MITRE | Intelligence After Next

Intelligence After Next

SERIES # 24

PREPARING FOR FUTURE CRISES: HOLISTIC CRITICALITY MANAGEMENT OF NATIONAL SYSTEMS

by John Rodman

National Threat Modeling and Criticality Analysis

National security requires us to anticipate and address future crises while operating in a fluid environment. Success rests on the ability to identify, preserve, and share essential information, while limiting the legacy human interactions and technical systems that may impede interoperability—holistic criticality management. Past U.S. responses to crises provide lessons learned and a way forward for developing risk mitigation solutions. These insights can help establish national security enterprise (NSE) criticality processes to prepare our nation for future crises.

The U.S. government, despite well-intentioned efforts, continues to struggle with determining crisis-essential information and minimizing the human, organizational, and technical systems that slow progress. Data and information are the lifeblood of national security, but determining their future value and optimizing their use in a crisis requires hard, early decisions on unimportant data and systems. Likewise, organizations must also consistently strive to eliminate human, institutional, and organizational barriers that limit our preparation for a future crisis.

To better anticipate potential catastrophic threats, we must combine strong and weak signals with creative thinking, ascertain whether essential data is available or can be collected, and develop possible ways to counter the threats. These steps become increasingly difficult as the NSE environment becomes more complex, entangled, and harder to manage in a crisis.

Establishing national security criticality factors for future crises is essential to mitigation and preparation. Defining criticality at the national level—as it has been for individual government organizations since at least 2010[1]—is a logical, first step.

Proposed Definition for National Security Criticality:

The degree to which a nation depends on information and human and technical systems in the future as the scale and scope of conflicts or crises increase.

A crisis-based approach to national security helps determine criticality, creates situational awareness, and institutionalizes a response that may avoid future intelligence failures, catastrophic losses, or diminished national power that reduces U.S. leverage and competitiveness. Analysis of historical vignettes and the U.S. response to them illustrates the need to:

- Identify essential data and systems.
- Determine human and technical barriers.
- Integrate national crisis planning.

Although seemingly unconnected, the U.S. response to crises in terrorism, semiconductor development, and pandemic control demonstrate why determining criticality is essential to preparedness and success. All three issues were identified by the mid-1980s as emerging threats and eventually elicited major national responses and changes in authorities and resources. Their paths to crisis were different—existential (terrorism and 9/11), growing (semiconductors), and rolling (epidemics and pandemics). A national process for crisis identification and mitigation based on holistic criticality planning may have changed the outcomes. A nationally managed crisis response mechanism embeds the strategic, enduring, interorganizational, cross-discipline approach that is essential for our nation's most at-risk futures.

The Vignettes

Terrorism: Existential Crisis

Terrorist incidents occurred before the 1980s, but attacks like those in Beirut and the bombing of Pan Am Flight 103 were a turning point in international terrorism.[2] In 1980, two of 64 groups conducting terrorism were assessed as largely religious in motivation. By 1995, that number had reached almost half, with 26 of 56 groups conducting international terrorism classified as religiously motivated.[3] Despite this trend and the first attack on the World Trade Center in 1993, it was the attack on September 11, 2001, that ushered in the Global War on Terrorism (GWOT) and the biggest changes in the Intelligence Community (IC) since 1947. Estimates of GWOT costs vary widely, from $1.55 trillion[4] to $8 trillion.[5]

Several major events followed 9/11, including the war in Iraq from 2003 to 2011, the stand-up of the National Counterterrorism Center, and the build-up of counterterrorism operations around the world. The 9/11 attacks were also the catalyst for the Patriot Act and changes in authorities and legislation for monitoring and handling information. The event was declared the largest intelligence failure since Pearl Harbor. It has been argued that 9/11 was as much a policy failure as intelligence failure. There were Al Qaeda–claimed bombings preceding 9/11 and warnings in 1999 that Al Qaeda could crash an aircraft packed with explosives into high-value national targets. The data was building for this crisis but lacked specificity and critical mass to counter an individual attack.[6]

The 9/11 Commission cited as a primary failing, “pieces of the puzzle were to be found in many corners of the U.S. government but that no one connected the dots well enough or in a timely enough manner to predict with sufficient accuracy the attack that came.”

Findings suggest this was an interoperability problem of information, organizations, and systems.

