinking through the processes and procedures to institutionalize two-way flow of personnel/information between/among industry, academia, the press, and the government.

Education. All these efforts would implicate professional education. In the same way that Goldwater Nichols recognized the need to get military officers joint specialty qualified, we need government employees well-versed in interagency operations. To break down "silos", future leaders of D/As should "grow up" together throughout their careers, building trust, cohesion and a "good government" outlook. Part of that implies increasing joint duty rotations between/among organizations (perhaps required for promotion). Beyond that, we need career-long interagency training. National Defense University needs to become National Security University, further expanding students drawn from non-DoD entities. The movement of National Intelligence University to ODNI was appropriate, but NIU doesn't have the cache of CIA's Kent School; there needs to be greater investment in quality instructors and incentives for NIU attendance. And efforts like William and Mary's Whole-of-Government program for midlevel officers should be resourced to support attendance from across Government.

Impediments:

There would be countless roadblocks to updating the National Security Act: resources, turfiness within both the Executive and Legislative Branches, and pushback from within the advocacy community as we attempt to deal with the blurring of foreign and domestic. But strategic impediments would be more problematic: this paper assumes political consensus that our Country should play a leading role in the world, that alliances are key, and that military strength is necessary but not sufficient when it comes to national security; it also assumes that both Congress and the highest levels of the Executive Branch see beyond their inboxes and muster the sustained political will to engage in the single greatest overhaul of the national security establishment in 80 years. In today's polarized political environment both assumptions are suspect.

Imagining A New U.S. National Security Act for the 21st Century

Sophie Faaborg-Andersen (MPP)

Second-place winner

Executive Summary

Since the end of the Cold War, the United States' national security policy has been grounded in a set of assumptions about how conflicts unfold and the means by which they are fought and won. The decline of U.S. hegemony driven in part by a post-Cold War complacency and a rapidly evolving threat environment under digital, globalized conditions demands a fundamental rethink of the current structuring of American national security institutions. To date, this complex network of defense and security organizations has been led by the hierarchical committee system of the National Security Council (NSC). This system, built to address 20th century problems, cannot stand in today's more connected and fast-paced world, and must be replaced. A new National Security Act should reinstate NSC common law enforced by Congressional oversight, harness the innovative power of the American private sector to operationalize open and commercially sourced intelligence, and implement a unified, multi-year national security budget to link interagency funding decisions to the President's National Security Strategy (NSS).

The Changing Face of 21st Century Security

Global strategic competition is the defining security challenge of the 21st century.[1] The National Security Act of 1947 tailored American national security institutions to address America's primary threat: the Soviet Union. This confrontation represented an ideological conflict regarding how to organize industrial-age societies. Today's great power competition is a long-term and open-ended struggle for influence amongst great powers to determine the best way to organize societies in the information age: democracy or autocracy. This competition is playing out every day across geographies and domains, both inside and outside America's borders in a struggle for influence that blurs the lines between foreign and domestic, military and non-military, and public and private sectors.

While sustained interstate competition is not new, the last decade has seen dramatic shifts in the international security environment. Traditional threats including terrorism and great power competition are now joined by new challenges posed by emerging and disruptive technologies. Ever expanding networks of human and technology connections are accelerating the generation of information as well as diffusing power away from their traditional centers. Lulled by three decades of first-among-equals primacy, America has grown complacent in the face of these changes. The United States no longer enjoys a monopoly on the conditions that granted its privileged status - geography, economic supremacy, and uncontested military superiority.[2] From global pandemics to cyber-enabled attacks, successive crises have offered sobering reminders that oceans and borders will not keep threats at bay. China has already surpassed the U.S. as the world's preferred trading partner and largest economy as measured by purchasing power parity (PPP).[3] Indeed, many

[1] "Interim National Security Strategic Guidance." The White House, The United States Government, 3 Mar. 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/03/interim- national-security-strategic-guidance/.

