Chapter 5: AI and the Future of National Intelligence

Blueprint for Action

Intelligence will benefit from rapid adoption of artificial intelligence (AI)-enabled technologies more than any other national security mission. However, critical barriers keep the Intelligence Community (IC) from turning this potential into real capabilities that are scaled across agencies.

An Ambitious Agenda: AI-Ready by 2025.

To build on the progress that individual agencies have made, the IC should set the ambitious goal of adopting and integrating AI-enabled capabilities across every possible aspect of the intelligence enterprise as part of a larger vision for the future of intelligence.

Recommendation

Recommendation: Empower the IC's science and technology leadership.

Actions for Office of the Director of National Intelligence (ODNI):

- **The DNI should designate the Director of Science and Technology (S&T) as the IC Chief Technology Officer (CTO)[1] and direct the IC CTO to:**
    - Develop and monitor IC-wide metrics for AI investments, AI implementation, AI outcomes, and AI readiness.
    - Ensure maximum sharing and reuse of AI models, code, and tools across the IC to prevent unnecessary duplication where possible.
    - Establish policies on, and supervise, IC research and engineering, technology development, technology transition, appropriate prototyping activities, experimentation, and developmental testing activities.
    - After congressional approval and appropriation, manage a fund that would allow the ODNI to identify and invest in AI applications with outsized potential that may not have an identified source of agency or program funding as they near the end of their S&T life cycle.
- **The IC CTO, in coordination with the IC Chief Information Officer (CIO), Chief Data Officer (CDO), and Chief Information Security Officer, should oversee the establishment of common technical standards and policies for the IC. These standards and policies should be coordinated with the DoD to promote maximum interoperability, reciprocity, and data-sharing[2] in the following areas:**

- An Application Programming Interface (API)–driven open architecture and associated policies that support the infrastructure to enable AI.[3]
- Multi–level security standards for technical solutions allowing the movement of data across security clearance levels and the policies to enable it.
- Data tagging and labeling.
- Data sharing and access, including incentives for data stewards that reward their ability to share their data; shift the culture such that data stewards make it a default practice of externalizing their data via APIs, with appropriate levels of access restriction and control.
- Common standards for machine readable processing, exploitation, and dissemination (PED) products.
- Automated and reciprocal Authority to Operate (ATO) processes that include rapid code certification and accreditation processes.
- Documentation strategies for data, models, and systems, and of the AI life cycle infrastructure to support traceability, training and testing procedures, and human–AI design guidelines.[4]
- Technical standards for algorithms in support of interpretability and explanation, and policies to strengthen accountability.
- Technologies and operational policies that align with privacy preservation, fairness, inclusion, human rights, and documentation of value considerations and trade–offs.[5]
- Alternative hiring authorities for term–limited appointments appropriate for technical positions, such as Special Government Employees (SGE), highly qualified experts (HQE), and Intergovernmental Personnel Act (IPA) detailees.
- Expanding the use of prize challenges as alternatives to traditional procurement.
- Program and contracting guidance for well–documented and hardened APIs, data access and sharing across the IC, and provisions for the sharing and reuse of software products across the IC.

- **The IC CTO, in coordination with DoD, should develop a Technology Annex to the National Intelligence Strategy (NIS).[6]**
  - The appendix should establish technology roadmaps to adopt AI–enabled applications to solve operational intelligence requirements. The appendix should address current issues within the IC, to include:
    - Aligning technical standards and policies with DoD to ensure seamless interoperability as well as make the Executive branch a better customer and more attractive market for industry.
    - Identify and promote acquisition reforms and methods that ensure the IC can rapidly procure and field systems to its intelligence professionals.
  - The Technology Annex to the NIS should, at a minimum, include:
    - Intelligence support requirements, including how the IC analyzes the global environment and monitors technological advancements, adversarial capability development, scientific and technical cooperation among U.S. competitors, and emerging threats.

