H-Diplo | Robert Jervis International Security Studies Forum

Policy Roundtable III-1

The Future of Intelligence: A Forum on the US Intelligence Community in Honor of Robert Jervis

10 September 2023 |PDF: https://issforum.org/to/jprIII-1 | Website: rjissf.org

Editor: Diane Labrosse | Commissioning Editor: Richard H. Immerman | Production Editor: Christopher Ball

Contents

© 2023 The Authors | CC BY-NC-ND 3.0 US

Introduction by Richard H. Immerman, Emeritus, Temple University

In January 2023, a year and a month after Robert Jervis passed away, the advisory board of the International Security Studies Forum (ISSF), under the aegis of Keren Yarhi-Milo, Arnold A. Saltzman Professor of War and Peace Studies and Dean of the School of International and Public Affairs at Columbia University, along with its senior managing editor, Diane Labrosse, and managing editor, Jennifer Erickson, renamed it the Robert Jervis International Security Studies Forum (RJISSF).[1] By attaching the already-legendary political scientist's name to this invaluable outlet for publishing scholarship on international relations, foreign policy, and the spectrum of related subfields and disciplines, the board not only paid tribute to Bob, but it also acknowledged what was well known to the readers of and contributors to both RJISSF and H-Diplo: No one was a more ardent believer in the potential of each of the forums and their partnership. Further, no one was more committed to the success of each of the forums and their partnership. Although a political scientist, Bob was as devoted to the Society for Historians of American Foreign Relations (SHAFR), *Diplomatic History*, and H-Diplo as any historian.[2] Yet he also appreciated the distinction between IR scholars and historians of US foreign relations.[3] He founded ISSF in 2009 with the purpose of bridging that gap by facilitating and even institutionalizing dialogues among the two, welcoming representatives from other disciplines in the humanities and social sciences as well.[4]

Over the next fourteen years, Jervis nurtured ISSF as a complement to H-Diplo. He contributed to it with astounding frequency, and he conceived of exciting projects with interdisciplinary appeal, to which he wrote many of the introductions. The marriage of H-Diplo and the now-named RJISSF is at its most elemental level a reflection of Bob Jervis: eclectic in its scope, encouraging of innovation and imagination, generous in its openness to new approaches and often junior scholars, never content with the conventional wisdom and forever in search of an original question to address, and always a platform for inclusive, civil debate and discourse. Its roundtables, its reviews, its essays, and its commentaries are read by hundreds of thousands of scholars and practitioners across the globe. It is the realization of Bob's vision.

While Bob's scholarship over his lengthy career was so wide-ranging as to defy characterization, he increasingly concentrated, albeit far from exclusively, the last twenty-five years on the study of intelligence. One can trace his interest to the late 1970s, when a temporary consultancy at the CIA led to his selection by his friend and former Harvard colleague, Robert Bowie, to prepare a postmortem on the agency's failure to anticipate and to provide the Carter administration with warning of the fall of the Shah.[5] Although that postmortem remained classified for decades, it served as a catalyst for Jervis's emergence in the twenty-first century as, in my judgment and that of many others, America's most respected scholar of US intelligence. His 2010 *The Failure of Intelligence*, which he based on his postmortem on the fall of the Shah and a similar

[1] Diane N. Labrosse and Jennifer Erickson, "The Robert Jervis International Security Forum," January 8, 2023, https://issforum.org/admin/the-robert-jervis-international-security-studies-forum.

[2] Excluding his numerous contributions to ISSF, Bob in combination published more than a dozen book reviews, articles, and commentaries in H-Diplo and *Diplomatic History*.

[3] Jack Levy, "Robert Jervis as a Social Science Methodologist," in *The Jervis Effect*, ed. Richard H. Immerman, Stacie Goddard, and Diane N. Labrosse (NY: Columbia University Press, forthcoming 2024).

[4] For a more detailed and extensive discussion of Bob's role in the origins and evolution of the RJISSF, see For a more detailed description of the origins of ISSF, see Diane N. Labrosse, "Bob Jervis and H-Diplo/ISSF," in Richard Immerman, Labrosse, and Marc Trachtenberg, eds., "H-Diplo | ISSF Tribute to the Life, Scholarship, and Legacy of Robert Jervis: Part I," 4 February 2022 | https://issforum.org/to/JervisTribute-1. A revision of this essay will be published in Immerman, Goddard, and Labrosse, *The Jervis Effect*.

[5] Robert Jervis, "How I Got Here," H-Diplo Essay Series on Learning the Scholar's Craft: Reflections of Historians and International Relations Scholars, March 4, 2020, https://networks.h-net.org/node/28443/discussions/5920317/h-diplo-essay-198-robert-jervis-learning-scholars-craft.

© 2023 The Authors | CC BY-NC-ND 3.0 US

retrospective analysis of the Intelligence Community's (IC's) faulty National Intelligence Estimate (NIE) and parallel judgments about President Saddam Hussein's alleged concealment of Weapons of Mass Destruction, is canonical.[6] A decade later he helped to organize, contributed an essay to, and guest-edited a special issue of *Intelligence and National Security* that unpacked the controversial 2007 NIE on Iran's nuclear program. He subsequently co-edited a volume composed of the articles and supplementary ones that Routledge published the year he passed away.[7] One could teach a course on intelligence and US foreign policy relying almost exclusively on Bob Jervis's scholarship, which the authors of the essays that follow cite frequently.

Jervis's audience was never limited to only scholars and students. Bowie invited Bob to write the postmortem on the fall of the Shah as a lessons-learned project for future intelligence analysts. He appreciated that Jervis's expertise in political psychology, most notably his application of psychological theories to explain perception and misperception in international relations, could be applied productively to intelligence analysis.[8] Jervis appreciated that as well. In addition to the intellectual stimulation that he derived from identifying the pathologies that pervaded the IC, he was committed to serving the national interest by exposing these pathologies so that analysts were at least aware of them. Hence he consulted, wrote other postmortems, and cultivated rich relationships within and throughout the IC. He aimed not to expose but to improve.[9]

It was therefore highly appropriate that senior managing editor Diane Labrosse proposed a forum on the contemporary state of the Intelligence Community to signal the synergy between Bob and H-Diplo| RJISSF. Diane's guidance was broad. She asked me to assemble experts who could contribute essays on the IC's current challenges and opportunities and their implications for today's and tomorrow's global affairs. I accepted without hesitation, confident that the connection between the name Robert Jervis and the salience of the topic would appeal to a cohort of distinguished scholars, practitioners, and combinations of both whom I thought of immediately. It did; all accepted my invitation. I gave each wide latitude, with the result that readers will be treated to historical and prescriptive essays that address different pieces of a complicated mosaic composed of old and new problems that the contemporary IC faces and its anticipated future requirements. Reflecting the complexity of that mosaic, there is less direct overlap among the essays than many of this forum's readers might have expected. Yet the extent to which they complement and are in dialogue with each other may prove equally counterintuitive. What will come as no surprise is that the essays are all informed and informative.

Dick Betts's intimate connection with intelligence studies and the IC dovetailed closely with those of Bob, his colleague at Columbia. His *Enemies of Intelligence*[10] sits next to the *Failure of Intelligence* at the center of my bookshelf, and he also served for decades as a valuable advisor to the US intelligence enterprise in a variety of capacities. Betts draws on both of these perspectives to provide what he calls "random impressions" of how the changes in intelligence capabilities and the global environment that have occurred and accelerated particularly since the end of the Cold War present the IC with new opportunities even as they continue to

---

[6] Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca, NY: Cornell University Press, 2010). See also Jervis, "Reports, Politics, and Intelligence Failures," *Journal of Strategic Studies* 29 (February 2006): 3-52

[7] "Anatomy of a Controversy: The 2007 Iran Nuclear NIE Revisited," Robert Jervis, Guest Editor, *Intelligence and National Security* 31 (March 2021); Jervis and James Wirtz, eds., *The 2007 Iran Nuclear Estimate Revisited: Anatomy of a Controversy* (Milton Park, UK: Routledge, 2022).

[8] Bowie told me this explicitly in a private conversation.

[9] Richard H. Immerman, "Robert Jervis: The Art and Science of the Post-Mortem;" Janice Gross Stein, "Political Psychology and the Analysis of Intelligence Failures: Robert Jervis in the Policy World:" and Michael Warner, "Robert Jervis and Official History," all in the forthcoming *The Jervis Effect*.

[10] Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (NY: Columbia University Press, 2007).

© 2023 The Authors | CC BY-NC-ND 3.0 US

pose traditional problems. His key examples include the requirement to conduct net assessments of a range of allies and adversaries; the continuing challenges of classification, overclassification, and balancing information-sharing with protecting sources and methods; and the IC's need to overcome the barriers to realizing the full potential of all-source intelligence. Betts leaves the reader hoping that intelligence analysis will matter more to policymakers in the future than it has in the past, but he cannot confidently forecast that this will be the case.

The focus of Sarah Jane-Corke, who ranks in the top tier of historians (in contrast to political scientists) who write about intelligence and who co-founded the North American Society for Intelligence History, is the establishment, evolution, and prospects of the US Director of National Intelligence (DNI), the juxtaposition of the DNI and the Director of the Central Intelligence Agency (DCIA, previously the Director of Central Intelligence, or DCI), and the salience of their relationship for the IC's future effectiveness. The proposal to create the DNI and an office to support it garnered little support and must resistance among the IC's senior leadership. Congress nevertheless included its establishment as integral to the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA), thereby all but preordaining bureaucratic competition between the DNI and the DCIA, who previously ruled over the IC and also served as the president's chief intelligence advisor. Corke provides a history of this competition, manifested initially with the tenures of John Negroponte and Peter Goss, to uncover the extent to which it infected ODNI's relationship with the CIA, and for that matter other elements of the IC as well. She observes much-needed improvement beginning with the succession of Michael McConnell and Michael Hayden, but seamless integration and collaboration remain works in progress.

One can make the argument, and I will make it, that no one brings to the study of US intelligence, and particularly the question of the IC's current state and future prospects, the profound expertise and insightful perspective that Thomas Fingar does (full disclosure: Tom was my boss when I worked at ODNI). A PhD in Political Science, he spent decades in the IC, rising to the head of the State Department's Bureau of Intelligence and Research (with the rank of Assistant Secretary of State) and Deputy Director of National Intelligence for Analysis. Since returning to academia, he has been remarkably prolific. Having played a central role in the IC reforms that followed the IRTPA legislation, the subject of one of his books,[11] Fingar writes in his essay about the IC's need to adapt to a new environment punctuated by information overload, especially but not exclusively that generated by Artificial Intelligence. This condition will require its interfacing with an array of non-governmental entities, its development of deeper and broader expertise, and its exploitation of new tools and techniques. But Fingar cautions against exaggerating the consequences of this brave new world. The core mission of the IC will not change, and machines can never replace analysts in terms of the analysis they produce and their relationships with the "customers" (whether policymakers, war-fighters, or law enforcers) they support. Fingers counsels that the effectiveness of the IC's support will depend on how well it strikes a balance between competition, integration, and collaboration.

The first holder of the Francis DeSerio Chair in Strategic and Theater Intelligence at the US Army War College after it was transformed into a full-time position, Genevieve Lester is likewise concerned with analysts and their customers, with an emphasis on the latter. She has spent much of her career educating senior military officers in the nuances of intelligence and how most effectively to exploit it. Her essay evolved from that perspective and her experiences. Prompted by the questions raised by Jervis and unwittingly engaging Fingar, Steve Marrin, and Amy Zegart in a conversation (none of the contributors knew the subjects of the others' essays), Lester unpacks the relationship between the producers and consumers of intelligence. She describes this relationship as historically "asymmetric," with primary responsibility, particularly for

[11] Thomas Fingar, *From Mandate to Blueprint: Lessons from Intelligence Reform* (Stanford, CA: Stanford University Press, 2021).

© 2023 The Authors | CC BY-NC-ND 3.0 US

failures, ascribed to the dominant partner: the producer. That needs to change, Lester argues, and it is changing. As is already evident in the Russo-Ukraine War, technological advances in collecting and communicating intelligence and the requisites of sometimes instantaneous decision making are dramatically altering this balance toward more equitable burden-sharing. She proposes a series of measures to prepare consumers better for this increased responsibility.

Steven Marrin, a former CIA analyst and the current editor of *Intelligence and National Security*, writes about the value and limits of strategic intelligence, a subject about which he is especially expert.[12] Like Betts, Marrin appreciates that intelligence plays a lesser role in policymakers' decisions than it should—and much of the public believes it does. Nevertheless, he argues that better intelligence does not necessarily produce better outcomes. A case in point is the suicide bombings that were integral to the 9/11 tragedy. The problem, he claims, paralleling Lester, lies more with policy than intelligence, or the nexus between them. Building on the recommendations of the 9/11 Commission, Marrin argues that for strategic intelligence most effectively to influence decision making, there must be a much tighter and more cohesive relationship between intelligence analysts and policymakers so that the intelligence produced by the analyst becomes the policy makers' knowledge.

For decades Amy Zegart has produced scholarship that exposed the deficiencies that have been baked into the IC's, most notably but not exclusively the CIA's, organizational structure since its inception.[13] The growth and evolution of the IC through the Cold War, the collapse of the Soviet Union, and the fall-out from 9/11 did not eliminate these deficiencies, and some even metastasized. As she writes in this essay, their legacy will affect how the United States confronts what she labels "two tectonic shifts": the rise of China and its resultant strategic rivalry with the United States, and the emergence and convergence of new technologies, especially but not limited to the connectivity produced by the Internet, the potential of Artificial Intelligence, and the capabilities of commercial satellites. The question she addresses is how the IC can adapt, and the answer, she makes clear, is not more money. Or at least it can't involve only more money. The IC's budget is insufficient, but increased appropriations will not inexorably translate into improved performance and greater effectiveness in safeguarding US interests in a world that the emerging technologies are revolutionizing in myriad ways. Indeed, agreeing with many of Fingar's claims, but not all of them, Zegart asserts that the convergence of these technologies confronts the IC with a "moment of reckoning." She is not pessimistic about the prospects for the IC's adapting to the new environment. Her prescription will, however, surprise many readers of this forum and probably generate pushback from many in the IC: the creation of an open-source intelligence agency.

If I were still teaching courses on intelligence and US foreign policy, I would make this forum required reading. Now retired, the best I can do is make it recommended reading for us all.

Contributors:

Richard H. Immerman is Professor and Edward Buthusiem Distinguished Faculty Fellow in History Emeritus and Emeritus Marvin Wachman Director of the Center for the Study of Force and Diplomacy at Temple University. He also served as an Assistant Deputy Director of National Intelligence and held the

[12] See, for example, Stephen Marrin, "Why Strategic Intelligence Has Limited Influence on American Foreign Policy," *Intelligence and National Security* 32 (September 2017): 725-742.

[13] Begin with Amy Zegart, *Flawed by Design: The Evolution of the CIA, the JCS, and the NSC* (Stanford, CA: Stanford University Press, 1999).

© 2023 The Authors | CC BY-NC-ND 3.0 US

Francis Deserio Chair in Strategic Intelligence at the US Army War College. A former SHAFR president and author of several books and articles on intelligence, he is currently a co-editor, along with Stacie Goddard and Diane Labrosse, of *The Jervis Effect*, and along with Susan Brewer and Doug Little, of *Thinking Otherwise: How Walter LaFeber Explained the History of US Foreign Relations*. Both are scheduled for publication in 2024, with Columbia University Press and Cornell University Press, respectively.

Richard K. Betts is the Leo A. Shifrin Professor Emeritus at Columbia University and formerly Director of Columbia's Saltzman Institute of War and Peace Studies, Senior Fellow at the Brookings Institution, and Director of National Security Studies at the Council on Foreign Relations. Among his books related to intelligence are *Surprise Attack* (Brookings Institution, 1982); *Soldiers, Statesmen, and Cold War Crises*, 2d edition (Columbia University Press, 1991); *Military Readiness* (Brookings Institution, 1995); *Enemies of Intelligence* (Columbia University Press, 2007); and *American Force* (Columbia University Press, 2012).

Sarah-Jane Corke, PhD, is the co-founder and past-president of the North American Society for Intelligence History (nasih). She is currently an associate professor of history at the University of New Brunswick. Her first book, *US Covert Operations and Cold War Strategy: Truman, the CIA and Secret Warfare*, was published by Routledge in 2008. Her second book, an edited collection with Mark Stout, *Adventures in Intelligence History: Stories from The International Spy Museum and Beyond* is under contract with the University Press of Kansas. Her third monograph, *The Nine Lives of Patricia and John Paton Davies* was awarded a Social Sciences and Humanities Research Council (sshrc) grant in 2022. She also plans to continue working on the history of the DNI.

Thomas Fingar is Shorenstein Asia-Pacific Research Center Fellow at Stanford University. Previous positions include Deputy Director of National Intelligence for Analysis, Chair of the National Intelligence Council, and Assistant Secretary of State for Intelligence and Research. His recent publications include *From Mandate to Blueprint: Lessons from Intelligence Reform* (Stanford University Press: 2021); *Fateful Decisions: Choices that will Shape China's Future,* co-editor with Jean C. Oi (Stanford: 2020); *Uneasy Partnerships: China and Japan, the Koreas, and Russia in the Era of Reform*, editor (Stanford: 2017); *The New Great Game: China and South and Central Asia in the Era of Reform*, editor (Stanford: 2016); and *Reducing Uncertainty: Intelligence Analysis and National Security* (Stanford: 2011).

Genevieve Lester is the De Serio Chair of Strategic Intelligence at the US Army War College. Her areas of interest are intelligence; accountability; leadership, and decisionmaking. She is also an Associate Fellow for Strategic Intelligence at the International Institute for Strategic Studies. She holds a PhD and MA in Political Science from the University of California, Berkeley, an MA in International Economics/International Law and Organizations from the Johns Hopkins University, School of Advanced International Studies, and a BA in history from Carleton College. She is the author of *When Should State Secrets Stay Secret? Accountability, Democratic Governance, and Intelligence* (Cambridge University Press, 2015) and numerous other publications on intelligence and related matters.

Stephen Marrin is the Director of the Intelligence Analysis Program and Professor in the School of Integrated Sciences at James Madison University. He is the editor of the journal *Intelligence and National Security* (Taylor & Francis), the premier scholarly journal in intelligence studies. Previously Dr. Marrin spent 10 years as the chair and program chair of the Intelligence Studies Section at the International Studies Association, as well as 3 years on the board of the International Association for Intelligence Education. He has also been on the advisory boards for a number of intelligence studies journals to include the *International Journal of Intelligence* and Counterintelligence. Dr. Marrin is a holder of a BA (political science) from Colgate University and MA and PhD degrees (foreign affairs) from the University of Virginia. He is the author of the book *Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice* (Routledge, 2011) as well as many articles on

© 2023 The Authors | CC BY-NC-ND 3.0 US

intelligence analysis. Before his academic career began he spent 5 years as an analyst at the Central Intelligence Agency (CIA) and the US Government Accountability Office (GAO).

Amy Zegart is the Morris Arnold and Nona Jean Cox Senior Fellow at the Hoover Institution, Senior Fellow at the Freeman Spogli Institute for International Studies, and Professor of Political Science by Courtesy at Stanford University. Her most recent book is *Spies, Lies, and Algorithms: The History and Future of American Intelligence* (Princeton University Press, 2022).

© 2023 The Authors | CC BY-NC-ND 3.0 US

"Reflections on Evolution of the Intelligence Community"
by Richard K. Betts, Columbia University

My research, and most of my experience as an intermittent participant-observer on the periphery of the intelligence community, spanned the Cold War and about 25 years after it. In all this I paralleled Bob Jervis to a fair extent. Not only was his office at Columbia a dozen steps from mine; we also crossed paths often in our advisory work in the Intelligence Community (IC), such as in a four-person post-mortem for George Tenet on the intelligence failure before the second war against Iraq.

My involvement with the IC began with work on the staff of the original Senate Intelligence Committee (the Church committee) and briefly on the NSC staff. I later served as an occasional consultant to the National Intelligence Council, a member of the National Security Advisory Panel for several Directors of Central Intelligence in the 1990s, commissioner of the National Commission on Terrorism, and briefly on the External Advisory Board for the Director of CIA. My access to the inside, however, attenuated rapidly in recent years. I have a sense of how much twenty-first century intelligence problems and activities have changed in fundamental ways given the information technology revolution and the new dependence of modern society on an infrastructure that did not exist in the Cold War (the internet), but I don't have a reliable sense of exactly how these changes manifest themselves in problems of institutional functioning. The following are a few random impressions of what old problems may recur and what new opportunities should be considered.

Economic and Military Net Assessment

Net assessment is the analysis of the balance of capabilities between competitors—which has what advantages and deficiencies compared to the other—as distinct from enumeration and analysis of the adversary's assets in themselves. When the question is which side is likely to come out on top in a crisis, war, or long-term rivalry, net assessment is the only analysis that matters. Yet most intelligence analysis is directed toward judging an adversary's capabilities in terms of absolute numbers and the qualities of its forces or resources rather than a relative balance of total capacity.

In a period of unipolarity and great power cooperation, net assessment was not a natural concern simply because no apparent threat seemed worth worrying about enough to focus attention on measuring its power against the US. After a long post-Cold War hiatus during which peacekeeping and then counterterrorism displaced the old preoccupation with great power politics, however, a new cold war of sorts, or at least the return of dangerous conflict between great powers, has emerged. The crucially new aspect of the new cold war is the economic entanglement of the contestants with each other, and its effect on military capabilities and options. In the old Cold War, the Communist states were more or less isolated from the West economically. Today globalization, the delicacy of supply chains, and the interdependence of US, Chinese, European, Russian, and other producers and consumers is dramatically greater, despite the recent trend of attempting to reverse or mitigate their effects on national security.

At present the effects of this economic and technological entanglement on the Ukraine War and the Taiwan issue are starkly evident but not definitively assessed. An important challenge for the IC, therefore, in collaboration with outside sources of expertise, is to do a net assessment of present and potential vulnerabilities of the US, European Union, Japan, China, and Russia to economic leverage from their adversaries, and vice versa: how much leverage, in what forms, do they have against each other? Such net assessment needs to be done at two levels.

© 2023 The Authors | CC BY-NC-ND 3.0 US

The first level is the current conflict between the West and Russia over Ukraine. How potent and over what time span will western economic sanctions on Moscow be, in light of plausible counterstrategies and workarounds, and vice versa—how much will Russian energy supplies give Moscow leverage or not as time passes and how will the answers affect trends in the capability of fielded forces in Ukraine? The second level of net assessment is a more comprehensive survey of the balances of vulnerability and leverage of the West and other groupings in the world as a whole. Perhaps one or both sorts of exercises have already been done or planned, but past practice suggests that it would be no surprise if demand for current and tactical intelligence has driven out attention to longer-term strategic intelligence.

Among the potential obstacles to such net assessment, two from the past stand out. One is the general norm that constrained net assessment by the IC in the past: American intelligence in general is not supposed to assess American capabilities or intentions or to recommend policy. Net assessment by its nature will imply certain policy choices to remedy deficiencies revealed by the assessment. This inhibiting norm has sometimes been bent or overlooked in the past but can be summoned by any player who is worried about how an attempt at net assessment might challenge the player's policy preference. This points to the second obstacle: the usual opposition of the US military to civilian agencies rendering judgments on military capability.

During the old Cold War, episodic military success in keeping civilian analysts in their ostensibly proper lanes, suppressing assessment of how adversary forces stacked up against those of the US, contributed to strategic surprises. Secretary of Defense Robert McNamara came to distrust his own Defense Intelligence Agency (DIA) and the services' intelligence units had to ask CIA for independent assessments. His skepticism was not typical of secretaries of defense. Overemphasis on static bean-counts of material inputs and underemphasis of subjective or hard-to-measure factors like training or tactical doctrine contributed to a pattern of overestimation of Iraqi capability before the 1991 war and Russian capability before the 2023 war, as well as underestimation of Ukrainian capability in the latter case.

I am not up to date on whether or how net assessment of either economic leverage or military capabilities has been done in recent years. The norm against policy recommendations from intelligence personnel, the proper strategic caution and budgetary interests of operating departments, and especially the methodological complexity and ambiguity of evidence in the practice of rigorous net assessment all naturally inhibit trenchant analysis of relative capabilities. This presents a problem to be managed, however, not an excuse for overlooking the fact that in international competition "capability" really has *no meaning* apart from net assessment.

The Classification Tradeoff

There is close to a consensus that overclassification is a serious problem, yet no compelling solution has been proposed. The main barrier is that given the apparent imbalance in risks of over- and under-classification, that is, risks to the personal careers of functionaries deciding on classification as well as risks to national security, uncertainty about an item's status naturally makes secrecy the default option. The irony is that the sheer volume of data in the system probably bears some responsibility for disasters inflicted by the [Edward] Snowdens, [Chelsea] Mannings, [Reality] Winners, and [Jack] Texeiras of the intelligence world. If real top secrets consisted of a few hundred items, would a system so complex as to require tens of thousands of people with Top Secret clearances, let alone several million with other clearances, be necessary?

There seems to be a wider and stronger interest than there used to be within the system in finding a way to grapple with the problem. There is also refreshing evidence of awareness of policy benefits in overriding the risks of revealing intelligence: the active American publicity over the course of several months of Russian preparations to invade Ukraine and the subsequent revelation of Russian plans for false flag operations and of Chinese leadership discussions of potential military aid to Moscow, both of which were probably undercut by

© 2023 The Authors | CC BY-NC-ND 3.0 US

the revelations. These policy decisions conquered the pervasive goal displacement that infects all bureaucracies, reminding us that the purpose of intelligence is to improve policy action, not to protect secrecy for its own sake.

The fact remains nevertheless that revealing secrets risks danger to sources and methods that cannot be discounted. Simply changing the default option to non-classification is no solution, since the volume and complexity of data would produce an accidental scandal in no time. Refinement of ideas and norms for managing the tradeoff should remain a management priority now that the tradeoff seems to be recognized as one where the crucial costs do not necessarily lie only on one side of it. Threading the needle between "need to know" and "responsibility to provide" is a daunting task.[1] The refinement probably requires investment in more institutionalized formal checks and balances in the system in order to generate regular challenges to classification that have to be refuted by specific rather than vague assertions of exactly how declassification of the item in question would create genuinely plausible danger. In any case, the solution has to involve concrete mechanisms beyond exhortation, and some sort of penalties for cases of unjustified classification that are egregious.

Comparative Advantage

For a long time the IC has been prodded to take an expansive view of information that is relevant to national security, especially in the realm of economic and environmental policies. Since the turn of the century, moreover, the profusion and increased accessibility of non-secret information of all sorts has highlighted the salience of "open source" intelligence (OSINT, in the inevitable bureaucratic term of art). This generated some debate about how much the system's priorities should be reoriented to exploiting non-secret information.

In economic terms, comparative advantage means that normally a country should not produce what it can get from another country that produces it more efficiently. The intelligence system's comparative advantage in the open marketplace of information and ideas in a democratic society is in collection and analysis of facts that adversaries or allies are trying to keep secret. Stealing and assessing secrets should remain the first priority of American intelligence; analysis that can be done without access to secrets is not the IC's comparative advantage. Priority for secrets, however, does not by any means imply that other sources should be neglected. The sense that proper exploitation of open source intelligence degrades concern for secrets has been a feature of debate about organization but is utterly illogical. The two are complementary, not competitive. No issue of importance in modern society can be handled responsibly without integrating all available knowledge, most of which, on most issues, is not secret.

While secrets are the comparative advantage of government intelligence, the equally important responsibility of the IC is what I have in the past called the "library function,"[2] providing a place where analysts or policymakers can go to get all of the information that is relevant to a problem. Should this place be an autonomous agency as periodically proposed? The rationale for that option seems to be that professional culture will prevent sincere attention to OSINT if the mission remains situated in agencies that are attuned to secrets.