[2] Brown, Zachery Tyson. "America's National Security Software Needs an Upgrade." Foreign Policy, 6 Apr. 2020, https://foreignpolicy.com/2020/04/06/america-united-states-national-security-apparatus- software-outdated-upgrade/.

[3] Allison, Graham, Nathalie Kiersznowski and Charlotte Fitzek. "The Great Economic Rivalry: China vs the U.S." Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, March 23, 2022.

parts of the international community - and increasingly Americans themselves - now see the United States as a declining power.[4]

While the U.S. military remains the most advanced fighting force in the world, it is not equipped to solve all or even most of these problems. Rapid advances in defense-relevant technologies from semiconductors to artificial intelligence are condensing timelines for understanding and responding to new threats. This increased pace of technology development - led largely by the private sector - has also resulted in a tighter coupling of economic and security issues. Decisions about trade and export controls are more intertwined with security decision-making than ever before. In an era where everything is digital, many modern wars will be won before the first shot is fired and militaries with the most advanced tanks and bombers will find their capabilities irrelevant if they cannot access systems due to cyber-attacks, fall victim to strategic surprise, or lack the relevant legal authorities to respond.

In an environment where threats cut across government authorities, a lack of integration across departments and agencies has resulted in duplicative efforts and bureaucratic knife-fighting that illustrate the challenges of executing "whole-of-government" efforts. This system is reinforced by a budget process that allocates funding along hard departmental lines and through distinct appropriations bills that offer legislators little incentive to balance and integrate across different categories of the President's National Security Strategy (NSS).[5] Rigid allocation of authorities and funding has resulted in lowest common denominator solutions and further bifurcation of defense and foreign policy agendas, with the former thinking in terms of military and intelligence and the latter in terms of politics and diplomacy.

Such traditional divisions are inadequate to address the cross-cutting national security issues facing the global community today. The NSC was built specifically to coordinate the integration of these tools of government but has instead become the strategic engine of national security options

[4] Parker, Kim, et al. "Looking to the Future, Public Sees an America in Decline on Many Fronts." Pew Research Center's Social & Demographic Trends Project, Pew Research Center, 26 Aug. 2020, https://www.pewresearch.org/social-trends/2019/03/21/public-sees-an-america-in-decline-on- many-fronts/.

[5] Rosenberg, Brett, and Jake Sullivan. "The Case for a National Security Budget." Foreign Affairs, 12 Nov. 2021, https://www.foreignaffairs.com/articles/2019-11-19/case-national-security-budget.

generation and execution. Determining which issues merit attention, developing plans for each, and overseeing their day-to-day implementation is neither practical nor desirable for a body of several hundred staffers operating thousands of miles from the frontlines and foreign capitals. This structure also makes ineffective use of government talent by leaving America's generals and diplomats to implement policies they have less and less ownership over. A new National Security Act must enable seamless exchange of information at every level and pivot away from the military as the default instrument of foreign policy toward long-term investments in diplomatic and economic tools to enhance America's position in a renewed era of strategic competition.

U.S. National Interests

Revising a national security enterprise fit for digital-era great power competition requires asking difficult questions about what we mean by national security and what really keeps America safe. The United States' most vital national interests will continue to be the ability to credibly deter attacks against the homeland and prevent the emergence of hostile powers in Europe, Asia, and on U.S. borders.[6] But in a renewed competition that is increasingly playing out in non-kinetic ways, the United States must act urgently to implement the political and societal reforms necessary to make its system more competitive at home. The most important 21st century national interests are protecting the security of the American people from threats that respect no national borders including cyberattacks, disinformation, infectious disease, climate change as well as defending the democratic values on which the United States was built.

[6] Ellsworth, Robert, Andrew Goodpaster, and Rita Hauser, Co-Chairs. "America's National Interests: A Report From The Commission on America's National Interests, 1996." Belfer Center for Science and International Affairs, Harvard Kennedy School, 60.

