HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

BRIEF
belfercenter.org/Intelligence

INTELLIGENCE PROJECT | DECEMBER 2020

An Intelligence Agenda for a New Administration

America's Intelligence Community (IC) faces a daunting array of traditional national security challenges. Terrorism remains a persistent global problem in form of Islamic extremism as well as far-right nationalism. Russia, China and other nation state threats have become a higher priority after a long period of neglect. Regional conflicts simmer and occasionally boil over, reminding us that our agencies must provide global coverage. And we are now engaged in perpetual cyber conflict, with ambient digital espionage and conflict raging across global networks.

At the same time, the Covid-19 pandemic has shown us that there are other threats to national security which require our intelligence agencies to broaden their focus beyond the familiar threats that have defined their missions since inception. America's intelligence agencies must be able to support our national response to the existential challenges of our time - pandemic and biothreats, climate change, and nuclear insecurity. Each represents a high probability and high consequence set of risks for the nation and the world.

As a President-Elect Biden's team prepares to assume power, it should examine:

- **Independence:** Has political interference degraded the IC's capability to collect and protect intelligence, and has the IC's independence and objectivity eroded? How can we ensure that political interference never degrades IC capabilities and objectives?

- **Priorities:** How well prepared is our Intelligence Community (IC) to play its role of providing warning, perspective and options in a new world of disinformation, pandemic and climate change?
- **Keeping Pace**: Has the IC's ability to provide intelligence needed to keep America safe kept pace with the rapid changes in technology and society?

The Fellows of the Intelligence Project at the Harvard Kennedy School Belfer Center for Science and Technology, all seasoned intelligence veterans and scholars, have identified select priorities and accompanying actions to improve America's ability to address evolving global threats even while they continue to protect us against the efforts of adversaries of all stripes to do us harm.

We suggest that the next administration consider the following suggestions when setting America's intelligence priorities. Collectively, these steps would significantly enhance the IC's ability to meet the evolving threats we face now and over the decades to come:

Independence

Affirm the independence, integrity and objectivity of the Intelligence Community

The Intelligence Community has been drawn into domestic politics and attacked as harboring a "deep state." Sources and methods have been imperiled by leaks and partisan cherry picking of reports. Public trust, essential for the place of intelligence in a democracy, has eroded.

- On his first day in office, President Biden should sign an open letter, or issue an Executive Order, re-affirming the principal tenets of "Truth to Power." The Presidential directive would set expectations for independence, objectivity, whistle-blower protection, and the independence and autonomy of IC Inspectors General.
- To help restore morale and mission focus, an IC-wide employee survey and a special analytic integrity survey should be conducted in the first 120 days of the new administration. Together, these actions would help resurrect and reinforce the traditional hallmarks of the IC's apolitical provision of the best possible intelligence to the President, Congress and the American people.

Recommit to a Diverse Intelligence Community

Diversity of perspective and views are mission essential components of IC independence and objectivity. Equality and diversity in race, religion, gender, and sexual orientation provide the IC and therefore US national security with an advantage over its peer competitors. Previous orders to cancel diversity and inclusion training contracts, declaring them "un-American propaganda" sent precisely the wrong message, demoralizing members of the IC and inhibiting recruitment of minority candidates so necessary to mission success.

- We recommend that the Biden administration and a new DNI immediately and publicly reaffirm that the IC embraces, and benefits from, diversity.
- We recommend creation of National Intelligence Scholarships aimed at providing pathways for students of color or underrepresented on religious, gender, sexual orientation grounds to enter operational, analytic and scientific intelligence fields. During the Cold War, similar scholarships under the National Defense Education Act helped create a pipeline of mathematicians, scientists, Russia experts and linguists who filled critical national security needs. Scholarships aimed at diversifying the IC and National Security talent pool, including in the private sector, could widen the pipeline of candidates needed to build the IC's workforce and leaders of tomorrow.

Priorities

Review Collection Activities

The beginning of a new administration is the right inflection point for a high-level NSC review of collection targets, methods and effectiveness to ensure that the community is focused on the highest priorities and to guard against surprise and hidden risk. Intelligence collection programs and activities carry a high degree of inertia due to long lead times, significant investments, and entrenched interests. In the constrained fiscal environment the IC will undoubtedly confront, it is crucial that intelligence resources be re-allocated based upon the new administration's needs and priorities. This must be done by the NSC; it should not be done by the IC itself.

Prioritize Biological, Climate, and Information Threats

Twenty years after 9/11, our national intelligence resources are still heavily focused on terrorism at the expense of collection on greater strategic risks. Counterterrorism remains an important mission, but no terrorist group poses a strategic threat to our national existence or institutions without acquiring chemical, biological, or nuclear weapons. We must focus more tightly on these and find savings elsewhere within the counterterrorism budget to increase our ability to succeed against our most dangerous threats – climate, pandemic, and disinformation.