[1] On the tension between "need to know" and "responsibility to provide," see the Office of the Director of National Intelligence, Intelligence Community Policy Memorandum (ICPM) 2007-200-2, "Preparing Intelligence to Meet the Intelligence Community's "Responsibility to Provide," December 11, 2007, https://www.dni.gov/files/documents/ICD/ICD_501.pdf.

[2] Richard K. Betts, *Enemies of Intelligence* (New York: Columbia University Press, 2007), 5-6.

© 2023 The Authors | CC BY-NC-ND 3.0 US

An autonomous agency that is tasked with monitoring, packaging, or providing any relevant publicly available information on foreign affairs, however, will inevitably grow to gargantuan size given the virtually limitless proportions of open information. Housing the function outside the regular intelligence agencies could also give an excuse to the regular agencies to focus even more exclusively on secrets. However it is organized, whether outside or only inside the regular agencies, the library function should approximate just that—a place for collection planners and analysts to go for background and supplementary data to ensure that their work is comprehensive. In any case, if OSINT has its own agency it must not be used as a reason to reduce the organization for the function that exists within the regular agencies. The natural tendency to preserve redundancy might prevent such reduction but the natural managerial tendency to economize and consolidate would push in the wrong direction.

Conclusion

The suggestions mentioned above, for reemphasizing and refining net assessment, institutionalizing mechanisms to counter overclassification, and facilitating integration of open and secret knowledge, imply adding in one way or another to the organizational size and complexity of what is already a colossal IC. Yet the size of the IC is both a source of some dysfunctions as well as of great strength. The data are complex and not all public, but it seems clear that the rate of spending and the aggregate number of personnel in the IC have increased significantly in real terms from what they were at the height of the old Cold War, and that they did so before the recent return of great power conflict.

Critics see this as bureaucratic bloat, but I suspect it more or less reflects the information technology revolution which has exponentially increased the amount of data available and the means for collecting it. Even so, intuitively the size is a problem. Almost all of the hugeness can probably be attributed to the scope of the technical collection process, which also encouraged the personnel practices (such as access by Snowden et al.) that produced disasters. How can complexity be better managed without reducing size and thereby increasing risks of losing important things along the way? The answer is not obvious. Improving analysis is problematic for many reasons, but not because the corps of analysts is big enough to make much difference in IC personnel totals. In fact a huge amount has been done since the old Cold War to upgrade and refine the training of analysts, to examine and alert them to the psychological, cognitive barriers to objectivity, and to give them a sense of how to write in a way that will make their assessments relevant to policymakers. Has this made a detectable difference in the success rate, in terms of accuracy, forecasting, and influence, of intelligence analysis? I have no idea how one would try to measure results in order to answer the question, but for people like those who would read this symposium, it's the question that matters.

How often and when does IC analysis affect decisions and implementation in the policy realm? In other words, when does it matter? In principle, analysis is the funnel through which most of the vast intelligence apparatus passes its work to the point where it can affect tactics, operations, strategy, and policy. Yet high policymakers in the past were often impatient with or uninterested in IC analytical products. I do not have a sense of how much this may have changed in recent times, since the greater inward-looking attention to analytical tradecraft, at least in the CIA. How much analysis actually matters is a question Bob Jervis would have been happy to explore if he had had had more time.

© 2023 The Authors | CC BY-NC-ND 3.0 US

"Navigating the Personal and the Political in the Post-IRTPA World: A History of America's First DNI/DCIA"

by Sarah-Jane Corke, University of New Brunswick

In the fall of 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act (IRTPA).[1] It was the most significant piece of intelligence legislation in sixty years.[2] The most notable and certainly the most controversial change was the creation of a Director of National Intelligence (DNI), whose job it was to oversee the American Intelligence Community (IC) in the post-9/11 world. The act charged the DNI with four responsibilities: to serve as the principal advisor to the president on all intelligence matters; to ensure that the IC worked "as a single unified enterprise," to establish common standards for intelligence community personnel, and to oversee the budgetary process.[3] Although the DNI would eventually have "authority" over 18 different intelligence agencies and organizations, including the Office of the Director of National Intelligence (ODNI), critical to their success—according to General Michael Hayden, who served as both the DNI's Principal Deputy and the Director of the Central Intelligence Agency (DCIA) during the George W. Bush administration—"was a series of intangibles" which included "the DNI's political deftness, the DNI's closeness to the President, and the DNI's relationship to the CIA director."[4] For Hayden, the personal dynamic between the DNI, and the newly created DCIA was critical. As he put it in his memoirs, "get CIA right…and everything will be ok. Get it wrong and the rest won't matter."[5] He also later acknowledged, however, that "even in the best of times," this relationship would be "a challenging one."[6]

Although America's first DNI, John Negroponte (21 April 2005 –13 February 2007) and the first DCIA, Porter J. Goss, (21 April 2005–5 May 2006) knew each other "very well,"[7] Negroponte's position effectively meant that Goss was "demoted" from Director of Central Intelligence (DCI) to DCIA.[8] As a result, he was no longer President George W. Bush's primary intelligence advisor; and in Washington D.C. access was, and is, everything. Thus, despite their ties, which were forged at Yale University, navigating the personal and political was not easy for either man. The situation became fraught because the creation of the DNI "signaled the end of the CIA's nearly 60-year run as the undisputed center for power and influence in the secret world

[1] I would like to thank all of those who offered comments on a first draft of this paper. Some I can acknowledge publicly, others I cannot. In alphabetical order I am deeply indebted to Diana Bolsinger, Sara Castro, Michael Miner, Richard Immerman, David Priess, and Michael Warner for their substantive engagement with my work. I also want to acknowledge the exceptional research assistance provided by Bradley Garlie and Susan Parker, two graduate students at the University of New Brunswick. Their work was financed through Social Sciences and Humanities Research Council and the Department of History at the University of New Brunswick. I also want to express my gratitude to General Michael Hayden and his wife Jeanine Hayden, who took the time to sit down with me, twice, to discuss his experiences. Finally, a big thanks to David Priess for encouraging General Hayden to talk to me.

[2] For an excellent discussion of the passage of IRTPA see, Michael Allen, *Blinking Red: Crisis and Compromise in American Intelligence After 9/11*, (Washington DC: Potomac Books, 2016); Also indispensable is Richard A. Best, "Leadership of the US Intelligence Community: From DCI to DNI*," International Journal of Intelligence and Counterintelligence,* 27:2 (Summer 2014): 253-333.

[3] George W. Bush Transcript, "Bush Appoints a Director of National Intelligence," *New York Times*, February 17, 2005.

[4] Testimony of Michael V. Hayden, "Ten Years After 9/11: Is Intelligence Reform Working?" Part I. US Senate. https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/TestimonyHayden20110512.pdf

[5] Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror,* (New York: Penguin Press, 2016), 167.

[6] Testimony of Michael V. Hayden, "Ten Years After 9/11".

[7] "Interview with John Negroponte" September 14, 2012. George W. Bush Oral History Project, Miller Center, University of Virginia, 61.

[8] Hayden, *Paying to the Edge*, 169.

© 2023 The Authors | CC BY-NC-ND 3.0 US

of intelligence."[9] These changes, notwithstanding the wording of the legislation, did not immediately reflect the bureaucratic loyalties of the men and women whose lives were affected.

Even more crucially, the timing of the IC leadership transition could not have been worse. It coincided with one of the most challenging periods in the Agency's history, during which the CIA had to grapple with the task of rebuilding its "bruised credibility" and "tarnished reputation."[10] These challenges resulted from a series of intelligence failures, notably the failure to foresee the 9/11 attacks and the debacle over its estimates of Iraq's concealment of weapons of mass destruction (WMD). Not surprisingly, the bureaucratic shift to ODNI, coming when it did, left many in the Agency angry and upset.[11] The result, according to Hayden was, significant and "destructive pushback from Langley."[12] Unable to resolve the situation in a timely fashion, and with encouragement from a number of senior government officials, including both President Bush and his father, former President George Herbert Walker Bush—who had served as DCI under Gerald Ford but continued to keep a close eye on what was happening at Langley—Negroponte told Goss that he must resign.[13] However, as he later acknowledged, this was one of the most "personally wrenching"[14] moments in his career.

What happened? Because IRTPA did not clearly delineate the lines of authority between the DNI and the DCIA, the lack of legislative clarity ensured that a new relationship would need to be negotiated between the two directors. For that reason, we cannot understand the first years of the ODNI without first grappling with the personal and political characteristics of the individuals involved. In this case, and to different degrees, neither Negroponte nor Goss exhibited the "political deftness" that Hayden alluded to above. Each

[9] Dafna Linzer, "Goss, 8 Ex-Chiefs of CIA Mark Old Post's Passing" *Washington Post*, August 17, 2005.

[10] Nomination of the Honorable Porter J. Goss to be the Director of Central Intelligence, Hearings before the Select Committee on Intelligence of the United States, 108th Congress, Second Session, September 14 and 20, 2004. https://www.govinfo.gov/content/pkg/CHRG-108shrg96698/pdf/CHRG-108shrg96698.pdf. 3.

[11] One of my primary concerns in writing this paper is that the voices of those who worked at the Agency are not heard. Many felt constrained from speaking publicly about their experiences. As a result, I have not been able to fully share their views on how they believed the new ODNI would impact their work. For example, some analysts had serious misgivings about what the ODNI would mean for independent intelligence analysis. Those involved in operations, who faced life and death situations throughout their careers, were anxious about who would control their destinies; whether having a new agency involved in human intelligence (HUMINT) would get people killed or harm American national security. Others believed that different government departments simply did not have the experience with intelligence "tradecraft" that those in the agency did. Many recruits, for example, spent months in training exercises that were designed to teach them how to do their jobs effectively. Yet there is very little in the public record for me to draw on to support of their views. As a result, their very real concerns, which help explain their hostility to the DNI, remain invisible. It is my hope that as the history of this period continues to be written, more people will feel comfortable talking about their experiences. For this to happen, however, the CIA needs to realize there is a difference between classified information and the day-to-day lived experiences of those who take on these very difficult jobs. They need to open a space for these people to talk about these experiences. It should be possible to write what Christopher Moran and Andrew Hammond have termed, the "social history of intelligence," without upsetting the apple cart. See Christopher Richard Moran and Andrew Hammond, "Bringing the 'social' in from the cold: towards a social history of American Intelligence," *Cambridge Review of International Affairs,* 34, 5 (September 20, 2021): 616-636.

[12] Michael V. Hayden, Interview, George W. Bush Oral History Project, Miller Center, University of Virginia, November 20, 2012, 17. See also: Richard Immerman, *The Hidden Hand: A Brief History of the CIA*, (United Kingdom: Wiley Blackwell, 2014), 196.

[13] According to Hayden, three or four months before Goss resigned, Negroponte told him that he wanted him to go to the CIA. Hayden replied he was happy at ODNI and the matter was dropped until early May when Negroponte informed Hayden that the President wanted to speak to him about "changes at the CIA." Interview with Michael V. Hayden, Zoom, Friday, July 7, 2023, 2:00 PM Eastern. See also Hayden, *Playing to the Edge*, 179.

[14] George W. Liebmann, *The Last American Diplomat: John D. Negroponte and the Changing Face of US Diplomacy,* (New York: I.B. Tauris, 2012) 285.

© 2023 The Authors | CC BY-NC-ND 3.0 US

man came to their position with a carefully defined persona that they refused to change, even when it became clear that the needs of the IC called for a different approach. For his part, Negroponte came to the ODNI after having carefully cultivated an image of a conservative, albeit, pragmatic, diplomat.[15] He was a "realist" who was skeptical of the "Wilsonian" rhetoric emanating from the White House. Moreover, he was not interested in partisan politics.[16] He tended to approach difficult questions with "quiet negotiation" and "unfailing courtesy."[17] His senior staff was also made up of "strong leaders with solid credentials."[18]

In contrast, Goss re-entered the CIA as an aggressive, partisan warrior determined to change the agency's operational and analytical culture.[19] Second, his in-your-face leadership vision was somewhat at odds with his operational style. According to Negroponte, although Goss enjoyed "breaking the China,"[20] the DCIA tended to avoid direct conflict and instead allowed his team—the majority of whom were former Congressional staffers—to run his office, as they saw fit. Unfortunately, they developed a very poor reputation within the Agency.[21] Thus, the evidence suggests that Negroponte and Goss were philosophically and temperamentally, at odds. They also had very different management styles. The result was a chaotic mishmash of the personal and the political, which alienated not only much of Goss's workforce, but key players in the Bush Administration, as well. In the end, the situation became too difficult for Negroponte to manage and after a little more than a year, on 5 May 2006, Goss was replaced by Hayden.[22] For his part, Negroponte remained DNI for another nine months until he was replaced by Michael McConnell. This change of personnel was a necessary first step in forging a relationship between the DNI and DCIA, and the ODNI and CIA, on which the IC's future effectiveness depends.

Arguably, always arguably, this story begins almost seven months to the day before Negroponte assumed the office of DNI, as it was in September of 2004 that Goss became the 19th, and final, DCI. As John D. Rockefeller IV, the vice chairman of the Senate's Select Committee on Intelligence, noted during Goss's confirmation hearings, the next director "will be the most important ever confirmed by the United States Senate." He went on to add, "[n]ever before in the 57-year history of the intelligence community has there been a need for a DCI with unimpeachable character, proven leadership and management experience, and a strong national security set of credentials."[23] Rockefeller was right on all accounts. However, the timing of Goss's appointment was equally important as it came two months before one of "the most bitter presidential

---

[15] The only biography of Negroponte is titled, *The Last American Diplomat*. However, when relying on this as a primary source one should approach it with caution. According to Negroponte, his biographer "could have done a better job." See: "Interview with John Negroponte" Miller Center, September 14, 2012, 8.

[16] "Ambassador John D. Negroponte," Interviewed by Charles Stuart Kennedy, 2000-2009. Foreign Affairs Oral History Project, The Association for Diplomatic Studies and Training (ADST). 95; and Interview with John Negroponte, the Miller Center, September 14, 2012.

[17] Scott Shane, "Poker-Faced Diplomat, Negroponte is Poised for role as Spy Chief, *New York Times*, March 29, 2005.

[18] Pat Neary, "Intelligence Reform 2001-2009: Requiescat in Pace," *Studies in Intelligence*, 54:1 (March 2010): 5.

[19] David Ignatius, "The CIA at Rock Bottom," *Washington Post*, May 7, 2006; See also Dana Linzer and Walter Pincus, "Goss Forced Out as CIA Director: Gen Hayden is Likely Successor," *Washington Post*, May 6, 2005.

[20] John Negroponte interview by Kennedy, February 11, 2000.

[21] For a good discussion of the problems with Goss's management style, see Siobhan Gorman, "I Spy Mismanagement," *Government Executive*, November 24, 2004. https://www.govexec.com/management/2004/11/i-spy-mismanagement/1808/

[22] According to Hayden his appointment to DCI was the first and only time that the DNI was able to choose who filled the role. Testimony of Michael V. Hayden, Senate Testimony, "Ten Years After 9/11."

[23] Nomination of the Honorable Porter J. Goss to be the Director of Central Intelligence, Hearings before the Select Committee on Intelligence of the United States, 108th Congress, Second Session, September 14 and 20, 2004. https://www.govinfo.gov/content/pkg/CHRG-108shrg96698/pdf/CHRG-108shrg96698.pdf. 3.

© 2023 The Authors | CC BY-NC-ND 3.0 US

campaigns in modern history,"[24] which pitted George W. Bush against his Democratic challenger John Kerry. The polls were close. If Kerry won, Goss's tenure would be a short one.

Goss also assumed his position at a time when the United States faced a series of international challenges that included an ongoing threat from al-Qaeda and burgeoning wars in Iraq and Afghanistan. What's more, he was replacing George Tenet, who over his long tenure had developed a good working relationship with agency employees, Congress, and more importantly, the president of the United States.[25] Finally, the House and the Senate were poised to pass legislation that would forever alter the role of the DCI. As a result, Goss's duties remained undefined.

Further raising the stakes, Goss's appointment was controversial. On the one hand, he brought a degree of experience to the job. He had joined the CIA in the early 1960s after being recruited during his junior year at Yale University. Although he went on to work for the Directorate of Plans—recruiting and running agents—until 1972, he quit the agency at age thirty-four after he was found unconscious in a hotel room in Washington D.C., suffering from "systemic blood poisoning."[26] Independently wealthy, he moved his family to Florida and together with two former CIA colleagues started an Island Boat Rental Company. The lifestyle suited Goss, who would later become known for his casual and "low-key" *modus operandi*.[27]

In 1972, the three men founded *The Island Reporter*, a newspaper which they ran successfully for several years. Two years later, in 1974, Goss ran for Mayor of Sanibel. After spending over a decade and a half in local politics in 1988 he moved to Washington and the House of Representatives, where he spent the next sixteen years. His tenure culminated in his appointment as the Chair of the House Permanent Select Committee on Intelligence (HPSCI) where he served from 1997 to 2004. There he was recognized as both a defender and a sometimes critic of the CIA. For example, during the Clinton Presidency he defended both the CIA and its budget. Under President George W. Bush he refused to blame the 9/11 attacks on intelligence failures, and he did not take up the Weapons of Mass Destruction (WMD) controversy. He also avoided investigating the prisoner-abuse scandal at Abu Gharib. According to journalist Robert Dreyfuss, as chairman of the Committee, Goss preferred "partnerships to oversight."[28] In the summer of 2004, however, Goss oversaw a House report that "blasted" the CIA's Directorate of Operations and argued the agency was "so badly managed it risked becoming 'a stilted bureaucracy incapable of even the slightest bit of success.'" If they continued down the road they are on, the report concluded, they will go over "a proverbial cliff."[29] Despite

---

[24] John McLaughlin, "The New Intelligence Challenge," *Washington Post,* January 7, 2007.

[25] Although Tenet's relationship with many of Bush's advisors had apparently soured by the time he resigned, his relationship with Bush was still solid, and marked by a shared love of sports and "male talk." Elisabeth Bumiller and Douglas Jehl, "Resignation from the CIA: Intelligence; Tenet Resigns as CIA Director; 3 House Reports on Agency Due," *New York Times*, June 4, 2004.

[26] There remains some disagreement over where he served while at the agency. *The Washington Post* has him in the Middle East, Central Europe, South America, and Africa. *The New York Times* has him posted in Latin America, the Caribbean and Europe. Goss said he served in Haiti, Santo Domingo, and Mexico. See Laura Blumenfeld, "Goss Hailed as Old Pro," *Washington Post*, September 13, 2004. Elisabeth Bumiller and Douglas Jehl, "Resignation from the CIA: Intelligence; Tenet Resigns as CIA Director; 3 Reports on Agency Due," *New York Times*, June 4, 2004; Richard Leiby, "A Cloak but no Dagger," *Washington Post*, May 18, 2002.

[27] Blumenfeld, "Goss Hailed as Old Pro".

[28] Robert Dreyfuss, "The Yes-Man" *The American Prospect,* May 8, 2006; https://web.archive.org/web/20080511235246/http://www.prospect.org/cs/articles?article=the_yesman;.

[29] Frank Davies, "Goss has been a Defender, Critic of CIA," *The Ledger,* August 11, 2004. https://www.theledger.com/story/news/2004/08/11/goss-has-been-a-defender-critic-of-cia/26127221007/

© 2023 The Authors | CC BY-NC-ND 3.0 US

the harsh rhetoric, however, many at the time saw it, "as a careful calculation" on Goss's part, to demonstrate to the White House, his commitment "to reforming the agency."[30]

During his service on the HPSCI Goss also developed a reputation as a partisan warrior. He maintained a close working relationship with Vice President Dick Cheney and the 50th Speaker of the US House of Representatives, Newt Gingrich, who until a few years ago, would have been considered one of the most partisan figures in American political history. [31] As a result, Goss spent the last few years doing his part to ensure that Bush's agenda was not compromised. Most damning, Goss refused to open a hearing after CIA officer Valerie Plame's name was leaked to the press. At the time he stated, "somebody sends me a blue dress and some DNA, I'll have an investigation."[32] Despite his warrior status, however, Goss was also known for his somewhat lackadaisical approach to his job.[33] Hayden puts it best: He was "a hands-off manager."[34] He loved nothing more than to spend time at his 575-acre organic farm in Orange Country, Virginia, where he raised "miniature donkeys and conservancy chickens that laid pale green eggs."[35] When he was absent from Washington, he tended to allow his staff to run the show.

Although Democrats voiced their concerns about his appointment, for all the reasons mentioned above, he was eventually confirmed, possibly because many of those who voted for him were convinced that he would not have the job for more than a few months.[36] They were wrong. On 2 November 2004, George W. Bush was re-elected to a second term. By this point, Goss had been the director of the CIA for a little over a month and the agency was at a crossroads. Even as its workforce struggled to revive its morale following the 11 September 2001 attacks on New York and the Pentagon that were ordered by al-Qaeda leader Osama bin Laden, they faced an additional challenge as senior policymakers in the Bush administration ramped up, in the words of Negroponte, their "fascination, if not obsession with Iraq."[37]

The scholarly debate over the degree of the politicization of intelligence in the build-up to the war in Iraq is contentious even today.[38] As an example, foremost scholars in the field of intelligence history disagree over the degree to which the intelligence was politicized. [39] These debates, in some ways, mirror the positions taken

---

[30] "The Guardian Profile: Porter Goss," *The Guardian*, August 13, 2004. https://www.theguardian.com/world/2004/aug/13/usa.suzannegoldenberg

[31] On Goss and Gingrich see Sidney Blumenthal, "The Ruin of the CIA," *Open Democracy*, May 16, 2006. https://www.opendemocracy.net/en/cia_ruin_3554jsp/

[32] Laura Blumenfeld, "Goss Hailed as Old Pro".

[33] David Ignatius, "Danger Point in Spy Reform," *Washington Post,* October 21, 2005.

[34] Michael V. Hayden, Interview, Miller Center, November 20, 2012, 22.

[35] Laura Blumenfeld, "Goss Hailed as Old Pro".

[36] Historian Richard Immerman argues that at this point neither party wanted "to face off over intelligence." see Richard Immerman, *The Hidden Hand: A Brief History of the CIA*, (Malden, MA: Wiley Blackwell, 2014), 191.

[37] John Negroponte, Interview, Miller Center, September 14, 2012. 15.

[38] The literature on this topic is voluminous. In chronological order see as examples: Robert Jervis, "Reports, Politics and Intelligence Failures: The Case of Iraq," *Journal of Strategic Studies*, 29:1(2006): 3-52; Richard K. Betts, "Two Faces of Intelligence Failure: September 11 and Iraq's Missing WMD," *Political Science Quarterly*, 122:4(Winter, 2007/2008): 585-606; Scott Lucas, "Recognizing Politicisation: The CIA and the Path to the 2003 War in Iraq," *Intelligence and National Security*, 26: 2-3(2011): 203-227; Glenn Hastedt, "The Politics of Intelligence and the Politicization of Intelligence," *Intelligence and National Security*, 28:2(2013): 5-31; Richard Immerman, "Intelligence and the Iraq and Afghanistan Wars," *Political Science Quarterly*, 131:3(Fall 2016): 477-501l; and Giovanni Coletta, "Politicising Intelligence: What went wrong with the UK and US assessments on Iraqi WMD in 2002*," Journal of Intelligence History,* 17:1(2018): 65-78.

[39] The debates have Richard Immerman and Robert Jervis on one side and Rhodri Jeffreys-Jones and Joshua Rovner on the other. See Immerman, *The Hidden Hand*, 178-179, 195-196; Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca: Cornell University Press, 2010), 124, 127, 131-136; Rhodri Jeffreys-Jones,

© 2023 The Authors | CC BY-NC-ND 3.0 US

by those in the IC. Although there were some, like Hayden, who argue that it was "an urban legend,"[40] and others, like, Negroponte who saw the whole thing as "a comedy of errors,"[41] within the CIA, some of the analysts involved felt "pressured" and "pushed beyond the evidence that they had" to come up with the conclusions that would support the President's agenda.[42] What is indisputable is that enough intelligence analysts expressed their unhappiness with the direction that the administration was going that their voices made their way into the public square. According to journalist Robert Dreyfuss, "the dissent within the agency, and the anger about being manipulated, were palatable by 2004."[43] The result was a series of leaks.[44] This led some conservative commentators, like Robert Novak, to suggest that Bush and the CIA [were] "at war with each other."[45] Not surprisingly then, on assuming the directorship, Goss hit the CIA "like a wrecking ball."[46]

As *Washington Post* journalist Dana Priest aptly pointed out at the time, "transitions between CIA directors are often unsettling for career officials."[47] Goss's arrival was particularly difficult, however, not only because of his worldview and management style, but also because of his determination to overhaul the Directorate of Operations "from beginning to end."[48] To do so he elevated senior officials who were sympathetic to his vision. As he pushed for a series of reforms, he also turned to the management team he had brought with him from the House of Representatives. In addition to the politics at play, the personalities of all involved is key to understanding the events that unfolded. These men, and they were all men, "were known for their abrasive management style and for their criticism of the clandestine services." Three were "former mid-level CIA officials who had left the agency disgruntled."[49] The fourth, Patrick Murray, had served as Goss's chief of staff on the HPSCI, and was also known to be "highly partisan."[50] As Michael Scheuer, the former head of

---

CIA: A Question of Standing: The History of the CIA (London: Oxford University Press, 2022), 155 and Joshua Rovner, *Fixing the Facts: National Security and the Politics of Intelligence*, (Ithaca: Cornell University Press, 2011), 17, 138-139, 142, 149-157.

[40] Hayden argued that he "never experienced such pressure, and when he got to the CIA and talked to those more directly involved, they reported that they felt no pressure either." He believes the agency "just got [the WMD estimate] wrong." Hayden, *Playing to the Edge*, 50. His conclusions were supported by the *Unclassified Version of the Report on the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, which argued the IC "simply did not do the job it exists to do" and as a result there were "failures at all stages of the intelligence process." *Unclassified Version of the Report on the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction,* March 31, 2005, 47; https://www.govinfo.gov/app/details/GPO-WMD/context. I would like to thank David Priess for sending me the link to this document.

[41] Negroponte, Interview by Kennedy, February 11, 2000, 202.

[42] Richard Kerr in Dreyfuss, "The Yes-Man"; See also Paul R. Pillar, "Intelligence, Policy and War in Iraq," *Foreign Affairs,* 85:2(March-April 2006): 15-27.

[43] Dreyfuss, "The Yes-Man".

[44] On the leaks themselves see Neary, 7 (footnote 15).

[45] Robert Novak, in Dreyfuss, "The Yes-Man"; See also: Sidney Blumenthal, "The Ruin of the CIA."

[46] Dreyfuss, "The Yes-Man". In as much as Goss alienated several senior employees, it is also important to note he also did his part to protect agency personnel from additional criticism. After the release of the report by CIA Inspector General John. L. Helgerson, on 9/11, that "severely criticized senior officers" he announced that the report would remain classified, and no agency officers would be reprimanded. As journalists Dafna Linzer and Walter Pincus pointed out, had they taken a different track this would have further pitted the new director against his workforce. See Dafna Linzer and Walter Pincus, "CIA Rejects Discipline for 9/11 Failures: Goss Cites Fear of Hurting Agency," *Washington Post,* October 6, 2005.

[47] Dana Priest, "Deputy Chief Resigns from CIA," *Washington Post*, November 13, 2004.

[48] Timothy J. Burger, "10 Questions for Porter Goss," *Time Magazine,* Wednesday, June 22, 2005.