A New Paradigm: Defense and Intelligence Structures

In 1949, the NSC operated on a set of common laws prioritizing objectivity over advocacy and coordination over operational responsibility.[7] Then-Director of Central Intelligence Sidney Souers characterized the body as a "broker of ideas in crisscrossing proposals" from across the national security agencies.[8] In the aftermath of 9/11 as the world grew increasingly interconnected, a more powerful NSC shifted from a policy coordination body to a policy-making body, seizing responsibility for developing strategies from those in the military and bureaucracy. The resulting organization is both too large to be effectively managed and poorly integrated with military and technological experts.[9] Structural changes are required to improve information sharing, cut overly-complicated governance processes, overhaul the oversight process, and incentivize long-term planning.

Although many factors have contributed to the NSC's successes and failures, history suggests they do best with the "right-size" job.[10] To meet the needs of a new strategic environment that requires integrated use of all elements of national power, a new National Security Act should de-layer the NSC and disperse its experts into the agencies to serve in supporting roles to leadership offices across government.[11] This bottom-up approach empowers agencies with relevant expertise to serve as the center of gravity for their various issues but retains a single advisor on emerging technology - dual-hatted with the NSC and the Office of Science and Technology Policy (OSTP) - to serve a coordinating function. The advisor

[7] Gans, John. White House Warriors: How the National Security Council Transformed the American Way of War. Liveright Publishing Corporation, a Division of W. W. Norton & Company, 2019.

[8] Souers, Sidney W. "II. Policy Formulation for National Security." The American Political Science Review, vol. 43, no. 3, [American Political Science Association, Cambridge University Press], 1949, pp. 534–43, https://doi.org/10.2307/1950074.

[9] Restructuring National Security Organizations and Decision-Making." Restructuring National Security Organizations and Decision-making | Center for Strategic and International Studies, 31 Mar. 2022, https://www.csis.org/analysis/restructuring-national-security-organizations-and-decisionmaking.

[10] In his book, White House Warriors: How the National Security Council Transformed the American Way of War, historian John Gans notes, "the 1990s staffs, with between fifty and one hundred policy staffers, or around half of the current total, probably did the best work and had the best relationships with their peers".

[11] McCord, Brendan, and Zoe Weinberg. "Emerging Technology & the Future of the National Security Council." FSI, 28 Dec. 2020, https://fsi.stanford.edu/news/emerging-technology-future-national- security-council.

would also work closely with the National Economic Council (NEC) to coordinate agencies working at the intersection of economics and technology including export controls and supply chains. This approach is preferable to creating a new directorate which would only serve to further silo emerging technology issues. The trimmed NSC should focus on fewer issues and prioritize grand strategic questions regarding American national interests, objectives, and capacities in advance of major decisions. A leaner, better managed, and less aggressive NSC will play its intended role of coordinating national security players and policy. While such structural changes across the executive level are necessary, simpler endeavors - such as integrating email servers to allow for searching a unified national security directory across agency and rank - would also go a long way toward improving current barriers to interagency collaboration with immediate effect.

Intelligence Capabilities

In addition to broad structural change across the Executive level, managing 21st century security challenges requires filling intelligence capability gaps. Competition is about the pursuit and use of advantages: successful competitors devise strategies that draw on their strengths while managing their weaknesses, informed by a clear understanding of how opponents will seek to do the same. To be successful competitors, we must play to our essential advantages by restoring the sources of long-term domestic strength — including unmatched academic and private sector innovation — while identifying areas in which we need to improve our capabilities.

The most essential capability gap to fill involves bringing the power of commercial and open-source information to bear on intelligence work. Critical sources of information for policymakers seeking to understand 21st century strategic competition are often produced as byproducts of the day-to-day operations of commercial industry. These public and commercially available data, generated through activities like financial trading and global shipping, frequently fall outside of government analysts' traditional toolkits. Yet this mosaic of commercial and open-source data provides the sensemaking context for the exquisite intelligence collected by the United States interagency in addition to unique intelligence not found elsewhere. The U.S. Government (USG) must scale solutions for collecting, analyzing, and assessing this data to allow for early warning and decision advantage. This will require data-literate analysts working across industry, government, and academia to give policymakers the context they need for understanding competitor actions and intentions. Harnessing these data sets a foundation for authorities to address evolving mission challenges within hours and days instead of months and years.