Climate change intelligence: Climate change and the extreme weather it creates touch every aspect of U.S. national security. They pose threats to U.S. territory, people, and infrastructure, and thus the US economy. They expand the threats faced by the US government's national security agencies as they will both increasingly destabilize governments and increase demands for U.S. resources during and after extreme weather events. Many national, state and local government agencies are involved in documenting and better understanding the climate threats and others are responsible for responding to the damage it creates, yet there is no clear central U.S. government climate authority to drive policy and actions.

- **Conduct an initial study of the IC's role and responsibilities.** The IC will be but one source of input of intelligence related to climate change for policymakers, but can uniquely contribute with geospatial intelligence, with collection on plans and intentions of key states and players, and with analysis of its broader national security implications. An early study to define requirements, assess collection capability, and prioritize efforts would help set expectations and maximize IC contributions.
- **Consider a Climate Intelligence Center** within the ODNI, modeled on NCTC, to assess and address the national security implications of climate change, including spreading disease, desertification, inequality, migration, and resource conflict. The IC should enlist the private sector, e.g. academicians and medical professionals, and make maximum use of open source collection.

Biohazard intelligence - Human synthesized and natural biohazards threaten our nation at a scale which dwarfs the damage that terrorist groups and most nations could cause. Our national response to COVID-19 exposed significant gaps in how intelligence is focused on and interacts with public health, many of which likely have already been addressed. These gaps must be permanently sealed as the IC must play a significant supporting role in warning of emerging biothreats, of understanding the actions of international actors, and in using open source and clandestine collection to supplement traditional public health surveillance programs.

- **Enhance the National Center for Medical Intelligence (NCMI):** The NCMI needs to be significantly expanded and be given increased visibility, connectivity, and influence under the auspices of the ODNI. Its collection should be supported by the capabilities of the entire intelligence community, and its finished analysis should be closely integrated by the ODNI and CDC in warning of biological and disease threats.
- **Establish a Biothreat Directorate** within the NSC to ensure IC and government wide surveillance and response efforts are coordinated, properly resourced, and support national and international policy response.

Information Integrity Intelligence: America will remain under sustained assault from foreign and domestic use of disinformation and deep fakes designed to sow distrust and exacerbate extremism.

- **Create an Information Integrity Intelligence Center (IIIC)** within the ODNI with the remit to direct efforts across the IC to detect and counter media manipulation, deep fakes, and other threats to information integrity which undermine US security and national interests. The IIIC would ensure broad US government understanding of foreign information operations and lead government responses to the threats. The IIIC should also be mandated to provide open source based, unclassified reporting for the private sector to provide an objective, factual and substantiated baseline of deceptive information operations directed against the US.

Geo-Political Rivals

Amid a resurgence of great power rivalries, intelligence collection by all agencies against traditional threats from adversaries - Russia, China, North Korea and Iran - requires improved and sustained focus. The IC must be able to provide deep insights into the leadership decision making of our key adversaries and an annual review of their progress should be undertaken to identify resource gaps. Building agent networks and platforms for technical collection against such hard targets is time consuming, labor intensive, and highly risky. Even when successful, hard target collection by human and technical sources is astonishingly fragile and must be constantly renewed.

- **Russia and China.** CIA, NSA, NGA and DIA must be able to answer core questions on Russian and Chinese plans and intentions. To be successful against these hard targets requires capability, tools and expertise which take years to build and are difficult to maintain, but which must be sustained. The IC's overall efforts should be driven by senior ODNI mission managers to ensure coherent and cohesive collection and analysis on these dangerous rivals.

- **Countering Espionage:** Post 9/11, resources devoted by FBI, CIA and NSA to countering foreign espionage in the US lagged even as hostile intelligence activities increased. Given the impact on US security and economic competitiveness, the US still devotes too few resources to combat human and digital espionage. Accompanying an increased CI focus should be greater outreach to and communication with the private sector and universities to educate on the threats and to make it more difficult for hostile foreign intelligence powers to operate against the US government and private sector.
- **Nuclear Threats and Proliferation:** With lagging arms control protections and new weapons systems and doctrine rapidly evolving, IC focus on nuclear security issues, state and non-state, must be a paramount focus. There are few areas where getting the intel wrong could have more dangerous consequences.

Keeping Pace

Artificial Intelligence and Data Dominance

The foundation of intelligence advantage is data and the craft by which analysts assess its meaning and import. There is nothing about this that is different in 2020 than it was in 1947, other than the volume and availability of potentially useful information and our difficulty applying manual analytic processes at scale and speed. In 2020 and beyond, threat and opportunity are to and through information and the Intelligence Community needs to be driving the research that will allow assurance of data and algorithms necessary to trust their use and incorporating AI and ML in everything from administrative processes (such as granting security clearances), to onboard processing integrated in collection systems to lessen the cost of data transport, to analysis tools that triage, adjudicate, and use large volumes of data for the purpose of detecting the patterns and anomalies that allow for early warning and decision advantage. Simply put, the IC must be the best users, if not drivers, of these new data handling and analytic technologies.