Semiconductors: Growing Crisis

The U.S. chip industry is in crisis due to overseas competition, but the year was 1986 not 2022. We clawed our way back through the 1990s with the efforts of a non-profit industry consortium called Sematech, government funding, and trade actions against Japan.[7] The domestic industry took another hit during the financial crisis in the mid-2000s because of increased dependency on semiconductors in all sectors of the economy. The financial crisis reduced customer purchases and increased the cost of capital needed for developing innovative semiconductor technology in the United States. At the same time, constant development was needed to keep pace with demand for faster processing with greater capacity (Moore’s Law).[8]

By focusing on science policy instead of industrial policy for semiconductors, the United States gained in cutting-edge capabilities but became more reliant on the fragile, overseas production of lagging-edge semiconductors used by many market products.[9] In 2015, alarms sounded in the United States over China’s unfair industrial practices and the country’s progress in developing chips. In its 2014 national planning, China announced and launched a 20-year plan to cut imports of semiconductors in half in 10 years and entirely by 20 years.[10]

The weakening of the U.S. semiconductor industry’s fabrication capacity and competitive position for nearly 40 years was amplified by China’s $100 billion plan for its semiconductor industry. These factors, combined with the exponential rise in demand for semiconductors in our daily lives, were known but the national response was insufficient until the CHIPS and Science Act of 2022.

This was a foresight and national crisis planning problem predicated by economic, political, and social factors.

Epidemics/Pandemics: Rolling Crisis

There were devastating pandemics in the early 20th century, but this summary starts in the 1980s to be consistent with the other examples and because modern vaccine modeling and production capabilities developed during this were a game changer. Acquired immunodeficiency syndrome (AIDS) has claimed at least 32 million lives since 1981. There have been more recent recurring epidemics or pandemics, such as severe acute respiratory syndrome (SARS), the "swine" flu, Middle East respiratory syndrome (MERS), Ebola, Zika virus, Avian influenza, COVID, and Mpox.[11] By the late 2000s, medical journals were making the case that pandemics were 1) mutating and creating subtypes, causing increased death rates in younger populations; 2) consisting of successive waves; and 3) displaying higher transmissibility rates.[12] All of these attributes were seen—and are still being seen—with COVID.

Funding for global health security generally ranges from $400 to $500 million a year, with spikes for response going above $1 billion. U.S. funding against epidemics and pandemics waxes and wanes, with large increases in funding almost entirely driven by specific disease events.

The outbreak of SARS in 2004 changed U.S. Department of Health and Human Services (HHS) rules for controlling communicable diseases and quarantining authorities.[13] This change in how HHS manages diseases benefited our response to COVID, but the estimated financial cost to the United States was still $16 trillion in 2020.[14]

This was a behavior and systems problem combined with inconsistent funding.

> **A crisis-based approach to national security helps determine criticality, creates situational awareness, and institutionalizes a response that may avoid future intelligence failures.**

Pick a Future National Crisis

The United States is facing many challenges. Climate change and increasingly volatile weather events have caused food shortages, population displacement, and catastrophic human and property loss. The proliferation of weapons of mass destruction has been a growing crisis for decades as nuclear-capable nations have increased in number and capability (i.e., accuracy and scalability of warheads). Recently, international treaties have proved inadequate to contain and limit proliferation. The growing dependence, congestion, and competition in the space domain could soon reach a crisis point. Lack of societal cohesion, a more intangible crisis, is tied to income disparity, social discord, and government ineffectiveness, and possibly impacts our ability to respond to any crisis.

A successful response to a catastrophic climate event in the United States will require coordination of emergency services, law enforcement, possibly the military, and intranational authorities. Climate change was formally recognized as a future crisis by the U.S. government in 1990 with the establishment of the U.S. Global Change Research Program, which for 33 years has been bringing together researchers and assessments on the impact of climate change.[15] It was not until 2023 that the Department of Homeland Security (DHS) was added as the first new member in two decades, despite its leading role in national disaster preparedness and response.

A recent disaster preparedness assessment identified shortcomings in a federal response to climate change and recommended:

- **Developing a strategic plan**—with clear priorities, roles, and responsibilities—to guide the nation's efforts to adapt to climate change.
- **Taking a government-wide approach** to providing decision makers with the best available climate-related data.
- **Designating a federal entity** to develop and update climate information and a national climate information system.

- **Incorporating climate resilience issues**, like natural hazards and climate change, into agency risk management programs for infrastructure and facility planning.
- Establishing a federal organizational arrangement to periodically **identify and prioritize climate resilience projects** for federal investment.[16]

Like the vignettes, the government response to climate change follows a familiar response path: decades of awareness; insufficient investment and integration; and lack of a focused, sufficient national response until the 11th hour. The solutions recommended for a federal response and organizations' preparation for a climate disaster are equally applicable to other future crises and threats.