To bridge the gap between open and commercially sourced intelligence and the USG, a new National Security Act should establish a new Center for Commercial and Open-Source Intelligence. Working across government, this new Center will be charged with improving mechanisms and amending authorities for bringing in outside expertise and data from academia and the private sector to support the USG. The Center will be chartered to operate in a manner that is consistent with privacy protections, ethical use of data, and oversight accountability.

Efforts to improve interagency coordination will remain ineffective if the national security enterprise is not working from the same assumptions or does not have access to the same baseline information. Currently no single entity has the resourcing and mandate to provide the required precursors for good analysis of alternatives. A new approach to information sharing in support of analysis will be coordinated by a Decision Support Cell (DSC) and report to the Office of the Director of National Intelligence (ODNI). This team would be charged with ensuring that decision support is transparent and that all relevant organizations have access to the same joint data, analytic methods and objectivity standards, risk metrics, operating concepts, and repositories of institutional knowledge.

Funding A Diplomacy-First National Security

The second structural change imposed by the Act will be reforming Congress' national security budget-making and oversight functions to fix what Ambassador Bill Burns has aptly termed the force-diplomacy "inversion" in U.S. foreign policy.[12] Simply trimming the Pentagon's funding is insufficient to address the structural overreliance on the military and broader limitations of U.S. strategy. To address these challenges, the Act should institute a unified and multi-year national security budget. An integrated budget, developed by merging existing authorization and appropriations committees, will directly link funding decisions to the President's NSS. By moving away from program-centric, defense-first funding, resources can be optimized across agencies best suited to specific objectives. Congressional oversight should also be overhauled to focus on program execution and flexibility to take advantage of new opportunities. To that end, cost assessments should include monetary comparisons but also opportunity costs, for example in terms of programs that could have been funded. This approach would also change incentives for politicians away from holding up the federal budget to secure funding for projects in their districts.

[12] Burns, William J. "An End to Magical Thinking in the Middle East." Carnegie Endowment for International Peace, https://carnegieendowment.org/2019/12/08/end-to-magical-thinking-in- middle-east-pub-80520.

Conclusion

Reforms will face significant resistance not only due to institutional inertia but also because the current national security architecture – which accounts for the majority of discretionary spending – is deeply entrenched into the fabric of federal, state, and local government across the country. Moreover, in an era of increased polarization, the breakdown of trust in Americans' faith that public servants are committed to every citizen's interest is threatening the nation's representative democracy. A larger challenge for the national security establishment, whatever form it takes, is rebuilding this trust with the American public through transparently demonstrating that they serve the public as much as the president.

Though it will not be easy, the costs of not adapting to meet the demands of today's competitive threat environment are too great. We risk an alternative in which individual authorities operate in silos that are at best not mutually reinforcing and at worst counteracting. Despite its challenges, the United States remains among the most adaptive nations in the world, with a robust network of alliances and innovative landscape of companies and universities revolutionizing the way people think and live. Though the threat environment has evolved since 1947, so too has America's ability to access new knowledge and experience in decision science, organizational design, and talent management. The United States should operationalize these unique advantages to implement a new national security enterprise fit for the next century.

Reimagining A New National Security Act:

Planning for Current and Future Asymmetries of Capability and Will

Marie Derilo Couture & Laurie LaPorte

Third-place winners

Introduction

Seventy five years have passed since President Harry S. Truman signed the National Security Act of 1947 into law amid well-established fissures in the U.S.-Great Britain-Soviet Union alliance. Ensconced in a vast ideological rift and underpinned by competing nuclear arsenals, the Cold War became the stage from which the National Security Act played. The act focused on responding to a threat of both scope and scale: a nuclear-armed adversary with demonstrated mastery in command and control of combat-honed militaries and exercised decision making that held other powers'–mainly the U.S. – strategies and infrastructures at risk. **The act was the legislative representation of the American will to protect its democratic values and leadership, if not its very existence.** International rules and norms for modern warfare are works-in-progress as the battlespace evolves to include domains in which borders and boundaries remain amorphous and not demarcated on a map. Deterrence, as a concept, has been reimagined to include cyber warfare, signaling the stark reality where asymmetric capabilities will take center stage as nation-states seek different ways to tip the balance against more powerful and capable adversaries. The National Security Act of 1947 does not account for this changed reality and its impact on U.S. leadership; as Seth Jones argues in his book *Three Dangerous Men*, "America is focused too exclusively on a potential conventional war and is not adequately acknowledging the irregular approaches of its competitors."[1]

[1] Webster, Andrew. (23 February 2022). Three Dangerous Men. *Real Clear Defense*. https://www.realcleardefense.com/articles/2022/02/23/three_dangerous_men_818254.html

The U.S. most prominent adversaries–China, Russia, Iran, and North Korea–have demonstrated not only the will, but the resolve to wield new capabilities in very lethal, crippling ways. Russia's invasion of Ukraine is the most visible and visceral example of the threat to a generations-long international order. Economic disruptions, open challenges to the U.S. and its allies' diplomatic resolve, and the punishing nature of ideological hubris have been on full display with Russia's invasion through Ukraine. There is absolutely no doubt that adversaries with similar aspirations have watched and learned as both the Russian and U.S. response playbooks were demonstrated over the last several months.

Threats are no longer limited to shooting wars; they have evolved into an integrated set of options that include cyber attacks and information warfare.

These threats are insidious, corrosive, and pernicious. Adversaries will take advantage of existing societal divides and sow the seeds for new ideological cleavages that threaten the very existence of free markets, democratic political structures, human dignity, and the legal frameworks that serve as the foundation of continued U.S. leadership. A reimagined National Security Act needs to acknowledge this changed landscape and restructure to adapt, respond, iterate, and evolve. **The future demands a more agile, strategic, expansive, transparent, and accountable effort to protect U.S. critical infrastructure; investments in public-private relationships that protect networks, research, and those sectors critical to innovation and the American way of life; and structural changes in the national security framework that minimizes the impact of political and partisan discord on the American grand strategy.**

Strengthening American Resolve and Protecting U.S. Critical Infrastructure

A new National Security Act must acknowledge that the U.S. domestic stability and global leadership is inherently dependent on a secure critical infrastructure backbone. U.S. critical infrastructure, existing within disaggregated and distributed public and private networks, will be vulnerable in the lead up to–and during–conflict. Disruptions to oil, gas, water, electricity, transportation, and financial networks will have alarming effects on social order, rendering the U.S. unable to stave off its adversaries' attempts to delay, disrupt, or undermine the U.S. public's will to engage in conflict.

The American public, in particular, has been a target ripe for influence, especially for political and information warfare. U.S. diplomat and architect of the U.S. Cold War containment strategy, George Kennan, described political warfare as "the employment of all means at a nation's command, short of war, to achieve its national objectives." While Kennan credits the Soviet Union with the "most refined and effective" conduct of political warfare, that threat evolved into a constant entanglement of political, economic, and information warfare.[2] **Asymmetric capabilities – those involving cheap, effective, and low-risk tools to shape events far outside a state's borders – have become essential in peace, deterrence, and wartime planning, as the U.S. adversaries attempt to bridge the gap between themselves and the decades-long American warfighting advantage.**

Telecommunications is particularly at significant risk from (largely) unvetted foreign telecommunications companies. Integrated into U.S. communications networks, these companies can potentially access or reroute U.S. traffic overseas, leverage expansive data analytics capabilities against U.S. communications, and apply advanced computing techniques to

