7

INTELLIGENCE COMMUNITY

Dustin J. Carmack

MISSION STATEMENT

To arm a future incoming conservative President with the knowledge and tools necessary to fortify the United States Intelligence Community; to defend against all foreign enemies and ensure the security and prosperity of our sovereign nation, devoid of all political motivations; and to maintain constitutional civil liberties.

OVERVIEW

The United States Intelligence Community (IC) is a vast, intricate bureaucracy spread throughout 18 independent and Cabinet subagencies.[1] According to the Office of the Director of National Intelligence (ODNI), the IC's mission is "to collect, analyze, and deliver foreign intelligence and counterintelligence information to America's leaders so they can make sound decisions to protect our country."[2]

An incoming conservative President needs to use these intelligence authorities aggressively to anticipate and thwart our adversaries, including Russia, Iran, North Korea, and especially China, while maintaining counterterrorism tools that have demonstrated their effectiveness. This means empowering the right personnel to manage, build, and effectively execute actions dispersed throughout the IC to deliver intelligence in an ever-challenging world. It also means removing redundancies, mission creep, and IC infighting that could prevent these collection tools from providing objective, apolitical, and empirically backed intelligence to the IC's premier customer: the President of the United States.

Today, as Abraham Lincoln famously said, "The occasion is piled high with difficulty, and we must rise with the occasion.... [W]e must think anew, and act

anew."[3] The Intelligence Community maintains an incredible capacity to achieve its mission, but both the IC and the somewhat antiquated infrastructure that supports it often place too high a priority on yesterday's threats and methodologies instead of trying to identify possible future threats or the methodologies that might be needed to combat them. The IC also often spends too much time overcorrecting for past mistakes. The unintended consequences include hesitancy, groupthink, and an overly cautious approach that allows personal incentives to drive preset courses.

The IC must be perceived as a depoliticized protector of America's civil rights and security. The American people are understandably frustrated by the fact that those who abuse power are rarely held to account for their actions. This must change, beginning with leadership that is both committed to ensuring that these agencies faithfully execute the laws of the land under the Constitution and resolved to punish and remove any officials who have abused the public trust.

The IC must also start to look forward, not backward. A concerted, disciplined, leadership-led initiative must be undertaken to refocus and shift IC prioritization, funding, and authorities to new and emerging threats, technologies, and methodologies if the United States is to prevail against its global adversaries.[4] Unfortunately, America's major strategic threat is a nation-state peer and possibly ahead of the U.S. in strategic areas. An incoming President must understand that today's intelligence competition could well require analyzing technologies the U.S. does not have or compartmentalizing certain information as was done during the Cold War because of intelligence penetration. A future President's ability to drive the resources needed to defeat another nation-state giant should therefore be the focus of near-term IC reforms.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI)

The ODNI was established in the aftermath of the attacks on 9/11 and intelligence failures leading up to the 2003 U.S. war in Iraq. The office and its functions stem from authorities established under executive orders promulgated by President George W. Bush in 2004, followed by statutory authorizations in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[5]

Proponents of an ODNI hoped to establish reforms similar to the Goldwater–Nichols Department of Defense (DOD) reforms of the 1980s, which identified recurring problems within DOD's command-and-control architecture and led to unified Combatant Commands with the Chairman of the Joint Chiefs of Staff as the senior ranking member of the armed forces and principal military adviser to the President. The ODNI was envisioned as a small but powerful IC coordinating agency led by a Director of National Intelligence (DNI). As the President's principal intelligence adviser, the DNI would lead and provide oversight of the President's intelligence authorities while wielding a cudgel—budget and appointment

authorities—to break institutional silos that had caused past intelligence integration failures.

Originally envisioned by the 9/11 Commission as a strengthened, authoritative position, the final congressionally negotiated product signed by President Bush has led to ambiguous and vague authorities that are dependent on who is selected as DNI and Central Intelligence Agency (CIA) Director and their level of support from the White House and National Security Council (NSC). 9/11 Commission Executive Director Philip Zelikow warned in a 2004 hearing that creating a new agency "lacking any existing institutional base...would require authorities at least as strong as those we have proposed or else it would create a bureaucratic fifth wheel that would make the present situation even worse."[6] The ODNI has become that bureaucratic fifth wheel about which Zelikow warned.

For example, under the Bush Administration's initial legislative proposal, the CIA Director would have been under the "authority, direction, and control" of the DNI and no longer the head of an autonomous agency. Additional mechanisms envisioned full budget authority for the DNI, including within DOD's intelligence components, as opposed to coordinating authority. Through arduous "sausage-making" and relatively quick negotiations, lawmakers produced statutorily vague authorities that traded away the DNI's ability to direct budgetary authority across the entire IC, including DOD, and left the CIA a subordinate but independent agency with duties to report to the DNI without explicit directing authority.

These statutory developments were what led President Bush's first choice to serve as DNI, Robert Gates, to turn down the position. In discussions with the White House over the post, Gates noted that the "legislation weakened the leadership of the community" and that "instead of a stronger person, you ended up with a weaker person because the DNI had no troops and no additional powers really on the budget, hiring, and firing."[7] Gates noted that success would require the President to "make explicit publicly that the DNI is head of the Intelligence Community, not some budgeter or coordinator," and that "[t]he position's only prayer of success is for the president to say plainly...how he sees the job. Without his explicit mandate...the endeavor is doomed to fail."[8]

One of the two DNIs confirmed by the Senate during the Trump Administration, John Ratcliffe, acknowledged that Gates's theoretical concerns became the practical reality that he inherited:

> Prior DNIs were the head of the IC only on paper and were routinely accustomed to yielding IC actions and decisions to the preferences of the CIA and other agencies. My ability to begin reversing that capitulation was accomplished solely because President Trump made it repeatedly clear to the entire national security apparatus that he expected all intelligence matters to go through the DNI.[9]

To help further the legislative intent behind IRTPA, DNI Ratcliffe advised during the transition of incoming Biden DNI Avril Haines that the DNI should be the only Cabinet-level intelligence official.[10] While his recommendation was adopted and has corrected the previously allowed imbalance by making the DNI the only Cabinet official and head of the IC at the table, the ODNI's effectiveness and direction leave much to be desired.

A conservative President must decide how to empower an individual to oversee and manage the Intelligence Community effectively. To be successful, the DNI and ODNI must be able to lead the IC and implement the President's intelligence priorities. This includes being able to exercise both budget and personnel authority and being able to rely on timely, useful feedback from subordinate components of the IC, many of which are located within other Cabinet agencies.

The ODNI needs to direct, not replicate in-house, the other IC agencies' analytic, operational, and management functions. Considerations like mismanagement of human resources, joint-duty assignments, and accelerated growth in senior personnel can cause a President to dictate to his incoming DNI a desire to slash redundant positions and expenditures while simultaneously giving the DNI the authority to drive necessary changes throughout the IC to deal with the nation's most compelling threats, including those emanating from China. As John Ratcliffe has noted, "These are essential to the DNI having the abilities and authorities to effectively direct, coordinate, and tackle the immense national security challenges ahead for the Intelligence Community as intended under IRTPA."[11]

Otherwise, other Cabinet and subordinate IC agencies will continue to regard the ODNI as an annoyance and not as a positive contributor to the National Intelligence Program (NIP) budget. They will continue to work around or circumvent ODNI leadership decisions with appropriators and the Office of Management and Budget (OMB) or seek to wait out an Administration or DNI to prevent a policy or intelligence priority from reaching fruition.

Intelligence and interagency coordination has improved significantly since 9/11. Nevertheless, interagency rivalries and festering issues continue to cause duplication of effort on intelligence analysis and technology purchases as well as overclassification and ever-increasing compartmentalization. Additional issues include the abuse of mandated onboarding approval and reciprocity timelines by some agencies, recruitment and retention failures, and a lack of will to remove underperforming or timely adjudicate the misconduct of senior managers and other employees.

Finally, future IC leadership must address the widely promoted "woke" culture that has spread throughout the federal government with identity politics and "social justice" advocacy replacing such traditional American values as patriotism, colorblindness, and even workplace competence.

EXECUTIVE ORDER 12333

IRTPA was passed in the aftermath of the 9/11 attacks against the homeland. It was intended to improve the sharing of information among the elements of the IC, recognizing that the nature of the threats we now face blurs the lines between foreign and domestic intelligence in detecting and countering national security threats against the homeland. An equally important objective in passing the most significant intelligence reform since the National Security Act of 1947[12] was creation of the position of DNI, charged with assuming two of the three principal roles that formerly belonged to the Director of Central Intelligence (DCI): serving as principal intelligence adviser to the President and leading the IC as an enterprise.

Nearly two decades later, the DNI's record of effectiveness in improving the sharing of information and operating the IC as an enterprise is mixed. Implementation of the DNI's roles as leader of the IC and principal intelligence adviser to the President has been challenging. However, despite flaws in the legislation and intelligence agencies' bureaucratic jockeying that undermine the DNI, it is impossible to know what would emerge if Congress were to revisit the act. Seeking a legislative solution therefore might carry with it more risks than benefits. Instead, an incoming conservative President's immediate focus should be on modifying Executive Order 12333, the President's direction for implementing IRTPA.[13]

Executive Order 12333 was last amended on July 30, 2008, by President George W. Bush.[14] The revisions were aligned with IRTPA with significant emphasis on having the IC address the threats to the homeland from international terrorism and the proliferation of weapons of mass destruction. There is scant mention of cyber threats and the evolving national security challenges posed by China, Russia, and other U.S. adversaries. By extension, the revised order fell short of stipulating how the DNI would execute his authority to organize the IC in a manner that improves the delivery of timely intelligence to a wide array of customers.