- **Commit the resources to data use**. Historically, collection systems get the money, in part because our history was one of being hunters for data. Now, the balance needs to shift to spending more on data integrity, infrastructure, protection, integration, and use—across every mission set. We cannot keep thinking about this as an efficiency play—it's a mission effectiveness play.
- **Commit to data as a community asset**, vice the purview of the collector. We have to

make the cost of data integration zero, and the best way to begin is at the beginning. Make all collectors adhere to data use standards; stop allowing bespoke data-sharing arrangements; and invest in the security solutions that will allow confidence that the data are protected and appropriately available.

- **Invest in hiring and education of intelligence officers who are both technically capable AND technically savvy**. Not every intelligence officer has to be able to create, but all have to be able to understand and use the data and systems that will have to dominate our future if we are to maintain advantage in a digitally connected world.

Open Source Source Intelligence

There was a time when intelligence that the United States needed was hidden behind veils of secrecy. Today, however, the world is awash in extraordinarily valuable open source intelligence. Organizations such as Bellingcat have amply demonstrated that open source collection can be used to unveil deep secrets such as who killed Sergei Skripal, or which unit fired the missile which brought down Malaysia Airlines Flight 17 over Eastern Ukraine.

Open source intelligence (OSINT) supports decision-maker requirements at low cost and risk and should be the tool of first resort, with riskier and costlier clandestine collection focused on the IC's most challenging requirements. An OSINT center would bring significant advantages to the IC including:

- Ability to supplement classified intelligence with creatively acquired OSINT
- Capacity to share unclassified intelligence with private and foreign partners
- Opportunity to employ new hires pending background investigations
- Ability to hire foreign and uncleared linguists and analysts
- Facilitate academic, think-tank and corporate interaction on IC requirements

To supercharge OSINT, we recommend transforming the CIA's Open Source Enterprise (OSE) into an independent Open Source Intelligence Center (OSIC) within the DNI. OSIC would be the IC's focal point for open source collection, analysis, and tradecraft with a mandate for and new resources to oversee collection and analysis to assist the IC, and the private sector, in defending against cyber-attack, espionage, and information warfare.

Popping the IC Bubble

By very nature of its secretiveness, the IC is largely insulated and isolated from the private sector of businesses, academia, and NGO's, many of which are dealing with the same problems and challenges the IC itself confronts. Turgid clearance processes, cultural insularity, and government HR rules prevent the dynamic exchange of people and ideas which drive innovation and adaptation. The IC has a hard time moving people across agency silos, let alone in and out of government. Making it easier for employees to leave the IC cloister and return enriched and refreshed would pay dramatic dividends. Likewise, enabling the IC to more easily attract mid-career professionals and experts would bring fresh ideas, continually refresh government's understanding of cutting-edge technological advances, and bring more diverse approaches and perspectives into the IC.

- **Programmatically enable IC members at key career junctions to learn, train and work in outside organizations.** The US military model and expectation of career long training would be a good place to start. This requires the commitment and capability to take employees off-line
- **Target Mid-Career Recruitment:** Attracting entrepreneurs, business professionals, and academics into the IC for set term contracts would provide an injection of talent and outside perspective.

Conclusion

The role of the IC is simple: to provide our policy makers with decisive decision advantage, with capability to influence events; and with tools to bolster our diplomatic, military, and economic advantage. These missions are immutable, but how they are accomplished must keep pace with changing technical, social, economic and geo-political environments. Some aspects of espionage will endure, particularly the unique value of human agents. But to deliver the right intelligence at the right time in a form that can be used, the IC will need to relentlessly adapt and improve.

The Biden Administration will face a myriad of challenges as it takes office. COVID-19 is in full force across the country, our political divisions have rarely been more volatile and pervasive, and our adversaries have taken advantage of perceived opportunities as we struggle with both. As the new White House tackles these domestic challenges, setting an aggressive course for addressing these national security challenges will be equally important. The recommendations here are those we see as among the best places to start.

Contributors

Gen (Ret) **James Clapper**, former DNI, D/DIA, D/NGA

Sue Gordon, former PDDNI, DD/NGA

Rolf Mowatt-Larssen, former DoE Intelligence Director, CIA Senior Executive

Mike Rogers, former Chairman/HPSCI

Norm Roule, former CIA Senior Executive, ODNI National Intelligence Manager for Iran

Dan Hoffman, former CIA Senior Executive, Chief Near East Division

Bern Hudson, former Director Counterterrorism Center, CIA

Kristin Wood, former CIA Senior Executive, PDB Briefer

Gen (Ret) **Kevin Ryan**, former Defense Attache Moscow, Belfer Center Defense and Intelligence Project Director

Caitlin Chase, Intelligence Project Coordinator

Calder Walton, Intelligence Project Research Fellow

Paul Kolbe, Belfer Center Intelligence Project Director, former CIA Senior Executive

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

belfercenter.org/Intelligence