Not Organized to Optimize

Access to essential information and systems interoperability is critical for organizations to build resilience to a national threat or crisis. This includes how organizations approach information sharing and use, reduce harmful institutions, and eliminate costly legacy systems and potential barriers.

Organizations and the NSE have recognized, since the late 1980s, the need to manage the overwhelming flow of data and rapid pace of technology change to mitigate risk and counter threats. Yet, essential intelligence, response capacity, and common services often lack interoperability. The costs to our nation are clear and measurable. Industry estimates that the average firm spends about 30 percent of its IT budget on legacy systems.

- In 2021, the U.S. government spent about $100B on IT. If we apply the 30 percent rule, then it spends nearly $33B annually on legacy systems that may be unable to sync in a crisis.
- The Government Accounting Office (GAO) estimates that between 2010 and 2017, overhead and management costs on existing systems reduced new investment for IT modernization by $7.3B.[17]
- In 2021, GAO identified 10 critical systems ranging from 8 to 51 years old with an estimated operations and maintenance cost of about $337M a year, including some that required rehiring programmers in languages no longer used.[18]

> **We lack both a centralized process to identify threats that may become a national crisis and a planning manager with the authority to manage the process of optimizing information sharing or information management across systems prior to, during, or after a crisis.**

Methodologies like MITRE's Crown Jewels Analysis are invaluable for helping organizations identify critical assets in single systems and for fulfilling national requirements for federal organizations to determine critical assets. However, there are currently no required or standard approaches to threat modeling in the NSE to determine essential information or criticality analysis at a system-to-system level across government to focus resources and optimize actions. There are efforts we can improve upon:

- Multiple commissions and findings since 1955 have advocated for stronger, centralized, and integrated NSE resource management—key to a national response.
- Federal Continuity of Operations Planning seeks to ensure mission-essential functions continue in individual departments and agencies during and after a crisis. As we saw in the vignettes, however, whole-of-government planning integrated into civil society may be lacking for nascent, future threats.

- DHS National Prevention and Protection Frameworks provide excellent guidance for organizations, but they may be applied by individual agencies, departments, and local governments in a decentralized, inconsistent, and independent way that may impact future national risk.

Planning to Avert Future Crises

We lack both a centralized process to identify threats that may become a national crisis and a planning manager with the authority to manage the process of optimizing information sharing or information management across systems prior to, during, or after a crisis. There are many examples in the U.S. government of planning at the department and agency levels (e.g., the Defense Threat Reduction Agency) that could be leveraged in scaling up to a national plan.

The lack of long-term, interagency identification of future national crises and threat-based criticality management increases our risk of unacceptable losses.

An independent assessment of federal system criticality that includes proposals for preventive actions against future crises is essential and may entail:

- Establishing data-based capabilities, accountability, and monitoring requirements across the federal government for integrating critical data, organizations, and resources based on multisector crisis impact.
- Determining realistic lines of funding for multiagency integration of critical data and systems that is consistent and spans administrations over the 10–20 year crisis preparedness period.
- Developing interoperability for foundational behaviors, processes, and systems in select crises to focus our extensive government resources and optimize our preparedness.
- Institutionalizing new approaches for early identification of threats and crises, emphasizing the multisector and multistakeholder nature of a hyper-interconnected world.

Preparing for Specific Threats

A national model to prepare and respond to threats decades in the making requires determining the essential information, organizations, and systems needed now and in the future. This includes reducing legacy attributes and behaviors that affect NSE interoperability and its capacity for innovative response to future crises with three key steps:

- **Identify:** Determine interagency criticality for a successful, common response against high-priority threats with the potential for a national crisis. Separately, the Department of Defense (DoD), IC, and private industry are very good at this, but they must be integrated.
- **Forecast:** Imagine scenarios and outcomes associated with each potential crisis through a centralized and standardized organization and process. Focus on adapting the required authorities, behaviors, lines of effort, and legacy attributes in stakeholders.
- **Plan:** Create solutions that rapidly actualize the preparatory work so that the national response scales to the increasing level of crisis at the speed needed to avoid catastrophic losses. Ensure a consistent budget for and focus on impending crises over decades by establishing interagency program stewardship with resource management, similar to acquisition programs for major military and space platforms.