Executive Order 12333 should be amended to take account of the changing landscape of threats and improve the functional aspects of America's intelligence enterprise. To that end, a revised order should:

- **Address the threats to the United States and its allies in cyberspace.** These threats range from cyberwarfare to information operations. The amended order should clearly delineate the roles and responsibilities of the various U.S. government cyber missions, including the recently created National Cyber Director's Office and power centers at the NSC, while protecting the privacy and civil liberties of U.S. citizens.

  Under the DNI's direction, the cyber mission should explicitly identify how information in the cyber domain will be shared promptly with the warfighters, from law enforcement agencies to the broader IC and state,

local, and tribal elements. The order should consider stipulating what to do with DOD cyber agencies, most notably the NSA, in terms of strategic (for example, the President and the DNI) vs. tactical support (for example, support for the warfighter) in conjunction with ongoing congressionally mandated reviews of the future dual-hatted relationship.

- **Enhance the DNI's role in overseeing execution of the National Intelligence Program budget under the President's authority.** This should be done in a manner that is consistent with Congress's intent as embodied in IRTPA. Under the executive order as written today, the DNI "shall oversee and direct the implementation of the National Intelligence Program." In practice, the DNI's authority to oversee execution of the IC's budget remains constrained by an inability to address changing intelligence priorities and mandate the implementation of appropriated NIP funding to higher intelligence priorities.

  The DNI should have the President's direction to address emerging but catastrophic threats such as those posed by bioweapons. Clarifying how much budget authority the DNI has in conjunction (within the limits of congressional appropriations) with OMB and IC-member Cabinet officials to move around money and personnel is crucial, but positions will not always be fungible. It will probably be necessary to hold IC leadership accountable at intransigent agencies and to restructure areas through executive orders in close conjunction with OMB, as needed.

- **Clarify the DNI's role as leader of the IC as an enterprise in building the IC's capabilities around its open-source collection and analytic missions.** The exponential growth in open-source information, often called OSINT, is not disputed. In the IC, the use of publicly available information, notwithstanding the authorities within IRTPA for the DNI to manage OSINT, remains disaggregated. The explosion of private-sector intelligence products and expertise should signal to IC leadership that duplicative efforts are unnecessary and that limited resources should be focused on problematic collection tasks.

  The IC should avoid duplication of what is already being done well in the private sector and focus instead on complex questions that cannot be answered by conventional and frequently increasing numbers of commercial tools and capabilities. If necessary, for lack of results from the National Open Source Committee, the DNI should appoint the Principal Deputy Director of National Intelligence (PDDNI) as chairman to prioritize and promote accountability for the IC's 18 agencies toward this effort.

- **Prioritize security clearance reform.** Security clearance reform has made significant progress under Trusted Workforce 2.0, a governmentwide background investigation reform that was implemented beginning in 2018 with the goal of creating one system with reciprocity across organizations. This included allowing movement from periodic reinvestigations toward a Continuous Vetting (CV) program with automated records checks, adjudication of flags, the "mitigat[ion of] personnel security situations before they become a larger problem," or the suspension or revocation of clearances.[15] However, human resources onboarding operations in major agencies such as the CIA, FBI, and NSA remain to be resolved.

  As executive agent for security clearances, the DNI must require results from agencies that resist implementation, enforce the 48-hour reciprocity guidance, and target human resources operations that fail to attract and expediently onboard qualified personnel. Additional "carrots and sticks" from executive order reform language, including moving the Security Services Directorate from NCSC to ODNI with elevated status, may be necessary. It is unacceptable for agencies to hinder opportunities for cross-agency assignments, use public–private partnerships inefficiently because of constraints on the transferability of security clearances, and lose future talent because of extraordinary delays in backend operations. Proper vetting to speed the onboarding of personnel with much-needed expertise is vital to the IC's future.

- **Ensure the DNI's authority.** The DNI's authority should be similar to an orchestra conductor's. An incoming conservative President will appoint whomever he chooses as DNI, but there should be agreement between the incoming DNI and President with advice and counsel from the Presidential Personnel Office on selecting positions overseen by the DNI throughout subordinate agencies, as well as concurrence by relevant Cabinet officials and the CIA. This exists by executive order, but many Presidents, PPOs, and Cabinet agency heads do not follow executive order guidance and necessary norms. The importance of trust, character, and the ability to work together to achieve a joint set of intelligence goals established by the President cannot be overstated: It is a mission that can be accomplished only with the conductor and his orchestra playing in sync.

- **Provide additional support for such economic and supply chain–focused agencies as the Department of Commerce.** Information sharing and feedback can help subagencies like the Commerce Department's Bureau of Industry and Security to improve their understanding of the

threat from China and thereby counter it more effectively. They can also aid the development of export control mechanisms and potential outbound investment screening where necessary. Brief, specific governance language should be considered that would apply counterterrorist authority models to the broader functions of the U.S. government insofar as they are needed to counter 21st century nation-state threats.

The success of any DNI rests with support from the President. Any revised Executive Order 12333 must serve to express unequivocal support for the DNI in executing the mandates that an amended order would provide.

CENTRAL INTELLIGENCE AGENCY (CIA)

The CIA is a foreign intelligence collection service tasked with collecting human intelligence (HUMINT), providing all-source intelligence analysis and reporting, and conducting covert action when required to do so by the President. The CIA has its roots in the Office of Strategic Services (OSS), which the United States established during World War II as a paramilitary and intelligence collection organization. After World War II, President Harry Truman disbanded the OSS, and the CIA was established in law by the National Security Act of 1947.

As with every agency in government, the President's election sets a new agenda for the country. Public servants must be mindful that they are required to help the President implement that agenda while remaining apolitical, upholding the Constitution and laws of the United States, and earning the public trust. The President requires a CIA that provides unbiased and apolitical foreign intelligence information and, when necessary, can act capably and effectively on any covert action findings.

Executing the Mission. The CIA's success depends on firm direction from the President and solid internal CIA Director–appointed leadership. Decisive senior leaders must commit to carrying out the President's agenda and be willing to take calculated risks. Therefore:

- The next President-Elect and incoming Presidential Personnel Office should identify a Director nominee who can foster a mission-driven culture by making necessary personnel and structural changes.

- The President-Elect should choose a Deputy Director who, without needing Senate confirmation, can immediately begin to implement the President's agenda. This includes halting all current hiring to prevent the "burrowing in" of outgoing political personnel. Additional appointees should be placed within the agency as needed to assist the Director in supervising its functioning.

- The Director and Deputy Director should request briefings on all CIA activities and presence overseas, as well as any CIA-controlled access programs and existing covert action findings, without exception.

- The Director and Deputy Director should meet with all directorates and mission centers, prioritizing those that are aligned most closely with the President's priorities and calibrating collection and operations based on the President's intelligence requirements. This includes any areas where the CIA might be conducting its own diplomacy parallel to official State Department policy. It must be clear that the CIA's liaison relationships overseas must follow and not contradict those set at the policy level by the President through the State Department.

The other principal offices responsible for executing the CIA's mission include the Directorate of Operations, Directorate of Analysis, Directorate of Science and Technology, Directorate of Support, and Directorate of Digital Innovation. If senior leadership finds any program or operation to be inconsistent with the President's agenda, the Director should immediately halt that program or operation.

Reining in Bureaucracy. The CIA's bureaucracy continues to grow. Because mid-level managers lack accountability, there are areas in which personnel are not responsive to any authority, including the President. The President should instruct the Director to hire or promote new individuals to lead the various directorates and mission centers. This new crop of mid-level leaders should carry out clear directives from senior CIA leadership, which means more accountability and new ways of thinking to benefit the mission.

In addition, the President should task the Director with significantly broadening recruitment, expediting onboarding practices, and shifting resources away from headquarters, including terminal generalist GS-15s when OPM buyouts, forced rotations, or up-and-out personnel policies are set for particular positions. The CIA must find creative ways to align mission requirements with hiring needs, recruit diverse sets of individuals with unique backgrounds, and become more open to hiring private-sector experts directly into senior positions. In addition, the Director should break the cabal of bureaucrats in D.C. by permanently moving various directorates, such as Support and Science and Technology, out of Virginia and possibly open campuses outside of D.C. where analysts and other experts could contribute virtually.

Redirecting Resources. Certain CIA employees and offices have focused on promoting divisive ideological or cultural agendas and fostering a damaging culture of risk aversion and complacency. As soon as possible, the Director should divert resources from any activities that promote unnecessary and distracting social engineering. The Director should implement changes in promotion criteria

that reward individuals for creative thinking and quality of recruitments and products rather than numeric metrics or the achievement of benchmarks that are not essential to the mission.

Not all careers in espionage are created equal, and the Director should incentivize and reward applicants who are willing to accept high risks over those who are climbing the ranks simply by doing business as usual. The Director should refocus the CIA to an OSS-like culture and mandate that all CIA employees acquire, as a condition of securing senior (GS-14+) rank, additional or enhanced language skills, technical or cyber expertise, or field training or serve in overseas assignments.