[49] Dana Priest, "Deputy Chief Resigns from CIA."

[50] Dana Priest, "Deputy Chief Resigns from CIA." The other men that Goss brought with him were Merrell Moorhead who was deputy staff director at the House committee and Jay Jakub, who had worked as a CIA analyst. See

© 2023 The Authors | CC BY-NC-ND 3.0 US

"Alec Station"—Alec Station was the virtual CIA station that was set up to hunt Osama bin Laden—told *The Guardian,* "[t]here's nothing wrong with being a little gruff and a bit abrasive but I've heard these people have been real bastards."[51]

The situation came to a head after the DCI designated Michael V. Kostiw, one of the "gosslings"—as Goss's executive team came to be called—the CIA's Executive Director, the third highest position in the Agency. In response to the appointment someone in the agency leaked to the media that while Kostiw had previously worked for the CIA, he had left after he was arrested for stealing a package of bacon. The story eventually made its way to the *Washington Post*, thus setting the gosslings off in pursuit of the leaker. Toward that end, they threatened a long-time agency employee. She alerted Michael Sulick, Associate Deputy Director of Operations, to what was happening.[52] He in turn told his boss, Steve Kappes. A heated meeting was subsequently held between Goss, Murray, Kappes, and Sulick. Dana Priest reported that Goss walked out of the meeting, refusing to deal with what he termed "personnel issues" and things devolved from there. [53]

In the end, Murray demanded that Kappes order Sulick to resign. Kappes refused and resigned instead. Sulick followed suit. This left the DO without its two most senior officers. The following month four deputy directors of operations, (Thomas Twetten, Jack Downing, Richard F. Stolz and James L. Pavitt) tried to get an appointment with the Director to discuss the quickly deteriorating situation. Goss refused to see them.[54] Then, after fighting his own battles with the gosslings, John McLaughlin, the highly respected Deputy Director of the CIA, announced his retirement on 12 November 2004. Within days of McLaughlin's announcement, Goss circulated a memorandum to agency employees, in which he argued that the job of intelligence analysts was "to support the Bush Administration and its policies." The memo provoked outrage among veteran intelligence officers who believed that the director was trying to stifle "independence" and "suppress dissent".[55] Although Goss quickly sought to walk the memo back, morale within the agency continued to plummet.[56]

Two months later, Jami A. Miscik, the CIA's Deputy Director of Intelligence, announced her resignation. By this point, dozens of senior intelligence officials had left the agency; indeed, only one member of Tenet's leadership team remained, Donald M. Kerr, the Director of Science and Technology. [57] Unsurprisingly, the media followed the situation that was unfolding closely. Many journalists, who covered the story, blamed Goss for both his partisanship and his management style. For example, famed *Washington Post* correspondent, David Ignatius, argued that the "attacks on senior officers were reckless" as "they peeled away a generation of

---

David Wise, "Sycophant Spies," *Los Angeles Times*, November 21, 2004. https://www.latimes.com/archives/la-xpm-2004-nov-21-op-cia21-story.html

[51] Julian Borger, "CIA memo urging spies to support Bush provokes furore," *The Guardian*, Thursday, November 18, 2004. https://www.theguardian.com/world/2004/nov/18/usa.julianborger.

[52] Dreyfuss, "The Yes-Man."

[53] Dana Priest, "Deputy Chief Resigns from CIA."

[54] Walter Pincus, "Goss Reportedly Rebuffed Senior Officials at CIA: Four Fear New Chief is Isolating Himself," *Washington Post*, November 14, 2004.

[55] Julian Borger, "CIA memo urging spies to support Bush provokes furore," *The Guardian*, November 18, 2004, and Douglas Jehl, "New CIA Chief Tells workers to Back Administration's Policies," *New York Times*, November 17, 2004.

[56] For Goss's position see, David Ensor, "Officials: CIA Memo not an order to 'back Bush'" *CNN Washington Bureau,* November 18, 2004. https://edition.cnn.com/2004/ALLPOLITICS/11/17/cia.memo/

[57] Walter Pincus, "Goss's Shake Ups leave Some Questioning Agency's Role" *Washington Post*, January 6, 2005.

© 2023 The Authors | CC BY-NC-ND 3.0 US

senior CIA managers."[58] The situation could not have been more fraught as John Negroponte assumed his position as DNI in April of 2005.

Although there was no question that whomever George W. Bush picked to be DNI he had "better be a hell of a choice,"[59] Negroponte was not the President's first choice or even his second. Indeed, it remains unclear where Negroponte ranked on Bush's shortlist.[60] Nevertheless on paper, at least, he appeared to be a good fit. He was sixty-five years of age and had spent forty-five of these years in government service that included several ambassadorships and senior government postings. During the Bush Administration, he had taken on two delicate tasks; first as US Ambassador to the United Nations (19 September 2001–23 June 2004) and second as United States Ambassador to Iraq (29 July 2004–17 March 2005). Moreover, during his career, he had worked closely with the CIA in Vietnam, Central America, and Honduras. Thus, he had experience working with intelligence officers in dicey situations. In the words of John MacGaffin, a former CIA officer, "no one had ever accused him of being a 'pass the crumpet's' diplomat."[61] Finally, he was also believed to be politically astute; he had survived the release of a cache of documents that seemed to suggest that he had a troublesome record on human rights.[62]

Because of his background and personal attributes, and despite the controversy that still followed him, Negroponte was also viewed as someone who knew how to oversee a complex bureaucracy. Although he had no direct experience in the IC, his reputation for managing difficult situations without ruffling too many feathers suggested he could serve as a "stabilizing force."[63] Timing, however, would be critical. As Jane Harman, a Democratic Congresswoman who sat on the House Intelligence Committee told both Negroponte and Hayden during their confirmation hearings, they had "a six-month window before the turf-protectors, and forces of inertia in Washington, [would] destroy their ability to succeed."[64] It was clear, almost from day one, that one of the biggest turf wars would be with the CIA; the other was with Secretary of Defense Donald Rumsfeld and the Pentagon, but that is another story.

On assuming office, Negroponte was aware that most of the men and women at the CIA did not support the 2004 intelligence reform bill. After it was passed, many in the agency, according to Hayden, were "just pissed."[65] Thus, both men knew that they would face pushback as they began to build the ODNI. One of the central problems they faced was that IRTPA's language did not outline the exact nature of the relationship between the DNI and the CIA. It still needed to be negotiated.[66] But Negroponte also felt he and Goss had a good relationship; they had belonged to the same fraternity at Yale University and knew each other very

---

[58] David Ignatius, "The CIA at Rock Bottom", *Washington Post*, May 7, 2006.

[59] Hayden, *Playing to the Edge*, 161.

[60] There is a clear consensus that Bush preferred Robert Gates. Other candidates who were considered include: Goss, General Tommy Franks, and the Former Governor of New Jersey Tom Kean. Negroponte Interview by Kennedy, 11 February 2000.

[61] Dana Priest, "Relationship with Bush Will be Key," *Washington Post*, Feb 18, 2005.

[62] According to Peter Kornbluh of the National Security Archives, Negroponte was "not an honest broker." See Scott Shane, "Poker-Faced Diplomat, Negroponte is Poised for role as Spy Chief, *New York Times*, March 29, 2005; Scott Shane, "Cables Show Central Negroponte Role in 80s Covert War Against Nicaragua," *New York Times,* April 13, 2020; Michael Dobbs, "Negroponte's Contra Role: Newly Released Documents Show Intelligence Chief was Active in US Effort," *Washington Post,* April 12, 2005.

[63] David E. Sanger, "An Old Hand in New Terrain for Top Intelligence Job," *New York Times*, February 18, 2005.

[64] Douglas Jehl, "Senators to gauge spy chief's intentions," *New York Times,* April 11, 2005.

[65] Hayden, Interview, Miller Center, November 20, 2012, 21.

[66] Neary, 4.

© 2023 The Authors | CC BY-NC-ND 3.0 US

well.[67] As he began to consolidate his power, however, he, and his staff "repeatedly clashed with Goss and his staff."[68]

In one of his first moves, Negroponte decreed that CIA station chiefs around the world were to report to him on any matter related to the larger intelligence community. Although some in the agency thought this trespassed on CIA's turf, they were forced to go along with it.[69] A second conflict emerged over the President's Daily Brief (PDB), which had been a CIA product since it was first presented to President Lyndon Johnson on 1 December 1964. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction had suggested that the PDB be moved to the ODNI and Negroponte went ahead and did this. However at least initially, he encouraged Goss to join him during his first intelligence briefings with President Bush.[70] The report also recommended that the PDB reflect the views of the IC, as a whole. To some extent, it already did this, but Negroponte wanted to make even more of an effort to include a diversity of voices.[71] Today the PDB remains primarily a CIA product even as it is under the direction of the ODNI. According to intelligence scholar Michael Miner, "although it is a community wide product, CIA personnel are first among equals" in its development.[72] While both moves were pre-ordained, they proved to be controversial and difficult to implement as they signaled "a diminution of the power of the CIA."[73]

A third conflict over resources proved to be more difficult to manage. Negroponte needed people, and at least initially, to get them quickly, he would have to raid existing government agencies and departments. This stirred up resentment, especially as the ODNI's demands continued to grow. The situation came to a head when Negroponte announced that he needed twenty more analysts to staff the newly created National Counterterrorism Center (NCTC), which as mandated by the 2004 legislation, was set up under the DNI's office. Having already seconded between 70-80 men and women to the ODNI, Goss refused Negroponte's request.[74]

According to *New York Times* journalist, Scott Shane, the conflict that erupted went beyond resources, however. It was also over NCTC's mandate. When it was set up, NCTC appeared to be in direct conflict with

---

[67] Both men were members of *Psi Upsilon* (the Fence Club). A third member was George H.W. Bush's brother, William "Bucky" H.J. Bush. See Liebmann's *The Last American Diplomat*, 3. Goss was also a member of Book and Snake, one of Yale's "above ground," albeit secret societies. Negroponte was not. Daniel Horowitz, *On the Cusp: The Yale College Class of 1960 and a World on the Verge of Change,* (Boston: University of Massachusetts Press, 2015), 234. On Negroponte and William "Bucky" Bush see, Negroponte Interview by Kennedy, 95. Negroponte's nickname was "Ponte," which President Bush apparently called him, 78.

[68] Mark Mazzetti and Scott Shane, "Director of the CIA is Stepping Down under Pressure." *New York Times*, May 6, 2006.

[69] Walter Pincus, "Negroponte Steps into Loop: CIA Station Chiefs Are Instructed to Include Him in Reporting," *Washington Post,* May 13, 2005.

[70] David Priess, *The President's Book of Secrets: The Untold Story of Intelligence Briefings of American Presidents* (New York: Hatchette Books, 2016), 268.

[71] Nancy Bernkopf Tucker, "The Cultural Revolution in Intelligence: Interim Report," *The Washington Quarterly*, 31:2 (Spring 2008): 47-67, 50.

[72] Mike Miner, Note to Author, Wednesday, August 9, 2023.

[73] Douglas Jehl, "Early Clues to a New Spy Chief's Muscle," *New York Times,* February 20, 2005. Many analysts were concerned that if the State Department or the Pentagon were to write the PDB their policy preferences could influence the analysis. Second, many from DO were worried about sharing operational human intelligence to those who did not understand the stakes behind its collection. They were concerned that lives could be lost.

[74] Scott Shane, "Year into Revamped Spying, Troubles and Some Progress," *New York Times,* Feb 28, 2006.

© 2023 The Authors | CC BY-NC-ND 3.0 US

the CIA's Counterterrorist Center (CTC).[75] CTC was set up with the Directorate of Operations in 1986. It housed experts from all over the Agency, as well as members from the Federal Bureau of Investigation (FBI) and the Secret Service. In contrast, NCTC employed experts from all over the IC, including the agencies listed above. It was designed to "blend foreign and domestic, intelligence and law enforcement, information;"[76] but in its first few years it remained unclear "where the CTC's responsibilities ended and NCTC's began."[77] The issue became a serious point of contention between Goss, Negroponte, and their two centers as long-time agency employees found themselves seconded to NCTC. According to former CIA intelligence briefer, David Priess, "tensions" between the two units, and the people in them, "remained high for years."[78]

Given the growing hostility to the ODNI there were people at the CIA who were "directing a nasty rear-guard action, denying the ODNI goods and services and transportation while trying to countermand DNI directives." A lot of this, Hayden argued "was pure petulance."[79] As the DNI's principal deputy, he encouraged Negroponte to push back forcefully on the CIA's behind-the-scenes machinations. He believed that, in both thought and action, the new DNI had to show the IC that there was "a new sheriff in town."[80] As he put it in his memoirs, during this period he often reflected on Voltaire's rationale for killing an admiral, occasionally: "*pour encourager les autres*." Negroponte, however, preferred a much more subtle approach and told Hayden, "I hear you Mike, but I'm not here to pick fights."[81] In the end, Goss and his gosslings, left him no choice as questions over resources and mandates became "recurring problem[s]" for the DNI.[82]

It is impossible not to acknowledge the way in which Negroponte's and Goss's *Weltanschauung* exacerbated the unfolding situation. According to *Washington Post* reporter David Ignatius, part of the IC's trouble was the result of two warring impulses that had been "apparent in the Bush Administration's foreign policy from the start—a 'realist' support for strong independent spy agencies and a 'neo-conservative' mistrust, bordering on outright hatred, of the CIA as a supposed obstacle to the President's goals."[83] Negroponte came to embody the first impulse, Goss the second.

As the relationship between the ODNI and DCI continued a downward spiral, Goss's leadership style again came into question. In September of 2005, Robert Richer, who was the number two officer in the CIA's Directorate of Operations left. He had been at the agency for over thirty-five years. At the time he announced publicly that he was leaving because he had lost confidence in Goss. By this time more than three dozen people had resigned from the agency.[84] In the spring of 2006, Goss had also come under fire from the President's Foreign Intelligence Advisory Board (PFIAB). The board's mission was to offer an independent

[75] On the CTC see John O. Brennan, *Undaunted: My fight Against America's Enemies, at Home and Abroad*, (New York: Caladon Books, 2020), 87.

[76] Hayden, Interview, Miller Center, November 20, 2012, 21.

[77] Scott Shane, "Year into Revamped Spying, Troubles and Some Progress".

[78] Priess, 269-270. On this topic, see also: Karen De Young, "A Fight Against Terrorism and Disorganization," *Washington Post,* August 9, 2006.

[79] Hayden, *Playing to the Edge,* 162.

[80] Hayden, *Playing to the Edge,* 163.

[81] Hayden, *Playing to the Edge,* 163.

[82] Hayden, *Playing to the Edge*, 164.

[83] David Ignatius, "Danger Point in Spy Reform," *Washington Post,* October 21, 2005; See also Rovner, 146.

[84] Dafna Linzer, "In Hearing, Hayden Distinguishes Himself from Goss: Nominee's Testimony Might have been for Agency as Much as for Lawmakers," *Washington Post,* May 21, 2005.

© 2023 The Authors | CC BY-NC-ND 3.0 US

voice on intelligence collection, analysis, and operational issues. Their report on Goss and his subordinates, was "devastating"[85]

By this point Goss's poor record was starting to rub off on Negroponte. According to Mark Lowenthal, a former top CIA official, within the IC there was a "huge hunger for leadership that is not being met."[86] At one point, HPSCI chair, Jane Harman became so frustrated that she stated that although Negroponte was "a smart diplomat" he "needs to stop being an ambassador."[87] It was becoming clear that Negroponte was going to have to get rid of his college chum. The final straw proved to be both personal and political.

After Kostiw was disqualified—remember the bacon— Goss appointed a close friend, Kyle "Dusty" Foggo as Executive Director of the Agency. During his tenure Foggo "waged guerrilla warfare against the DNI."[88] That was not what got in him into trouble, however. Rather, he came under investigation by the CIA's Inspector General for steering a military contract to a close high school friend of his, Brent Wilkes.[89] In May of 2006, the FBI searched Foggo's home and work.[90] For a time there was yellow police tape around the office of the CIA's Executive Director.[91] The optics were terrible, and the media quickly picked up on the story. Negroponte, who had also known Foggo personally, ordered the DCIA to fire him. Goss prevaricated.[92] Negroponte did not. In April he informed Goss he had a month to provide the president with his resignation letter. On 5 May 2006, Goss resigned, and Hayden became the second DCIA. [93]

In an interesting postscript to this story, it was Hayden who went on to embody the "political deftness" that was required for the job of DCIA. After carefully assessing the room he was about to enter, he did so not as General Michael Hayden—the "disrupter"—who had governed the NSA from March1999 to April 2005, but as Director Hayden—the "buffer"— whose principal concern was protecting a workforce that had been deeply traumatized. Sensing the delicate position he was in on his first day in office, he assured those who had come to greet him in the CIA's auditorium that he was not there "to blow anything up."[94] Instead, he advised

[85] David Ignatius, "The CIA at Rock Bottom"; See also Mark Mazzetti and Scott Shane, "Director of the CIA is Stepping Down under Pressure." *New York Times*, May 6, 2006.

[86] Scott Shane, "In New Job, Spymaster Draws Bipartisan Criticism," *New York Times*, April 20, 2006

[87] Walter Pincus, "Some Lawmakers Doubt DNI has taken Intelligence Reins," *Washington Post*, February 2, 2006.

[88] Michael V. Hayden, Interview, Miller Center, November 20, 2012, 17.

[89] Apparently the two men were so close that they were best men at each other's wedding, and they named their sons after each other. See Sidney Blumenthal, "The Ruin of the CIA."

[90] Mark Mazzetti, "Career CIA Figure is at Eye of Scandal," *New York Times*, May 12, 2006. Foggo was eventually convicted of "honest services fraud" and was sentenced to 37 months in prison.

[91] Michael V. Hayden, Interview, Miller Center, November 20, 2012, 23.

[92] Negroponte Interview with Kennedy, February 11, 2000.

[93] By the time Goss left, somewhere between 30 and 60 intelligence officers had left the Agency. This included a dozen senior officers including one director, two deputy directors, several station chiefs and division directors, many of whom had key language skills and extensive experience in the field. Apparently one third of counter-terrorism officers had also left since Goss had become director. Dana Linzer and Walter Pincus, "Goss Forced Out as CIA Director: Gen Hayden is Likely Successor," *Washington Post*, May 6, 2005. It is important to note that not all these exits were due to Goss. Apparently, job dissatisfaction was caused by other matters, including fights over parking spaces, job titles, incompatibility over computers (the meaning of the previous phrase is not clear—what is incompatibility over computers?), and who worked where. Scott Shane, "Year into Revamped Spying, Troubles and Some Progress," *New York Times,* Feb 28, 2006.

[94] Hayden, 167. In his memoirs Hayden argues that he "always characterised [his] immediate superiors as transmitters, amplifiers or buffers, when it came to bureaucratic pressure coming at them." He believed that both he and George Tenet were "buffers." But when I pushed him on this and pointed to the ways in which he seemed to relish in disrupting the status quo at the National Security Agency, he nodded and then added "but not at the CIA." Zoom

© 2023 The Authors | CC BY-NC-ND 3.0 US

everyone to "blow into the paper bag [and] get your CO_2 levels back to normal. This stuff's over." He added, "just go back to work. I'll take care of the other stuff outside."[95]

Hayden went on to be an effective Director of the CIA. Over the next three years he rebuilt both the agency's morale and its stature. However, in the process he also had to negotiate a new relationship with his old boss, Negroponte, and his successor, Mike McConnell. And as he noted, none of this was easy.[96] The tension between the DNI and DCIA reached its zenith during Barak Obama's administration. Obama's first DNI, Dennis Blair (28 January 2009–28 May 2010), and DCIA, Leon Panetta (13 February–30 June 2011), came to loggerheads over who would appoint station chiefs abroad. It was a complicated question and one which both Negroponte and McConnell had been able to side-step. Unfortunately, Blair and Panetta went on to fight "an intense and acrimonious turf battle" over the issue.[97]

Although in the end the president came down on the side of the CIA,[98] the controversy left a lasting mark on both institutions. Indeed, it was not until James Clapper became DNI in 2010 that tensions between the CIA and DNI began to diminish.[99] Despite Clapper's managerial skills, during Donald J. Trump's presidency, the credibility of both offices was nevertheless again called into question.[100] As noted intelligence historian Richard Immerman has pointed out, throughout his tenure Trump both, "abused and ignored,"[101] the IC. The chaos that defined much of his administration finally came to an end with the inauguration of Joe Biden. Biden appointed Avril Haines as DNI on 21 January 2021, and William J. Burns as DCIA a few months later. While today the IC again appears to be moving in the right direction, it remains unclear what the future will hold. What is clear is that in no small way the relationship between the DNI and the DCIA will continue to be heavily dependent on the political deftness of both the men, and now, finally, the women, who are appointed to these positions. "Intelligence" in the words of James Clapper—the longest serving DNI to date—"is [and, I would add, was always] all about the people."[102]

---

interview with General Michael Hayden, Friday, July 7, 2023, 2:00 PM Eastern. I confirmed my use of the term "disrupter," to characterize his leadership style at NSA during a second interview on Thursday, July 27, 2023, 2:00 PM Eastern. During his confirmation hearings Hayden also went to great lengths to separate himself from Goss. See Dafna Linzer, "In Hearing, Hayden Distinguished Himself from Goss: Nominee's Testimony have been for Agency as Much as for Lawmakers," *Washington Post,* May 21, 2005.

[95] Hayden, Interview, Miller Center, November 20, 2012, 24.

[96] According to Hayden, he, and McConnell "had known each other for years, were friends and between us had nearly three quarters of a century of intelligence experience—I found that relationship took a lot of effort." Senate Testimony of Michael V. Hayden, "Ten Years After 9/11"

[97] Marc Ambinder, "The Real Intelligence Wars: Oversight and Access," *The Atlantic*, November 18, 2009. https://www.theatlantic.com/politics/archive/2009/11/the-real-intelligence-wars-oversight-and-access/30334/. For an excellent discussion of all the issues involved see Immerman, *The Hidden Hand,* 211-213.

[98] Mark Mazzetti, "White House Sides with CIA in Turf Battle," *New York Times*, November 12, 2009.

[99] David Ignatius, "James Clapper; on top of the secret empire," *Washington Post,* October 23, 2013.

[100] See Michael Morell, Avril Haines, and David S. Cohen, "Trump's Politicization of US Intelligence Agencies Could End in Disaster, *Foreign Policy,* April 28, 2020. https://foreignpolicy.com/2020/04/28/trump-cia-intimidation-politicization-us-intelligence-agencies-could-end-in-disaster/; Robert Draper, "Unwanted Truths: Inside Trump's Battles with US Intelligence Agencies," *New York Times*, August 8, 2020.

[101] Richard Immerman, "Trump to the Intelligence Community: You're Fired," H-Diplo/ISSF Policy Series, January 28, 2021. https://networks.h-net.org/node/28443/discussions/7158950/h-diploissf-policy-series-2021-4-trump-intelligence-community-you, and Immerman, "Trump to the Intelligence Community: You're Fired," in Robert Jervis, Diane Labrosse, Stacie Goddard, and Joshua Rovner, eds., *Chaos Reconsidered: The Liberal Order and the Future of International Politics* (New York: Columbia University Press, 2023), 138-151, here, 138.

[102] James Clapper, in Loch Johnson, "A Conversation with James R. Clapper Jr., "The Director of National Intelligence in the United States," *Intelligence and National Security*, 30, 1(2015): 1-25. 3.

© 2023 The Authors | CC BY-NC-ND 3.0 US

There is no question that the creation of the DNI "muddled lines of authority, touched off turf battles and confused everyone."[103] But bureaucracies do not usually make or break intelligence; people do. Congruent with this perspective, as I argued above, one cannot begin to understand the history of the ODNI without coming to grips with the personal characteristics and political ethos of those involved. Although friendly in college, Negroponte and Goss were temperamentally different, held contrasting world views, and had incompatible management styles. While this did not necessarily mean that it was inevitable that they would come into conflict, the yet undefined relationship between the DNI and the DCIA made the situation extraordinarily difficult to navigate. In the end, the evidence available to date indicates that neither man possessed the political agility that was necessary to overcome the complex set of circumstances that he faced.

[103] Chris Whipple, *The Spy Masters: How the CIA Directors Shape History and the Future*, New York: Scribner, 2020, p. 216.

© 2023 The Authors | CC BY-NC-ND 3.0 US

"The Intelligence Community Meets the Twenty-First Century: Evolution, Not Revolution" by Thomas Fingar, Stanford University

Members of the US Intelligence Community (IC) are again being told that they can and must make dramatic changes in order to remain relevant and useful.[1] Calls for reform and/or restructuring of the intelligence enterprise are probably as old as the profession of intelligence; so too are assertions that the IC is stuck in the past, reluctant to change, and incapable of meeting new challenges.[2] Common characterizations and caricatures of the IC exaggerate its resistance to reform, ignore the frequency and magnitude of evolutionary change, and trivialize factors which require a high degree of stability.

Tools and methods change, but the fundamental missions of intelligence, providing warning, information, and insight to national security decisionmakers, and maintaining trust between intelligence professionals and the people they support must not be diminished by infatuation with new ideas. The Intelligence Community is very different today than it was when I first obtained codeword clearances in 1970. It is also different than it was before passage of the Intelligence Reform and Terrorism Prevention Act of 2004, and after the changes adopted during my tenure as Deputy Director of National Intelligence for Analysis in 2005–2008.[3] Most changes were and will be driven by developments in the international situation, the scope and priorities of the national security establishment, and the availability of new tools and techniques. They were adopted and adapted to meet new requirements and to enhance performance of enduring responsibilities.

Some prophets and proponents of change emphasize the potentially transformative impact of Artificial Intelligence (AI) and other uses of big data. Others point to increasing competition from groups using only or mostly open source information. Most advocate the continued separation of intelligence and decisionmaking as necessary to ensure objectivity and prevent politicization.[4] In contrast, a small but growing number of commentators seem to imply that intelligence findings or judgments should drive or even dictate policy decisions.[5] It is a very small step from asserting that AI judgments about national security issues will often be more accurate than human judgments to implying that AI algorithms should determine policy responses.

I find it inconceivable that policymakers will abdicate fundamental responsibilities to a machine. They will not and should not do so. But machine-generated assessments and empirically based policy recommendations will

[1] See, for example, Amy B. Zegart, *Spies, Lies, and Algorithms: The History and Future of American Intelligence* (Princeton, NJ: Princeton University Press, 2022); and Center for Strategic and International Studies, *Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation* (Washington, DC: Center for Strategic and International Studies, 2021).

[2] Timothy Walton, *Challenges in Intelligence Analysis: Lessons from 1300 BCE to the Present* (New York: Cambridge University Press, 2010); Michael Warner and J. Kenneth McDonald, *US Intelligence Community Reform Since 1947* (Washington, DC: Center for the Study of Intelligence, 2005).

[3] For background on the ways in which the US Intelligence Community has evolved see, for example, *Foreign Relations of the United States, 1945-1950: Emergence of the Intelligence Establishment* (Washington, DC: Office of the Historian, US Department of State, 1996), https://1997-2001.state.gov/about_state/history/intel/summary.html; *Intelligence Reform and Terrorism Prevention Act of 2004* (Public Law 108-458, December 17, 2004), https://www.dni.gov/files/documents/IRTPA%202004.pdf; and Thomas Fingar, *Reducing Uncertainty: Intelligence Analysis and National Security* (Stanford, CA: Stanford University Press, 2011).

[4] See the critique of this view in Neveen S. Abdalla and Philip H. J. Davies, "Intelligence, Policy, and the Mandate: A Third Form of Strategic Failure," *The International Journal of Intelligence, Security, and Public Affairs*, 23:2 (2021), 105-124, https://www.tandfonline.com/doi/full/10.1080/23800992.2021.1881724.