    - Functional requirements and technical capabilities necessary to enable concepts that address each challenge.
    - A prioritized, time-phased plan for developing or acquiring such technical capabilities, that takes into account research and development timelines, a strategy for public private partnerships, and a strategy for connecting researchers to end users for early prototyping, experimentation, and iteration.
    - Additional or revised acquisition policies and workforce training requirements to enable IC personnel to identify, procure, integrate, and operate the technologies necessary to address the intelligence requirements.
    - Infrastructure requirements for developing and deploying technical capabilities, including data, compute, storage, and network needs; a resourced and prioritized plan for establishing such infrastructure; and an analysis of the testing, evaluation, verification, and validation (TEVV) requirements to support prototyping and experimentation and a resourced plan to implement them, including standards, test beds, and red-teams for testing AI systems against digital "denial & deception" attacks.
    - Consideration of human-factor elements associated with priority technical capabilities, including innovative human-centric approaches to user interface, human-machine teaming, and workflow integration.
    - Consideration of interoperability with allies and partners, including areas for sharing of data, tools, and intelligence products.
    - Flexibility to adapt and iterate appendix implementation at the speed of technological advancement.

- **ODNI should advance and continue to build out a purpose-built IC Information Technology Environment (ITE) that can fuse intelligence from different domains and sources.**
    - The IC ITE should be built in concert with the DoD digital ecosystem outlined in Chapter 2 of this report; they should focus on a federated system that is interoperable, integrated, and designed with building block services using the same interfaces as the DoD ecosystem.
    - The IC should accelerate ad hoc work and continuous experimentation to learn better how to integrate their systems.
        - Intelligence fusion promised by AI can only occur when all relevant data is made available across all systems. Building on the promise of IC ITE, the IC CIO and CTO should work with their counterparts across the IC and mission partners to ensure that IC integration and interoperability are given priority when evaluating technology investments.
        - The IC CTO should establish a multi-agency accredited learning environment and test bed where ad hoc work and continuous experimentation can occur using all relevant intelligence data.

Actions for Congress:

- **Designate the Director of S&T within ODNI as the IC CTO, and grant that position additional authorities for establishing policies on, and supervising, IC research**

and engineering, technology development, technology transition, appropriate prototyping activities, experimentation, and developmental testing activities.

- **Establish a fund that would allow the DNI to identify and invest in AI applications with outsized potential that may not have an identified source of agency or program funding as they near the end of their S&T life cycle.**
- **Grant the Director of National Intelligence sufficient budgetary authorities to enforce technical standards across the IC, including the ability to fence or otherwise withhold funding for programs that are not compliant with established common standards and policies.**
- **Establish a 10-year, $1 billion, Program of Record to provide long-term, predictable funding for technologies identified in the Technology Annex to the National Intelligence Strategy.**
    - This funding should target programs or departments with a proven track record of transitioning new or critical technologies to meet mission needs.

Recommendation: Change risk management practices to accelerate new technology adoption.

Recommendation

Actions for ODNI:

- **Establish an IT modernization Senior Risk Management Council (IT SRMC).**
    - The IT SRMC should be tri-chaired by the IC CTO, CIO, and CDO to promote the effective governance of significant risk across the IC.
        - The IT SRMC should report to the Principal Deputy Director of National Security (PDDNI).
        - The IT SRMC should become a regular briefing entity in the Deputies Executive Committee (DEXCOM).
    - The IT SRMC should include a senior member from the following IC entities:
        - ODNI Office of General Counsel
        - ODNI Office of Civil Liberties, Privacy, and Transparency
        - ODNI Mission Integration Directorate
        - Each intelligence agency and service branch
    - The IT SRMC responsibilities should include:
        - Reviewing existing policies or creating new policies to ensure the IC uses informed risk acceptance and management practices when considering the adoption and use of AI technologies.
        - Advising the DNI on enterprise risk associated with not adopting AI technologies.
- **Address shortcomings in the current implementation of the National Institute of Standards & Technology (NIST) Federal Information Security Modernization Act (FISMA) Risk Management Framework (RMF).**[7]