COVERT ACTION

Covert action can be a valuable tool in helping further the President's foreign policy agenda if implemented in concert with other forms of government power. As codified in the U.S. Code, "the term 'covert action' means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly...."[16]

The President initiates a covert action with a written finding that explains why "such an action is necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States."[17] The statute assumes the President will use the CIA as the principal action element to achieve the objectives of covert action findings; however, the President need not feel constrained to utilize only the CIA: "[E]ach finding shall specify each department, agency, or entity of the United States Government authorized to fund or otherwise participate in any significant way in such action."[18]

For example, the Department of Defense maintains certain clandestine capabilities under Title 10 authorities that may resemble but far exceed in scale similar capabilities outside of DOD. Generally, such DOD capabilities can be employed outside a combat theater only if they are determined to be traditional military activities. In practical terms, this means that many DOD capabilities, including those in the space and cyber domains, can be employed only after the initiation of armed conflict.[19] Given the range of global threats the United States faces today, the President should consider whether DOD's complete set of capabilities should be used to support potential covert actions.

The problem, unfortunately, is that certain elements in the State Department, IC, and DOD trade on risk aversion or political bureaucracy to delay execution of the President's foreign policy goals. A future conservative President should therefore identify individuals on the transition team who are familiar with the implementation of covert action with a view to placing them in key NSC, CIA, ODNI, and DOD positions. These knowledgeable teams can assist in any review of current covert actions and, potentially, planning for new actions.

Immediately after the inauguration, the President should task the NSC's Senior Director for Intelligence Programs with conducting a 60-day review of any current covert action findings, including their effectiveness; evaluating new covert actions that might be needed to implement the President's foreign policy goals; and reporting back to the President. Such an assessment should be conducted independently of the agencies responsible for the actions under review. As part of the review, the Senior Director for Intelligence Programs should identify which departments or agencies, such as the CIA or DOD, are best equipped to achieve the objectives set out in new and existing findings.

After the 60-day review, the President should demand creative thinking and a clear strategy as to how covert action fits within the President's broader foreign policy strategy, to include possibly modifying or rescinding any current findings, drafting new findings, and streamlining or eliminating needless bureaucracy, particularly at State, to facilitate more expeditious decisions on tactical covert action. Careful thought should be given to the metrics by which the effectiveness of covert action programs will be measured to ensure the appropriate use of government resources and to guard against the possibility of covert action's being used with little scrutiny in ways that are inconsistent with overt foreign policy goals.

ODNI AND CIA ORGANIZATIONAL RECOMMENDATIONS

The ODNI and CIA operate under authority provided by the Central Intelligence Agency Act of 1949,[20] which means they have greater latitude than the rest of the federal government with respect to the hiring and firing of personnel. Both organizations and other areas of the IC have struggled from a human resources and talent management standpoint to recruit, onboard, and maintain personnel in a timely fashion to fill the IC's ever-changing needs. At a time when the Intelligence Community needs significantly more personnel with the proper technical, language-capable, and diverse backgrounds, including applicants from elements of the business community, the incoming Directors of both agencies need to make this effort a top priority.

Past DNIs' Chiefs of Staff and additional front-office staff historically have come from outside the IC, commonly under a misconstrued "staff-reserve" structure that is intended to avoid a Schedule C designation within the IC. The Director should handpick qualified, properly cleared personnel for front-office and managerial leadership positions, such as the DNI's Chief of Staff and heads of Legislative Affairs and Strategic Communications, to oversee those divisions with career IC staff reporting to them.

The incoming DNI and CIA Director should also consider changes in the Senior National Intelligence Service (SNIS)/Senior Intelligence Services (SIS). Senior officers should be required to sign mobility agreements that allow ODNI and CIA leadership to move them within the IC every two years if necessary. Many qualified

and distinguished senior officers serve throughout the IC, but some long-serving generalist officers no longer perform at a high capacity, are management-driven, do not serve the IC's changing needs, and limit junior officers' prospects for growth and advancement. An incoming Administration should consider studying and implementing additional requirements as a condition for promotion to GS-15/SNIS/SIS and explore concepts such as "Up and Out" beginning at the GS-14/15 levels and above for some fields.

The IC should evaluate areas of bloat and underperforming cadre and work with OPM on authority for voluntary separation buyouts. Allowing ODNI and CIA leadership to shrink size and reduce duplication of effort while promoting healthy turnover within their senior ranks would encourage new ideas and perspectives from mid-career officers and, potentially, from employees hired from outside their agencies. The ODNI and CIA should maximize their direct-hire and incentive-building authorities to bring in talented and properly cleared individuals to serve in positions requiring technical, language, and cyber expertise.

Finally, the human resources and talent management systems for onboarding purposes at the ODNI, CIA, and some other elements of the IC are fundamentally broken. For example, according to current CIA Director William Burns, it recently took more than 600 days, on average, for a CIA applicant to receive his or her necessary security clearance.[21] Although security clearance procedures have been somewhat improved in recent years and Burns has committed CIA to reducing that to no more than 180 days, degradation in other areas of the process has limited the IC's capacity to attract qualified and needed expertise.

PREVENTING THE ABUSE OF INTELLIGENCE FOR PARTISAN PURPOSES

The intelligence function must be protected from bottom-up and top-down politicization if it is to play its proper role in our national security decision-making process. Unfortunately, both types of politicization have occurred recently to the detriment of the Intelligence Community's reputation and credibility. More important, the politicization of intelligence risks contributing to policy failures (as we saw with the Iraq War) or even undermining our democratic system here at home.

In particular, the IC must restore confidence in its political neutrality to rectify the damage done by the actions of former IC leaders and personnel regarding the claims of Trump–Russia collusion following the 2016 election and the suppression of the Hunter Biden laptop investigation and media revelations of its existence during the 2020 election. But the problem is not confined to the executive branch struggle between the IC and policymakers; it also relates to the IC's relationship with Congress as evinced by DNI James Clapper's failure to answer honestly in response to congressional questions about government surveillance programs.

The ODNI and CIA are undergoing a crisis of confidence based on several factors. First, President Barack Obama's CIA Director, John Brennan, gravely damaged the CIA by minimizing the Directorate of Operations and exploiting intelligence analysis as a political weapon after he left office. Brennan's role in the letter signed by 51 former intelligence officials before the 2020 election is unclear, but in dismissing the Hunter Biden laptop as "Russian disinformation," the CIA was discredited, and the shocking extent of politicization among some former IC officials was revealed.

Restoring respect for the IC as an independent provider of information and analysis while also ensuring that it is responsive to the legitimate needs of policymakers will require reinforcing essential norms and institutions. However, we should also recognize that achieving the perfect balance that avoids the pathologies of too much distance or too much closeness and responsiveness to policymakers is not only difficult, but probably impossible.[22] Thus, given the very nature of the business and the political process, much will depend on the promotion of certain norms or virtues on both sides of the principal–agent relationship. Specifically:

- The DNI and CIA Director should use their authority under the National Security Act of 1947 to expedite the clearance of personnel to meet mission needs and remove IC employees who have abused their positions of trust. An area of particular concern is that personnel under investigation for improprieties have been allowed to retire before internal investigations have been completed. Directors of both agencies must instill further confidence in their workforces, Congress, and the American people that they can and will deal effectively with personnel that fail to live up to their oath to the Constitution, adhere to ethical and moral standards as expected by America's taxpayers, and faithfully execute the law.

- The President should direct the DNI and the Attorney General, by direction of the respective Inspectors General and IC Analytic Ombudsman, to conduct a further audit of all IC equities of past politicization and abuses of intelligence information. For example, a recent IC ombudsman analysis during the 2020 election cycle noted, "If our political leaders in the White House and Congress believe we are withholding intelligence because of organizational turf wars or political considerations, the legitimacy of the Intelligence Community's work is lost."[23]

- The President should immediately revoke the security clearances of any former Directors, Deputy Directors, or other senior intelligence officials who discuss their work in the press or on social media without prior clearance from the current Director. IC agencies, including the CIA, should minimize their public presence and vigorously investigate any and all leaks

of information, classified or otherwise. The ODNI and CIA should fire or refer for prosecution any employee who is suspected of leaking information, and penalties should include the removal of pension benefits for those who are found guilty. Additional tools are needed to prevent leaked intelligence from being used as a weapon in policy debates by IC leaders or decision-makers in the executive branch or Congress.

- In addition, the Department of Justice should use all of the tools at its disposal to investigate leaks and should rescind damaging guidance by Attorney General Merrick Garland that limits investigators' ability to identify records of unauthorized disclosures of classified information to the media. Personnel have sufficient access to legitimate whistleblower claims under protections provided by Inspectors General and Congress. The Director and IC must prioritize hiring additional counterintelligence and security personnel to assist in this effort.

- Military and civilian IC training should include stronger emphasis on the norm of political neutrality, including a mandatory course on professionalism and repercussions for abuse in the execution of duties in all degree programs at the National Intelligence University.

- Intelligence leaders need to model norms of neutrality and respect for the decision-making authority of the President, appointed officials, and Congress. This includes building trust with key decision-makers by not using their positions and privileged access to information to influence policymaking indirectly or directly in an inappropriate fashion (especially by engaging in threat inflation). IC leaders should practice extreme restraint in engaging with the public and the media. They should seek to work in the shadows rather than in the limelight. Potential restrictions on such appearances could supplement this norm, preventing political leaders from using IC officials to support an Administration position as they do with military leaders.

- Retired IC leaders should similarly support the neutrality norm by not becoming public figures.

- Congress should not use IC leaders as pawns in policy struggles with the President or the other party during their appearances before committees of the House and Senate. While Congress has a proper oversight role, it should distinguish between information that needs to be public and information that should be discussed in private with members of the IC. A DNI should call "balls and strikes" to those on both sides of the aisle on Capitol

Hill who attempt to weaponize the use of selective intelligence to feed political narratives.