Building National Criticality Systems

Create a process to identify and prioritize future national crises

This process should align participants and stakeholders, optimize the critical information and processes, and be integrated into foundational national strategy documents. This can be accomplished by 1) employing unbiased experts to apply strategic foresight methodology to identify future threats, 2) performing system-of-systems analysis to determine critical resources, and 3) making trade-space decisions that preserve essential behaviors, data, and systems for countering future crises.

Develop sustainable efforts

For crises that develop over long periods, sustaining momentum and resources is essential for critical interoperability across organizations—both to preempt and correct insufficient capabilities and to remove institution, organization, and system barriers.

- Place key organizations on a common crisis footing for information sharing, systems integration, and workforce reciprocity to ensure a rapid response.
- This might include an NSE model similar to the United Kingdom's Civil Contingencies Secretariat, which is responsible for national emergency planning at all levels, including maintaining a National Risk Register, coordinating cross-government resilience and aligning senior decision makers, and contingency planning.[19, a]
- A post-pandemic government study of the U.S. emergency response to COVID found that the Federal Emergency Management Agency (FEMA) had not determined what steps were needed to address the nation's capability gaps across all levels of government—another way to think about national criticality crisis preparation.[20] While FEMA is addressing many of the recommendations for improving readiness, lack of funding, qualified personnel, and comprehensive assessments capabilities slow our ability to manage fragmentation across federal disaster preparedness and recovery.[21]

Establish oversight to enforce the requirements and authorities

This might require establishing a new function that bridges the National Intelligence Officers (NIOs) who inform our most senior decision makers on critical, emerging intelligence issues and the National Intelligence Managers (NIMs) who guide security planning for functional and regional issues. This new function might take the form of a National Risk and Resilience Manager (NRRM).

- The NRRM would oversee national risk and resilience issues (e.g., supply chains, deterrence, natural disasters) in a holistic fashion by focusing on the enablers (e.g., institutions, people, technology) needed in a crisis.
- The staff might be tasked to define future threats and trade space, while also conducting net assessments of the U.S. capability to respond to a national crisis. Intelligence would flow from the NIOs to the NRRM and then to the NIMs for implementation.
- The role of the NRRM for national crisis estimation could also be assigned to the White House Office of Science and Technology Policy, raising the visibility and keeping the function outside the IC and leveraging our national acquisition, R&D, and crisis management system to focus on technology resilience.

Implement national systems planning

A command structure for future crises should be lightly applied to individual agencies during normal operations, but quickly scaled and implemented when needed.

- A strong national and international community of advocates and experts in resiliency methods, practices, and science already exists. Common traits that define resilience engineering are the ability of a system to anticipate, absorb, accommodate, or recover from a hazardous event.[22]
- National security criticality elevates resiliency engineering from an agency application—primarily against natural disasters—to a whole-of-government approach with a management structure designed for crisis preparedness.[23, 24]

[a] COBR or COBRA is shorthand for the Civil Contingencies Committee that is convened to handle matters of national emergency or major disruption. Its purpose is to coordinate different departments and agencies in response to such emergencies.

Apply rigorous response system testing

A strong resilience, risk, and crisis management system may include modeling, simulations, and exercises to ensure an integrated national response mechanism.

- Historically, exercises for future homeland crises are not integrated throughout the NSE and struggle to integrate lessons learned that could drive holistic change.[25]
- Gaming, Exercising, Modeling, and Simulation has become a priority for DoD planning of complex battlespace/multi-domain scenarios. Expanding this capability for attacks and threats to our security, society, and stability is essential for preparation.

Prevent Future Crises Now

The slow pace of progress in interoperability for information, operations, and systems in the national security enterprise has been costly in many ways. Anecdotally, we know that there are 75 years of intelligence failure findings and multiple studies for revolutionary change that are discouragingly similar, and include the period since the 9/11 reorganization. The definition of national security is expanding into critical infrastructure, emerging and disruptive technology, and supply chains. National Security Memorandum 22 on Critical Infrastructure Security and Resilience moves the nation in the right direction on this issue. Its implementation may provide many lessons learned in scaling to a larger, national criticality system that can be applied to a broad range of emerging issues and threats.

In the future, the national security enterprise will likely require even greater sharing, creativity, and innovation to bridge these disparate issues. National security criticality requires that we identify essential data and systems, isolate the primary impediments to change, and establish their drag effects on our national security enterprise against our most concerning future threats. These actions are challenging, but essential if we are to move more rapidly, coherently, and strategically than ever before.