[5] See, for example, Marty Z. Khan, "Intelligence Analysts Not Providing Options for Consideration to Policymakers: An Anachronism Whose Time Has Passed?" *American Intelligence Journal* 32:1 (2015), 34-39, https://www.jstor.org/stable/26202101.

© 2023 The Authors | CC BY-NC-ND 3.0 US

become increasingly common and compete for attention with other inputs to the already-crowded decisionmaking environment. This will add to, but not fundamentally change, IC responsibilities and the relationship between national security decisionmakers and the intelligence professionals who support them.

Competition

Much has been written about the need for the IC to adjust to a world in which non-governmental organizations are increasingly capable and eager to collect, analyze, and provide "intelligence" input to the policymaking process.[6] Some putative competitors utilize classified intelligence; others rely solely on unclassified information. Types of information once accessible only to US Intelligence Community analysts, such as satellite and drone imagery, is now available commercially. Indeed, non-US Government (USG) customers can sometimes task the collection of imagery on places or developments in the same way—albeit less bureaucratically than—IC analysts can task collection by USG systems. General and specific fruits of collection can be utilized by analysts in-and outside the IC.[7]

Having more eyes on a problem increases the opportunities to detect and analyze developments, but it also introduces the potential for counterproductive competition in the form of ill-considered interpretations (by private or IC organizations) that affect public perceptions and pressures on policymakers to "do something" about the problem. Expansion of the number and scope of alternatives to IC collection and analysis will have multiple consequences, some more disruptive than others. More eyes and minds on problems should enhance understanding by bringing diverse perspectives to bear and facilitate larger critical masses of expertise. But the quality of resultant assessments is bound to be uneven, and there will be fewer mechanisms to evaluate, compare, and adjudicate judgments than exist within the Intelligence Community.

Peer review and equivalent mechanisms take time and will become even more problematic as the volume of output increases and expert reviewers are overwhelmed by requests. Quality control within academic units or firms will help, and reviews by independent organizations would be beneficial albeit difficult to structure. Initially, however, and probably for some time, primary responsibility for assessing the quality of externally produced analysis will fall to the Intelligence Community.

For non-urgent subjects and developments, cooperation (peer review) among competitors and even in conjunction with the IC is desirable and feasible, but probably difficult to achieve. Part of the reason it will be difficult is captured by the idea of competition. In an ideal world, insights and judgments would compete on the basis of quality, utility, and timeliness. But in the real world, the desire to scoop competitors and the ability to disseminate products instantaneously will pose formidable obstacles to both quality control and integration into IC thinking and products.

This is not a new problem. One of the challenges I faced when charged with leading the transformation of IC analysis two decades ago was the use of the term "competitive analysis" in Executive Orders and IC guidance.[8] The clear intent of the term was to ensure that all problems would be examined by at least two

[6] See, for example, Marla A. Robson Morrow, "Private Sector Intelligence: On the Long Path of Professionalization," *Intelligence and National Security*, 27:3 (2022), 402-420, https://www.tandfonline.com/doi/full/10.1080/02684527.2022.2029099.

[7] See, for example, Jeff Wise, "The DIY Intelligence Analysts Feasting on Ukraine: Meet the Would-be Jack Ryans of OSINT," *Intelligencer*, March 4, 2022, https://nymag.com/intelligencer/2022/03/the-osint-analysts-feasting-on-ukraine.html.

[8] See the repeated use of "competitive analysis" in *Executive Order 12333: United States Intelligence Activities*, December 4, 1981, https://www.archives.gov/federal-register/codification/executive-order/12333.html. This

© 2023 The Authors | CC BY-NC-ND 3.0 US

independent organizations as a form of check-and-balance in order to ensure against single-point-of-failure errors. That was the intent, but competition was too often interpreted to mean being the first to produce a judgment and/or having one's own interpretation accepted and utilized by policymakers. Being first has no virtue if the judgment is wrong and could have been made less wrong by some form of peer review or independent analysis of the same information.

Regardless of how good (or bad) the information and judgments provided by non-IC actors are, they are likely to be disseminated by digital media as quickly as the producers can move them into the marketplace of ideas. At a minimum, this will mean that the IC must discover, evaluate, and comment on externally generated products as quickly as possible. This will entail significant opportunity costs. Failure to quickly jump on input of uncertain quality risks having erroneous ideas shape the thinking and statements of policymakers who are eager to be first to pronounce on a proclaimed problem or opportunity. Reeling them in after they have internalized and committed to defective judgments is neither easy nor a process that is likely to win the confidence of IC customers.

AI-generated analyses will sometimes be as good as those produced by human analysts. But not always. Determining which are good and which are flawed (and how and why they are flawed) will be a daunting challenge. Among other reasons is the fact that humans cannot realistically process anywhere near the volume of information utilized by AI algorithms. Expanding the scope and volume of information utilized, whether by humans or machines, magnifies the necessity and the difficulty of identifying faulty, deliberately misleading, and in other ways problematic "facts" and judgments.

Nevertheless, increasing use of AI—inside and outside the IC—is inevitable. This means that IC analysts and managers must determine soon and continuously how AI's capacities are to be utilized. Machines can do things that humans cannot, and obviously should be used where and how it is advantageous to do so.

The addition and intensification of competition compounds the perennial challenges of the Intelligence Community. For example, more information about more developments, and the likelihood that some will be depicted as worrisome, detrimental to US interests, or opportunities to be seized without delay will fuel the already excessive proclivity of specific constituencies and/or officials to "do something" about the problem. Doing something, preferably quickly, is not the same as doing something that is prudent or effective. Providing information and insight to help decisionmakers avoid blunders and devise strategies and policies to achieve desired outcomes is a core mission of the IC. This can be, and will be, a time-consuming task that diverts attention and effort from support to other missions and customers.

Day-in and day-out operation of the IC—targeting collection, enhancing understanding of developments and what shapes them, and addressing the declared and implicit needs of customers across the national security enterprise—is guided by policymaker-established priorities and routine monitoring requirements. The system requires prioritization of tasks, including assignments of and to people, but it also requires agility and expertise to respond quickly to pop-up developments and new policymaker requirements. The more external or competitive inputs are added to the mix, the greater the difficulty of performing all missions and satisfying all customers.

terminology was dropped in the amended version issued in 2008, https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf.

© 2023 The Authors | CC BY-NC-ND 3.0 US

Times and Tools Change but Fundamentals Do Not

Older people tend to think the future will be much like the past and that what they/we did in the past will be appropriate for the future. There is also a tendency for younger people to dismiss lessons offered by their elders as largely irrelevant for the problems of today. Both views are wrong. During my five decades in the IC, I have seen many new approaches and technologies to improve intelligence analysis. Many have promised silver-bullet answers to real and imagined analytic challenges. Most have been disappointing but some have changed the way analysts work. None has changed the core missions of intelligence analysis.

My 2011 book *Reducing Uncertainty* described the dramatic increase in the volume of information and the scope of intelligence analysis after the Cold War.[9] The phenomena and trends it described twelve years ago continue at an accelerating pace. Intelligence analysts continue to be asked to provide more precise information and analytic insight on more issues to more diverse customers, and to do so more quickly. Analysts today and in the future will have more information to work with but less time to evaluate, interpret, and analyze what it means and how it is relevant to the missions and customers that depend on the IC for support.

As in the past, governments and non-state actors will try to protect secrets, and collectors will have to deal with more and better denial and deception efforts. Secrets will be harder to find and harder to unravel. But unclassified information will remain as—or more—important for most analytical challenges.[10] On most subjects of importance to decisionmakers, the analytical challenge will be to cope with a surfeit of information, not absolute scarcity. The most fundamental mission of intelligence is the same as it has always been, namely, to provide information and insights that help decisionmakers to understand the situation they face and to make better informed—and hopefully better—decisions. Sometimes this involves providing warning of potential dangers, but it should also alert decisionmakers to possible opportunities to shape the trajectory of events. Discovering secrets is a small but important part of the mission. But because something was secret or previously undiscovered does not automatically make it important or relevant to the mission that is being supported. More common, and often more important, tasks include explaining puzzles, solving mysteries, and interpreting developments that may (or may not) be relevant to decisionmaker responsibilities and objectives.

Understanding the responsibilities and objectives of the agencies and individuals being supported is a prerequisite for providing helpful intelligence support. Let me underscore this last point by asserting that intelligence analysis that is not helpful to decisionmakers is not good in any meaningful definition of that word. Scanning the horizon to discover things that no one has yet focused on can be informative, but looking for interesting things is not a major responsibility of intelligence analysts. Others can and should do that. The primary responsibility of intelligence professionals is to provide informed insights that help national security decisionmakers to do their jobs.

Decisionmakers receive copious input from myriad sources.[11] Intelligence differs from other input for reasons beyond its access to classified information. What makes it unique and uniquely valuable is its presumptive objectivity and its direct utility to specific customers and missions. One-size intelligence is an

[9] Fingar, *Reducing Uncertainty*, chapter 1.

[10] See, for example, Bowman H. Miller, "Open Source Intelligence (OSINT): An Oxymoron?" *International Journal of Intelligence and Counterintelligence*, 31:4 (2018), 702-719, https://www.tandfonline.com/doi/full/10.1080/08850607.2018.1492826.

[11] See the examples in Roger Z. George and Harvey Rishikof, eds., *The National Security Enterprise: Navigating the Labyrinth* (Washington, DC: Georgetown University Press, 2011).

© 2023 The Authors | CC BY-NC-ND 3.0 US

oxymoron. To be useful, intelligence must be tailored and timely.[12] Meeting those requirements requires close, even intimate knowledge of primary customers and their missions.

Intelligence-Policy Interface

One of the most harmful myths about intelligence is that objectivity and avoidance of politicization require arms-length separation from policy customers. Physical, and more importantly interpersonal distance is a serious impediment to useful intelligence support. The danger that analysts will be co-opted by the people they support and skew information and analysis to please their primary customers is far less than the danger that their work will be unhelpful because the analysts—and thus the IC—do not properly understand what the customer knows, does not know, wants to know, or what, in the judgment of the analyst, the decisionmaker needs to know in order to understand the issue or situation. Good intelligence support also requires knowledge of what the customer is trying to do and when key decisions will be made. The best intelligence in the world is unhelpful if it arrives after key decisions have been made.[13]

Acquiring such knowledge requires both frequent interaction and a high degree of mutual trust. Decisionmakers will not share what they need or want to know if they fear that an analyst will abuse their trust. And analysts cannot provide tailored support unless they understand what is desired or needed. We are a very long way from the time when decisionmakers confide in and take guidance from an advanced version of the *Star Wars'* robot C-3PO. Decisionmakers expect and need intelligence analysts to help them in three ways.

One way is to serve as their eyes and ears by tracking developments germane to the missions and responsibilities of the decisionmaker and his or her agency. Policymaking subordinates are supposed to do the same thing and they do. Intelligence analysts are the second line of defense against surprise and failure to note developments with the potential to affect decisionmaker performance. Performing this function obviously requires accurate understanding of what the decisionmaker is trying to do.[14]

The second way is to obtain, evaluate, and assess additional information germane to agency missions and decisionmaker responsibilities. This requires knowing what information the decisionmaker already has and what he or she thinks is needed. It also requires sufficient understanding of decisionmaker thinking to be able to assess what he or she needs but has not requested.[15] To perform this role, analysts must know what to ask and where to seek the desired information, usually through a combination of classified collection and use of unclassified sources.

The third way is to put information and developments into a strategic context by explaining how they fit into broader patterns and megatrends. Most decisionmakers are very focused on immediate tasks (the in-box) and

[12] See, for example, Fingar, *Reducing Uncertainty*, chapter 3.

[13] These points are further developed in Amanda J. Gookins, "The Role of Intelligence in Policymaking," *The SAIS Review of International Affairs*, 28:1 (Winter-Spring 2008), 65-73, https://www.jstor.org/stable/pdf/27000118.pdf; and Thomas Fingar, "Understanding and Using Intelligence," Forthcoming.

[14] See Thomas Fingar, "Analysis in the US Intelligence Community: Missions, Masters, and Methods," in Baruch Fischhoff and Cherie Chauvin, eds., *Intelligence Analysis: Behavioral and Social Science Foundations* (Washington, DC: National Academies Press, 2011), 3-27.

[15] Fingar, "Understanding and Using Intelligence."

© 2023 The Authors | CC BY-NC-ND 3.0 US

do not have time or the inclination to ask bigger questions about longer term trends. They need analysts—which generally means intelligence analysts—to do that for and with them.[16]

Presenting decisionmakers with more secret information or machine-generated speculation does not assure utility. To be useful, new information and insights must be germane to the mission being supported. Life is full of noise. Merely adding to the noise bombarding decisionmakers is not helpful. Indeed, it can be a distraction that discredits both the analyst and the function of intelligence. Conversely, being useful is the best way to build and sustain confidence in both analysts and the intelligence enterprise, and to reinforce habits of collaboration that facilitate sustained high-quality intelligence support.[17]

Good Analysis Requires Good Analysts

More information and better tools are desirable, but they are not a substitute for good analysts who employ good analytic tradecraft. Access to more information is usually preferable to having to make do with scant, inconsistent, and problematic intelligence, and the ability to use machines and smart algorithms to separate wheat from chaff is almost always better than having to plow through great stacks of information in hopes of finding nuggets of potentially useful data. But not even the most sophisticated algorithms or smartest AI system can produce good analysis without help from good analysts.

Increased collection, machine translations, programs to identify information germane to the problem at hand, and other advanced tools increase the size of the intelligence haystack and provide help in winnowing the pile down to more manageable amounts. Advanced tools and other algorithms are increasingly helpful for identifying patterns, trends, trajectories, and discontinuities, and AI has the potential and probably the likelihood of assisting and accelerating the transformation of data into insight, but for the foreseeable future, it will remain a contributor to good analysis but not a substitute for good analysts.

Assembling large amounts of data is not the same as—and is much less useful to decisionmakers than –data that has been processed through the heads of experienced and knowledgeable analysts. Stated another way, until intelligence is processed in the mind of an analyst, it is just data. Delivering "data" to decisionmakers with the expectation that they have the time and skill to evaluate, assess, and interpret what it means is an unhelpful abdication of analyst responsibility.

AI requires and can make use of larger and larger amounts of data, but that is of little value unless it is working with the "right" data with the dual objectives of producing insights that are germane to the missions and objectives of specific customers in the national security enterprise and identifying anomalies and discontinuities that might be consequential. In other words, it must combine the analytic responsibilities to enhance understanding of developments, trends, and trajectories and provide timely strategic warning. Good analysts do this all the time with regularly updated knowledge of policymaker goals, concerns, and understanding of the issues involved. Machines can probably be built and trained to issue warning and deepen understanding at the same time, but it is hard to imagine how AI-assisted analysts without the continuous updating of information that comes from daily interaction with decisionmakers could have equal or greater

[16] See Mathew Burrows, *The Future, Declassified: Megatrends that will Undo the World Unless We Take Action* (New York: St. Martin's Press, 2014); and Fingar, *Reducing Uncertainty*, chapter 4.

[17] See, for example, James B. Steinberg, "The Policymaker Perspective: Transparency and Partnership," Roger Z. George and James B. Bruce, eds., *Analyzing Intelligence: National Security Practitioners' Perspectives, Second Edition* (Washington, DC: Georgetown University Press, 2014), 93-101; and Roger Z. George, *Intelligence in the National Security Enterprise* (Washington, DC: Georgetown University Press, 2020).

© 2023 The Authors | CC BY-NC-ND 3.0 US

ability to provide timely, tailored, and truly useful input to national security customers. They can assist but will not replace skilled IC analysts who have constant and trusted interaction with the people they support.

Computers have become far more capable, and the compilation of data has become much more sophisticated and useful for producing better large-N studies of all kinds of phenomena. But most large-N studies produce answers to small questions. Such studies are more helpful to academics seeking promotion than to decisionmakers seeking useful insight. Most decisionmakers, most of the time, are interested in big questions involving intentions, the cumulative effects of interactions across time and space, and whether, when, and how nascent problems might resolve themselves or become threats or issues requiring action. Stated another way, good data and good AI can probably provide pretty good predictions about how a specific military unit that is commanded by a particular officer will utilize the weapons at its disposal in a defined situation. But AI cannot predict decision outcomes of deliberations at the top of opaque political systems because requisite high-quality and reliable data are not available.

Even with the development and adoption of increasingly capable data processing and AI analytics, producing truly useful intelligence support to national security customers will require knowledgeable, experienced analysts able to work collaboratively with colleagues in and outside the US government. Use of computers will further reduce the number of intelligence tasks amenable to human-wave approaches that utilize many relatively unskilled people to compile data, but they will not replace trusted analysts as providers of useful support relevant to the kinds of problems on which decisionmakers turn to intelligence and intelligence analysts for assistance. Decisionmakers turn to intelligence when they wish they had better understanding of a problem, development, or situation; when they know they need more information, better information, and better understanding of the information they do have; and when they want help to decide whether and when they must act, and what actions are most likely to produce desired outcomes and avoid unwanted ones. The key link between such requirements and the intelligence enterprise is the analyst.

To serve as this critical link, an analyst must understand the situation or problem as well as or better than the decisionmaker who is being supported. In other words, the analyst's expertise on the policy or problem area must be equal to or better than that of the decisionmaker being supported. That is a high bar. Analyst expertise is also required to recognize and understand how the decisionmaker views the matter under consideration; what information, interpretations, and assumptions likely undergird current judgments; and what information or insight might deepen or even change decisionmaker understanding and preferred courses of action. Without such knowledge, the analyst is reduced to simply responding to—or referring to other analysts or to AI programs—specific questions posed by the decisionmaker. Expertise is needed to determine whether the questions posed are the right or best questions to deepen understanding and reduce uncertainty, whether those or alternative questions can be answered in the timeframe specified by the decisionmaker, and where to seek the information required to answer the most germane questions.

Getting the question right is a critical first step. Chasing data on questions that probably cannot be answered in the time available can only produce unhelpful input to the decision process. It takes expertise and experience to formulate the right questions. The converse is also true. Providing intelligence or insight on matters unrelated to a decisionmaker's responsibilities is unhelpful and can be a distraction. Knowing who needs such information and when they need it is not always self-evident. Mass dissemination of the "Dear Boxholder" variety is unlikely to reach the right decisionmakers. Targeting of information is an analyst responsibility.

Developing the right questions requires expertise on what information is available or attainable, what prior assessments have concluded, and on how to convey requirements to intelligence collectors. Conveying requirements requires knowledge of both collection systems and where desired information might be obtained. When I was Deputy Director of National Intelligence for Analysis, I repeatedly told my analysts

© 2023 The Authors | CC BY-NC-ND 3.0 US

that they could not levy requirements unless they could tell collectors where to look for the answers. Being able to provide that kind of guidance requires substantive expertise as well as understanding of the intelligence system.

Reviewing old information and analyses to determine whether ideas that might have shaped decisionmaker (and analyst) understanding of the problem under study also requires expertise, experience, and a trusted relationship with key customers. So too does the interpretation of new information considering what was known and judged previously and utilizing both old and new information to provide timely and targeted input to decisionmakers. As new and old information is being considered, good analysts convey preliminary judgments to decisionmakers to make them a part of the process. They do so to capture the expertise and evolving thinking of the people and missions being supported. Answering the "right" questions entails not just the "what question, if it can be answered in the time available, promises to produce the most insight" challenges, but also determining whether decisionmaker thinking about the problem has changed significantly. If decisionmaker thinking has evolved, analytic support must do likewise. Better answers to questions already overtaken by events may be useful outside the national security enterprise or at some time in the future but are not very helpful to dealing with immediate problems. All these requisites for good—useful—intelligence support depend ultimately on the expertise of the analyst and the nature of the analyst's relationship with the decisionmaker who is being supported.

They also depend, of course, on good analytic tradecraft: utilizing all available information, whether classified or unclassified; evaluating information and interpreting what it means by using logic and the laws of evidence and inference; clearly identifying information gaps and the means—such as analogies or assumptions—used to close the gaps to produce a coherent story; and clearly articulating judgments about probability and levels of confidence in the information used and the judgments reached. Customers need to understand what is known, what is not known, and the means used to produce judgments on matters they want to understand. Advanced tools and interaction with outside experts can help, but it will not be a substitute for trust-based integration into a single system linking intelligence to policy decisions.

Smart Analysts, Smart Tools, and Smart Systems

Over time, the quantity and character of information have changed, but core missions, key relationships, and essential requisites of good intelligence analysis largely remain the same as they have always been. What is different, in addition to the volume of information available, is that analysts are now expected to monitor and analyze a wider range of developments in more places with greater precision. They are also often expected to do so while meeting deadlines that approximate real-time.[18] Recent examples that illustrate the tendency to assign to the Intelligence Community primary responsibility for assessing developments that once would have been considered largely outside its areas of expertise and responsibility include President Joe Biden's directive to the Intelligence Community to investigate the origins of the COVID-19 virus and the IC's investigation into the causes of Havana Syndrome.[19] Both of these examples clearly have an intelligence dimension, but the

[18] Fingar, *Reducing Uncertainty*, chapters 1-2.

[19] See, for example, Michael D. Shear, Julian E. Barnes, Carl Zimmer, and Benjamin Miller, "Biden Orders Intelligence Inquiry Into Origin of Virus," *New York Times*, May 27, 2021, https://www.nytimes.com/2021/05/26/us/politics/biden-coronavirus-origins.html; and Cindy Smith and Conor Finnegan, "US Intelligence Community Convenes New Panel to Probe, 'Havana Syndrome' Causes amid New Cases in Austria," *ABC News*, July 20, 2021, https://abcnews.go.com/Politics/us-intelligence-community-convenes-panel-probe-havana-syndrome/story?id=78931427.

© 2023 The Authors | CC BY-NC-ND 3.0 US

core issues are medical ones. Both reports were criticized for, among other reasons, the IC's failure to produce definitive answers.[20]

Increases in the volume of information; number, complexity, and scope of subjects to be analyzed; and demands for speed and precision will continue for the foreseeable future. They will also continue to intensify more rapidly than increases in personnel or funding devoted to intelligence analysis. Intelligence professionals in the United States and around the world will require higher levels of expertise, but deeper expertise and more experience alone will not be adequate. Meeting increased demands and rising expectations will require smarter analysts, smarter tools, and smarter systems.

My observation that we will need smarter analysts can be disaggregated to underscore the importance of three different types of expertise and experience. One type refers to substantive knowledge about specific places and problems, such as China or Iran, and/or economic development or nuclear proliferation. This is not a new requirement, but requisite levels of knowledge are higher than before and typically take longer to acquire. To acquire the necessary levels of substantive expertise generally will require more formal training and longer time on an account. Specialization will be more important than general analytical skills. Analysts will also need greater understanding of what smart tools can and cannot do, how to use data mining and other tools, and how to complement and magnify their own expertise by tapping the expertise of colleagues and counterparts inside and outside the analyst's home organization and even the US Intelligence Community.[21] This is different than substantive expertise but no less important. To do the job in the time available, analysts must know where to look for help and how to use the ever-more-capable tools available to them.

The third requisite for becoming a smarter analyst is to develop and master systemic arrangements to clarify what customers want and need, share information and ideas with collaborators, and integrate work done by multiple analysts in multiple organizations into a single, coherent, timely, and useful product. This entails developing and exercising networks of collaborators, habits of cooperation, and procedures to ensure quality and timeliness.[22]

Networks and partially systematized arrangements to capture information and insights within and beyond the Intelligence Community have existed for a long time and are becoming more common. But they lag far behind where they should be and must be to meet the intelligence needs of the national security enterprise and to utilize the capabilities of new tools and non-USG analytical organizations. Nearly twenty years ago, when I was assigned responsibility for transforming the US intelligence establishment, we had only scattered elements of an integrated system. I think we made important steps toward creating and utilizing a more integrated system, but what exists today in the United States still falls short of what is necessary and possible. Expanding and enhancing collaborative, outreach, and integrating mechanisms can no longer be characterized as "nice but too hard to do." The passage of time, technological advances, and the proliferation of entities

[20] See, for example, Carmen Paun, "Congress Sends Bill Requiring Declassification of Covid-19 Origin Intel to Biden," *Politico*, March 10, 2023, https://www.politico.com/news/2023/03/01/havana-syndrome-cia-intelligence-00085021; and "House Intelligence Committee Chairman Turner and Ranking Member Himes Respond to 'Havana Syndrome' Report by Intelligence Community," House Permanent Select Committee on Intelligence Press Release, March 1, 2023, https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=1203.

[21] This point is developed further in Thomas Fingar, *From Mandate to Blueprint: Lessons from Intelligence Reform* (Stanford, CA: Stanford University Press, 2021), especially 131-165.

[22] See Thomas Fingar, "Building a Community of Analysts," in Roger Z. George and James B. Bruce, eds., *Analyzing Intelligence: National Security Practitioners' Perspectives, Second Edition* (Washington, DC: Georgetown University Press, 2014), 287-301; and Julian E. Barnes, "Spy Agencies Turn to Scientists as They Wrestle with Mysteries," *New York Times*, October 11, 2021, https://www.nytimes.com/2021/07/08/us/politics/intelligence-agencies-science.html.

© 2023 The Authors | CC BY-NC-ND 3.0 US

created to provide empirically based analysis to the national security establishment have made it imperative and urgent to develop more systematic procedures.

There are many obstacles to the creation and use of more integrated systems to produce better intelligence support to decisionmakers, but my own subjective judgment about which obstacles are most important is that most intelligence establishments would rather impose greater demands on analysts to be smarter or better, or expect smart tools to compensate for analyst and systemic defects than to tackle the hard tasks of systemic reform. This, in my judgment, is a misplaced hope.

The four most important factors differentiating the IC from all competitors are its proximity and integration into specific components of the national security enterprise (the IC is an integral part of the national security team), its statutory and professional obligation to be objective and eschew policy recommendations, the ability of the IC to utilize the full array of US government capabilities to acquire specifically desired information, and the bonds of trust and confidence between individual policymakers and the IC professionals (usually analysts) with whom they work daily. No external competitor has the same access, experience-based trust, or detailed understanding of decisionmaker wants, needs, objectives, and preferred ways to acquire information.

That does not mean that external information providers can play no useful role in the national security enterprise. As noted above, the fact that they will produce and disseminate ever more products means that they will play greater roles in the policymaking process. The IC will be called upon to evaluate and comment on externally produced assessments that are pushed directly to decisionmakers and the media. Since non-IC produced materials will influence the thinking of IC customers and other relevant constituencies, it would be better for all concerned if those products are factually correct and methodologically sound. It would not be in the interest of either the IC or the United States to have the intelligence community win a putative competition because competitors are perceived to have failed in important ways.

A far better arrangement would be one of collaboration through an expanded and regularized form of the outreach to non-IC experts that has long been an under-utilized tool in the IC toolbox. The Office of the Deputy Director of National Intelligence for Analysis made a valiant effort to expand outreach during the mid-2000s, but inertia and counter-intelligence arguments proved to be formidable impediments.[23] In a reimagined IC, external players should be treated as partners rather than rivals.

Establishment of working relationships should—must—involve institutional as well as individual ties. Expanding the pool of experts to achieve synergies and greater overall capacity makes sense and should be considered a necessity. Capable external partners might operate entirely in the realm of unclassified information, but they might also be given access to classified intelligence with the goal of establishing independent interpretive capabilities. Even at a time of increased salience of mishandled classified documents, one should debate rather than focus exclusively on the risks and dismiss the possible benefits of expanding the number of actors using classified materials.