- Political leaders should avoid "manipulation-by-appointment," a practice by which intelligence leaders are selected for their policy views or political loyalties instead of their skilled expertise.[24] Presidents should also avoid public rebukes and pressure from the intelligence profession, which can include intimidation and bullying, to shape IC analysis. This will be easier if IC leaders live by the norms of neutrality and thus are not seen as political actors, for whom political responses are deemed necessary.

- Intelligence leaders and professionals should never "cook the books" for Presidents or change or shape their analysis to preserve access or status.[25]

FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

A future President should understand the importance of FISA[26] while also seeking reforms and accountability for any abuses of its authorities. When discussing FISA and what changes may need to be made, it is important to note and recognize that there are stark differences among the individual FISA authorities.

Section 702 of FISA, for example, allows the IC to target foreign terrorists, spies, cyber hackers, and other bad actors (but only if they are non-U.S. persons) when their communications pass through the United States. While this authority may lapse if Congress does not resolve the issue by the end of 2023, Section 702 should be understood as an essential tool in the fight against terrorism, malicious cyber actors, and Chinese espionage. These are two major national security priorities for an incoming President, and it is imperative that the need to use properly maintained and accountable authorities to counter these challenges be recognized.

Section 702 is a vital program that often provides the lion's share of intelligence used in the President's Daily Brief (PDB).[27] An independent review by the Privacy and Civil Liberties Oversight Board (PCLOB) found that it was not abused. Nevertheless, Congress should review the PCLOB's upcoming 2023 report to help it determine whether any reforms or codification of recent administrative changes in FISA processes are needed.

Other authorities in Title I and Title III, often referred to as "traditional" FISA, have elicited valid concerns about the politicization of intelligence collection authority in recent years. When seeking surveillance of Trump campaign adviser Carter Page, for example, the FBI and the Department of Justice concealed vital information from a specialized court and submitted applications that were riddled with errors. An incoming conservative President should consider reforms designed to prevent future partisan abuses of national security authority. A package of strong provisions to protect against such partisanship might include:

- Stiffer penalties and mandatory investigations when intelligence leaks are aimed at domestic political targets,

- Tighter controls on otherwise lawful intercepts that also collect the communications of domestic political figures,

- An express prohibition on politically motivated use of intelligence authorities, and

- Reforms to improve the accountability of the Justice Department and the Foreign Intelligence Surveillance Court.

To keep intelligence credentials from being used for partisan purposes, former high-ranking intelligence officials who retain a clearance should remain subject to the Hatch Act after they leave government to deter them from tying their political stands or activism to their continuing privilege of access to classified government information. The IC should be prohibited from monitoring so-called domestic disinformation. Such activity can easily slip into suppression of an opposition party's speech, is corrosive of First Amendment protections, and raises questions about impartiality when the IC chooses not to act.

CHINA-FOCUSED CHANGES, REFORMS, AND RESOURCES

The term "whole of government" is all too frequently overused, but in responding to the generational threat posed by the Chinese Communist Party, that is exactly the approach that our national security apparatus should adopt. CIA Director William Burns has formally established a China Mission Center focused on these efforts, but it can be successful only if it is given the necessary personnel, cross-community collaboration, and resources. That is uncertain at this point, and just how seriously the organization is taking the staffing of the center is unclear.

A critical strategic question for an incoming Administration and IC leaders will be: How, when, and with whom do we share our classified intelligence? Understanding when to pass things to liaisons and for what purpose will be vital to outmaneuvering China in the intelligence sphere. Questions for a President will include:

- What is our overarching conception of the adversarial relationship and competition?

- How does intelligence-sharing fit into that conception?

Some Members of Congress have said that intelligence relationships such as the Five Eyes[28] should be expanded to include other allies in the Asia–Pacific in, for example, a "Nine Eyes" framework. This fails to take into account the fact that any blanket expansion would necessarily involve protecting the sources and methods of a larger and quite possibly more diverse group of member countries that might or might not have congruent interests. That being said, however, a future conservative President should consider what resources and information-sharing relationships could be included in an ad hoc or quasi-formal intelligence expansion (for example, with the Quad) among nations trying to counter the threat from China.

Significant technology, language skills, and financial intelligence resources are needed to counter China's capabilities.[29] The IC was caught flat-footed by the recent discovery of China's successful test of a nuclear-capable hypersonic missile. No longer can America's information and technological dominance be assumed. China's gains and intense focus on emerging technologies have taken it in some areas from being a near-peer competitor to probably being ahead of the United States. China's centralized government allocates endless resources (sometimes inefficiently) to its strategic "Made in China 2025" and military apparatuses, which combine government, military, and private-sector activities on quantum information sciences and technologies, artificial intelligence (AI), machine learning, biotechnologies, and advanced robotics.

The IC must do more than understand these advancements: It must rally non-government and allied partners and inspire unified action to counter them. In addition, to combat China's economic espionage, authorities and loopholes in the Foreign Agents Registration Act (FARA)[30] will have to be examined and addressed in conjunction with the Attorney General.

Many issues within the broader government can be tied back to a more general congressional understanding of the threat due to the compartmentalization of committee jurisdictions and the responsibilities of executive agencies to brief on the nature of the threat. Broader committee jurisdictions should receive additional intelligence from IC agencies as necessary to inform China's unique and more comprehensive threat across layers of the U.S. government bureaucracy and economy.

Former DNI John Ratcliffe increased the intelligence budget as it related to China by 20 percent. "When people ask me why I did that," he explained in an interview, "I say, 'Because no one would let me increase it by 40%.' I had an $85 billion combined annual budget for both the national intelligence program and military intelligence program. My perspective was, 'Whatever we're spending on countering China, it isn't enough.'"[31] From an intelligence standpoint, the need to understand Chinese motivations, capabilities, and intent will be of paramount importance to a future conservative President. It is therefore also of paramount importance that the "whole of government" be rowing together.

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER (NCSC)

The Senate Select Committee on Intelligence (SSCI) has taken a keen interest in possibly updating the codified language underpinning much of the nation's counterintelligence apparatus. "Spy vs. spy" threats continue to exist, but the rise of China and (to an extent) Russia's machinations move beyond the governmental sphere to technological, economic, supply chain, cyber, academic, state, and local espionage threats at a level our country has never seen. The asymmetric threat includes cyber, nontraditional collection, and issues involving legitimate businesses serving as collection platforms.

Barring statutory changes that could occur before 2025, a future conservative President should further empower and resource the IC by executive order or through suggested changes in the Counterintelligence Enhancement Act (CEA) of 2002.[32] NCSC was given some authority for outreach efforts on behalf of the IC for counterintelligence education, insider threats, and broader U.S. government best practices, but there remain significant deltas between Title 50 and non–Title 50 entities' protections. Primary operational elements should remain at the FBI and CIA, with the Bureau and NCSC collaborating on nongovernmental outreach.

While there is no need to create a separate agency, a future President and DNI should amplify NCSC's authorities and roles with respect to counterintelligence strategy, policy, outreach, and governance, including supporting necessary Joint Duty Assignments (JDA) for FBI and CIA personnel. At the same time, the FBI requires significant additional resources and legal authorities to fulfill its statutory role as the lead operational counterintelligence agency in dealing with the ever-growing threats posed by our adversaries. The CEA should be updated to include foreign espionage efforts aimed at universities.

Corporate America, technology companies, research institutions, and academia must be willing, educated partners in this generational fight to protect our national security interests, economic interests, national sovereignty, and intellectual property as well as the broader rules-based order—all while avoiding the tendency to cave to the left-wing activists and investors who ignore the China threat and increasingly dominate the corporate world. Reinstitution of the National Security Higher Education Advisory Board and the National Security Business Alliance Council should be prioritized with leadership from the NCSC, the FBI, or a combination of both entities.

When the CCP steals at least $400 billion–$600 billion in intellectual property each year, it is time to devote some strategic thinking to exactly how and to what degree counterintelligence efforts can help to protect America's commercial endeavors. If Chinese strategic technology gains are happening almost entirely in transnational commercial space, for example, and the private sector is also gathering and analyzing some critical intelligence, these essential data points should assist in national-level counterintelligence efforts.

The NCSC was created in the aftermath of 9/11 as the Terrorist Threat Integration Center (TTIC), which later became the National Counterterrorism Center (NCTC) pursuant to President George W. Bush's Executive Order 13354.[33] The NCTC was an organization of approximately three dozen detainees from across the U.S. government with a mandate to integrate counterterrorism intelligence and missions, including terrorist screening. Eventually:

> In November 2014 the Director of National Intelligence (DNI) established NCSC by combining [the Office of the National Counterintelligence Executive] with the Center for Security Evaluation, the Special Security Center and the National Insider Threat Task Force, to effectively integrate and align counterintelligence and security mission areas under a single organizational construct. The Director of NCSC serves in support of the DNI's role as Security Executive Agent (SecEA) to develop, implement, oversee and integrate personnel security initiatives throughout the U.S. Government.[34]

NCSC has added value in such areas as fusing cross-community intelligence for terrorism watchlisting purposes and improving information sharing while carrying roughly half of the overall cadre for the ODNI. An incoming Administration should focus NCTC on integrative tasks, many of which cannot be carried out elsewhere in the IC, but should not use personnel and resources for redundant analyses that duplicate the work of such other IC entities as the FBI and CIA.