[2] Pottinger, Matt. (2021 September/October). Beijing's American Hustle: How Chinese Grand Strategy Exploits U.S. Power. *Foreign Affairs.* https://www.foreignaffairs.com/articles/asia/2021-08-23/beijings-american-hustle

collect intelligence and conduct information operations.[3] **A new National Security Act must legislate the U.S. response to the growing number of foreign data centers located within the U.S., complicating the U.S. government's ability to protect and secure domestic communications.** Limiting Chinese companies like Huawei and ZTE from further proliferating and integrating equipment into U.S. telecommunications networks will stave off potentially malicious actors from holding U.S. networks and the public at risk.[4] The recently signed Secure Equipment Act is the first step towards protecting and preventing specific products from infiltrating U.S critical infrastructure.[5] **Success, however, will depend on broad expansion with strict oversight and accountability that keeps pace with foreign adversaries' technological advancements. Section 214, which allows foreign telecommunications companies to interconnect with U.S. networks, should be reshaped to more severely restrict access and to impose strict oversight mechanisms focused on interoperability.**

A new act must include the **minimum defensive cyber security requirements and protocols for sectors that manage and own facets of U.S. critical infrastructure at the local, state, and federal levels**. By legislating the shared responsibility of protecting the U.S. critical infrastructure while also allowing companies to protect financial interests; maintain unconstrained agency and independence; and meet minimum network security thresholds, the significant investments needed to achieve compliance becomes less threatening to businesses. Network changes, configurations, upgrades, and network defense activities are expensive and resource intensive. **Without legislated incentivization to harden these networks and improve cyber hygiene, the very networks that the U.S. government relies on will be at increased risk of compromise; the human, economic, and national security toll of not getting this aspect of national security correct could be catastrophic and insurmountable if not addressed in the short term.**

[3] Lucas, Edward. (7 December 2020). A China Strategy. *The Center for European Policy Analysis* (CEPA). https://cepa.org/a-china-strategy/

[4] Yuen Yee, William. (10 December 2020). With U.S. Restrictions on Huawei and ZTE, Where Will Rural America Turn?; *Center for Strategic and International Studies.* https://www.csis.org/blogs/new-perspectives-asia/us-restrictions-huawei-and-zte-where-will-rural-america-turn

[5] The Hill. (28 October 2021). Senate Approves Bill to Protect Telecommunications Infrastructure from Foreign Threats. *The Hill.* https://thehill.com/policy/cybersecurity/579028-senate-approves-bill-to-protect-telecommunications-infrastructure-from

Reinforcing Cyber Defense and Public-Private Sector Ties

Further expanding on the idea of legislated incentivization of minimum network defense for U.S. critical infrastructure sectors, public-private partnerships must be defined by clearly articulated and mutually-endorsed recommendations for prioritizing cyber security. A new National Security Act must **create a clear framework providing situational awareness to threats in the cyber environment, but more importantly, setting standards and norms for information sharing and mitigations in a timely, responsive manner.** We witnessed the financial and national-level impact of adversaries targeting U.S. networks with the ransomware attack on Colonial Pipeline[6] and SolarWinds.[7] [8] Events like these, while momentarily disruptive, can compel organizations to act but only after a potentially disastrous threat has already materialized. Many in the electric utility and cybersecurity sectors have installed sensors to detect malicious intrusions into their networks, signaling that there is an opportunity to expand the conversation to a broader swath of the U.S. critical infrastructure community.[9]

A new national security act must deliberately address the increasingly pressing need for more resilient encryption of systems, networks, and databases that support all levels of national decision making. It must be understood across the decision making spectrum–and this includes partners in the private sector–that effective and resilient encryption is necessary to protect data, online privacy, and the systems critical to national security. **From product or service conception, to acquisition, and through operationalization, the path to securing key national**

[6] Sanger, David E. & Perlroth, Nicole. (2 June 2021). White House Warns Companies to Act Now on Ransomware Defenses. *New York Times*. https://www.nytimes.com/2021/06/03/us/politics/ransomware-cybersecurity-infrastructure.html

[7] Canales, Katie and Jibilian Isabella. (15 April 2021). The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