References

1. Marianne Swanson, Pauline Bowen, Amy Wohl Phillips' Dean Gallup, David Lynes. National Institute of Standards and Technology. Special Publication 800-34 Rev.1. May 2010.
2. John Moore, The Evolution of Islamic Terrorism: An Overview, Frontline. August 11, 2002.
3. Bruce Hoffman, Old Madness New Methods, Revival of Religious Terrorism Begs for Broader U.S. Policy, RAND Review, Winter 1998-99.
4. Christopher Mann, U.S. War Costs, Casualties, and Personnel Levels Since 9/11, Congressional Research Service, IF11182, April 18, 2019.
5. Neta Crawford, Catherine Lutz, Stephanie Savell. Costs of the 20-year war on terror: $8 trillion and 900,000 deaths. Annual Report. September 1, 2021
6. Thomas Kean (Chair), Lee Hamilton (Vice Chair), National Commission on Terrorist Attacks Upon the United States, 2004.
7. Robert Hof, Lessons from Sematech, MIT Technology Review, July 25, 2011.
8. Chip History Center, The DRAM Crash of 2008. Available: https://www.chiphistory.org/720-the-dram-crash-of-2008, August 10, 2018
9. Alex Williams and Hassan Khan, A Brief History of Semiconductors: How the U.S. Cut Costs and Lost the Leading Edge, Employ America. Available: https://employamerica.medium.com/a-brief-history-of-semiconductors-how-the-us-cut-costs-and-lost-the-leading-edge-c21b96707cd2, March 20, 2021.
10. Nigel Cory, China's Exaggerated Semiconductor Trade Deficit No Justification for Mercantilist Policies, Information Technology & Innovation Foundation, October 28, 2015. Available: https://itif.org/publications/2015/10/28/china%E2%80%99s-exaggerated-semiconductor-trade-deficit-no-justification/
11. Major Epidemics of the Modern Era, Council on Foreign Relations, 2023. Available: https://www.cfr.org/timeline/major-epidemics-modern-era
12. Viboud Miller and Simonsen Balinska, The Signature Features of Influenza Pandemics—Implications for Policy, The New England Journal of Medicine, June 18, 2009.
13. Foster Misrahi and Cetron Shaw, HHS/CDC Legal Response to SARS Outbreak, National Library of Medicine, February 10, 2004. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3322897/
14. Josh Michaud, Kellie Moss, and Jennifer Kates. The U.S. Government and Global Health Security, Kaiser Family Foundation: Global Health Policy, May 21, 2021. Available: https://www.kff.org/global-health-policy/issue-brief/the-u-s-government-and-global-health-security/
15. White House, Department of Homeland Security Joins the U.S. Global Change Research Program, Office of Science and Technology Policy, February 9, 2023.
16. Government Accounting Office, Climate Change: Enhancing Federal Resilience, GAO-22-106061, September 19, 2022.
17. Government Accounting Office, Federal Agencies Need to Address Aging Legacy System, GAO-16-468, May 2016.
18. Government Accounting Office, Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems, GAO-21-524T, April 27, 2021.
19. Catherine Haddon, COBR (COBRA), Institute for Government, London, UK, January 23, 2020.

20. Government Accounting Office, National Preparedness: Additional Actions Needed to Address Gaps in the Nation's Emergency Management Capabilities, GAO-20-297, May 4, 2020.

21. Government Accounting Office, DHS Priority Recommendations, GAO-23-106483, June 23, 2023.

22. Peter Hall, Colin Carter, Eric Bill, Mark O'Connor, Dr. Murray Simpson, Resilience Return on Investment (RROI), Summary Report, The Resilience Shift, Amec Foster Wheeler, London, UK, June 30, 2017.

23. Senator Gary Peters, S.3510 Disaster Resiliency Act, 117th Congress, December 5, 2022 (became law).

24. FEMA, National Resilience Guidance, Department of Homeland Security, March 8, 2023. National Resilience Guidance | FEMA.gov

25. Lauren Stienstra. National Level Exercises: History, Authorities, and Congressional Considerations. Congressional Research Service. IF 11879. July 15, 2021.

Author

John "Jack" Rodman is a Strategy and Policy Principal at MITRE. Previously a Senior Analyst at the CIA and U.S. Navy, he was also Chairman of the Foreign Denial and Deception Committee on the National Intelligence Council.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the Intelligence Community. The views expressed in this publication are those of the author(s) and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. government department/agency.

You can receive all of MITRE's Intelligence After Next papers by subscribing to the series at mitre.org/IntelligenceAfterNext

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded research and development centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE
mitre.org

JULY 2024