ADDITIONAL AREAS FOR REFORM

Analytical Integrity. The "tradecraft" of intelligence analysis is mostly a collection of lessons learned over decades about what works and does not work in a profession whose high-stakes work is performed by thousands but that also bears little outside scrutiny and provides few metrics by which to gauge success or failure on a regular basis. These lessons have accumulated from:

- The perceived misuse of intelligence by consumers as was the case with respect to war-related assessments in the Johnson and Bush Administrations;
- Failures such as the failures to warn of the collapse of the Soviet Union and the specific threat of 9/11;
- Successes in piecing together tactical and often technical puzzles such as estimates of Iranian nuclear program maturation; and
- Strategic victories such as anticipating critical geopolitical developments that have been years in the making.

Historically, this tradecraft has been passed on in the form of unwritten rules learned on the job and in agency-specific training classes, but increasingly since the intelligence reforms of 2004, they have been codified IC-wide under the direction of the Deputy Director of National Intelligence for Mission Integration.

A RAND study of U.S. intelligence tradecraft notes that the "vast majority of intelligence analysts reside outside the Central Intelligence Agency and do work that is tactical, operational, and current."[35] The study goes on to note that the Defense Intelligence Agency (DIA) has as many analysts as the CIA has and that the National Security Agency (NSA) has several times as many analysts, as does the National Geospatial-Intelligence Agency (NGA), indicating both the breadth of the IC's technical collection and its emphasis both on developing analysts who can interpret secret human or technical intelligence in quick-turnaround pieces and on countering tactical, asymmetric threats like terrorism.

During the Cold War, however, there was a more balanced analytic focus with greater emphasis on strategic intelligence issues as a means of outcompeting the Soviet Union. This kind of analysis deals not only in secrets, but also in mysteries—making well-founded but ultimately unknowable predictions about future actions by a competitor or adversary. The tradecraft necessary to succeed in strategic analysis requires substantive regional and topical expertise developed over the years to supplement experience in the daily collection and understanding of secrets. Institutionally, it also requires that agencies' analytic processes be open to discussion, debate, and dissent because analysts must work together to describe a probable range of future outcomes and warn about unproven current threats rather than using the collection to solve a single puzzle with a definitive answer.

Regarding its mission to follow longer-term issues, the IC is falling short in resourcing and in openness to dissenting opinions, which (if taken seriously) can help responsible officials respond more effectively to threats and threat actors. The IC Analytic Ombudsman has expressed concern that hyperpartisanship "has threatened to undermine the foundations of our Republic, penetrating even into the Intelligence Community."[36]

For example, the Ombudsman noted in a report on the IC's handling of election-threat analysis in 2020 that, in his view, CIA officials had deliberately downplayed dissenting views and coordination comments expressed by experts at the National Intelligence Council and elsewhere who felt there was evidence of Beijing's intent to exert at least some influence on the 2020 election as opposed to the consensus view that Beijing did not interfere in U.S. elections. Senior CIA analysts and leaders made it "difficult to have a healthy analytic conversation in a confrontational environment" while violating multiple official IC tradecraft standards. By not allowing dissents or considering alternatives, the CIA exercised "undue influence on intelligence."[37] Subsequent exposure of China-linked online

influence and the FBI's warnings about continued efforts through the 2022 midterms highlight the folly of undue certainty without consideration of alternatives.

On election influence and other controversial issues, such as the origin of COVID-19, analysts at the most powerful intelligence agencies have increasingly tended to use the leeway they have been given to insert their political views into their work in order to influence (if possibly even control) the analytic process. They do this in ways that attempt to squash dissent and impair the creation of a culture in which entrenched views are challenged and unpopular analytical lines can survive or not according to their merits.

To help the United States and its leaders to outcompete China across multifaceted societal, economic, military, and technological threats, the IC's capability to conduct strategic intelligence analysis that is relevant to policymakers in both parties must be rebuilt and strengthened. Because Beijing may be a peer or even exceed U.S. capabilities in some areas, the post-9/11 analytic focus on quick-turnaround secrets is not good enough. Strategic planning—informed by intelligence—must take place for the United States to stay ahead of whatever new threats China may pose.

An incoming conservative President will have the opportunity to signal the demand for such strategic products and prioritize their production through communications to intelligence leaders and formal mechanisms such as shifting priorities within the National Intelligence Priority Framework and structuring the President's Daily Brief. The incoming DNI should also emphasize implementing the recommendations in the Ombudsman's report, especially regarding objectivity, the inclusion of dissenting viewpoints, and more serious efforts to hold senior leaders accountable for backchannel attempts to change or suppress analytic views.

Accounting for the long history of intelligence failures and surprises, an incoming conservative President must appreciate the ambiguity, complexity, limits, and assumptions inherent in intelligence assessments. Intelligence often deals with the human dimension in complex decision systems within a foreign country or organization, and this makes consistently accurate predictions difficult if not impossible to develop. Seeing something and understanding what you are seeing are two different things, so a President should consistently and patiently press the IC about its potential biases, assumptions, methodology, and sourcing.

With regard to election-threat analysis and politically controversial topics, agency leaders should take seriously the Ombudsman's admonition that we need to maintain tradecraft standards across all countries and topics by ensuring that equitable standards apply across all foreign threat actors. Analysis should be put forward without regard to the domestic political ramifications of intelligence conclusions.

"Obligation to Share" and Real-Time Auditing Capability. The federal government has made admirable progress in recent years by being more

forward-leaning in sharing cyber threat intelligence with private-sector partners and the public, emphasizing that the protective nature of such information is of value only if put into the right hands at the right time. Since critical infrastructure and services are overwhelmingly owned, managed, and defended by the private sector in the United States, there has been an increasing emphasis on declassifying intelligence and sharing actionable information with private-sector partners, often through industry-specific Information Sharing and Analysis Centers (ISACs); regional meetings of government and private-sector experts called InfraGard, run by the FBI; direct public notification from the Department of Homeland Security, the FBI, and (increasingly) the NSA; and more discreet one-on-one engagements led by the collecting agencies.

These programs properly recognize the private sector's role in providing cybersecurity for Americans; in practice, however, the intelligence shared by the U.S. government through these venues is too often already known or no longer relevant by the time it makes its way through the downgrade process for sharing. In addition, government-shared information often needs to take advantage of the opportunity to provide contexts, such as attribution, trends, and size of the observed cyber problem. As warranted, additional context should be provided to the private sector as a matter of routine.

To continue improving the U.S. government's ability to defend the country's most vital networks, the IC must adopt an "obligation to share" policy process, including the capacity for "write to release" intelligence products whereby newly discovered technical indicators, targeting, and other intelligence relevant to cyber defense are automatically provided either to the public or to targeted entities within 48 hours of their collection—which is how counterterrorism intelligence has been managed for years when it comes to a "duty to warn." Under this policy, agency heads should still have the flexibility to withhold intelligence for operational or counterintelligence reasons but would need to report regularly to Congress on the number of and justification for exceptions. This policy would make sharing intelligence and defending networks the default, as it already is in the rest of the cybersecurity community outside the IC, to improve the quantity, relevance, and timeliness of defensive information while ensuring accountability for top leaders when they must withhold this information.

One of the most significant challenges within the IC is presented by the need to share information promptly among the 18 elements of the intelligence enterprise. The only long-term solution to the understandable tension between the need to share information and the need to protect intelligence sources and methods is a robust real-time auditing capability that electronically flags unauthorized access. Under an identity management system with real-time audit, even the most sensitive information acquired by America's intelligence agencies can be shared, and the access to and use of that information are appropriately monitored. Establishing

a real-time auditing capability is essential to decreasing the risk for the heads of intelligence agencies in meeting their statutory requirements to ensure that they protect sources and methods associated with the classified information their agencies collect.

Overclassification. There is broad consensus across the U.S. government and among stakeholders that the system for classifying, declassifying, and otherwise marking and handling sensitive information is at a crossroads. Exorbitant amounts of classified data are created daily, and agency personnel often mistakenly choose classification as the default selection to ensure national security. At the same time, the effectiveness of downgraded and carefully declassified information to support foreign policy efforts has been borne out in, for example, alerting the broader world of Russia's buildup and likely plans for its invasion of Ukraine.

Two executive orders principally govern how the U.S. government handles classified and sensitive information.

- Executive Order 13526, "Classified National Security Information," issued in 2009,[38] prescribes the classification levels and procedures for declassification.

- Executive Order 13556, "Controlled Unclassified Information," issued in 2010,[39] aimed to establish a uniform program for managing all unclassified information that requires safeguarding or dissemination controls.

The current system for declassifying classified national security information (CNSI) is extraordinarily analog, requiring experts' review of individual records. Declassification policies are based on human review of paper and need to contemplate and handle the proliferation and volume of digital records created by agencies. The U.S. government will soon reach the point at which manual review is impossible. The declassification of CNSI should support key U.S. national security objectives, reflect mission priorities, and not serve solely as a necessary procedural function. Reforms should include:

- Tighter definitions and greater specificity for categories of information requiring protection.

- More stringent policies to effect significant reductions in the number of Original Classification Authorities (OCAs).

- Stricter accountability measures at the OCA level and more detailed security classification guides.

- Enhanced metrics for accuracy of classification.
- A general simplification of the overall system for the benefit of users.

On the back end, an ODNI-run declassification process that is faster, nimbler, default-to-automated, and larger-scale should be a priority.

Additionally, investments in IT are required to deal with the growing volumes of CNSI collected and produced in the digital age, along with many years' worth of existing analog and digital holdings that could provide valuable historical insights. An incoming Administration needs to explore options to prioritize funding for innovation in declassification management: for example, by establishing a budget line item specifically for the modernization of declassification or designating funding for program classification management as a special-interest item.

