A Better Way to Identify and Address Threats to National Security

JANUARY 2021

Samuel Brannen

The Biden-Harris administration inherits a volatile and dangerous global threat landscape. Persistent and emerging threat vectors have increased over the past four years, from climate change and Covid-19 to homegrown violent extremism and military and gray zone challenges from China, Russia, Iran, and North Korea.

As the new administration seeks to prioritize its approach to these threats through its strategy making process, it should endeavor to think comprehensively and methodically. Creating as objective and informed a picture of the current and emerging security environment as possible at the outset of a new administration is a worthy use of senior leader and staff time, and is certain to pay future dividends. This threat picture must also be frequently updated in an era of continuous change. This straightforward approach to creating structure around current and future threats could enable more efficient allocation of resources, fewer threat blind spots, and better outcomes for U.S. national security.

Q1: How do threats inform U.S. national security strategy formulation?

A1: Threats are identified as part of the national security planning process and reflected in guidance documents drafted at the outset of a new administration, including the National Security Strategy (NSS) and National Defense Strategy (NDS). The threats identified in these documents often reflect the policy inclinations and preferences of senior leaders who suffer from the same cognitive biases as anyone else (e.g., recency bias, anchor bias, confirmation bias), which can only be rooted out through a more rigorous process. As a result, these documents and the decisions they inform across the federal government routinely overstate the relative importance of some threats while understating others, or are simply presented as "laundry lists" without prioritization.

The U.S. government lacks a centralized approach to tiering national security threats in an adaptive or dynamic sense outside of the release of these strategic planning documents. Moreover, the top threats to the United States presented in the NSS are then recast internal to federal departments and agencies by subordinate strategic guidance and other planning documents. The direction provided by the NSS is often further diluted or outmoded by real-world developments. The Director of National Intelligence (DNI) and other intelligence officials, including the FBI director, are frequently asked in private and public settings to update administration and congressional leaders on what they consider top national security threats, while the "official" guidance documents remain unchanged.

More importantly, a threat is different than a risk. Risk is the probability and the consequences or impact of a given threat, if and when it manifests. National security strategy should be formulated around clear understanding of risks, not threats. And understanding and rating risks must be done dynamically, adapting to real-world events.

Past national security leaders have, to some extent, grasped all of this. To varying degrees over the course of past administrations, the National Security Council has attempted to prioritize national security risks through a clear interagency methodology and to more centrally direct resources to address them, especially through its Strategic Planning Directorate. However, such efforts often happen later in an administration, missing the opportunity of greatest impact with the release of the first set of guidance documents and the formation of a strategic culture around the process.

Q2: Who leads U.S. national security threat assessments, and what do recent legislative changes mean for the process and for congressional oversight?

A2: The 17 organizations comprising the United States Intelligence Community (IC) under the DNI have a responsibility to monitor foreign and domestic threats to the United States. They report their findings to relevant executive branch officials starting with the president, and to department agencies and departments at the federal, state, local, tribal, and territorial levels, as well as to members of Congress and their staff who are deemed by the executive branch to have a "need to know"—especially in their oversight functions through the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI).

From 2006 through 2019, the DNI issued an annual public report providing the IC's Worldwide Threat Assessment. This was the most comprehensive briefing on threats publicly provided by the government outside of the aforementioned NSS and NDS. The SSCI annually hosted an unclassified, open hearing on this topic. HPSCI, the Senate Armed Services Committee (SASC), and the House Armed Services Committee (HASC) also hosted public hearings on the topic, though not consistently. However, the briefing became politically charged in 2020 ahead of the U.S. presidential election, and the document was not released—nor did Congress hold the traditional accompanying hearings that year. The fiscal year 2021 omnibus spending bill enacted a new requirement for the report to be produced annually, with public and private hearings as requested by SSCI, HPSCI, SASC, and HASC. This annual cycle will begin in February 2021.

In 2020, the Department of Homeland Security (DHS) produced the first Homeland Threat Assessment. DHS is also responsible for the National Terrorism Advisory System, which provides information on specific terrorist threats to the U.S. public. DHS's Cybersecurity and Infrastructure Security Agency has responsibility to monitor threats to critical infrastructure, including "5G, election security, electromagnetic pulses, national critical functions, pipeline cybersecurity and more" and to communicate those threats with stakeholders across the public and private sectors, including through its National Risk Management Center. There are numerous other reporting requirements from Congress related to specific threat assessments: some that are one-offs and some that are on a recurring basis, many of which also involve public hearings. These requirements are well intentioned, but they are often a distraction from understanding specific threats in a broader national security context. That can lead to overly focusing on one threat and overstating its importance relative to other threats and driving more attention and resources than warranted, all the while leaving other threats under-resourced or appreciated.

Q3: How could the government improve its approach to better identify threats and prioritize national security risks?

A3: A better approach for U.S. national security would involve putting into place a process that is more rigorous and more agile at the outset of a new administration. This process should strive to overcome the cognitive biases that inevitably cloud human judgment about the future, and also to focus on clear understanding of risks with the best

available information. The methodology also should account for risks across two time frames in national security planning: the immediate and the emerging.

The new approach should also adopt a clear methodology that produces a more objective result. It could be implemented with a commitment from the national security adviser that they will take seriously the results of the process and present those results in front of principals, as well as share them with Congress and the U.S. public as appropriate. The process could begin with a "data call" for top threats from the IC potentially linked to a classified version of the DNI's Worldwide Threat Assessment. Input could also be solicited from close U.S. allies and partners with existing sophisticated threat assessment and risk management processes, such as the United Kingdom, Germany, Australia, Japan, New Zealand, and Singapore. The resulting list of risks could be discussed at interagency working levels and then graded by National Security Council staff—and potentially the strategic planning staffs of other key agencies and departments—by probability, timeframe, and impact to generate a list of top immediate and emerging risks to the United States for presentation to deputies and principals and to inform the NSS. This list could be revised annually and revalidated through the same process. Such a process additionally would benefit from closer collaboration between the National Security Council, Domestic Policy Council, and Office of Management and Budget. It also would require strong communications and support between the White House and relevant congressional committees.

This more rigorous risk assessment could help to better align resources to address or mitigate identified risks and to increase U.S. national security overall. It could also enable discussions of trade-offs at the highest levels of government across issues rather than permit such decisions to be taken in isolation and often on the basis of crisis events rather than with broad strategic context.

Author

Samuel Brannen leads the Risk and Foresight Group at the Center for Strategic and International Studies (CSIS) and is a senior fellow in the International Security Program.

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS is ranked the number one think tank in the United States as well as the defense and national security center of excellence for 2016-2018 by the University of Pennsylvania's "Global Go To Think Tank Index."

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

About Defense360

The Defense360 microsite is the home for research conducted by experts from the CSIS International Security Program (ISP). Defense360 features reliable, nonpartisan analysis and commentary from ISP experts on key elements of national security policy including strategy, budget, forces, acquisition, and reform. This analysis informs policymakers' decisions on the threats and opportunities shaping U.S. interests at home and abroad.