- Recommendations from the IT SMRC should inform the operational risk of not adopting a new technology as a balance to the technical risks considered in the RMF, allowing agencies to make better informed decisions on what systems they choose to bring on line or delay.
- The IC should automate the implementation and simultaneous assessment of RMF considerations to the greatest extent possible.
- Agencies within the IC often implement the RMF with different, but associated, policies that can prevent reciprocal accreditation and make it difficult to share tools among agencies.
- The IC should make accreditation reciprocity within the RMF the standard and apply a high level of scrutiny to any agency that seeks to not recognize the accreditation of others.

Actions for Congress:

- **Assess the IC's approach to risk and work with the IC to ensure the proper balance between risk acceptance, risk management, and risk avoidance.**

Recommendation

Recommendation: Improve coordination between the IC and DoD.

Actions for ODNI:

- **In coordination with the Secretary of Defense, the DNI should immediately issue a directive designating the PDDNI as a standing member and/or co-chair to the tri-chair Steering Committee on Emerging Technology.[8]**
  - Absent of Congressional action, the Director of National Intelligence should work with the Secretary of Defense and members of the Steering Committee on Emerging Technology, including the Deputy Secretary of Defense and Under Secretary of Defense for Intelligence and Security, to identify the method and means to drive sustained coordination on emerging technology intelligence, policy, and resourcing.
- **Assist DoD, as requested, in developing the Technology Annex to the National Defense Strategy.[9]**
- **Work with DoD to establish an AI integration team focused on maximizing knowledge, data, and model sharing across and between the IC and DoD.**

Actions for Congress:

- **Revise the National Defense Authorization Act for Fiscal Year 2021 (FY2021 NDAA) provision authorizing a Steering Committee on Emerging Technology by designating it to be tri-chaired by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of National Intelligence.[10]**

Recommendation

Recommendation: Capitalize on AI-enabled analysis of open source and publicly available information.

Actions for ODNI:

- **Develop a coordinated and federated approach to integrate open source intelligence into all current intelligence processes and products. ODNI should promote coordination by taking the following actions:**
    - o Develop common standards and policies that enable the individual agencies to be more effective, such as contracting publicly available data sources for common use across the IC and clarifying or updating policy guidance on the appropriate use of publicly available and open source information, including with respect to privacy and civil liberties for U.S. persons or entities.
    - o Support the IC by identifying reliable industry partners across the spectrum of information sources and creating contract vehicles to rapidly integrate them into intelligence work across the IC. This should include establishing a pilot project to test "data-for-tools" exchanges in public-private partnerships.
    - o Aid the IC in communicating emerging risks and threats to industry and academia by coordinating the right expertise from across the IC; —for example, by connecting non-government entities to the Federal Bureau of Investigation for counterintelligence guidance, or to the U.S. Cyber Command/National Security Agency for cybersecurity.
    - o Develop a robust capability for bringing in individuals without security clearances or awaiting security clearance adjudication and allowing them to work on unclassified projects that directly support the IC.
- **Each individual agency should develop open source capabilities focused on the specialized applications of open source and publicly available information within their unique intelligence domains.**

Recommendation

Recommendation: Aggressively pursue security clearance reform for clearances at the Top Secret level and above, and enforce security clearance reciprocity among members of the IC.

Actions for ODNI:

- **Develop a Blueprint for Action for security clearance reform for clearances at the Top-Secret-and-above level including detailed timelines and metrics. The Blueprint for Action should include:**
    - o A collaborative effort with the private sector and academia to develop data-informed behavioral approaches to understanding risk factors and security clearance adjudication.[11]
    - o Reforming identity management to ensure there is seamless security clearance reciprocity across the IC.
    - o A mechanism to enforce security clearance reciprocity among members of the IC and DoD.