The Administration will also need to transition to using technology, including tools and services for managing Big Data (which provide a robust electronic record repository, making information within and across agencies easier to organize and locate and facilitating more rapid review and release capabilities for records of emerging interest); artificial intelligence/machine learning (which, when incorporated into existing business practices, enables machine interpretation of unstructured text and data, applies decision support technology to enable more consistent classification decisions, and expedites reviews between agencies); and expansion of Commercial Cloud services (which facilitate the rapid testing and deployment of new tools and technologies).

However, technology is not a panacea; human expertise in information holdings and routine validation of the technology will always be necessary. With or without machine assistance, agencies will require more people and more varied skill sets to improve their ability to meet the electronic records era's classification and declassification demands and serve an incoming Administration's goals.

Broader U.S. Government and IC Intelligence Needs. Increasingly, conflicts among U.S. adversaries such as China, Russia, Iran, and North Korea are conducted in the realms of technology and finance.[40] This challenge requires new tools, authorities, and technological expertise across the U.S. government, particularly at the Commerce Department's Bureau of Industry and Security (BIS) and the Committee on Foreign Investment in the United States (CFIUS), which is housed at the Treasury Department.

An incoming conservative President should task his DNI and Secretary of Commerce with increasing coordination, the resources needed for BIS and SCIF capacity, and proper and necessary intelligence sharing to counter the activities of multifaceted adversaries such as China. This would include additional work with private-sector expertise, granting clearances to niche sector experts and United States citizen commercial and financial partners as needed.

Cover in the Digital Age. Even in the public domain, it is becoming increasingly clear that protecting the identities of undercover intelligence officers is difficult in the digital age.[41] The truth is that as our daily activities are conducted predominantly in the digital domain, our antiquated system for providing cover to undercover officers has lagged woefully behind the threat from foreign adversaries.

The DIA, CIA, and FBI are increasingly aware of this threat and are devoting resources to the problem. Their back-office infrastructure, however, is such that they are still using methods for providing cover from decades past that put valuable intelligence officers at unnecessary risk. How intelligence officers and their families are taught to use smartphones and social media, travel, conduct banking, and take and share pictures—even how and when they are paid—can make it difficult to protect identities.[42] Legends, fake backstories, and identities are often weak, incomplete, and unable to stand up to a basic Google search.[43] Officers operating under nonofficial cover are offered even less protection and training to help them succeed.

In addition, ubiquitous technical surveillance (UTS) techniques being refined by technologies emanating from the regimes in China and Russia will continue to be highly challenging for intelligence officers. An incoming Administration will need to double down on resourcing and training so that members of the IC will have the expertise they need to operate clandestinely (and successfully) against hard targets.

Privacy Shield. For many years, the European Union (EU) has tried to force U.S. companies operating in Europe to follow its data privacy regulations. Misleading claims in the 2013 Snowden leaks destroyed the initial Safe Harbor Framework[44] that allowed American companies to transfer data across the Atlantic; its successor, the Privacy Shield Framework,[45] was struck down by European courts on the grounds that it provides insufficient protections for EU citizens against hypothetical U.S. government surveillance. Those same European courts exempted the intelligence services of EU member states from the standards applied to the U.S., suggesting that trade protectionism may be the real motive behind data privacy regulations.

In 2022, the Biden Administration negotiated a new agreement, the Trans-Atlantic Data Privacy Framework,[46] intended to withstand European legal challenges. Given the fate of its predecessors, it is not certain that it will survive. Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities,"[47] implements this new framework by attempting to align signals intelligence collection practices with European privacy regulations. At most, the executive order's changes will be helpful support for the framework in future European litigation; at worst, they could throw sand in the gears of important intelligence programs.

An incoming conservative President should reset Europe's expectations. Brussels has always arbitraged the difference between being a military ally against, for

example, Russia and conducting a full-blown trade conflict with the United States. Restrictions on data exports have been part of the trade conflict, but now they could seriously harm our military and intelligence capabilities. Moreover, restrictions on U.S. intelligence collection hurt the Europeans themselves, especially as the United States shares unprecedented amounts of intelligence on Russia's invasion of Ukraine with Europeans.[48]

Europe is telling the United States to meet intelligence oversight standards that no European country meets. At the same time, exports of data to China are unexamined and (so far) free from legal challenges. That violates World Trade Organization agreements as an arbitrary and discriminatory data protection standard. It is a betrayal by a nominally allied jurisdiction. European court rulings that struck down prior data privacy frameworks were grounded not in constitutional law but in a treaty among European nations. If the EU accepted an international agreement that data may flow to the United States under a more reasonable standard than the one adopted by the court, that interpretation would be binding, at least as a gloss on the earlier treaty.

The United States has never seriously pushed back against the EU; now is the time. An incoming President should ask for an immediate study of the implementation of Executive Order 14086 and suspend any provisions that unduly burden intelligence collection. At the same time, in negotiations with the Europeans, the United States should make clear that the continued sharing of intelligence with EU member states depends on successful resolution of this issue within the first two years of a President's term. It is time for a real solution, not the 30 years of stopgaps imposed by Brussels.

President's Daily Brief (PDB). An incoming conservative President should make clear what the President's Daily Brief is and is not. The PDB should be for the President specifically, with a much narrower distribution and addressing areas of strategic concern. During the transition, the future National Security Advisor, along with the DNI, should conduct a review of current PDB recipients and determine which should remain recipients when the President's term begins.

Instead of being used as the statement of record for the agencies, the PDB often misses the areas of interest for Presidents and their senior advisers. The President should want the PDB to focus on providing the information needed for the often imperfect and complex decisions that a President needs to make, which should always be based on the best intelligence that can be gathered. Where consensus and agreement are possible, an IC-coordinated product is excellent, but insights provided by properly channeled dissent can lead a President to ask relevant questions of his DNI and IC.

A future DNI determines the PDB briefer based on recommendations made by the Deputy Director of National Intelligence for Mission Integration (MI). Historically, briefers have come from the CIA, but a future President and DNI should

consider a primary briefer or a rotation of briefers from other IC elements. Additionally, the entirety of the PDB staff and production should be located at ODNI.

National Intelligence Council (NIC). The National Intelligence Council is the IC's premier analytic organization and includes more than a dozen National Intelligence Officers (NIOs), each of whom leads the IC's analysis within a regional (China, Russia, Iran, etc.) or functional (cyber, counterproliferation, economics, etc.) mission area. This includes authoring National Intelligence Estimates on major strategic issues with the entire IC, overseeing and deconflicting the annual analytic plans of each agency, and weighing in on day-to-day major analytical issues, sometimes individually (for example, by writing the NIC's strategic memos or providing detailed expert briefings to the President before major decisions).

Historically part of the CIA, the NIC was reorganized into the ODNI as was the PDB. It retains the CIA's objective analytic culture and is staffed primarily with CIA officers; however, as many as 25 percent of its NIOs over the decades have come from academia or the private sector, bringing in much-needed outside expertise to collate and understand intelligence with perspective and skills that are not necessarily nurtured within the IC. In recent years, there has been a greater emphasis on encouraging officers from other agencies—particularly the DIA, NSA, and FBI—to serve as NIOs or as their deputies.

To encourage greater analytic independence and debate, the incoming Administration should require that non-CIA officers comprise at least 50 percent of the NIC's membership and that the first-among-equals NIC Chairman is an outsider from one of the three major IC agencies with reporting responsibility to the PDDNI. Opening these senior analytic roles to the best analysts regardless of agency would also encourage the continued maturation of analytic cadres and tradecraft at those agencies and give them an equal voice in interagency analytical disputes, which in turn would give the President access to the best thinking and a variety of sources and perspectives from across the entire IC rather than from the CIA alone.

IC Chief Information Officer. The Intelligence Community Chief Information Officer (ICCIO) directs and oversees all aspects of the classified IT budget for all of the IC's 18 elements. As the DNI's principal adviser for technology, the ICCIO must be well-versed in technology, acquisitions, operations, and intra-agency cooperation to advance our technical prowess and simultaneously direct a bureaucracy that, left unchecked, will serve each element's own preferences. To ensure that procured and implemented technology and policy reflect the Administration's agenda, the ICCIO must have the support of the DNI and possess the ability to command cooperation between and promote interoperability across IC members.

Because of the unique responsibilities entrusted to this position, incumbency has seesawed between political appointees and career civilians; due to its congressionally capped salary, the position is often filled by an SES-level member administratively detailed to support the DNI. At times, the ICCIO is incorrectly

referred to as the ODNI CIO. By law, and to secure unbiased execution across all of the IC's 18 elements, the same individual may not serve as ICCIO and ODNI CIO. They are two distinct positions.

Critical areas and IC IT portfolio priorities for the ICCIO include but are not limited to:

- Transparent accounting and allocation of IT investments across the IC, including commercial cloud computing and storage (C2E);
- Recognized and uniform security access for people, systems, and capabilities to enable interoperability across IC elements;
- 5G/6G data transmission and network interoperability, which is vital to IC element operations;
- Artificial intelligence and machine learning;
- Quantum cryptography and post-quantum encryption (PQE); and
- Cybersecurity infrastructure where Biden Administration changes have realigned and reassigned management oversight and IT architecture responsibilities to NSA and DHS/CISA, conflicting with ICCIO-delineated roles.