[8] Heckman, Jory. (18 February 2021). Agencies 'Building Back Better' after SolarWinds Breach, Top Biden Cyber Official Says. Federal News Network. https://federalnewsnetwork.com/cybersecurity/2021/02/agencies-building-back-better-after-solarwinds-breach-top-biden-cyber-official-says/

[9] Uberti, David. (20 June 2021). White House Sees Electric Grid as Blueprint for Post-Colonial Pipeline Cyber Push. Wall Street Journal. https://www.wsj.com/articles/white-house-sees-electric-grid-as-blueprint-for-post-colonial-pipeline-cyber-push-11625045401

systems and networks needs to be based on an explicit understanding of the risks and vulnerabilities that already exist and a commitment to improve investments in network security. Improper configuration of systems, the use of out-of-date or legacy encryption keys, and a fragmentary understanding of risk are hallmarks of vulnerable systems. Codifying the sharing of sophisticated and advanced encryption tradecraft and technology reinforces the idea that encryption is an effective last line of defense in a layered security model[10]--some sharing already exists, but it could certainly be better and faster.

The partnership between the U.S. government and the private sector is the cornerstone of American cybersecurity–a reimagined act should state this explicitly and clearly. Provisions for financial incentives–tax credits, low interest loans, grants–to companies that continually meet the demands of the changing network security environment gets us closer to a more coordinated approach to defend U.S. critical infrastructure. **With defined thresholds based on localities and sectors, incentivization for compliance to close security gaps, minimize risks from legacy networks, continuously upgrade software/hardware, and improve encryption could pay immediate and future dividends.** Shared commitment to dedicate resources, expertise, and information to identify, counter, and prevent cyber attacks balances the burden of cyber defense equally on private and public sector entities.[11]

[10] Hardcastle, Jessica Lyons. (18 May 2021). White House Cyber Chief at RSA: 'Cost of Insecure Tech Is Staggering'. SDXCentral. https://www.sdxcentral.com/articles/news/white-house-cyber-chief-at-rsa-cost-of-insecure-tech-is-staggering/2021/05/

[11] Inglis, Chris and Harry Krejsa. (21 February 2022). The Cyber Social Contract: How to Rebuild in a Digital World. Foreign Affairs. https://www.foreignaffairs.com/articles/united-states/2022-02-21/cyber-social-contract

National Security Structural Changes

A future-forward approach to a new act should include the creation of a national security and defense leadership structure that oversees progress in this area. Since its inception in 1947, the National Security Council (NSC) remains the President's statutory body that assesses objectives, commitments, and risks on matters related to national and international security. While the NSC's processes and institutions remain agile enough to keep pace with a president's changing security needs, new challenges demand increased focus to ensure effective coordination across the government. The proposals below include shifts in or redefinition of roles for existing director positions, as well as provisions to guarantee that national security strategies are not encumbered or slowed down by currently unresponsive budget and appropriations timelines:

National Cybersecurity and Critical Infrastructure Director: The current structure is bifurcated–split between the National Cyber Director and the Deputy National Security Advisor (D/NSA) for Cyber and Emerging Technology–with both positions reporting directly to the President. An additional component of this undertaking involves the Cybersecurity and Infrastructure Security Agency (CISA), tasked to "understand, manage, and reduce risk to our cyber and physical infrastructure."[12] It is conceptually and practically impossible to disentangle cybersecurity from critical infrastructure and a provision that brings the current D/NSA for Cyber under the umbrella of the National Cyber Director and representation of CISA's role in national security decisionmaking will introduce efficiencies in strategic planning; policy coordination and implementation; and public-private integration.