Collaboration with external entities could take multiple forms, ranging from the exchange of preliminary assessments and discussion of the reliability of individual pieces of information to contractual arrangements whereby the entities would become subcontractors of the IC. Two-way exchanges on the development and use of analytic tools and methods could prove mutually beneficial. Another form of collaboration that might

[23] See Susan H. Nelson, "Analytic Outreach: Pathway to Expertise Building and Professionalization," in Roger Z. George and James B. Bruce, eds., *Analyzing Intelligence: National Security Practitioners' Perspectives, Second Edition* (Washington, DC: Georgetown University Press, 2014), 319-336; and Fingar, *Mandate to Blueprint,* 162-165.

© 2023 The Authors | CC BY-NC-ND 3.0 US

involve outsourcing or subcontracting could be used to prepare some of the unclassified reports assigned to the intelligence community or for which the IC provides input to policy agencies. A more valuable type of subcontracting could be used for subjects on which the IC does not have a comparative advantage but is asked to provide support because it is there, has a can-do attitude, and is a free good to other parts of the US government. Candidate topics include work on global health/pandemic disease, effects of global warming, economic and trade developments, and human rights conditions around the world. The added value of classified intelligence reporting on many such issues is minimal, and using classified information makes the resultant products harder to use. It might be better to collaborate in order to enhance confidence that the analyses were done in accord with IC standards and methods and to put a bit of distance between the judgments and the USG.

Division of Labor and Lanes in the Road

Many forecasts depict increasing collection and analytical capabilities of non-IC organizations as a threat to the privileged place and influence of the US intelligence community. Imputation or assertion that competition from such entities will displace existing intelligence-policy relationships and produce more accurate, more timely, and/or more useful insight and information are overwrought and display a woeful lack of understanding of the intelligence process.

One of the principal ways that IC support to policymakers differs from input generated by academics, think tanks, and other individuals and entities is the IC's knowledge of what the people and organizations they support think that they know, what they find worrisome, and what they are trying to accomplish. In theory, and in the future, there may be ways to collect and analyze sufficient data on individual predilections, operational codes, etc., to predict how they will act individually and collectively under specified conditions, but that capability is still in the realm of science fiction. For the foreseeable future, there will be no substitute for regular and trusted interaction between IC professionals, usually analysts, and the decisionmakers they support.

This is important because decisionmakers need more than just more information and more fulsome and more accurate interpretations of what that information means. They also need information and insight that is tailored to their understanding of the situation (e.g., to enhance or erode confidence in their understanding), what they are trying to accomplish, and their timelines for decision. Providing great answers to irrelevant questions is not helpful.

As a general principle, having more eyes and minds working on a problem is better than having fewer, but that is true only if the result is a net increase in coverage, insight, or utility to customers. More data does not automatically yield greater understanding, and flawed interpretation of available information can lead to ineffective or counterproductive policy responses. Fresh perspectives and independently produced insights can provide valuable prods for the IC to rethink assumptions and reassess analytical methods. Competition that does so would be highly beneficial. But a precondition for using competitive products in this way is confidence that the information and analytical techniques used to produce them are reliable and unbiased. Determination of reliability is a prerequisite for decisions on whether to use a competitor's products instead of those produced by the IC.[24]

[24] Tradecraft standards for IC analytic products are prescribed in the following *Intelligence Community Directives*: ICD 203- Analytic Standards (https://www.dni.gov/files/documents/ICD/ICD_203_TA_Analytic_Standards_21_Dec_2022.pdf); ICD 205-Analytic Outreach (https://www.dni.gov/files/documents/ICD/ICD%20205%20-%20Analytic%20Outreach.pdf); ICD 206

© 2023 The Authors | CC BY-NC-ND 3.0 US

Given the near certainty that policy customers will have neither the inclination, the time, nor in some cases the competence to make such assessments and the likelihood that evaluation by an expert and trusted third party (if one were to be established) would slow the process and decrease the timeliness and utility of the analysis, evaluation of the competitor's product would have to be made by the Intelligence Community. That would also slow the process and divert effort from other tasks.

Calling input from non-IC entities competitive intelligence, even if produced using commercial collection capabilities, more open-source information, and advanced artificial intelligence programs, does not make it fundamentally different than inputs from scholars, think tanks, lobbyists, foreign governments, media outlets, or any of the other long-extant competitors. Government customers have long received voluminous input from inside and outside the US government. Some is methodologically sound and incorporates information neglected or evaluated differently by IC analysts. Regardless of other virtues of such analyses, under current and foreseeable conditions, they will be less well-informed about customer knowledge, concerns, and objectives than the work of IC professionals. They will also be assumed to be less objective than the work of IC analysts

Changing conditions, new requirements, and new tools will, as in the past, necessitate and shape the continuous evolution and adaptation of the US Intelligence Community. But the core responsibilities and fundamental structural dimensions of intelligence-policy relationships in the national security arena will not change nearly as much or as quickly. Utilization of AI and other advanced tools by analytic entities outside the USG will create new opportunities and pose new challenges for IC professionals, but it will not diminish the centrality of the Intelligence Community in the national security enterprise.

Sourcing Requirements for Disseminated Analytic Products (https://www.dni.gov/files/documents/ICD/ICD%20206.pdf); and ICD 208-Maximizing the Utility of Analytic Products (https://www.dni.gov/files/documents/ICD/ICD%20208%20-%20Maximizing%20the%20Utility%20of%20Analytic%20Products%20(09%20Jan%202017).pdf).

© 2023 The Authors | CC BY-NC-ND 3.0 US

"The Complexities of Intelligence Consumption: Creating the Educated Consumer" by Genevieve Lester, US Army War College

Famed political scientist Robert Jervis was well known not just for his storied academic contributions but also for his ability to span the boundaries between the academic and intelligence practitioner worlds with ease.[1] Jervis had much to say about the relationship between intelligence producers and the decisionmakers who consume intelligence. Scholars of intelligence tend to focus on the woes and mistakes of the intelligence producers—the collectors and analysts who comprise the Intelligence Community (IC), but they touch upon the responsibilities of the consumers only briefly. We talk about politicization in the relationship but elide the importance of being an educated consumer. Further, examinations tend to describe the consumer of intelligence as an anonymous senior policymaker, when the actual consumers range across a broad spectrum of roles, from strategic to tactical, and from political appointee, civil service, and military commander, to name a few. Finally, and paradoxically, while the relationship between producer and consumer is asymmetrical—the producer is the junior partner—in our explorations of intelligence failure or success, the consumer is left with very little responsibility, even though he/she has the agency in the dyad. Decisionmakers are the actors, and the quality of the intelligence provided is entirely moot if it is not acted upon.

Following the thread of Jervis's work on the issue, from his essay on the friction between producers and consumers, aptly named "Why Intelligence and Policymakers Clash" to later treatments of intelligence failure, including his book-length *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War,* this essay investigates the role of the intelligence consumer, considers how the dynamics of the war in Ukraine are challenging old assumptions about it, and offers some recommendations on how to improve the relationship between the intelligence producer and the decisionmaker.[2]

Consumption Foundations and Dynamics: The Asymmetric Relationship

Most discussions of the producer-consumer relationship begin with Sherman Kent, the Yale historian turned analyst who is still known as a "larger than life figure in the history of the Central Intelligence Agency."[3] He produced a methodology for analysis and developed standards that mandated disinterested, objective analysis and distance from the consumer.[4] Much like the current adherents to the magical doctrine of "rigor," such as professional military educators attempting to refine the critical thinking skills of their uniformed students, Kent believed the scientific method and strong methodology could help hone both knowledge of the world and prediction about it.[5] As he wrote in his seminal book *Strategic Intelligence for American World Policy:* "Proper relationship between intelligence producers and consumers is one of utmost delicacy. Intelligence must be close enough to policy, plans, and operations to have the greatest amount of guidance, and must not be so

[1] The views expressed are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

[2] Robert Jervis, "Why Intelligence and Policymakers Clash," *Political Science Quarterly* 125, no. 2 (Summer 2010): 185-204; Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca: Cornell University Press) 2010.

[3] J. Kenneth McDonald, "Foreword, in Donald P. Steury, *Sherman Kent and the Board of National Estimates*, (Washington, D.C., Central Intelligence Agency, 1994); https://www.cia.gov/static/sherman-kent-and-the-board-of-national-estimates-collected-essays.pdf , 13.

[4] J. Peter Scoblic, "Beacon and Warning: Sherman Kent, Scientific Hubris, and the CIA's Office of National Estimates," *Texas National Security Review* 1, Issue 4 (August 2018) 100.

[5] See James Joyner, "Professional Military Education and the Rigor Problem," *War on the Rocks* (15 March 2016). https://warontherocks.com/2016/03/professional-military-education-and-the-rigor-problem/

© 2023 The Authors | CC BY-NC-ND 3.0 US

close that it loses its objectivity and integrity of judgment."[6] The issue of the closeness of the relationship between these two sides is a long-standing one and crucial to the understanding of the complexity of effective intelligence consumption.

Kent also highlighted a second issue which forms the core of this essay: the asymmetric relationship between the producer and the consumer. The producer of intelligence is the "junior partner." In Kent's words: "Intelligence is not the formulator of objectives; it is not the drafter of policy; it is not the maker of plans; it is not the carrier out of operations. Intelligence is ancillary to these; to use a dreadful cliché, it performs a service function."[7] This dynamic is very penetrating: after all, the consumer is not required to use—or even listen to—the intelligence proffered by the producer. In Kent's example of a commander dismissing intelligence input based on spurious grounds: "Bull Head [the commander] did not override his G-2 [intelligence officer] because of a reasoned distrust of his data or a rational doubt of his objectivity; he overrode him on the basis of a hunch and probably a wishful one at that."[8] Kent's discussion of the commander, Bull Head, illustrates two crucial points: first, the decisionmaker is not forced to use, or even consider the intelligence; and second, not all producers respect the value that intelligence could and should provide.

The producer must meet the requirements and style of the consumer, and the process is designed to sharpen that message. The intelligence is also packaged to provide a logical narrative. The analyst is telling a story, no matter how *objective* the analysis is expected to be. There will be assumptions, beliefs, prior knowledge, depth, and context, all of which are provided through this story. "There is no such thing as 'letting the facts speak for themselves' or drawing inferences without using beliefs about the world, and it is inevitable that the perception and interpretation of new information will be influenced by established ideas," Jervis explains in his authoritative *Why Intelligence Fails*.[9] On the receiving end, this can be amplified if the receiver of the intelligence is at either end of the spectrum when it comes to interest and knowledge about a particular issue. On one end of this spectrum resides the senior leader with very little interest in intelligence, who dismisses briefings or does not engage at all.[10] On the other end of the spectrum is the decisionmaker who is informed and has already decided upon a particular interpretation of events. Intellectual rigidity can characterize both ends of the spectrum, making the absorption of new material difficult and misunderstanding between the producer and consumer rife.

It is not just the asymmetric relationship that challenges how intelligence is received and used by the consumer. The introduction of challenging or contradictory information complicates the decisionmaking process and can force a reconsideration of some or all aspects of a policy. Policies are usually the result of consensus-building and bureaucratic processes that require time, energy, and commitment. Changing or abandoning them is costly. "Intelligence officers do not wish to make policy," wrote one former practitioner, "but they must often provide information and analysis that complicates or raises questions about an administration's decisions or actions."[11]As Jervis put it: "…Despite the fact that decisionmakers always say they want better intelligence, for good political and psychological reasons they often do not, which is part of the explanation for why intelligence reforms are rarely fully implemented."[12] Or, as he wrote in a different

[6] Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton: Princeton University Press, 1949) 180.
[7] Kent, *Strategic Intelligence,* 182.
[8] Kent, *Strategic Intelligence,* 203.
[9] Jervis, *Why Intelligence Fails,* 131.
[10] LTG (ret) Karen Gibson, Strategy Forum, US Army War College, 4 November 2019. https://www.youtube.com/watch?v=tzawBWoduYA5rd
[11] Roger Z. George. *Intelligence in the National Security Enterprise.* (Washington, DC: Georgetown University Press, 2020) 8.
[12] Jervis, *Why Intelligence Fails,* 6.

© 2023 The Authors | CC BY-NC-ND 3.0 US

publication, "Policymakers say they need and want good intelligence. They do need it, but often they do not like it, and are prone to believe that when intelligence is not out to get them, it is incompetent."[13] What are the reasons for this friction? Intelligence is not provided in a vacuum, but rather into a context that is characterized by a range of factors, including ideological agendas and assumptions about the world, the tyranny of short time frames, the relationship of decisionmakers to risk, and personal characteristics.

Intelligence consumption escapes the bounds of idealized models and is compressed, complex, and *personal*. As scholar James Wirtz puts it: "Individuals' preferences and personalities influence outcomes, especially their response to information that threatens their organizational and personal priorities."[14] Further, the principal decisionmaker is not the only important actor at play in the dynamics of effective consumption, particularly in the case of senior leaders. Most decisionmakers are supported by staffs who are charged with gatekeeping, managing (and manipulating) schedules, and in other ways controlling the information that reaches their boss. The personal characteristics and interests of these staffs also come into play—some are themselves intellectually resistant to alternative courses of action, others soften news so as not to have to be its messenger, others edit, and still others refuse to provide bad news at all. These responses can be the outcome of fear, toxic leadership, professional incompetence, and bureaucratic incentive structures, on one hand, or even just the pursuit of efficiency in a tightly scheduled day, on the other.[15]

The dynamics that characterize staff activity are also a function of the institutional culture of a particular organization. Institutional culture can influence the use of language, the access one has to another individual, how open organizations are to new information, and how they deal with dissent. Further, culture can constrain the number of staff whose voices have the credibility to convey sometimes unwelcome or discordant information. Not mentioned in much of the literature is the interaction of different epistemic communities when it comes to the producer-consumer relationship. For the purposes of this discussion, to quote Peter Haas, "An epistemic community is a network of professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue-area."[16] Epistemic communities have shared norms, methodologies, and an understanding of what constitutes valid knowledge. Further, according to this authority, there is a common policy enterprise that the community shares and to which its efforts are oriented.[17]

There are high barriers to entry to these groups. Examples include communities that might focus on the environment, nuclear weapons control, or public health. Policymakers and intelligence communities could be considered two separate epistemic communities. The fact that analysts and decisionmakers often come from agencies with differing cultures, different norms, and different technical expertise can make a difference in the relationship. This is particularly the case in agencies that are culturally insular, such as the services, or the most dominant agencies, such as the CIA, which have strong internal institutional cultures, prestige within the national security apparatus, and institutional pride that is reinforced often through ceremony, symbols of exclusivity, and secrecy. An example from the author's own experience is the US Army, where knowledge introduced by non-uniformed experts is often not accepted or initially taken as seriously, thereby raising the question of what source of legitimacy the "outsider" must have to establish credibility and be effective in the

[13] Jervis, "Why Intelligence and Policymakers Clash, 185.

[14] James J. Wirtz, "Are Intelligence Failures Still Inevitable?" *International Journal of Intelligence and CounterIntelligence* (June 2023) 16; https://doi.org/10.1080/08850607.2023.2214328

[15] See Uri Bar-Joseph and Rose McDermott, *Intelligence Success and Failure: The Human Factor* (Oxford: Oxford University Press, 2017) for several case studies discussing these phenomena.

[16] Peter M. Haas, "Introduction: Epistemic Communities and International Policy Coordination," *International Organization* 46, No. 1 (Winter 1992): 1-35, here 3.

[17] Haas, 3.

© 2023 The Authors | CC BY-NC-ND 3.0 US

producer role. Other examples include the unwillingness of some agencies to engage with outside experts or external communities, leading to cultural and intellectual isolation.

The strength of these institutional cultures serves a purpose—providing cohesion to support the very difficult job they are expected to do—but it can also reject alternative thinking, leading to myopia, groupthink, and bureaucratic sclerosis. One could argue that some institutions are not as permeable because they are protecting their technical core from outside intervention. If this is the case, however, we must reconceptualize the relationship between the producer and the consumer more broadly, as the interaction of two wholly different expert communities, rather than focusing on the individual characteristics of each side of an interpersonal dyad.

The politicization of the producer-consumer relationship is the bogeyman of intelligence and emblematic of the asymmetric relationship. It reinforces the dominance of the consumer through varying levels of pressure on the producer. Politicization comes in many forms and is driven by issues such as the pressure of time, institutional pressure, emergency, surprise, agendas, ideology, ignorance, parochial thinking, and stove-piping. It can be as blatant as directing a particular outcome to support a policy agenda item, or as subtle as conveying quietly to an analyst that particular intelligence should be omitted from a briefing. Politicization is endemic, ambiguous, and extremely difficult to prove.[18]

Finally, intelligence failure is the *extremis* position of the producer-consumer relationship, and the study of the consumer's role in this dynamic cries out for increased nuance and depth. Assessments of failure frequently, one might even say normatively, get tangled in collection and analytical failures, usually leading to organizational reform, whereas the role of the consumer in receiving and responding appropriately to intelligence is understudied. This selection on the dependent variable problem of intelligence success and failure makes even-handed study complicated.

An important issue to assess in terms of failure is where, in fact, failure occurs in the decision cycle. While it is stated to the point of cliché that there are no intelligence successes but only intelligence failures and policy successes, a closer investigation of where the fault line exists can help an honest assessment of what change needs to occur. This phenomenon occurred publicly in the wake of the attacks on 9/11 when government officials, scholars, and pundits alike devoted extensive time to the dysfunctions and problems of the IC and much less on how decisionmakers reacted—or failed to react—to the intelligence that they had been provided. An interesting exercise to conduct with students who are military officers or intelligence professionals is to ask them to take an acknowledged intelligence failure—either a historical case study or a personal experience—and have them break down the decision process step by step. Their task is to discover where, in fact, the "failure" occurred. Usually, the process instigates a complete reassessment of what occurred and why, with consumer failure being the most common outcome.

When intelligence failures occur, there tends to be a focus on change, "reform," or "shifting the machinery" in Jervis's words—whereas, in actuality, a focus on the mechanical aspects of the intelligence function elides the responsibility of the decisionmaker.[19] The driving force behind this reform tends to be more performative than substantive, at least initially. The example of the aftermath of the attacks on 9/11 leap to mind, when public pressure deeply affected the policy outcome, driving the establishment of the institution of the Department of Homeland Security, Congress' enactment of the Intelligence Reform and Terrorism Prevention Act, the provisions of which included creation of the Director of National Intelligence and a supporting office, and the saturation of American society with security. "Policymakers also seem to believe

[18] Jervis, "Why Intelligence and Policymakers Clash," 202.
[19] Jervis, *Why Intelligence Fails*, 3.

© 2023 The Authors | CC BY-NC-ND 3.0 US

that the right reforms can in fact solve the problem of intelligence failure," Wirtz explained; "failures will no longer be inevitable if we identify what is wrong with intelligence."[20] While I do not argue that all of the blame rests with the policymakers, increased focus on the granularity of decisionmaking, iterative use of intelligence, and skills required to hone engagement could contribute to improved outcomes. Finally, to close our discussion of the asymmetric relationship and return to Jervis, "The grievances of the IC are several but less consequential because [the IC] has much less power than the intelligence consumers."[21]

The War in Ukraine and the Widening Aperture

First, to state the obvious, wartime decisionmaking is far different from decisions that are made in peace. Decision tradeoffs, speed, and urgency all are changed by a state of conflict. In terms of the producer-consumer relationship, the balance of power is recalibrated slightly in the direction of the producer. While the asymmetric relationship persists, the sheer number of players in the system increases drastically. The first stage of the Ukraine conflict was notable as the Biden administration used intelligence to "pre-bunk"—debunk the explanation put forward by the Russians prior to the attack—the Russian narrative on its pending invasion. This strategic declassification of intelligence introduced the public into the discourse as an additional consumer, while it also signaled to Russian President Vladimir Putin the intentions and capabilities of the United States.[22]

The aperture widened further as social media fueled the tracking of battlefield progress, enemy locations, and the order of battle. Civilians have used publicly available apps to collect information and forward it to analysts to be used in war. They have also generated and uploaded videos of Russian military activity to Telegram or TikTok. As David Gioe and Ken Stolworthy point out: "In a digitally connected context, everyone can be a sensor or intelligence collector, wittingly or *unwittingly*."[23] Reconnaissance drones have helped soldiers gather battlefield intelligence on crucial Russian targets and have helped the Ukrainian army monitor battlefield progress, allowing for collection at a very low price and in real time. The private sector has become actively engaged, with companies such as Maxar contributing imagery intelligence and Starlink providing internet access. After years of the discussion of the importance of open source intelligence, the war in Ukraine is demonstrating how valuable this source actually is. Complementing classified intelligence, it provides invaluable context from a range of sources and it can do so quickly.[24]

This is a just a brief overview of the use of technology and the "democratization of intelligence analysis" in the Ukraine war, but, overwhelmingly, this evidence points to the fact that the onus is increasingly on consumers to develop their own methods for screening, analysis, and comprehension.[25] The best consumers are already making progress toward this end by understanding and writing their own priorities, recognizing and appreciating the platforms that are available to them, and educating themselves and their staffs on which questions they should be asking. Even the best consumers, nevertheless, will be faced with rapidly changing technology, misinformation and disinformation, overwhelming flows of raw information, and an operational tempo that requires almost instantaneous decisionmaking.[26] The closeness of the producer-consumer

[20] Wirtz, 2.

[21] Jervis, "Why Intelligence and Policymakers Clash," 203.

[22] See Richard H. Immerman, "Trump to the Intelligence Community: You're fired," in *Chaos Reconsidered: The Liberal Order and the Future of International Politics*, ed. Robert Jervis, Diane N. Labrosse, Stacie E. Goddard, and Joshua Rovner (NY: Columbia University Press, 2023), 138-51.

[23] David V. Gioe and Ken Stolworthy, "Democratised and Declassified: The Era of Social Media War is Here" *Engelsberg Ideas*, October 24, 2022. Emphasis in original.

[24] See Amy Zegart's essay in this forum.

[25] Terminology borrowed from Gioe and Stolworthy, "Democratised and Declassified," 1.

[26] See Thomas Fingar essay in this forum.

© 2023 The Authors | CC BY-NC-ND 3.0 US

relationship that concerned Kent so deeply is rapidly growing closer. Arguably, at the same time, the shelter provided by institutional culture, bureaucratic processes, and gatekeeping staffs is growing less robust as decisions must occur at lower levels and with greater alacrity. Also, with these technological advances, what used to be secret is now increasingly public and available, thus enabling public pressure to influence decisionmaking. The producer no longer controls the story delivered to the consumer in this environment, but the consumer is no longer as empowered to ignore it either. A new balance in the asymmetric relationship must be struck.

Conclusions and Recommendations

The Russian-Ukraine war exemplifies how technology and intelligence are rapidly changing modern warfare, and how these shifts can alter the balance of the producer-consumer relationship toward greater equitability. I use this example because it demonstrates how exigency pushes the boundaries of established relationships and ways of thinking. There are several steps forward from this point. The entire national security enterprise should re-examine the dynamics of the asymmetric relationship and educate the consumer on how to effectively engage with intelligence.

A more holistic approach to intelligence should be developed to enable the new intelligence sources to integrate better with each other—this has been suggested in the discussions around the importance of open source intelligence.[27] Building the decisionmaker into the analytical discussion of the producer-consumer relationship raises several issues: education being one of them. Adjusting institutional priorities to incentivize using intelligence, providing instruction on the platforms used to collect intelligence, providing guidance on how to ask the right questions, and instructing how to establish a relationship that allows iteration and engagement are vital, as is breaking down the steps of the process and show the consumer how they impact it. Military leaders, in particular, tend to view intelligence as something immutable that is delivered to them twice daily. They need to understand that it is tailorable to their own needs if they take responsibility for it. Above all, they should break through the secrecy surrounding intelligence process and help consumers understand sourcing and methods (where appropriate). This will help consumers know what to expect of intelligence and where the limitations are.

If senior leaders from all arenas—the military, diplomacy, and technology—engage, the emphasis will trickle down through their organizations. Retired Army General Joseph Votel, who is widely known as an adept user of intelligence, conducted deep dives with his intelligence staff to make sure that he understood the issues thoroughly. This focus signals to the rest of the senior staff that intelligence is something to be included and valued. Major General Anthony Hale and Lieutenant General (retired) Karen Gibson, two senior Army intelligence professionals and leaders, also noted that their most engaged commanders would engage directly with the intelligence analyst to learn detail and ask questions.[28]

This engagement serves several purposes: it allows the decisionmaker to receive granular detail from the source, helps the analyst understand the decisionmakers' needs, and demonstrates that intelligence should viewed as a crucial part of the process, rather than an abstraction, spoiler, or support function. Further, in a longer-term project, leaders need to start building an awareness of the intelligence process that spans the

[27] See Biden Administration National Security Strategy, 2022, 46; Biden Administration National Intelligence Strategy, 2023, 5.

[28] Interviews with GEN (ret) Joseph Votel, 14 December, 2020; February 2, 2021. Interview with MG Anthony Hale, 15 May 2022. See LTG (ret) Karen Gibson, Strategy Forum, US Army War College, 4 November 2019. https://www.youtube.com/watch?v=tzawBWoduYA5rd for a wider discussion of the relationship between producers and consumers.

© 2023 The Authors | CC BY-NC-ND 3.0 US

boundaries between communities institutionally, rather than individually in the form of individual taskings and briefings.

Agencies should provide short courses to support the education of their consumers—these would be "intelligence for reading" courses, and they should be mandatory for all leaders. They would not be intended to create experts or specialists, but they would give decisionmakers are grounding in the fundamentals, much like courses on Congress and decisionmaking for newly elected members of Congress. As an example, across the Department of Defense, conversations are being held on how to counter near-peer competitor China and how to transition the force effectively to meet this need. While professional military education is adapting curricula to engage more thoroughly on China, not as much is being done to help military officers, diplomats, and other decisionmakers to become better consumers of intelligence. A reason for this is perhaps that intelligence is still considered a support function and not a core expertise by many. Another initiative to support intelligence consumption would be to educate leaders on the absorption of technology. It is often said that artificial intelligence will change everything; hyperbole and exaggeration aside, it will not if consumers do not understand how to use the tools effectively.

In conclusion this essay does something unusual; it does not recommend structural or organizational changes in order to "repair" or "reform" the relationship discussed above. Rather, it proposes a range of internal changes on the part of decisionmakers to better enable them to absorb and understand the intelligence that is provided for them. It also discusses the role of institutional culture and how the constraints built into it can both hinder and facilitate the effective use of new information. Robert Jervis, who was known among so many other things for introducing psychology into the study of political science, understood the importance of internal nuance when it comes to decisionmaking.[29] Scholars should follow in his footsteps and explore further how to dissect personal and institutional assumptions, understand the nuances and implications of success and failure in the intelligence sphere, and contribute to the crossing of the academic-practitioner divide that he did so adeptly.

[29] See Robert Jervis, *Perception and Misperception in International Politics* (Princeton: Princeton University Press, 1976).

© 2023 The Authors | CC BY-NC-ND 3.0 US

"Learning Lessons: Intelligence, 9/11, and the Failure of Imagination"
by Stephen Marrin, James Madison University

An appreciation of both the value and the limits of strategic intelligence in national security decisionmaking will enable the Intelligence Community (IC) to better position itself to support policy and prevent failures in the future. The purpose of strategic intelligence is to protect national security and advance national interests. Intelligence organizations increase the information that is available to decisionmakers and provide independent assessments that policymakers can use to improve their decisions. In theoretical terms, strategic intelligence is integral to the government's effort to acquire as accurate, reliable, and thorough information as possible. The absence of useful knowledge from the Intelligence Community at a time when a decision must be made to protect security or advance interests is frequently known as an intelligence failure. But even the provision of useful knowledge from the IC cannot on its own eliminate policy failures and associated costs. The reality is that knowledge—including that from intelligence—does not necessarily translate directly into effective action.