An incoming Administration should appoint the ICCIO as a primary member of the DNI staff along with the ODNI General Counsel, IC Chief Financial Officer, and ODNI Chief Operating Officer.

The President-Elect should require immediate reviews of the progress in implementing post-quantum encryption at a minimum for IC and Defense systems but preferably throughout the government. The President's National Security Memorandum specifying "the goal of mitigating as much of the quantum risk as is feasible by 2035"[49] needs to be revised in light of the magnitude of the threat. Accounting for the investment that will be needed to secure IT systems for national security should be a top priority.

ODNI, CIA, and IC Technology Issues. In recent years, the IC has had a mandate from multiple Administrations to advance technology needs for intelligence—needs that have seen massive changes as a result of such threats as China's advancements in technology and data infrastructure. Many of the projects coming out of ODNI and CIA's Science and Technology Directorate (S&T) focus on expensive, AI-driven open-source work, but there is likely duplication of effort in areas where the private sector and entrepreneurs are already making progress.

The Intelligence Advanced Research Projects Activity (IARPA) and S&T should focus primarily on challenging technology problems. Avoiding duplication of what is already being done well in the private sector in such areas as practical defense cyber intelligence and artificial intelligence research would help to focus the agencies on the complex shadow tasks at hand while simultaneously freeing limited resources for advancement in other areas.

President's Intelligence Advisory Board and PIAB Intelligence Oversight Board. The President's Intelligence Advisory Board (PIAB) is charged with providing the President with an independent source of advice on the IC's effectiveness while offering insights into the IC's future plans. The Board is meant to have access to all information needed to perform its functions and to have direct access to the President. The Intelligence Oversight Board is a standing committee within the PIAB. These entities should be tasked with giving independent, informed advice and opinion concerning major matters of national security focused on long-term, enduring issues central to advancing and protecting American interests. This should include taking a broader, deeper look at critical trends, developments, and their implications for U.S. national and economic security relying on unclassified and open-source information.

The Importance of Space. With China developing increasingly capable space and counterspace technologies and Russia taking more aggressive action in space, space has emerged as the latest warfighting domain. In response, the DNI created the Office of the Space Executive (OSX) in 2018 as an experiment to promote greater integration of IC space activities without incurring excessive overhead. The DNI mandated greater collaboration across the enterprise without adding personnel, altering authorities, and increasing budgets.

The Space Executive's design reflects the original design principles of the ODNI. The ODNI was explicitly not designed to be a departmental headquarters with command and control of the 18 agencies' vast bureaucracies. Rather, it was designed to be small and lightweight with a mission to coordinate and integrate the critical activities of the IC's 18 agencies without creating new bureaucracy. That goal should remain in force, and calls by outside entities or Congress to add new centers and layers should be rejected.

The Office of the Space Executive has been recognized as an effective governance model and has spawned similar efforts, including the Election Threats Executive, Economic and Threat Finance Executive, and Cyber Executive. With this in mind, the following initiatives should be pursued:

- **Expand collaboration with partners.** For too many decades, the IC and DOD have acquired and operated satellites independently. To improve their ability to meet the threat posed by China and Russia, the IC and DOD should:

1. Explore new methods for better integrating our space assets,

2. Examine the possibility of joint programs, and

3. Fully utilize unique Title 10 and Title 50 authorities to execute space defense (and offense) strategies jointly.

Additionally, the IC should support building international alliances with like-minded partners beyond the Five Eyes intelligence-sharing nations. Increasingly, potential allied nations (and their commercial companies) are developing innovative space capabilities to augment and strengthen the U.S. space defense and intelligence posture.

- **Refocus space-related intelligence collection.** The IC has developed a space threats collection posture predicated on three assumptions:

  1. The best information on developing space threats comes from collection against the adversaries' military institutions on Earth,

  2. There should be a clear dividing line between DOD's intelligence activities and the IC's, and

  3. Only government-developed "exquisite" capabilities can inform threat analysis and decision-making effectively.

  Developments by our adversaries and the emergence of a vibrant commercial space marketplace over the past decade have rendered all three assumptions false and even dangerous. The IC must therefore refocus and invest in methods that will enable it to characterize accurately the threats that already exist in space, not just on the ground; break down barriers to information sharing and collaboration with the DOD; and embrace commercially derived capabilities that can be adapted to a national security mission—all while emphasizing the need to protect critical supply chains and the cybersecurity needs that result from an increasingly government–commercial low Earth orbit.

  Our nation's economic and national security depends on being able to advance America's leadership position in space, which is eroding in the face of increasing threats from adversaries and our own inaction.

AN UNFINISHED EXPERIMENT

The Intelligence Community, including specifically the role of the DNI and ODNI, is an unfinished experiment. The envisioned design principle was a conservative one: a small, network-centric model for enterprise coordination as opposed to a large monolithic bureaucracy like DHS. The ODNI, however, has reverted in some ways to a bureaucratic and hierarchical model characterized by limited effectiveness.

Historically, the CIA has undercut the DNI and maintains primacy in the IC hierarchy, especially regarding the White House. An incoming conservative President can right the ship and return the IC governance model to first principles by using a limited but empowered leadership and coordination design to serve the nation's intelligence and national security needs while reclaiming the public trust with fiscal responsibility, political neutrality, personnel accountability, technological prowess, and necessary human capital needed to counter the immense nation-state and asymmetrical threats facing our country.

AUTHOR'S NOTE: The preparation of this chapter was a collective enterprise of individuals involved in the 2025 Presidential Transition Project. No particular policy statement, reform recommendation, or other view expressed herein should be attributed to any individual contributor or to the author.

ENDNOTES

1. "Two independent agencies—the Office of the Director of National Intelligence (ODNI) and the Central Intelligence Agency (CIA); Nine Department of Defense elements—the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the National Geospatial-Intelligence Agency (NGA), the National Reconnaissance Office (NRO), and intelligence elements of the five DoD services; the Army, Navy, Marine Corps, Air Force, and Space Force. 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 U.S. Coast Guard Intelligence; the Department of Justice's Federal Bureau of Investigation and the Drug Enforcement Agency'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." Office of the Director of National Intelligence, "What We Do: Members of the IC," https://www.dni.gov/index.php/what-we-do/members-of-the-ic (accessed March 8, 2023).
2. Office of the Director of National Intelligence, "Mission," https://www.intelligence.gov/mission#:~:text=The%20Intelligence%20Community's%20mission%20is,law%20enforcement%2C%20and%20the%20military (accessed February 24, 2023).
3. Abraham Lincoln, Second Annual Message to Congress, December 1, 1862, https://www.presidency.ucsb.edu/documents/second-annual-message-9 (accessed March 6, 2023).
4. Christopher Porter, "Seven Questions the Next President Will Need the Intelligence Community to Answer to Win the Technology Competition with China," LinkedIn, March 14, 2023, https://www.linkedin.com/pulse/seven-questions-next-president-need-intelligence-community-porter/?trackingId=DI9RF5CnSwWnAO7r9ggHiQ%3D%3D (accessed March 18, 2023).
5. H.R. 2845, Intelligence Reform and Terrorism Prevention Act of 2004, Public Law No. 108-458, 108th Congress, December 17, 2004, https://www.congress.gov/108/plaws/publ458/PLAW-108publ458.pdf (accessed March 6, 2004).
6. Testimony of Philip Zelikow, Executive Director, National Commission on Terrorist Attacks Upon the United States, in hearing, *Assessing America's Counterterrorism's Capabilities*, Committee on Governmental Affairs, U.S. Senate, 108th Congress, 2d Session, August 3, 2004, p. 55, https://ia802906.us.archive.org/31/items/gov.gpo.fdsys.CHRG-108shrg95506/CHRG-108shrg95506.pdf (accessed March 19, 2023).
7. Michael Allen, *Blinking Red: Crisis and Compromise in American Intelligence After 9/11* (Dulles, VA: Potomac Books, 2013), p. 155; Interview with Robert Gates, April 19, 2012.
8. Allen, *Blinking Red*, p. 154; Robert Gates e-mail to Andy Card, January 11, 2005; handwritten note from Robert Gates, January 20, 2005.
9. Interview with John Ratcliffe, December 15, 2022.
10. Ibid.
11. Ibid.
12. S. 258, National Security Act of 1947, Public Law No. 80-253, 80th Congress, July 26, 1947, https://govtrackus.s3.amazonaws.com/legislink/pdf/stat/61/STATUTE-61-Pg495.pdf (accessed March 6, 2023).
13. President Ronald Reagan, Executive Order 12333, "United States Intelligence Activities," December 4, 1981, in *Federal Register*, Vol. 46, No. 235 (December 8, 1981), pp. 59941–59954, https://www.govinfo.gov/content/pkg/FR-1981-12-08/pdf/FR-1981-12-08.pdf (accessed March 6, 2023).
14. President George W. Bush, Executive Order 13470, "Further Amendments to Executive Order 12333, United States Intelligence Activities," July 30, 2008, in *Federal Register*, Vol. 73, No. 150 (August 4, 2008), pp. 45325–45342, https://www.govinfo.gov/content/pkg/FR-2008-08-04/pdf/E8-17940.pdf (accessed March 6, 2023). See also President George W. Bush, Executive Order 13355, "Strengthened Management of the Intelligence Community," August 27, 2004, in *Federal Register*, Vol. 69, No. 169 (September 1, 2004), pp. 53593–53597, https://www.govinfo.gov/content/pkg/FR-2004-09-01/pdf/04-20051.pdf (accessed March 6, 2023).
15. U.S. Department of Defense, Defense Counterintelligence and Security Agency, "Trusted Workforce 2.0 and Continuous Vetting," https://www.dcsa.mil/mc/pv/cv/ (accessed March 9, 2023).
16. 50 U.S. Code § 3093(e), https://www.law.cornell.edu/uscode/text/50/3093 (accessed February 24, 2023).
17. 50 U.S. Code § 3093(a).
18. 50 U.S. Code § 3093(a)(4).