Actions for Congress:

- **Congress should require the DNI to develop a Blueprint for Action for security clearance reform for clearances at the Top-Secret-and-above level including detailed timelines and metrics.**
- **Where necessary, Congress should reinforce the DNI's authority as head of the IC to enforce uniform security clearance policies and practices across the IC.**
- **Congress should require the DNI and the directors of the major intelligence services to regularly report on progress to the oversight committees.**

Blueprint for Action: Chapter 5 - Endnotes

[1] We envision the IC CTO as having roles, responsibilities, and authorities similar to the Under Secretary of Defense for Research and Engineering (USD (R&E)) within the DoD and to help the IC implement guidance and priorities established by the Steering Committee on Emerging Technology and the Technology Competitiveness Council.

[2] In Chapter 3 of this report, the Commission recommends the creation of a Steering Committee on Emerging Technology that is tri-chaired by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director for National Intelligence. This Committee should act as a forum through which to drive coordination between the IC and DoD, including the Chief Technology Officers.

[3] Consistent with the DoD digital ecosystem described in the Chapter 2 Blueprint for Action, the API driven open architecture should: 1) Define a common set of well-documented common interfaces for the ecosystem's key components and building blocks; 2) Support and integrate the work of existing pathfinders up and down the ecosystem technology stack; and 3) Incorporate the process elements for data authorizations and continuous software ATO reciprocity.

[4] Chapter 7 of this report provides more details on improving documentation practices for achieving baseline robust and reliable AI.

[5] Chapter 8 of this report provides details on developing and testing systems per goals of privacy preservation and fairness.

[6] A Technology Annex to the NIS should complement the Technology Annex to the National Defense Strategy (NDS) recommended in Chapter 2 of this report. The recommended Executive Agent for the Technology Annex to the NDS (see the Chapter 2 Blueprint for Action), the Under Secretary of Defense for Research and Engineering (USD (R&E)) should act as the primary interlocutor with the IC CTO for the creation of a Technology Annex to the NIS.

[7] For more information, see *FISMA Implementation Project*, NIST (Dec. 3, 2020), https://csrc.nist.gov/projects/risk-management/rmf-overview.

[8] The Chapter 3 Blueprint for Action calls for the Secretary of Defense, with support from the Director of National Intelligence, to issue a directive immediately establishing a tri-chair Steering Committee on Emerging Technology to oversee development of concepts and capabilities that include emerging and disruptive technologies to meet the current and future operational challenges facing the nation.

[9] For a full discussion of the Technology Annex to the National Defense Strategy, see Chapter 2 of this report.

[10] This action mirrors the Chapter 3 Blueprint for Action. While DoD and ODNI have the authority to establish such a forum without legislative action, codifying it into law will ensure that it is sustained through leadership transitions. If, at the drafting of the FY2022 NDAA, the DoD and ODNI have established the tri-chaired Steering Committee recommended herein, Congress should use the FY2022 NDAA to codify the body into law. If DoD and ODNI have not established the Committee as described in this report, Congress should include in the FY2022 NDAA a provision revising the FY2021 NDAA, section 236, which permits the creation of a Steering Committee on Emerging Technology, but is not structured effectively to improve coordination between the DoD and the IC. For a full discussion of section 236, see the Chapter 3 Blueprint for Action. The Commission also recommends that the legislative language be sufficiently broad so as to enable flexibility in the Steering Committee's roles and responsibilities should they need to adapt as emerging technologies and Department efforts evolve. See the Draft Legislative Language Appendix to this report.

[11] For more information on the need for an academic and scientific review of behavioral approaches to security clearance adjudication, see David Luckey, et al., *Assessing Continuous Evaluation Approaches for Insider Threats: How Can the Security Posture of the U.S. Departments and Agencies Be Improved?,* RAND Corporation at 28-34 (2019), https://www.rand.org/pubs/research_reports/RR2684.html.