Robert Jervis effectively explored why intelligence fails through a set of historical case studies, using them to uncover general principles about why they happened and, even if they can't be eliminated, what can be done to prevent them on the margins.[1]

As Jervis has pointed out, intelligence assessments are used in decisionmaking less frequently than is conventionally understood.[2] One reason is that the information and knowledge received from intelligence organizations is frequently fragmentary and incomplete, and the assessments frequently increase uncertainty rather than decrease it.[3] In addition, other factors may inhibit effective policy response such as a limited range of policy options, or the knowledge that implementing a policy under conditions of uncertainty would result in guaranteed costs for uncertain benefits.[4]

This paper explores similar issues through a case study from 9/11 relating to the security concerns associated with suicide hijacking using aircraft as weapons. This case shows that the more significant problem was not the absence of useful intelligence but the ineffective aviation security policies that were being implemented at the time. In that context, more intelligence about the threat of suicide hijacking (other than details on the 9/11 terrorist plotters and plot itself) would likely not have helped prevent the terrorist attacks of 9/11. Instead, what was needed was improved integration of intelligence analysis into policymaking processes and improved policymaking more generally. The relationship between information, knowledge, and effective action is a challenging one, and good intelligence analysis does not always lead to good decisions.[5]

For that reason, when looking to the future, enhancing the performance of the Intelligence Community will require appreciating the limits of intelligence in both the big decisions that are related to the prevention of

---

[1] The most notable example is Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca, NY: Cornell University Press. 2010).

[2] Jervis "Why Intelligence and Policymakers Clash," *Political Science Quarterly* 125, no. 2 (Summer 2010): 185–204.

[3] For a discussion of this phenomenon, see page 730 in Stephen Marrin, "Why Strategic Intelligence Analysis has Limited Influence on American Foreign Policy," *Intelligence and National Security* 32:6 (2017): 725-742., DOI: https://doi.org/10.1080/02684527.2016.1275139

[4] Marrin, "The 9/11 Terrorist Attacks: A Failure of Policy Not Strategic Intelligence Analysis," *Intelligence and National Security* 26:2-3 (April-June 2011): 182-202, especially 201.

[5] For more on the limitations of intelligence in national security policymaking, see: Richard H. Immerman, "Intelligence and Strategy: Historicizing Psychology, Policy and Politics," *Diplomatic History* 32:1 (January 2008): 1-23).

© 2023 The Authors | CC BY-NC-ND 3.0 US

strategic surprise as well as other aspects of security related policy implementation. Improving the production of strategic intelligence in the future requires working with—rather than against—the reality of the relationship between information, knowledge, and policy making by working to better integrate intelligence analysis into policymaking.

Intelligence Analysis, 9/11, and the Failure of Imagination

In terms of the Intelligence Community's performance, the 9/11 Commission Report's emphasis on the IC's failure to assess the risk of suicide hijacking and using "aircraft as weapons"[6] is widely considered to be a "failure of imagination."[7]

The phrase "failure of imagination," however, has been widely misinterpreted by the general public, the media, and scholars. The Report does not say that no one imagined the possibility of the use of aircraft as weapons. As it observes, "the possibility of a suicide hijacking (of an aircraft)…was imaginable, and imagined."[8] The Report then goes on to cite specific examples where this scenario was raised and considered, and concludes by saying that "we can therefore establish that at least some government agencies were concerned about the hijacking danger and had speculated about various scenarios."[9] So the "failure of imagination" was not at the level of the individual analyst or even individual agency.

Instead, the authors of the Report intend the phrase "failure of imagination" to describe a failure of the system as a whole. This is why the recommendations for improving imagination address its "institutionalization" rather than fostering it on an individual level. As the 9/11 Commission Report reads, the problem was not with the creation of scenarios that included aircraft as weapons. Rather "the challenge was to flesh out and test those scenarios, then figure out a way to turn a scenario into constructive action."[10] As a result, the 9/11 Commission Report did not recommend increasing individual imagination through various forms of alternative analysis but by "institutionalizing imagination" by finding ways "of routinizing, even bureaucratizing, the exercise of imagination."[11]

The process the 9/11 Commission Report described for institutionalizing imagination within the IC is that of classic indications and warning, or I&W.[12] I&W is a process used to warn about potential bad outcomes. As the Defense Department has described, the steps are to "1) Identify anomalies/imagine alternatives 2) Produce scenarios 3) Identify conditions, drivers, and indicators 4) Determine warning threshold 5) Explore opportunities to influence or mitigate the threat 6) Communicate warning."[13]

---

[6] The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. (NY: W.W. Norton & Company). 2004. 344. Further identified as the 9/11 Commission Report.

[7] According to the 9/11 Commission Report, this phrase is originally attributable to Paul Wolfowitz, the Deputy Secretary of Defense in a memo to Secretary of Defense Donald Rumsfeld on Sept 18, 2001. Page 336.

[8] 9/11 Commission Report, 345.

[9] 9/11 Commission Report, 345.

[10] 9/11 Commission Report, 346.

[11] 9/11 Commission Report, 344.

[12] This process is described on pages 346-347 of the 9/11 Commission Report.

[13] Joint Chiefs of Staff. "Joint Staff J2. Defense Warning Staff. J2 Warning." Defense Warning Network Handbook. 4th ed. As cited in Bilyana Lilly et al., "Applying Indications and Warning Frameworks to Cyber Incidents," in 2019 11th International Conference on Cyber Conflict (CyCon). IEEE. (1–21). 8

© 2023 The Authors | CC BY-NC-ND 3.0 US

In applying the I&W framework to the institutionalization of imagination in the case of aircraft as weapons, the 9/11 Commission Report specifies that

> Since the Pearl Harbor attack of 1941, the IC has devoted generations of effort to understanding the problem of forestalling a surprise attack. Rigorous analytic methods were developed….These methods have been articulated in many ways, but almost all seem to have at least four elements in common: (1) think about how surprise attacks might be launched; (2) identify telltale indicators connected to the most dangerous possibilities; (3) where feasible, collect intelligence on these indicators; and (4) adopt defenses to deflect the most dangerous possibilities or at least trigger an earlier warning.[14]

After establishing the goal as a process approximating I&W, the 9/11 Commission Report concluded that, with some exceptions, CIA intelligence analysts failed to "regularly" analyze the threat using I&W, and that for that reason their intelligence analysis was deficient.[15] It says that "the CTC (Counterterrorism Center) did not analyze how an aircraft, hijacked or explosives laden, might be used as a weapon," nor did it "develop a set of telltale indicators for this method of attack," or monitor this set of indicators.[16] The Report goes on to say that "if it had done so, we believe such an analysis would soon have spotlighted a critical constraint for the terrorists" and provided a specific set of indicators as requirements for the various collection systems.[17]

Implicit in this critique of the analytic process is that 9/11 might have been prevented if only this procedure had been implemented. Unfortunately, the reality is that knowledge (in this case, intelligence) does not necessarily translate directly into effective action.

Concern about Suicide Hijacking using Aircraft as Weapons

The scenario of a suicide hijacking using aircraft as weapons was one of many that some national security officials had been concerned about for years prior to 2001. According to Daniel Benjamin and Steven Simon, two National Security Council staffers who were responsible for coordinating counterterrorism policy during the Clinton administration, in 1996 Richard Clarke, the then-coordinator of counterterrorism policy, "was worried about an airplane carrying out a suicide attack on the stadium or releasing a chemical or biological weapon" at the 1996 Olympics in Atlanta, Georgia.[18] Clarke says that he was concerned about the possibility that someone might blow up an airplane over the Olympic Stadium or fly one into it.[19] There were also additional concerns about the possibility of a plane crashing into a foreign location "where the president would be."[20]

In 1996, President Clinton announced new policies to enhance aviation security and the creation of a Commission on Aviation Safety and Security,[21] but these measures may have been inadequate. As Clarke

---

[14] 9/11 Commission Report, 346.

[15] 9/11 Commission Report, 346.

[16] 9/11 Commission Report, 347

[17] 9/11 Commission Report, 347

[18] Daniel Benjamin and Steven Simon, *The Age of Sacred Terror* (New York: Random House Trade Paperbacks, 2003), 249.

[19] Richard A. Clarke, *Against All Enemies: Inside America's War on Terror* (New York: Free Press, 2004), 106. The 9/11 Commission Report also cites Clarke's concerns and attributes them to his general awareness of the threat as per a "Tom Clancy" novel rather than specific warnings from the Intelligence Community. 9/11 Commission Report, 347

[20] Benjamin and Simon, *The Age of Sacred Terror*, 341.

[21] Clarke, *Against All Enemies,* 123

© 2023 The Authors | CC BY-NC-ND 3.0 US

observes, "the events of 1996…had not provided the political circumstances needed for the massive change in how the federal government performed aviation security."[22] He goes on to write that "the idea of aircraft attacking in Washington seemed remote to many people and the risks of shooting down aircraft in a city were thought to be far too high. Moreover, the opponents of our plan argued, the Air Force could always scramble fighter aircraft to protect Washington if there were a problem."[23] The 9/11 Commission Report observes that after 1996 Clarke remained "concerned about the danger posed by aircraft."[24]

The 9/11 Commission Report also describes efforts implemented between 1996 and 2001 to address the threat of terrorist attacks on civilian aircraft.[25] Specifically, "after the 1999–2000 millennium alerts …Clarke held a meeting of his Counterterrorism and Security Group (CSG) devoted largely to the possibility of a possible airplane hijacking by al Qaeda."[26] Since "the CSG (included) other agencies such as the Federal Aviation Administration (FAA) as the subject matter required,"[27] this coordinative body provided a mechanism for ensuring that the appropriate agency—in this case the FAA—knew about the threat and was addressing it appropriately.

In terms of civil aviation, before 9/11 the FAA was responsible for ensuring "the safety and security of U.S. civil aviation."[28] The FAA was also responsible for "promoting the civil aviation industry,"[29] however, which meant that its own internal goals conflicted when it came to the establishment of security measures that could cost air travelers money, time, or convenience.

For years prior to 9/11, the FAA and the aviation industry had received warnings about the potential threat of terrorism and were aware of the industry's own vulnerabilities.[30] According to the 9/11 Commission Report, a "1994 FAA assessment of the threat to civil aviation in the United States stated that "system vulnerabilities also exist with respect to hijackings…aircraft can be hijacked with either fake weapons or hoax explosive devices. Cabin crew or passengers can also be threatened with objects such as short blade knives, which are allowable on board aircraft."[31]

Then, former National Intelligence Officer (NIO) Paul Pillar observes that in response to the 1995 National Intelligence Estimate (NIE) titled "The Foreign Terrorist Threat In the United States," which included warnings about the terrorist threat to civil aviation, "senior representatives of the aviation industry" were briefed on the terrorist threat in order to "persuade the industry that the terrorist threat required that the security of civil aviation to be strengthened."[32]

---

[22] Clarke, *Against All Enemies,*130-131

[23] Clarke, *Against All Enemies,*131

[24] 9/11 Commission Report, 347

[25] Because the first step in any suicide hijacking is to hijack the airplane, efforts to prevent airplane hijackings should also apply to suicide hijackings.

[26] 9/11 Commission Report, 345.

[27] Paul R. Pillar, "Good Literature and Bad History: The 9/11 Commission's Tale of Strategic Intelligence." *Intelligence & National Security* (December 2006) 21:6: 1022 – 1044, especially 1028.

[28] 9/11 Commission Report, 82.

[29] 9/11 Commission Report, 82.

[30] For a history of security threats to the civil aviation industry in the 1970s, see: Silke Zoller, *To Deter and Punish: Global Collaboration Against Terrorism in the 1970s* (NY; Columbia University Press, 2021).

[31] 9/11 Commission Report, 476, citing FAA report, "The Threat to U.S. Civil Aviation in the United States," Sept. 1994.

[32] Pillar, "A Scapegoat Is Not a Solution," *New York Times*, June 4, 2004. See also Pillar, "Good Literature," 1029

© 2023 The Authors | CC BY-NC-ND 3.0 US

In addition, in 1996 the White House Commission on Aviation Safety and Security, chaired by Vice President Al Gore, pointed out that intelligence agencies "have been warning that the threat of terrorism is changing." The report went on to stress that the danger was "no longer just an overseas threat from foreign terrorists. People and places in the United States have joined the list of targets."[33]

By the late 1990s, knowledge of this threat was focused on al Qaeda specifically. A 9/11 Commission staff statement observes that before 9/11 "the potential threat of Middle Eastern terrorist groups to civil aviation security was acknowledged in many different official FAA documents" and that "the threat posed by Usama Bin Ladin, al Qaeda, and al Qaeda affiliates, including their interest in civil aviation, was well known to key civil aviation security officials."[34] The FAA was even aware of "the possibility of suicide hijackings" but discounted it because there was "no indication that any group is currently thinking in that direction."[35]

So the relevant decisionmakers at the FAA, the people who were responsible for the security of US civil aviation, were fully aware of the threat and vulnerabilities. What did they do about it? Did they tighten security? Implement new security measures? Task intelligence agencies to be especially alert for the threat to civilian aviation, which would have led to the implementation of an indications and warning process? Did they implement the warning processes that the 9/11 Commission Report highlighted?

Effective Action Not Taken

As it turns out, the FAA did very little of any of the above. For the most part, the air security sector was reactive rather than proactive in terms of threat response. As the 9/11 Commission Report observes, "Historically, decisive security action took place only after a disaster had occurred or a specific plot had been discovered."[36] In the absence of that disaster or specific plot, the general assumption was that security measures were working, so no additional changes needed to be made to policy.

This is a variation on the theme consistently found in evaluations of policy failure; that prior success can lead to complacency, and complacency can pave the way for the subsequent failure. According to the 9/11 Commission Report, the FAA believed "that domestic hijacking was in check—a view held confidently as no terrorist had hijacked a U.S. commercial aircraft anywhere in the world since 1986."[37] A 9/11 Commission staff study pointed out that "this explains, in part, the view of one transportation security official who testified to the Commission that the agency thought it had won the battle against hijacking."[38]

If decisionmakers were interested in an active defense against threats, they could have established the kind of I&W process that the 9/11 Commission suggests would have been necessary to identify the specifics of the

[33] George Tenet with Bill Harlow, *At the Center of the Storm: My Years at the CIA* (New York: Harper Collins, 2007), 104. While the 9/11 Commission Report observes that the Gore Commission's report "focused mainly on the danger of placing bombs onto aircraft" rather than "suicide hijackings or the use of aircraft as weapons" (see 9/11 Commission Report, 344), many security measures to address one would have worked to address the other.

[34] 9/11 Commission Staff Statement No. 3: The Aviation Security System and the 9/11 Attacks, Page 4. https://govinfo.library.unt.edu/911/staff_statements/staff_statement_3.pdf.

[35] 9/11 Commission Report, 264

[36] 9/11 Commission Report, 83

[37] 9/11 Commission Report, 85

[38] 9/11 Commission Staff Statement No. 3: The Aviation Security System and the 9/11 Attacks. Page 7. This comment was not repeated in the 9/11 Commission Report.

© 2023 The Authors | CC BY-NC-ND 3.0 US

9/11 plot. In fact, the originators of the phrase "institutionalization of imagination" did not intend to limit the process solely to intelligence agencies.[39]

In 2003 former NSC staffers Benjamin and Simon argued that decisionmakers should be "institutionalizing imaginativeness" as part of what is required "to limit the frequency and scale of the surprises that await us."[40] They attribute this phrase to Dennis Gormley, who was then a faculty member at the University of Pittsburgh after more than ten years of government service earlier in his career, who in 2002 argued that the 9/11 attacks were more a failure of "strategic imagination" or "strategic analysis" than intelligence because both intelligence analysts and decisionmakers had failed to focus on new or different ways that a terrorist attack might take place.[41]

Gormley suggests that "avoiding surprise and being prepared to cope with its consequences require a much more systematic approach to examining a broad range of threats," and as a result decisionmakers should ensure that their evaluative process includes "institutionalizing imaginativeness" through investment in and institutionalization of "systematic consideration of adversary strategies and attack options."[42]

Gormley, then, attributes failure of imagination—even the kind of imagination required for threat assessment—to the level of the decisionmaker. The reason is that intelligence collection and priorities are linked to decisionmaker interests. Decisionmaker interest in an outcome—such as knowing more about a particular threat geared at a known vulnerability—would then drive the intelligence collection and analysis process. But officials in the FAA were more reactive than proactive in terms of aviation security.

Even tactical warnings frequently led only to an ineffectual sort of responsiveness on the part of decision makers. For example, during the summer of 2001 many intelligence alerts were issued, but this did not lead to greatly improved aviation security. According to then-Director of Central Intelligence George Tenet, "between April 1, 2001, and September 11, 2001, as many as 105 daily intelligence summaries were produced by the FAA for airline industry leaders. These reports were based on information received from the Intelligence Community. Almost half of these mentioned al-Qaeda, its leader Osama bin Ladin, or both."[43] This led the FAA to contact "every airline and airport" to increase their alert status. [44] The agency also conducted many "special security briefings for specific air carriers."[45] The Report goes on to observe that "although the FAA had authority to issue security directives mandating new security procedures, none of the few that were released during the summer of 2001 increased security at checkpoints or on board aircraft. The information circulars mostly urged air carriers to "exercise prudence" and be alert."[46] The bottom line is that despite these warnings, "no new security measures were instituted."[47]

The reason that "no new security measures were instituted" is simple: the cost. According to the Inspector General of the Department of Transportation, "there were great pressures from the air carriers to control

[39] The 9/11 Commission Report also applied the phrase to the creation of policy options, but the general interpretation of the term in the wider discussions has been to focus on how imagination plays out in an intelligence context.

[40] Benjamin and Simon, *The Age of Sacred Terror,* 401

[41] Dennis Gormley, "Enriching Expectations: 11 September's Lessons for Missile Defense," *Survival* 44: 2 (Summer 2002): 19–35.

[42] Gormley, "Enriching Expectations," 29-31.

[43] Tenet, *At the Center of the Storm*, 105

[44] Benjamin and Simon, *The Age of Sacred Terror,*342

[45] 9/11 Commission Report, 264

[46] 9/11 Commission Report 264

[47] 9/11 Commission Report, 264

© 2023 The Authors | CC BY-NC-ND 3.0 US

security costs and to 'limit the impact of security requirements on aviation operations'."[48] According to Pillar, the Intelligence Community's warnings "were evidently insufficient to overcome the industry's resistance to expensive new security measures."[49] He later observed that "no amount of warning would have generated support for a major expansion of aviation security measures, which were quickly adopted after 9/11 but which the aviation industry had successfully resisted (because of the cost) for years."[50]

Even more problematic, the FAA—which "set and enforced aviation security rules (that) were supposed to produce a "layered" system of defense"[51]—did not ensure that the airline industry implemented them effectively. The 9/11 Commission Report concluded that "each layer relevant to hijackings—intelligence, passenger prescreening, checkpoint screening, and onboard security—was seriously flawed prior to 9/11."[52] It goes on to assert that "the FAA's capabilities to take aggressive, anticipatory security measures were especially weak. Any serious policy examination of a suicide hijacking scenario, critiquing each of the layers of the security system, could have suggested changes to fix glaring vulnerabilities."[53] But the FAA did not do so, as the Report goes on to say, because government agencies "are often passive, accepting what are viewed as givens, including that efforts to identify and fix glaring vulnerabilities to dangerous threats would be too costly, too controversial, or too disruptive."

In the aggregate, this is a policy failure; a failure to ensure that the security system was effective in preventing terrorist attacks or hijackings. Despite many warnings, and concern on the part of security officials for years before 9/11, the FAA did not take the steps necessary to ensure aviation security.

Improving the IC's I&W Analysis Would Not Have Prevented 9/11

In this context, the 9/11 Commission's implicit counterfactual that is related to enhancing the institutionalization of imagination in the Intelligence Community—particularly its emphasis on the specific mode of suicide hijacking rather than the terrorist threat against civil aviation writ large—appears to accurately critique the IC for its failure to implement an effective indications and warning process. Nevertheless, absent the acquisition of information on the 9/11 hijackers themselves, improved analysis would not have accomplished much given the weaknesses in the performance of the appropriate policy departments.

If specific information about a plot to hijack civilian aircraft and crash them into buildings had been uncovered by the Intelligence Community as a result of an improved indications and warning process, the resulting intelligence analysis might have proved useful to decisionmakers. This kind of granular or tactical information has utility for government agencies such as the Justice Department or the Defense Department, and they might have been able to make use of it.

Without this level of precise, "actionable" intelligence on the actual 9/11 plot, however, there is nothing to suggest that improved intelligence analysis would have led to a more effective policy response. Specific warnings drawn from indicators that are derived from the potential for suicide hijackings would likely have fallen into the same ineffective security process, and—except for enhanced warnings to airlines—then disappeared. This is because there was a serious disconnect between the FAA's intelligence production unit

[48] 9/11 Commission Report, 84-85
[49] Pillar, "A Scapegoat Is Not a Solution."
[50] Pillar, "Good Literature," 1038
[51] 9/11 Commission Report 83
[52] 9/11 Commission Report, 83
[53] 9/11 Commission Report, 352

© 2023 The Authors | CC BY-NC-ND 3.0 US

and their administrators. According to the 9/11 Commission Report, "the FAA's intelligence unit did not receive much attention from the agency's leadership. Neither Administrator Jane Garvey nor her deputy routinely reviewed daily intelligence, and what they did see was screened for them. She was unaware of a great amount of hijacking threat information from her own intelligence unit, which, in turn, was not deeply involved in the agency's policymaking process."[54] This highlights the reality of the challenging relationship between information, knowledge, and policymaking; even though information about the threat was available, it wasn't effectively integrated into policymaking processes.

Even if the Intelligence Community had implemented a more effective analytic process regarding the potential threat from suicide hijackers, it does not appear that the relevant policymakers were ready, willing, or able to implement effective security measures. As for the NSC's CSG, even if this kind of intelligence analysis had been provided to it, Clarke explained, "warning about the possibility of a suicide hijacking would have been just one more speculative theory among many, hard to spot since the volume of warnings of "al Qaeda threats and other terrorist threats, was in the tens of thousands—probably hundreds of thousands."[55] While Clarke recognized the prospect for suicide hijackings, the 9/11 Commission reports that he "did not, or could not, press the government to work on the systemic issues of how to strengthen the layered security defenses to protect aircraft against hijackings or put the adequacy of air defenses against suicide hijackers on the national policy agenda."[56]

In other words, while intelligence analysts may have failed to focus on and highlight a particular kind of weapons platform—the threat of attack from civilian aircraft, a bigger and more important issue relates to the failure of decisionmakers to respond to the warnings that were provided.

Looking to the Future

Learning the lessons of intelligence, 9/11, and the failures of imagination means being aware of and working with, rather than against, the limitations that information or knowledge can have on policy making and policy implementation. In short, good intelligence analysis does not always lead to good policy, but perhaps with that knowledge the Intelligence Community can lean forward and look for opportunities to better support policymaking.

The case study flags the key issues. First, the 9/11 Commission Report accurately critiques the Intelligence Community for failing to implement "the methods for detecting and then warning of surprise attack that the U.S. government had so painstakingly developed in the decades after Pearl Harbor."[57] This is based on the presumption that better analysis should lead to better policy.

In the context of an ineffective policy environment, however, it is not clear what improved warning would have accomplished. Decisionmakers were aware of the threat and were either unable or unwilling to implement effective policies that would have addressed it. As a result, improving intelligence analysis may be necessary to improve the information and knowledge provided to policymakers, but it is not sufficient on its own for producing improved or effective policies.

[54] 9/11 Commission Report; 83
[55] 9/11 Commission Report, 345
[56] 9/11 Commission Report, 347
[57] 9/11 Commission Report, 347-348

© 2023 The Authors | CC BY-NC-ND 3.0 US

This poses a challenge for the Intelligence Community and its support of policymaking. More and better intelligence is better than less and worse intelligence. Still, intelligence on its own is not sufficient to prevent costly national security outcomes.

So what can the IC do? It can study the policymaking processes that it supports. As I have argued elsewhere,

> [I]t appears that the influence that intelligence analysis has on decisionmaking depends on the decisionmakers, the resources available to them, the policy options they consider, and the political context that shapes the process. To understand the failure of decisionmakers to respond effectively to early warning…one must start with the policy environment at the time rather than the adequacy or sufficiency of the intelligence that they were provided with. One cannot understand the influence, or lack of influence, of intelligence analysis on policy by studying intelligence. Instead, one must study policy.[58]

And so must the Intelligence Community in the future as well in order to fulfill its function most effectively. With added insight on the limitations in the policy process, perhaps the IC can improve its warning function by implementing the kinds of processes the 9/11 Commission recommended. It then could ensure that the analysis permeates through the policy community. It could work to get its analysis as close as possible to the policymaking processes and policymakers themselves, so that there is awareness of both threat and vulnerability. It could work to integrate knowledge with action more effectively.[59] It will not be able to provide perfect information, but perhaps in doing so it can identify opportunities to engage in the policymaking process more effectively.

[58] Marrin, "The 9/11 Terrorist Attacks: A Failure of Policy Not Strategic Intelligence Analysis," 202.

[59] See recommendations for bringing intelligence and policy closer together in the conclusion to Marrin "Why strategic intelligence analysis has limited influence on American foreign policy."

© 2023 The Authors | CC BY-NC-ND 3.0 US

"Intelligence Transformation for the Technology Age" by Amy Zegart, Stanford University

Today, American intelligence agencies face two tectonic shifts: China's rise and the convergence of emerging technologies.[1] The two are intertwined but they are not the same. On the one hand, China is widely considered to be the "pacing challenge," as the 2022 National Defense Strategy put it.[2] Successfully managing the strategic rivalry with China has become the primary focus of policymakers in both the executive and legislative branches and one of the few issues garnering a strong bipartisan consensus in Washington. In many ways, Beijing poses the classic Thucydides's trap: a rising power with growing ambitions whose interests increasingly conflict with ours.[3] To be sure, understanding China's capabilities, intentions, and the dynamics of this evolving competition is no small task. But generally speaking, it does not require fundamental changes to how US spy agencies approach their mission. Great power competition with a nuclear-armed rival is a movie that intelligence agencies have seen before.

Emerging technologies are a different story. They pose novel challenges that require more wholesale reforms to nearly every aspect of the intelligence enterprise. Internet connectivity, Artificial Intelligence (AI), the proliferation of commercial satellite capabilities, and other technologies are not just transforming the future. They are revolutionizing the business of understanding the future. Where does insight come from? Who provides intelligence? Who should receive intelligence to advance the national interest? Answers to these questions are radically different today than they were a decade ago. And they are crucial for dealing with every aspect of the threat landscape, not just dangers arising from Beijing. Intelligence has always been a hard business, but it has never been this hard.

This essay examines how the US Intelligence Community (IC) can adapt to the technology age with an eye toward a crucial question: how much does money matter? If bigger intelligence budgets clearly produced better outcomes, then reforming US intelligence agencies for the twenty-first century would be a relatively straightforward endeavor of assessing tradeoffs between spending priorities. But if the United States cannot spend its way to meaningful intelligence improvement, the future of the IC and its ability to deliver a decision advantage to policymakers looks more problematic.