19. Michael E. DeVine, "Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions," Congressional Research Service *Report for Members and Committees of Congress* No. R45175, updated November 29, 2022, https://sgp.fas.org/crs/intel/R45175.pdf (accessed February 24, 2023).
20. H.R. 2663, Central Intelligence Agency Act of 1949, Public Law No. 81-110, 81st Congress, June 20, 1949, https://govtrackus.s3.amazonaws.com/legislink/pdf/stat/63/STATUTE-63-Pg208.pdf (accessed March 6, 2023).
21. Nicole Ogrysko, "Intelligence Community Workforce Is More Diverse, but Still Struggles with Retention and Promotion," Federal News Network, October 27, 2021, https://federalnewsnetwork.com/workforce/2021/10/intelligence-community-workforce-is-more-diverse-but-still-struggles-with-retention-and-promotion/ (accessed March 18, 2023).
22. See James J. Wirtz, "The Intelligence Policy Nexus," in Loch K. Johnson, ed., *Strategic Intelligence, Volume 1: Understanding the Hidden Side of Government* (Westport, CT: Prager, 2007), and Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," World Politics, Vol. 30, No. 1 (October 1978), pp. 61–89.
23. Letter from Barry A. Zulauf, IC Analytic Ombudsman, Office of the Director of National Intelligence, to Senator Marco Rubio, Acting Chairman, and Senator Mark Warner, Vice Chairman, Select Committee on Intelligence, U.S. Senate, "RE: SSCI #2020-3029," January 6, 2021, https://int.nyt.com/data/documenttools/ic-ombudsman-election-interference-with-responses/c50e548011fd6168/full.pdf (accessed March 14, 2023).
24. Joshua Rovner, *Fixing the Facts: National Security and the Politics of Intelligence* (Ithaca, NY: Cornell University Press, 2011), pp. 30–31.
25. Joshua Rovner, "Is Politicization Ever a Good Thing?" *Intelligence and National Security*, Vol. 28, No. 1 (2013), p. 58.
26. S. 1566, Foreign Intelligence Surveillance Act of 1978, Public Law No. 95-511, 95th Congress, October 25, 1978, https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf (accessed March 6, 2023).
27. The Cipher Brief, "702 Reauthorization: Defending a Key Intelligence Tool," remarks of Benjamin Powell, former General Counsel to the Director of National Intelligence, stating that FISA 702 provides "between 40 and 60 percent" of the intelligence in the PDB, December 18, 2017, https://www.youtube.com/watch?v=mRJ09GHVRFk&ab_channel=TheCipherBrief (accessed March 18, 2023).
28. An intelligence alliance that includes Australia, Canada, New Zealand, the United Kingdom, and the United States. Office of the Director of National Intelligence, National Counterintelligence and Security Center, "Five Eyes Intelligence Oversight and Review Council (FIORC)," https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc (accessed March 10, 2023).
29. Porter, "Seven Questions the Next President Will Need the Intelligence Community to Answer to Win the Technology Competition with China."
30. H.R. 1591, An Act to Require the Registration of Certain Persons Employed by Agencies to Disseminate Propaganda in the United States and for Other Purposes, Public Law No. 75-583, 75th Congress, June 8, 1938, https://govtrackus.s3.amazonaws.com/legislink/pdf/stat/52/STATUTE-52-Pg631.pdf (accessed March 6, 2023).
31. Kristina Wong, "Exclusive: Former DNI John Ratcliffe Pleased CIA Following His Lead on China Threat," Breitbart, October 13, 2021, https://www.breitbart.com/politics/2021/10/13/exclusive-john-ratcliffe-pleased-cia-following-lead-china-threat/ (accessed March 11, 2023).
32. H.R. 4628, Intelligence Authorization Act for Fiscal Year 2003, Public Law No. 107-306, 107th Congress, November 27, 2002, Title IX, https://www.govinfo.gov/content/pkg/STATUTE-116/pdf/STATUTE-116-Pg2383.pdf (accessed March 6, 2023).
33. President George W. Bush, Executive Order 13354, "National Counterterrorism Center," August 27, 2004, in *Federal Register*, Vol. 69, No. 169 (September 1, 2004), pp. 53589–53592, https://www.govinfo.gov/content/pkg/FR-2004-09-01/pdf/04-20050.pdf (accessed March 6, 2023).
34. Office of the Director of National Intelligence, National Counterintelligence and Security Center, "Who We Are: History of NCSC," https://www.dni.gov/index.php/ncsc-who-we-are/ncsc-history (accessed March 11, 2023).
35. Gregory F. Treverton and C. Bryan Gabbard, *Assessing the Tradecraft of Intelligence Analysis*, RAND Corporation, National Security Research Division *Technical Report*, 2008, p. 6, https://www.rand.org/pubs/technical_reports/TR293.html (accessed March 1, 2023).

36. Letter from Barry A. Zulauf, IC Analytic Ombudsman, Office of the Director of National Intelligence, to Senator Marco Rubio, Acting Chairman, and Senator Mark Warner, Vice Chairman, Select Committee on Intelligence, U.S. Senate, "RE: SSCI #2020-3029," January 6, 2021, https://int.nyt.com/data/documenttools/ic-ombudsman-election-interference-with-responses/c50e548011fd6168/full.pdf (accessed March 6, 2023).
37. "Independent IC Analytic Ombudsman's [Report] on Politicization of Intelligence," attached to January 6, 2021, Zulauf letter.
38. President Barack Obama, Executive Order 13526, "Classified National Security Information," December 29, 2009, in *Federal Register*, Vol. 75, No. 2 (January 5, 2010), pp. 707–731, https://www.govinfo.gov/content/pkg/FR-2010-01-05/pdf/E9-31418.pdf (accessed March 7, 2023).
39. President Barack Obama, Executive Order 13556, "Controlled Classified Information," November 4, 2010, in *Federal Register*, Vol. 75, No. 216 (November 9, 2010), pp. 68675–68677, https://www.govinfo.gov/content/pkg/FR-2010-11-09/pdf/2010-28360.pdf (accessed March 7, 2023).
40. Agathe Demarais, "How the U.S.–Chinese Technology War Is Changing the World," *Foreign Policy*, November 19, 2022, https://foreignpolicy.com/2022/11/19/demarais-backfire-sanctions-us-china-technology-war-semiconductors-export-controls-biden/ (accessed February 28, 2023).
41. Scott Stewart, "The Risk to Undercover Operatives in the Digital Age," *Stratfor Worldview*, October 29, 2015, https://worldview.stratfor.com/article/risk-undercover-operatives-digital-age (accessed February 24, 2023).
42. Lauren Pitruzzello, "Human Intelligence: Former CIA Officer Talks About Espionage in the Digital Age, University of Delaware *UDaily*, March 22, 2012, https://www1.udel.edu/udaily/2012/mar/global-agenda-grenier-032212.html (accessed February 24, 2023).
43. Jenna McLaughlin and Zach Dorfman, "'Shattered': Inside the Secret Battle to Save America's Undercover Spies in the Digital Age," Yahoo News, December 30, 2019, https://news.yahoo.com/shattered-inside-the-secret-battle-to-save-americas-undercover-spies-in-the-digital-age-100029026.html (accessed February 24, 2023).
44. U.S. Federal Trade Commission, "U.S.–Safe Harbor Framework," https://www.ftc.gov/business-guidance/privacy-security/us-eu-safe-harbor-framework (accessed March 11, 2023).
45. "Fact Sheet: Overview of the EU–U.S. Privacy Shield Network," U.S. Department of Commerce, https://2014-2017.commerce.gov/sites/commerce.gov/files/media/files/2016/eu-us_privacy_shield_fact_sheet.pdf (accessed March 11, 2023).
46. "Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework," The White House, March 25, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/ (accessed March 11, 2023).
47. President Joseph R. Biden Jr., Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities," October 7, 2022, in *Federal Register*, Vol. 87, No. 198 (October 14, 2022), pp. 62283–62297, (accessed March 7, 2023).
48. Warren P. Strobel, "Release of Ukraine Intelligence Represents New Front in U.S. Information War with Russia," *The Wall Street Journal*, updated April 4, 2022, https://www.wsj.com/articles/release-of-secrets-represents-new-front-in-u-s-information-war-with-russia-11649070001 (accessed February 24, 2023).
49. President Joseph R. Biden Jr., "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," The White House, May 4, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/#:~:text=To%20mitigate%20this%20risk%2C%20the%20United%20States%20must,the%20quantum%20risk%20as%20is%20feasible%20by%202035 (accessed March 12, 2023). See also President Joseph R. Biden Jr., Executive Order 14073, "Enhancing the National Quantum Initiative Advisory Committee," May 4, 2022, in *Federal Register*, Vol. 87, No. 89 (May 9, 2022), pp. 27909–27911, https://www.govinfo.gov/content/pkg/FR-2022-05-09/pdf/2022-10076.pdf (accessed March 12, 2023); and "Fact Sheet: President Biden Announces Two Presidential Directives Advancing Quantum Technologies," The White House, May 4, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/ (accessed March 12, 2023).