National Supply Chain and Critical Technology Czar: Whether in peacetime or during war, one of the advantages that the U.S. has benefited from is an industrial base that can be mobilized to reinforce and secure defense and national security advantages. The U.S. supply chain, however, has not been without its weaknesses–crumbling U.S. hospital systems

[12] Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/about-cisa

because of diminished access to Personal Protective Equipment during a global pandemic; barely-stocked grocery store shelves; and miles-long lines at gasoline stations–and we have seen this just in the last two years. The threat of disruptions to sectors that provide critical technologies–semiconductors, for one–have been all-but-consuming in the press and in global markets. The primary responsibility of the Supply Chain and Critical Technology Czar will be coordination of national security policies that protect the U.S. supply chain and critical technologies from future disruptions to research and development, production, delivery, and acquisition.

Executive Order to Establish National Security Agency (NSA) and U.S. CYBER COMMAND (USCYBERCOM) as a Dual-Hat Entity: In order to more effectively defend U.S. national security and military networks from malicious activity, exploitation, and compromise, it is absolutely critical for the synergy of NSA and USCYBERCOM to remain intact. Due to the prescribed, intertwined national security missions and roles of these organizations, their success is inherently dependent upon one another as intelligence collection sets the stage for operational preparation and execution. While NSA is charged with the defensive cyber mission and foreign adversary cyber threat information, USCYBERCOM is responsible for U.S. offensive activities and operations against foreign malicious cyber actors. A critical feature of the synergy between both organizations is their dependence on the same, robust infrastructures and capabilities. Policies that establish and introduce streamlined authorities to plan, implement and operationalize, and defend U.S. national security systems will shorten deconfliction/coordination timelines, increase timely information sharing, and clarify blurred lines of authority.

Optimizing Timelines for National Security and Defense Budget and Appropriations: In the past 26 years, Congress and the President have agreed to a year-long budget only three times: 1989, 1995, and 1997.[13] The average length of a continuing resolution is around three months, and in the last several years, agencies' regular appropriations bills have

[13] Bingham, Amy. (23 September 2011). Continuing Resolutions: The New Norm? ABC News. https://abcnews.go.com/blogs/politics/2011/09/continuing-resolutions-the-new-norm/

not been enacted until the second quarter.[14] A new act should establish Congressional penalties for appropriations acts and bills that compel defense and national security agencies to minimally operate because of continuing resolutions. This includes, but is not exclusively limited to, the Department of Defense Appropriations Act. Defense and intelligence activities stall or shutter, critical programs are put on hold, and military investments come to a halt when departments have to operate under a continuing resolution. Communities of experts in government hemorrhage talent as technical, language, and military professionals flee government employment for greener, sometimes more stable, but often more lucrative pastures in industry.

[14] U.S. Government Accountability Office. Continuing Resolutions: Uncertainty Limited Management Options and Increased Workload in Selected Agencies. September 2009. https://www.gao.gov/assets/gao-09-879.pdf

Conclusion

Despite the ever-present specter of conflicts past, the United States has experienced extensive economic growth and secured its global leadership since the end of World War II. U.S. economic leadership has held the international economic order (mostly) together, through the ebbs and flows of economic expansion and recession. American technological advancements, innovation, and a nearly unconstrained approach to open public discourse have led the global community towards the bleeding edge of information technology. But while the National Security Act of 1947 set the stage for U.S. leadership of the international order in the post-World War II environment, the question remains whether the act still has the needed agility to respond to the threats that have emerged and the now wider spectrum of conflict that global powers have to contend with.

The volume and speed at which information travels–especially in societies that value sharing information like the United States–are unprecedented. **The global public has seen the myriad ways that information has been weaponized by adversaries, threatening and eroding people's ability to discern and scrutinize facts from falsehoods.** Efforts to weaken the very institutions and ideals that have shaped American global leadership are persistent, seemingly caving in from the inside at times. And while war, as an idea, hasn't changed much in the last 75 years, how wars will be fought has dramatically changed. **A new act needs to reflect these changes and needs to not only acknowledge the inherent risks of geopolitical upheaval but create a meaningful way to strategize and empower the U.S. national security apparatus to meet those challenges.**

Intelligence Project | Applied History Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
belfercenter.org/project/intelligence-project
belfercenter.org/project/applied-history-project

Printed in the United States of America