Nobody really knows the relationship between spending and intelligence effectiveness, but this essay argues that it is probably less than we think. Consider this: Evidence clearly shows that the US Intelligence Community failed to adapt to the rising terrorist threat in the 1990s, when intelligence budgets were cut

---

[1] Earlier versions of this essay appeared as Amy Zegart, "I Spy a Problem: Transforming US Intelligence Agencies for the Technological Age," in Michael J. Boskin, John N. Rader and Kiran Sridhar, eds., *Defense Budgeting for a Safer World: The Experts Speak* (Stanford, Calif.: Hoover Institution Press, 2023); and Amy B. Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," *Foreign Affairs* 102, no. 1 (January/February 2023): 54–71. The H-Diplo|RJISSF editors and the author thank the respective editors for granting us permission to publish this essay here.

[2] US Department of Defense, 2022 National Defense Strategy, 4. Director of National Intelligence Avril Haines similarly noted in the 2023 world threat hearing held by the Senate Select Committee on Intelligence "…needless to say, the People's Republic of China—which is increasingly challenging the United States economically, technologically, politically, and militarily around the world—remains our unparalleled priority. The Chinese Communist Party, or CCP, under President Xi Jinping will continue efforts to achieve Xi's vision of making China the preeminent power in East Asia and a major power on the world stage." DNI Haines Opening Statement of the 2023 Annual Threat Assessment of the US Intelligence Community," March 8, 2023, available at: https://www.dni.gov/index.php/newsroom/congressional-testimonies/congressional-testimonies-2023/3685-dni-haines-opening-statement-on-the-2023-annual-threat-assessment-of-the-u-s-intelligence-community (accessed June 26, 2023).

[3] Graham Allison, *Destined for War: Can America and China Escape Thucydides's Trap?* (New York, NY: Houghton Mifflin Harcourt, 2017).

© 2023 The Authors | CC BY-NC-ND 3.0 US

dramatically after the Cold War. Yet the IC is also struggling to adapt to the technological age today, when intelligence budgets have never been higher. When budget scarcity and abundance both lead to the same suboptimal outcome, something more systematic is probably at work. Its name is organizational pathologies. To be sure, higher spending certainly helps shift intelligence priorities and deliver new capabilities. And reduced spending can hurt. But I find that organizational features of intelligence agencies are silent and deadly killers of innovation. Agency structures, cultures, and career incentives critically shape what is valued, what gets done, and how well. Unless these organizational features are aligned more rapidly to the threat landscape, intelligence agencies will struggle, no matter how much funding they have. And intelligence failures will be more likely.

Part one of this essay starts with a cautionary note about the difficulties of analyzing the relationship between intelligence spending and performance outcomes, offers a broad overview of declassified intelligence budgets over time, and examines how organizational weaknesses were the root cause of intelligence failures leading to 9/11. Part two examines how in a range of policy areas—from health care and K–12 education to defense—greater spending is not producing better results. Part three turns to intelligence, arguing that despite record government spending, US spy agencies are losing their relative advantage today. Thanks to the rise of emerging technologies and the explosion of data, intelligence is not just for superpower spy agencies anymore. Part four concludes with a discussion of what can be done, starting with the creation of a new dedicated open-source intelligence agency.

Breadcrumbs and Budgets

Studying anything in intelligence is tricky business because the public record is so incomplete. It is hard to identify the causal factors that lead to success or failure when failures are often public but successes are often secret.

The impact of budgeting decisions is especially challenging. Intelligence spending is so highly classified that until 2007, with rare exceptions, even the topline total intelligence budget remained secret.[4] As a result, for years, expert analysts have estimated intelligence spending over time based on breadcrumbs of data from declassified reports and remarks by government officials.[5]

Since 2007, the US government has released annually the total intelligence spending in two major categories. These are the National Intelligence Program (NIP), which covers the programs, projects, and activities of the

[4] "US Intelligence Community Budget," Office of the Director of National Intelligence, https://www.dni.gov/index.php/what-we-do/ic-budget (accessed December 7, 2022); Director of Central Intelligence George Tenet released the FY1997 and FY1998 total intelligence budgets after Steven Aftergood from the Federation of American Scientists filed a Freedom of Information Act lawsuit, but Tenet then reversed course in FY1999. Subsequent toplines remained classified until 2007, when Congress mandated that the Director of National Intelligence disclose "the aggregate amount of funds appropriated by Congress" for the National Intelligence Program in Section 601 of the Implementing Recommendations of the 9/11 Commission Act (Public Law 110-53). Freedom of Information Act requests have produced some agency-level budget justification documents but these are heavily redacted. See also Steven Aftergood, "CIA Discloses FY 1998 Intelligence Budget Total," press release, Federation of American Scientists, March 20, 1998, https://sgp.fas.org/foia/intel98.html#:~:text=CIA%20Discloses%20FY%201998%20Intelligence,Year%201998%20is%20%2426.7%20billion.; Brian Clampitt, " US Intelligence Budget Request Revealed," Harvard National Security Journal, February 23, 2011; "Intelligence Budget Data," Federation of American Scientists, accessed, https://irp.fas.org/budget (accessed December 7, 2022).

[5] Marshall C. Erwin and Amy Belasco, "Intelligence Spending and Appropriations: Issues for Congress," Congressional Research Service, R42061, September 18, 2013, 5.

© 2023 The Authors | CC BY-NC-ND 3.0 US

Intelligence Community; and the Military Intelligence Program (MIP), which covers the intelligence activities of military departments and agencies in the Defense Department that support tactical US military operations. In FY 2022, the NIP was $65.7 billion, and the MIP was $24.1 billion, for a total intelligence budget of $89.8 billion.[6] Yet even this aggregate figure is incomplete. It excludes other specific intelligence-gathering programs in cabinet departments and agencies (such as Homeland Security) as well as military programs that include intelligence but have a different primary purpose—such as the MQ-9 Reaper unmanned aerial strike platform.[7]

More importantly, declassified intelligence budgets do not provide meaningful data to assess whether the eighteen agencies of the US Intelligence Community are deploying their resources against the right priorities, particularly as the threat landscape changes.[8] How much does the US government spend per intelligence agency, activity, or capability? How much is spent on understanding and countering nation-state actors like China and Russia versus transnational terrorists, the proliferation of weapons of mass destruction, or cyber threats? Is the IC dedicating sufficient resources to attracting and retaining the right STEM talent?[9] Without a security clearance, it's impossible to know.[10] Even with a security clearance, it may be impossible. The Defense Department houses nine of the eighteen agencies constituting the US Intelligence Community and consumes the vast majority of the total intelligence budget, yet it has never yet passed an independent audit that accounts for how it spends its money.[11]

Here is what we do know: in broad-brush terms, spending for US intelligence increased significantly during the Cold War, declined by approximately 20 percent during the 1990s, and skyrocketed after 9/11. Figure 1 is an unclassified chart released by a 1994 Senate Report showing spending trends from 1965 to 1994 (note all actual numbers were omitted). The Senate report describes Cold War spending as experiencing "tremendous real growth" over thirty years.

---

[6] "US Intelligence Community Budget."

[7] Anne Daugherty Miles, Michael E. DeVine, and Sofia Plagakis, "Intelligence Community Spending Trends," Congressional Research Service, Report R4481, Version 16, January 9, 2023, 1–2, https://crsreports.congress.gov/product/pdf/R/R44381.

[8] The eighteen agencies of US Intelligence Community are: The Office of the Director of National Intelligence; the Central Intelligence Agency; nine Department of Defense elements (the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and intelligence elements of the Army, Navy, Marine Corps, Air Force, and Space Force); and seven elements of other departments and agencies (the Department of Energy's Office of Intelligence and Counter-Intelligence; the Department of Homeland Security's Office of Intelligence and Analysis and US Coast Guard Intelligence; the Department of Justice's Federal Bureau of Investigation and Drug Enforcement Administration's Office of National Security Intelligence; the Department of State's Bureau of Intelligence and Research; and the Department of the Treasury's Office of Intelligence and Analysis). See Office of the Director of National Intelligence, "Members of the IC," https://www.dni.gov/index.php/what-we-do/members-of-the-ic.

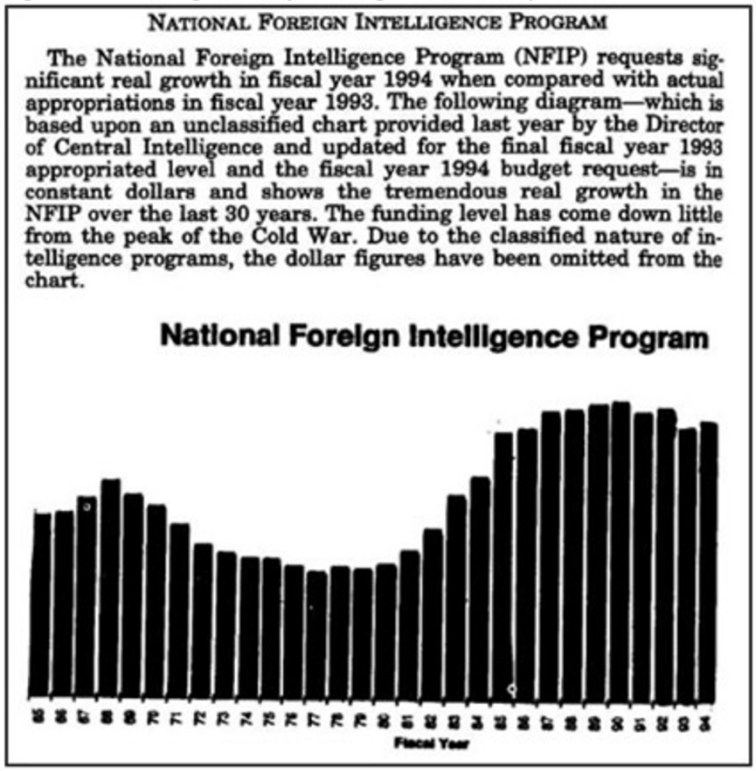
[9] STEM is the acronym for science, technology, engineering, and math.

[10] There are, of course, good national security reasons for not making this kind of information publicly available. My point is that analyzing the efficiency or effectiveness of intelligence spending, especially from the outside, is an exercise in speculation. Humility is in order.

[11] Government Accountability Office, "Financial Management: DOD Needs to Improve System of Oversight," GAO-23-104539, March 2023. See also *New York Times* editorial board, "The Pentagon Doesn't Know Where its Money Goes," December 1, 2018; and Bill Chappell, "The Pentagon Has Never Passed an Audit. Some Senators Want to Change That," *National Public Radio*, May 19, 2021.

© 2023 The Authors | CC BY-NC-ND 3.0 US

Figure 1: Intelligence Spending, 1965–94 (in 1994 constant US dollars)



Source: H Rept. 103-254, Department of Defense Appropriations Bill, 1994, to accompany H.R. 3116, reproduced in Michael E. DeVine, "Intelligence Community Spending: Trends and Issues," Congressional Research Service Report R44381, updated June 18, 2018, 14.

The Soviet Union's collapse in 1991 brought dramatic reductions to intelligence and defense budgets, which lawmakers dubbed the "peace dividend."[12] Some, including Senator Daniel Patrick Moynihan, argued that the CIA should be abolished because it was no longer needed, useless, and violated the American ideal of transparency. According to former Director of National Intelligence James R. Clapper, in the 1990s the IC experienced a 23 percent budget reduction, creating a "damaging downward spiral."[13] Director of Central Intelligence George Tenet told the 9/11 Commission that during the 1990s, the entire IC lost 25 percent of its workforce, the CIA suffered a 16 percent workforce decline, and the agency's budget declined by 18 percent in real terms. "This loss of manpower was devastating," noted Tenet,

> particularly in our two most manpower intensive activities: all-source analysis and human source collection. By the mid-1990s, recruitment of new CIA analysts and case officers had

[12] President George H.W. Bush, "U.S. Soviet Nuclear Forces Reduction," The White House, September 27, 1991, https://www.c-span.org/video/?21616-1/us-soviet-nuclear-forces-reduction..

[13] James R. Clapper, "Current and Projected National Security Threats to the United States," Senate Select Committee on Intelligence, March 12, 2013, 9, https://www.intelligence.senate.gov/sites/default/files/hearings/11389.pdf.

© 2023 The Authors | CC BY-NC-ND 3.0 US

> come to a virtual halt. National Security Agency was hiring no new technologists during the greatest information technology change in our lifetimes.[14]

The real picture was even worse than these numbers suggest. Personnel reductions were made through voluntary attrition rather than targeted cuts to retain top talent, weed out poor performers, or ensure key skill sets and geographic and functional areas were well covered.[15]

Declining budgets undoubtedly made it difficult for the IC to adapt to the rising terrorist threat in the years before the 11 September 2001, terrorist attacks. Yet the evidence suggests there's much more to the story than shrinking resources. My research finds that the roots of the failure to prevent 9/11 lay in broader and deeper organizational weaknesses in US intelligence agencies that had surprisingly little to do with funding. Throughout the 1990s, even as America's spy agencies warned of the growing terrorist danger, they remained stuck in their Cold War posture, operating with organizational structures, cultures, and career incentives that offered little chance of stopping Islamic terrorist organization al-Qaeda from committing the worst terrorist attack in American history. My five-year examination of thousands of pages of declassified documents and interviews with seventy-five current and former intelligence and government officials found that the CIA and FBI had twenty-three opportunities to penetrate and possibly stop the 9/11 plot. Organizational weaknesses led to failure every time.[16] Below are thumbnails of two such lost opportunities.

The CIA's Watchlisting Failure

The 9/11 Commission and the Congressional Joint Inquiry into the terrorist attacks both suggest that perhaps the best chance to stop 9/11 involved the travel of two al-Qaeda operatives named Khalid al-Mihdhar and Nawaf al-Hazmi. Both men were part of the team that crashed American Airlines flight 77 into the Pentagon.

They first tripped the wire in January 2000, when they attended a secret al-Qaeda meeting in Malaysia. The CIA was watching. The agency managed to get a photograph of al-Mihdhar, learn his full name, obtain his passport number, and uncover the fact that he held a multiple-entry US visa. By March 2000, CIA officials identified al-Hazmi as having attended the same meeting, learned his full name, and discovered he had already entered the United States. Between fifty and sixty CIA officials had access to this information about al-Mihdhar and al-Hazmi. And yet nobody put these two men on the State Department's watch list denying them entry into the United States or notified the FBI for the next year and a half.[17] Why?

The simplest answer is that the CIA had never been in the habit of watchlisting suspected al-Qaeda terrorists before. For more than forty years, the agency and the rest of the IC had operated with Cold War priorities, procedures, and thinking, all of which had little need to ensure dangerous foreign terrorists stayed out of the United States. Before 9/11, there was a watchlisting program in name but not in practice: there was no formal

---

[14] George Tenet, "Written Statement for the Record, National Commission on Terrorist Attacks Upon the United States," submitted testimony for the eighth public hearing of the 9/11 Commission, March 24, 2004, 24, https://9-11commission.gov/hearings/hearing8/tenet_statement.pdf.

[15] Amy B. Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton, NJ: Princeton University Press, 2007), 3, 73–74; Aspin-Brown Commission Final Report, "Chapter 9: The Need to 'Right-Size' and Rebuild the Community," March 1, 1996, 96-97, https://www.govinfo.gov/content/pkg/GPO-INTELLIGENCE/pdf/GPO-INTELLIGENCE-13.pdf.

[16] Zegart, *Spying Blind*, 12.

[17] Office of the Inspector General, OIG Report on CIA Accountability with Respect to the 9/11 Attacks, June 2005, declassified August 2007, xiv, https://irp.fas.org/cia/product/oig-911.pdf.

© 2023 The Authors | CC BY-NC-ND 3.0 US

training, no clear process, and no priority placed on it.[18] As one CIA officer told congressional investigators after 9/11, he believed it was "not incumbent" even on the CIA's special unit on Osama bin Laden, al-Qaeda's founder and mastermind, to place people like al-Mihdhar on the State Department's watchlist.[19]

The FBI's Failed Search for Two al Qaeda Operatives

On 23 August 2001, just nineteen days before 9/11, the CIA finally told the FBI that al-Mihdhar and al-Hazmi were probably in the United States and needed to be found. The FBI responded by putting the search for these two suspected terrorists at the bottom of the priority list and handing it to the C-team. The nationwide hunt was the focus of just one of the Bureau's fifty-six US field offices. It was designated "routine," the lowest level of priority. And it was assigned to a junior agent who had just finished his rookie year and had never led that kind of investigation before.[20]

Here too, organizational pathologies, not individual screwups, were to blame. The Bureau dedicated just one office to what should have been a nationwide search because the FBI had always been a decentralized organization where each field office operated largely autonomously—and that is how all cases were handled. Putting one office on each case made sense for catching criminals after-the-fact and tailoring priorities to local law enforcement needs. It was a poor organizational setup for collecting and coordinating intelligence about future national security threats to the nation as a whole. Culture explains why finding al-Mihdhar and al-Hazmi went to the bottom of the pile. Although the FBI's own strategic plan declared counterterrorism its number-one priority in 1998 and resolved to improve its domestic intelligence capabilities, the Bureau was first and foremost a law enforcement organization with a culture that prized catching perpetrators of past crimes far more than gathering intelligence to stop a possible future tragedy.[21]

In fact, a Justice Department investigation found that before 9/11, intelligence analysis was considered so unimportant that the vast majority of FBI analysts were rated unqualified to do their jobs.[22] Promotion incentives reflected this culture. Handing the search to a junior agent was not a mistake; it was how things were supposed to work. Because convictions made careers, finding two potential terrorists who had yet to commit a crime and might never do anything illegal went to one of the office's least experienced investigators because it was one of the least desirable jobs.[23] In short, the Bureau's decentralized structure guaranteed that the alarm would be sounded only in one place. Its law enforcement culture ensured that the alarm would be muffled by criminal cases and priorities. And incentives promised that someone with the least experience and expertise would be answering the call.

Khalid al-Mihdhar and Nawaf al-Hazmi should not have been that hard to find. For months before the attack, they hid in plain sight in San Diego, using their true names on everything from rental agreements and credit cards to a California ID card and the telephone directory. They even contacted several targets of FBI

[18] Zegart, *Spying Blind*, 2.

[19] Quoted in Eleanor Hill, "The Intelligence Community's Knowledge of the September 11 Hijackers Prior to September 11, 2001," statement before the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence Joint Inquiry, 107th Cong., 2nd sess., September 20, 2002, 8.

[20] Zegart, *Spying Blind,* 156-157.

[21] Federal Bureau of Investigation, Draft FBI Strategic Plan: 1998-2003: Keeping Terrorism Safe, unclassified version, May 8, 1998. For FBI culture and history, see Beverly Gage, *G-Man: J. Edgar Hoover and the Making of the American Century* (New York: Viking, 2022).

[22] Joint Inquiry Into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, report of the US Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence, S. Report No. 107-351, H. Report No. 107-792, 107th Cong., 2nd sess., December 2002, 340.

[23] Zegart, *Spying Blind*, 156–68.

© 2023 The Authors | CC BY-NC-ND 3.0 US

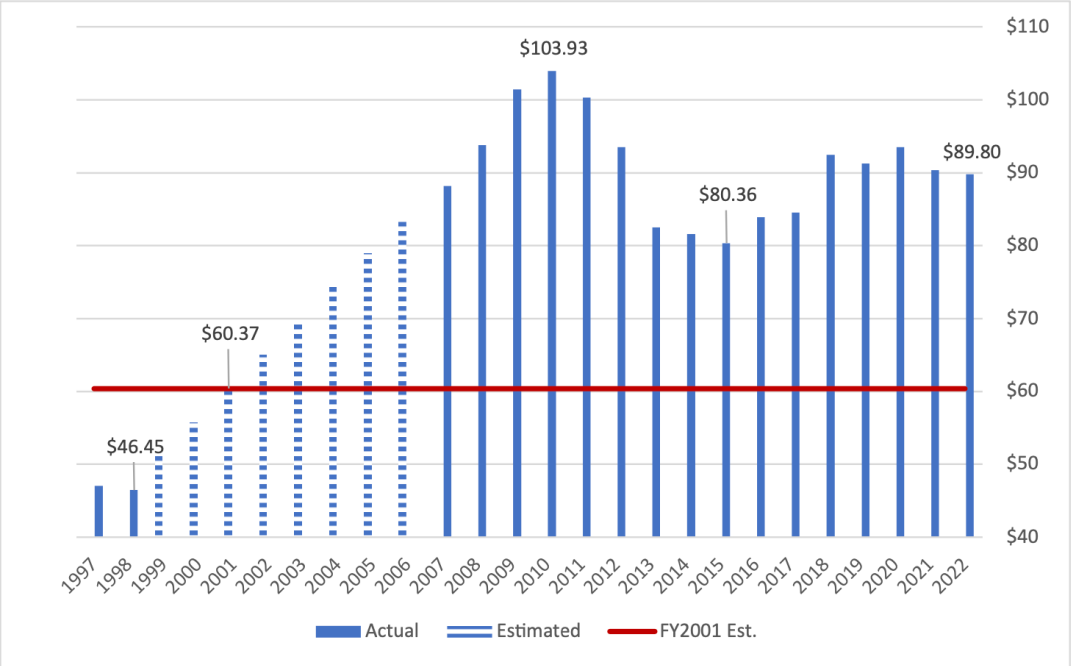
counterterrorism investigations, at one point living with an FBI informant—all unknown to the FBI. The two al-Qaeda operatives did not need secret identities or clever schemes to succeed. They just needed the CIA and the FBI to operate as usual.[24]

In short, while declining intelligence budgets in the 1990s certainly reduced the CIA's workforce and forced intelligence leaders to tackle a new problem set with fewer resources, the roots of failure on 9/11 appears to go deeper. Consider the counterfactual: If the CIA and FBI had unlimited resources in the run-up to 9/11, would they have succeeded in watchlisting and finding Khalid al-Mihdhar and Nawaf al-Hazmi before it was too late?

More Money, More Problems

Two decades later, intelligence agencies face a much more favorable budgetary environment, and yet they are struggling again to adapt to a shifting geopolitical landscape—driven this time by emerging technologies that are disrupting every facet of the intelligence enterprise. Despite record spending over the past twenty years, intelligence agencies are losing their relative advantage.

Figure 2: Total Intelligence Community Budget (in constant US dollars, billions)



Sources: Data for 1997 and 1998 from Steven Aftergood, "CIA Discloses FY 1998 Intelligence Budget Total," https://sgp.fas.org/foia/intel98.html#:~:text=CIA%20Discloses%20FY%201998%20Intelligence,Year%201998%20is%20%2426.7%20billion (accessed December 7, 2022); data for 2007 to 2022 from Office of the Director of National Intelligence, "US Intelligence Community Budget," http://www.dni.gov/index.php/what-we-do/ic-budget (accessed December 7, 2022). See footnote 17 for explanation of the author's analysis for 1999–2006.

The US intelligence budget has increased dramatically since 9/11, jumping from an estimated $60.37 billion in FY2001 to $89.8 billion in FY2022 in constant 2022 dollars—an increase of 49 percent over twenty years (see

[24] Zegart, *Spying Blind*, 156–68.

© 2023 The Authors | CC BY-NC-ND 3.0 US

fig. 2).[25] Although budgets dipped in the 2010 to 2015 period, the broader historical pattern is growth. Indeed, the Congressional Research Service estimates that intelligence spending quadrupled from 1980 to 2010 in real terms.[26]

Notably, increased government spending has not translated into better results in other policy areas during the same period. In health care, a 2021 study compared eleven of the world's richest countries and found that the United States spent the highest percentage of GDP on health care yet ranked last in affordability, access, and outcomes, including infant mortality and life expectancy at age sixty.[27] In education, economist Eric Hanushek has found that US K–12 spending per pupil quadrupled from 1960 to 2017 in constant dollars, yet student scores on national tests estimating achievement across subjects remained flat. He also found that American student performance on international tests has remained persistently poor, and racial and income gaps have persisted.[28] If the air force is any guide, moreover, bigger defense budgets have not translated into better military readiness. While air force budgets have fluctuated since the 1980s, the number of air force aircraft, personnel, and other measures of end strength have all gradually declined.[29] In 2021, House Armed Services Committee Chairman Adam Smith publicly called the F-35 Joint Strike Fighter—a fifth-generation fighter jet riddled with technical deficiencies which was the most expensive weapons program in history and ten years behind schedule—a "rathole."[30] Two years later, the Government Accountability Office found no improvement, noting the plane remained "more than a decade behind schedule and $183 billion over original cost estimates."[31] The United States is estimated to spend more than the following nine countries, in terms of

[25] FY2001 intelligence spending in nominal terms is estimated at $37.60 billion, based on the Congressional Research Service's 2013 report "Intelligence Spending and Appropriations: Issues for Congress." This figure was then inflation adjusted to $60.37 billion in 2022 dollars, using the Bureau of Labor Statistics' CPI Inflation Calculator, https://www.bls.gov/data/inflation_calculator.htm. Estimates for intelligence spending from 1999 through 2006 assume equal yearly increases between the unclassified 1998 and 2007 budgets and were also inflation-adjusted using the Bureau of Labor Statistics' CPI Inflation Calculator; Erwin and Belasco, "Intelligence Spending," 4–5; For FY2022 see: "US Intelligence Community Budget."

[26] Erwin and Belasco, "Intelligence Spending," 5.

[27] Eric C. Schneider, Arnav Shah, Michelle M. Doty, Roosa Tikkanen, Katharine Fields, and Reginald D. Williams II, "Mirror, Mirror 2021: Reflecting Poorly: Health Care in the US Compared to Other High-Income Countries," The Commonwealth Fund, August 2021. The eleven countries examined in the study were: Australia, Canada, France, Germany, the Netherlands, New Zealand, Norway, Sweden, Switzerland, the United Kingdom, and the United States; Health outcomes are a product of many causes, including underlying social and economic conditions. The study uses measures that focus more on outcomes likely to be affected by health care such as life expectancy at age sixty rather than life expectancy at birth.

[28] Eric A. Hanushek, "The Fall of Educational Productivity and Policy Paralysis" in *The Not-So-Great Society*, eds. Lindsay M. Burke and Jonathan Butcher, (Washington, DC: Heritage Foundation, 2019) 45- 51. See also Dana Goldstein, "'It Just Isn't Working': PISA Test Scores Cast Doubt on US Education Efforts," *New York Times*, December 3, 2019.

[29] Todd Harrison, "The Air Force of the Future: A Comparison of Alternative Force Structures," Center for Strategic & International Studies, October 29, 2019.

[30] Valerie Insinna, "Watchdog Group Finds F-35 Sustainment Costs Could Be Headed Off Affordability Cliff," Defense News, July 7, 2021; Sébastien Roblin, "The Air Force Admits the F-35 Fighter Jet Costs Too Much. So It Wants to Spend Even More," NBC News, March 7, 2021; Government Accountability Office, "F-35 Joint Strike Fighter: Cost Growth and Schedule Delays Continue," Report 22-105943, April 7, 2022; Aaron Gregg, "Powerful Lawmaker Calls F-35 Fighter Jet a 'Rathole,' Suggests Pentagon Should Cut Its Losses," Washington Post, March 5, 2021.

[31] Government Accountability Office, "Fast Facts—F-35 Joint Strike Fighter: More Actions Needed to Explain Cost Growth and Support Engine Modernization Decision," GAO-23-106047, May 30, 2023, available at: https://www.gao.gov/products/gao-23-106047 (accessed June 20, 2023).

© 2023 The Authors | CC BY-NC-ND 3.0 US

defense budgets, combined, and yet China's relative defense advantages are growing.[32] In short, American taxpayers seem to be getting less bang for their buck across a range of policy areas.

Increased intelligence spending after 9/11 produced arguably better outcomes than in these other policy areas, enabling the US to prosecute the war on terror and defend the homeland to great effect. Changes included the creation of the National Counterterrorism Center and the Office of the Director of National Intelligence, an expanded drone program, and tighter integration between intelligence and military counterterrorism operations. As a result of these and other measures, the United States has not suffered another major catastrophic terrorist attack on American soil.

However, the dramatic infusion of counterterrorism funding also ended up hard-wiring the bureaucracy to fight the last war. Great power competition, not transnational terrorism, now tops the threat list. And, as I discuss more below, emerging technologies are transforming both the future and how intelligence agencies go about understanding it. This is a moment of reckoning for American spy agencies. And it reveals the paradox of plenty: surging budgets led to widescale changes, but by the time US intelligence agencies mastered the al-Qaeda problem, al-Qaeda was no longer the problem.

The Tech Moment of Reckoning for Intelligence

Never before has the world stood on the cusp of so many technologies transforming so much so fast. Internet connectivity has transformed global commerce and supercharged global politics, fueling protests like the Arab Spring and Hong Kong's Umbrella Movement, empowering a new wave of government techno-surveillance led by Beijing, and enabling massive Russian deception operations to influence elections and undermine democracies from within. It is easy to forget how rapidly the internet has developed and how revolutionary it has been. In the early 1990s, less than 1 percent of the global population was online. Now two-thirds of the world is connected to the internet.[33] In the last three years alone, more than a billion people have come online.[34]

Artificial intelligence is also disrupting nearly every industry and changing how wars are fought—automating everything from logistics to cyber defenses to unmanned fighter jets that can overwhelm defenses with swarms and maneuver faster and better than human pilots. Some analysts estimate that AI could eliminate up to 40 percent of jobs worldwide in the next fifteen years.[35] Russian President Vladimir Putin has declared that whoever leads AI development "will become the ruler of the world," and China has made no secret of its plans to lead the world in AI by 2030.[36] AI has been likened to electricity: a foundational technology that affects everything.

---

[32] "US Defense Spending Compared to Other Countries," Peter G. Peterson Foundation, May 11, 2022; Anthony H. Cordesman, with the assistance of Grace Hwang, Chinese Strategy and Military Forces in 2021: A Graphic Net Assessment, revised August 3, 2021, 83–86; US Department of Defense, Military and Security Developments Involving the People's Republic of China 2022, Annual Report to Congress, November 29, 2022.

[33] "Individuals Using the Internet," ITU United Nations, 2022, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx; Kelsey Campbell-Dollaghan, "Why One of World's Most Remote Places Has the Fastest Internet," Gizmodo, April 1, 2014; "Help with Internet and Social Media in an Authentic Bedouin Camp in Wadi Rum, Jordan," Workaway.info, updated January 2023, https://www.workaway.info/en/host/458895548546.

[34] "Individuals Using the Internet."

[35] Kai-Fu Lee, "Facial and Emotional Recognition; How One Man Is Advancing Artificial Intelligence," 60 Minutes, interview by Scott Pelley, January 13, 2019.

[36] James Vincent, "Putin Says the Nation that Leads AI 'Will be the Ruler of the World,'" *The Verge*, September 4, 2017; Paul Mozur, "Beijing Wants A.I. to Be Made in China by 2030," *The New York Times*, July 20, 2017.

© 2023 The Authors | CC BY-NC-ND 3.0 US

Technology is also revolutionizing the ability of humans to detect events unfolding on Earth from space. Commercial satellite capabilities now offer eyes in the sky for anyone who wants them. The number of satellite launches more than doubled between 2016 and 2018.[37] Today, more than 5,000 satellites are orbiting the Earth, and the Paris-based firm Euroconsult estimates that 17,000 satellites will be launched in the next decade.[38] While US spy satellites have more sophisticated sensing capabilities, commercial satellites are rapidly improving.[39] Some have resolutions so sharp they can detect manhole covers, signs, and even road conditions from space.[40] Others can detect radio frequency emissions, observe dynamic activities like vehicle movement and nuclear cooling plumes, and operate at night, in cloudy weather, or through dense vegetation and camouflage. Constellations of small satellites are offering something new: faster revisit rates over the same location multiple times a day so that changes can be detected over shorter periods. In 1960, when a US CORONA spy satellite successfully delivered images of the Soviet Union for the first time, the CIA's Deputy Director for Science and Technology, Albert "Bud" Wheelon, remarked, "It was as if an enormous floodlight had been turned on in a darkened warehouse."[41] Commercial satellites are turning that occasional floodlight into a continuously running video.

That's not all. Advances in quantum computing could eventually unlock the encryption protecting nearly all the world's data. Synthetic biology enables scientists to engineer living organisms with the potential for revolutionary improvements in food production, medicine, data storage, and weapons of war.

Perhaps most important from a US national security perspective, nearly all of today's emerging technologies are invented outside the government, made available to the world, and have widespread applications for commerce and conflict. That is new.

In the Cold War, breakthroughs like the internet and GPS were invented by US government agencies and later commercialized by the private sector. Few technologies were inherently dual use, which meant that they could be classified at birth and restricted forever to keep them out of enemy hands. Nuclear technology, for example, was born secret and stayed that way, limiting the proliferation of the world's most dangerous weapons.

Now the script has flipped. Technological innovations are more likely to be developed in the private sector, where they are funded by foreign investors, developed by a multinational workforce of the best and brighest, and sold to global customers. Today's technologies are born open, not classified, and are widely available and not easily restricted. AI, for example, has become so widespread and simple to use that high school students with no coding background can make deepfakes—AI-generated fake videos that look and sound real. Already, deepfakes impersonating former US Ambassador to Russia Michael McFaul have been used to dupe Ukrainian officials and undermine the Ukrainian war effort, prompting McFaul to tweet, "WARNING. Someone using the phone number +1 (202) 7549885 is impersonating me. If you connect on a video

---

[37] Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, January, 29, 2019, 17.

[38] Alan Burkitt-Gray, "'Fourfold Increase' in Satellites over the Next 10 Years to 17,000," Capacity Media, December 10, 2021. The following section uses data from the Union of Concerned Scientists, which maintains one of the most comprehensive databases of active satellites. Data available at Union of Concerned Scientists, UCS Satellite Database, updated May 1, 2022, https://www.ucsusa.org/resources/satellite-database.

[39] Union of Concerned Scientists, UCS Satellite Database.

[40] Chris Gormeller, "Introducing 15 cm HD: The Highest Clarity from Commercial Satellite Imagery," Maxar Technologies, November 12, 2020.

[41] Quoted in Philip Taubman, *Secret Empire: Eisenhower, the CIA, and the Hidden Story of America's Space Espionage* (New York: Simon and Schuster, 2003), 35.

© 2023 The Authors | CC BY-NC-ND 3.0 US

platform with this number, you will see an AI-generated 'deep fake' that looks and talks like me. It is not me. This is a new Russian weapon of war. Be careful."[42]

This reversal gives private-sector leaders new power and national security officials new challenges. American social media platforms now find themselves on the front lines of information warfare, deciding what is real and what is fake, what speech is allowed, and what is suppressed. Startup founders are inventing capabilities that can be used by enemies they can't foresee with consequences they cannot control. As the war in Ukraine rages on and great-power competition with China intensifies, companies and investors have to weigh their economic interests against the national interest in new ways. Meanwhile, US intelligence agencies are struggling to adopt critical new technologies from the outside and move at the speed of invention instead of the pace of bureaucracy. Increasingly, private-sector leaders have responsibilities they don't want and government leaders want capabilities they do not have. Power isn't just shifting abroad. Power is shifting at home.

All these forces unleashed by emerging technologies have created a moment of reckoning for America's intelligence agencies. If we think of intelligence as a competitive contest for insight, then the challenges arising from emerging technologies become more clear. They fall into five core categories—the "five mores."

"The Five Mores": Threats, Speed, Data, Customers, and Competitors

The first challenge is more threats. Today's threat landscape has never been more crowded, complicated, or fast moving. After spending nearly half a century countering the Soviet Union and two decades fighting terrorists, US leaders now confront a diverse multitude of dangers that place demands on intelligence, including transnational threats like pandemics and climate change; great power competition with Russia and China; terrorism and other threats arising from weak and failed states; and cyberattacks that steal, spy, disrupt, destroy, and deceive at stunning speeds and scale.

The list isn't just longer. Thanks to technology, it's harder. Cyber threats operate in ways that make them far more consequential than they appear and far more vexing to understand, detect, and defeat than the threats of yesteryear. Cyberspace is not just another military battleground like air, land, and sea, where the old tools and rules apply.

For centuries, power and geography have been the mainstays of security. Countries with the most powerful militaries and the blessings of geography—like the two vast oceans separating the US from the world's dangerous neighborhoods—were more protected. Not anymore. In cyberspace, power brings vulnerability, because the most powerful countries tend to be digitally reliant. And there is no such thing as good geography online; anybody can inflict damage from anywhere.

The character of war is different, too. Physical warfare tends to involve big moves that generate big consequences. But cyberwarfare is a bleed-every-minute affair where small attacks add up to devastating damage before they can be detected. China has stolen its way to technological advantage one hack at a time, in what FBI Director Christopher Wray has called one of the greatest transfers of wealth in human history, and "the biggest long-term threat to our economic and national security."[43]

---

[42] Sami Quadri, "Former US Ambassador says Russia is Using 'Deepfakes' to Impersonate Him,'" *Evening Standard*, October 1, 2022.

[43] For greatest transfer of wealth see Russell Flannery, "China Theft of US Information, IP One of Largest Wealth Transfers in History: FBI Chief," Forbes, July 7, 2020; for biggest long-term threat, see Christopher Wray,

© 2023 The Authors | CC BY-NC-ND 3.0 US

Russia's interference in the 2016 US presidential election showed that cyberattacks can hack minds, not just machines, polarizing societies and undermining democracies from within at speed and scale. Russia wrote the playbook on using American tech companies to turn Americans against one another. Today, China has no need of it. The popular social media app TikTok is owned by Chinese firm ByteDance and has quickly amassed more than a billion users, including an estimated 135 million in the US. That's forty percent of the US population.[44] Alarm bells are ringing. Democrats and Republicans are worried that TikTok could enable the Chinese government to vacuum all sorts of data about Americans and launch massive influence campaigns that serve Beijing's interest under the guise of giving American consumers what they want. In a world of information warfare, where weapons don't even look like weapons, it is fair to say the threat landscape is not what it used to be.

Second, technological advances are generating the need for more speed in intelligence. Intelligence must be timely to be useful, delivering information when policy makers need it—before a missile launches, a summit convenes, or the National Security Council makes a decision.

Timeliness has always been important, but the speed of relevance is accelerating. In the 1962 Cuban Missile Crisis, President John F. Kennedy famously had thirteen days to pore through intelligence and consider his policy options in secret after U2 surveillance photographs revealed Soviet nuclear installations in Cuba. On 11 September 2001, President George W. Bush had less than thirteen hours from the time the first hijacked plane crashed into the World Trade Center to review intelligence on who was responsible and announce America's response to the world. Today, the volume of intelligence that needs to be consumed, analyzed, and digested has grown exponentially greater. And yet the time for presidents to consider intelligence before making major policy decisions may be closer to thirteen minutes or thirteen seconds, or it could already be too late because cyber breaches are often discovered long after the damage is done. In December 2020, for example, cybersecurity firm FireEye detected a massive breach of the software firm SolarWinds. Like a bad horror movie, when officials rushed to survey the damage, they discovered that hackers from Russia's elite foreign espionage service had been inside the house for a very long time—penetrating US nuclear labs, the departments of Defense, State, and Homeland Security, and much of the *Fortune* 500 more than a year before anyone found them.[45]

Now breaking events and hot takes are flowing directly into the hands of policy makers with the touch of a button, putting greater pressure on intelligence agencies to speed up or get left behind. But moving too fast also carries risks. It takes time to vet source credibility, tap expert knowledge across fields, and consider alternative explanations.[46] Without careful intelligence analysis, leaders may make premature or even dangerous decisions. The potential consequences of rash action became evident in December 2016, when a news story reported that Israel's former defense minister threatened a nuclear attack against Pakistan if Islamabad deployed troops to Syria. Pakistan's Defense Minister, Khawaja Muhammad Asif, quickly rattled his own nuclear saber, tweeting, "Israeli def min threatens nuclear retaliation presuming pak role in Syria against Daesh. Israel forgets Pakistan is a Nuclear state too, AH."[47] The original story, including the Israeli

---

"Director's Remarks to Business Leaders in London," July 6, 2022, https://www.fbi.gov/news/speeches/directors-remarks-to-business-leaders-in-london-070622 (accessed March 10, 2023).

[44] Lily Hay Newman, "It's Time to Get Real About TikTok's Risks," Wired, September 6, 2022.

[45] Natasha Bertrand and Eric Wolff, "Nuclear Weapons Agency Breached amid Cyber Onslaught," *POLITICO*, December 17, 2020; Jon Porter, "White House Now Says 100 Companies Hit by SolarWinds Hack, but More May Be Impacted," *The Verge*, February 18, 2021; Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack," *NPR*, April 17, 2021.

[46] Intelligence Community Directive 203, "Analytic Standards," January 2, 2015, available at: https://fas.org/irp/dni/icd/icd-203.pdf.

[47] "Fake News Sets Off Twitter Confrontation between Pakistan and Israel," CBS News, December 25, 2016.

© 2023 The Authors | CC BY-NC-ND 3.0 US

threat, had been fabricated, but the tweet apparently went out before it was verified. Satisfying policy makers' need for speed while carefully collecting, vetting, and assessing intelligence has always been a delicate balance, but it is harder to strike.[48]

The third challenge is data. The volume of data available online has grown so vast that it is hard to fathom. According to the World Economic Forum, in 2019, internet users posted 500 million tweets, sent 294 billion emails, and posted 350 million photos on Facebook every day.[49] Google answers several billion queries a day.[50] Every second, the internet transmits about 1 petabyte of data—the equivalent of binge-watching movies nonstop for over three years.[51] Data accumulation shows no sign of slowing. Some estimate that the amount of Earth's data doubles every twenty-four months.

American intelligence agencies are struggling to keep up. Already, they are collecting far more information than humans can analyze effectively. In 2020, one soldier deployed to the Middle East was so concerned about the crushing flow of classified intelligence emails he was receiving that he decided to count them. He received ten thousand emails in 120 days. And that's just the classified information.

Fourth, who needs intelligence to protect American lives and interests is changing radically, too. Until now, intelligence agencies produced classified reports for people with security clearances who read them in secured facilities with guards outside. Increasingly, however, important decision makers live worlds apart from Washington, making consequential policy choices in board rooms and living rooms, not just the White House situation room. Voters need intelligence about foreign election interference and influence campaigns. Big tech companies like Microsoft and Google need intelligence about cyber threats to and through their systems. Most of America's critical infrastructure, from energy companies to financial services firms, is in private-sector hands. They can't go it alone in cyberspace, either. And because cyber threats do not stop at the border, American security increasingly depends on sharing intelligence faster and better with allies and partners.

Serving a broader array of customers requires producing products at different levels of classification—including no classification at all—and engaging with the outside world.[52] For agencies which are used to operating in secret, this is an unnatural act. Important efforts are underway. In the fall of 2022, the CIA launched a podcast called *The Langley Files*. Its aim: demystifying the agency and educating the American public. "At CIA, there are truths we can share and stories we can tell," each podcast begins.

There are now public service videos from intelligence agencies about foreign threats to US elections. The National Geospatial-Intelligence Agency has launched a project called Tearline, a collaboration with think tanks, universities, and nonprofits to create unclassified reports about climate change, Russian troop movements, human rights issues, and more. Public-private partnerships in cybersecurity used to be a one-way street where the National Security Agency (NSA) and the FBI asked companies for information but rarely

[48] Chu Wang, "Twitter Diplomacy: Preventing Twitter Wars from Escalating to Real Wars," Belfer Center for Science and International Affairs, Harvard University, May 20, 2019; "Twitter Is the Prime Social Media Network for World Leaders," PR Newswire, May 31, 2017.

[49] Jeff Jardins, "How Much Data Is Generated Each Day?," World Economic Forum, April 17, 2019.

[50] Internet Live Stats, https://www.internetlivestats.com/one-second/#traffic-band (accessed December 7, 2022).

[51] Tim Fisher, "Terabytes, Gigabytes, & Petabytes: How Big Are They?" Lifewire, January 1, 2021; Pranshu Verma, "This Chip Transmits an Internet's Worth of Data Every Second," Washington Post, October 27, 2022.

[52] Intelligence Community Directive 208, "Maximizing the Utility of Analytic Products," January 9, 2017, available at: https://www.dni.gov/files/documents/ICD/ICD%20208%20-%20Maximizing%20the%20Utility%20of%20Analytic%20Products%20(09%20Jan%202017).pdf.

© 2023 The Authors | CC BY-NC-ND 3.0 US

provided any. Those days have changed. In 2021 NSA began issuing joint cyber advisories with the FBI and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency detailing major cyber threats, exposing the entities behind them, and explaining how to shore up defenses against them. In October 2022, these agencies even released the technical details of the top-twenty vulnerabilities exploited by the Chinese government to hack into US and allied networks, along with detailed instructions about how to defend against them.[53] The US government is now also issuing advisories with foreign intelligence partners.

The success of this public-facing strategy has been on full display in Ukraine. It helped the United States warn the world about Russia's invasion and rally the West behind a fast response. It continues to frustrate Moscow. More recently, after Washington revealed intelligence indicating that senior Russian military leaders were discussing using tactical nuclear weapons in Ukraine, Chinese president Xi Jinping issued a rare public warning against the "use of, or threats to use, nuclear weapons."[54] Xi's trumpeted "no limits" relationship with Putin suddenly had limits after all.[55]

The fifth challenge for intelligence agencies in the technological age is more competition. It used to be that government spy agencies were the only organizations capable of launching satellites, collecting information at scale, and analyzing global threats. Not anymore.

The explosion of online open-source information, commercial satellite capabilities, and automated analytics like AI enables all sorts of individuals and organizations worldwide to collect, analyze, and disseminate intelligence—often better and faster than governments can.

In the past several years, the amateur investigators of Bellingcat, which describes itself as "an intelligence agency for the people," have identified the Russian hit team that tried to assassinate a former Russian military officer named Sergei Skripal living in the United Kingdom, and located supporters of ISIS in Europe.[56] It also proved that Russians were behind the shootdown of Malaysia Airlines Flight 17 over Ukraine.[57]

Bellingcat is not the only civilian intelligence initiative. When the Iranian government claimed that a small fire had broken out in an industrial shed under construction in 2020, two American researchers working independently and using only their computers and the internet proved that Tehran was lying—within hours. David Albright and Fabian Hinz quickly found that the building was actually a nuclear centrifuge assembly facility at Natanz, Iran's main uranium enrichment site.[58] The damage was so extensive that the fire may well have been caused by an explosion, raising the possibility of sabotage. In 2021, nuclear sleuths at the James Martin Center for Nonproliferation Studies in California used commercial satellite imagery to discover more

[53] Cybersecurity Advisory, "Top CVEs Actively Exploited by People's Republic of China State-Sponsored Cyber Actors," White paper, October 6, 2022.

[54] Stuart Lau, "China's Xi Warns Putin Not to Use Nuclear Arms in Ukraine," *POLITICO*, November 4, 2022.

[55] Chris Buckley and Steven Lee Meyers, "In Beijing, Olympic Spectacle and Global Power Games," *The New York Times*, February 4, 2022.

[56] Eliot Higgins, "How Bellingcat Uncovered Russia's Secret Network of Assassins," *Wired*, April 2, 2021; Marjas Zatat, "Isis Supporters in Europe are Accidentally Revealing their Locations on Social Media," *indy100*, May 22, 2016.

[57] Will Croxton, "How Bellingcat Tracked a Russian Missile System in Ukraine," *60 Minutes Overtime*, February 23, 2020.

[58] Jon Gambrell, "Analysts: Fire at Iran Nuclear Site Hit Centrifuge Facility," *Washington Post*, July 2, 2020.

© 2023 The Authors | CC BY-NC-ND 3.0 US

than two hundred new intercontinental ballistic missile silos in China, a finding that could signal historic increases in China's nuclear arsenal.[59]

And in the past year, Russia's war in Ukraine has given rise to an array of experts wielding unclassified information to track daily events and offer longer-term analysis online, from the Twitter feeds of former US officials to the Institute for the Study of War, an American think tank whose website even features an interactive map. At Stanford University, there are now open-source intelligence courses for undergraduates, and a major volunteer effort has produced a series of reports compiling and confirming human rights atrocities in Ukraine for the United Nations. The Stanford student team, led by former army and open-source imagery analyst Allison Puccioni, used commercial satellite thermal and electro-optical imaging, TikTok videos posted online, geolocation tools, and more. "Today, anyone and everyone can access reasonably credible first-hand reports of attacks leveled against Ukraine," says Puccioni. "These pictures or videos are informative in and of themselves. But when cross-checked against other forms of freely or cheaply available information like satellite imagery, they can be triangulated to calculate location and time-stamp of the event, creating something akin to the synthesized, multi-sourced insight of conventional classified intelligence."[60]

Open-Source Intelligence Is Having a Moment

For American intelligence agencies, open-source intelligence brings significant new opportunities as well as risks. On the positive side, citizen sleuths offer more eyes and ears around the world, scanning for developments and dangers as they arise. The wisdom of the crowd can be a powerful tool, especially for piecing together tiny bits of information. Open-source information can be shared easily within government agencies, across them, and with the public, all without revealing sensitive sources or methods. As 9/11 showed, the barriers to sharing classified information are often too high, and the costs can be tragic.

But features are also flaws. Open-source intelligence is open to everyone, everywhere, regardless of their motives, national loyalties, or capabilities. Citizen sleuths do not have to answer to anyone or train anywhere. The line between the wisdom of crowds and the danger of mobs is thin. Assessing and expressing judgments about the reliability of information is crucial but often gets overlooked. As a result, small bits of information can deceive in big ways. After a 2013 terrorist attack on the Boston Marathon killed three people and wounded more than 260 others, for example, Reddit users jumped into action. Posting pet theories, unconfirmed chatter on police scanners, and other crowdsourced tidbits of information, amateur investigators quickly fingered two "suspects," and the mainstream media publicized the findings. Both of them turned out to be innocent.[61]

These weaknesses can create serious headaches for governments. When errors go viral, intelligence agencies have to burn time and divert resources fact-checking the work of others and reassuring policymakers about the job they were already doing and the assessments they had made before. Accurate open-source discoveries can cause problems, too. Findings, for example, can force leaders into corners instead of keeping things secret to make room for compromise and graceful exits in crises. To diffuse the Cuban Missile Crisis, for example, Kennedy agreed to secretly remove US nuclear weapons from Turkey if Soviets leaders took their

[59] Joby Warrick, "China Is Building More Than 100 New Missile Silos in Its Western Desert, Analysts Say," *Washington Post*, June 30, 2021; Editorial Board, "More Missile Silos Have Been Found in China. That's an Ominous Sign," *Washington Post*, July 30, 2021.

[60] Author interview, October 31, 2022.

[61] Alexis C. Madrigal, "#BostonBombing: The Anatomy of a Misinformation Disaster," *The Atlantic*, April 19, 2013; Jay Caspian Kang, "Should Reddit Be Blamed for the Spreading of a Smear?," *New York Times*, July 25, 2013; Chris Wade, "The Reddit Reckoning," *Slate*, April 15, 2014.

© 2023 The Authors | CC BY-NC-ND 3.0 US

missiles out of Cuba. Had satellite imagery been publicly available, Kennedy might have been too worried about the domestic political backlash to make a deal.

The Future of Intelligence: It's the Organization, Stupid

American intelligence leaders know that their success in the twenty-first century hinges on adapting to a world of more threats, more speed, more data, more customers, and more competitors. They have been working hard to get there—launching organizational reforms, technology innovation programs, and new hiring initiatives to recruit top science and engineering talent. But the challenges are hard, the efforts have been piecemeal, and the rate of progress remains slow.[62] The latter is especially worrisome given that the challenges are well known, the stakes are high, and intelligence weaknesses have been festering for years. Multiple reports and articles have found that intelligence agencies are not keeping pace with technological developments.[63]

If I am right, then Washington cannot address its present intelligence challenges merely by throwing more money at existing agencies. Instead, developing US intelligence capabilities for the tech age requires building something new: a dedicated, open-source intelligence agency that is focused on combing through unclassified data and discerning what it means.

Creating a nineteenth intelligence agency may seem duplicative and unnecessary, but it is essential. Because it cannot overcome existing organizational structures, cultures, and incentives, and despite Washington's best efforts, open-source intelligence has always been a second-class citizen in the US intelligence community. Open-source intelligence has no agency with the budget, hiring power, or seat at the table to champion it. As long as open-source intelligence remains embedded in secret agencies that value secret information above all, it will languish. A culture of secrecy will continue to strangle the adoption of cutting-edge technology tools from the commercial sector. Agencies will struggle to attract and retain desperately needed talent to help them understand and use new technologies. And efforts to harness the power of open-source intelligence collectors and analysts outside government will fall short.

A new open-source intelligence agency would bring innovation, not just information, to the US intelligence community by providing fertile soil for the growth of far-reaching changes in human capital, technology adoption, and collaboration with the burgeoning open-source intelligence ecosystem. Such an agency would be a powerful lever for attracting the workforce of tomorrow. Because it would deal with unclassified information, the agency could recruit top scientists and engineers to work right away without requiring them to wait months or years for security clearances. Locating open-source agency offices in technology hubs where engineers already live and want to stay—such as Austin, San Francisco, and Seattle—would make it easier for talent to flow in and out of government. The result could be a corps of tech-savvy officials who rotate between public service and the private sector, acting as ambassadors between both worlds. They would increase the intelligence community's presence and prestige in technology circles while bringing a continuous stream of fresh tech ideas back inside.

---

[62] "Artificial Intelligence and National Security," Congressional Research Service, R45178, November 10, 2020, 10.

[63] Amy Zegart and Michael Morell, "Spies, Lies, and Algorithms: Why US Intelligence Must Adapt or Fail," *Foreign Affairs*, May/June 2019; "Maintaining the Intelligence Edge: A Report of the CSIS Technology and Intelligence Task Force," Center for Strategic and International Studies, January 2021; Elizabeth Leyne and Yvette Nonte, "Is the Intelligence Community Staying Ahead of the Digital Curve?" Harvard Belfer Center Report, August 2021.

© 2023 The Authors | CC BY-NC-ND 3.0 US

By working with unclassified material, the open-source agency could also help the intelligence community to do a better and faster job of adopting new collection and analysis technologies. The open-source agency could test new inventions and, if they proved effective, could pass them along to agencies that work with secrets. The agency would also be ideally positioned to engage with leading open-source intelligence organizations and individuals outside the government. These partnerships could help US intelligence agencies outsource more of their work to responsible nongovernmental collectors and analysts, freeing up intelligence officials to focus their capabilities and clandestine collection efforts on missions that nobody else can do.

And there will still be many such missions. After all, even the best open-source intelligence has limits. Satellite imagery can reveal new Chinese missile silos but not what Chinese leaders intend to do with them. Identifying objects or tracking movements online is important, but generating insight requires more. Secret methods remain uniquely suited to understanding what foreign leaders know, believe, and desire. There is no open-source substitute for getting human spies inside a foreign leader's inner circle or penetrating an adversary's communications system to uncover what that adversary is saying and writing. Analysts with clearances will also always be essential for assessing what classified discoveries mean, how credible they are, and how they fit with other unclassified findings.

If history is any guide, the agencies, processes, and cultures that got us here will not get us there. The United States faces a dangerous new era that includes great power competition with China, renewed war in Europe, ongoing terrorist attacks, and fast-changing cyberattacks. New technologies are driving these threats and determining who will be able to understand and chart the future. To succeed, the US Intelligence Community must adapt to a more open, technological world.

© 2023 The Authors | CC BY-NC-ND 3.0 US