AMENDMENT TO RULES COMMITTEE PRINT 119-8
OFFERED BY MR. MOOLENAAR OF MICHIGAN

At the end of subtitle B of title II add the following new section:

SEC. 2___. INITIATIVE ON STUDYING ADVANCED ARTIFICIAL INTELLIGENCE, NATIONAL SECURITY, AND STRATEGIC COMPETITION.

(a) INITIATIVE REQUIRED.—The Secretary of Defense shall establish and carry out an initiative (referred to in this section as the ''Initiative'') to prepare the Department of Defense to fully harness the transformative potential of advanced artificial intelligence, assess the national security and defense implications of advanced artificial intelligence, and analyze strategic competition factors relating to the People's Republic of China's pursuit of advanced artificial intelligence.

(b) DESIGNATION OF LEAD OFFICE.—The Secretary of Defense shall designate an appropriate agency or office within the Department of Defense to have primary responsibility for carrying out the initiative described in subsection (a). Any such designation shall not prohibit other agencies or offices within the Executive Branch from being

consulted or otherwise supporting the efforts of the lead office.

(c) DUTIES.—Under the Initiative, the agency or office designated by the Secretary of Defense under subsection (b) shall do the following:

(1) Review industry documents and assessments of advanced artificial intelligence, including preparedness frameworks, scaling policies, and risk management frameworks of advanced artificial intelligence developers.

(2) Engage with leading artificial intelligence developers and researchers to characterize and anticipate the capabilities of highly advanced artificial intelligence relevant to national security to inform military planning, societal preparedness, and Department of Defense adopt plans, including via interviews, site visits, roundtables, expert discussions, and other forms of engagement with relevant experts.

(3) Identify strategies for the Department of Defense to encourage adoption and fully leverage advanced artificial intelligence systems, assess the comparative adoption to other nations, and manage national security threats from advanced artificial intelligence competition. In assessing adoption strategies,

the Secretary shall evaluate the implications of advanced artificial intelligence for the national defense and form a plan for addressing implications for the Department of Defense's processes, systems, functions, capabilities, and adoption pathways. The plan shall include—

(A) an assessment of the steps needed to prepare the Department of Defense workforce to leverage the transformative potential of advanced artificial intelligence;

(B) an assessment of Department of Defense processes and workflows that are most likely to be substantially impacted by the introduction of advanced artificial intelligence within or outside the structure of each process or workflow, and the offices that will be primarily responsible for managing the evolution of those processes;

(C) identifying internal Department of Defense policies that require revision, elimination, or creation to effectively and responsibly harness advanced artificial intelligence;

(D) a framework for developing the artificial intelligence infrastructure to scale the use

of advanced artificial intelligence, including requirements for—

(i) artificial intelligence factories that manage the entire artificial intelligence life cycle;

(ii) data foundries that effectively and efficiently manage government, commercial, and synthetic data;

(iii) edge infrastructure for employing advanced artificial intelligence in warfighting use cases at all levels of command; and

(iv) other critical enabling infrastructure, such as information technology systems and energy sources;

(E) recommendations for resourcing the materiel and nonmateriel solutions identified in subparagraphs (A) through (D); and

(F) recommendations for resourcing critical artificial intelligence assurance activities, such as test and evaluation, continuous monitoring, governance, and the creation of assurance case artifacts.

(4) Examine the potential implications of advanced artificial intelligence on key areas of national

defense, including chemical, biological, radiological, and nuclear capabilities, advanced cyber capabilities, model autonomy, strategic deception, advanced research and development capabilities for producing increasingly powerful artificial intelligence, military applications of artificial intelligence for warfighting functions, and other areas in which advanced artificial intelligence may pose a threat to national security or national defense.

(5) In consultation with the Director of National Intelligence, monitor and assess the progress of the People's Republic of China in developing advanced artificial intelligence and assess the implications of such development for strategic competition. In assessing such progress, the Secretary shall examine key factors in areas critical for People's Republic of China progress toward advanced artificial intelligence, including—

(A) an assessment of the People's Republic of China's overall efforts toward advanced artificial intelligence, including overall progress, activities to develop or acquire such systems, relative progress compared to United States entities, efforts to prevent loss of control from such systems, and attitudes of the Chinese Com-

munist Party and other influential figures toward advanced artificial intelligence risks and safety approaches;

(B) identification of the primary entities in the People's Republic of China that are leading in the development of advanced artificial intelligence;

(C) identification of the top researchers in the People's Republic of China who are most essential for the development of advanced artificial intelligence;

(D) identification of specific data centers, energy infrastructure, and other resources most critical to the People's Republic of China's progress toward advanced artificial intelligence (including plans for future data centers);

(E) identification and assessment of the top methods to robustly detect advanced artificial intelligence development by the People's Republic of China, including methods to assess the degree to which the People's Republic of China is developing advanced artificial intelligence capabilities that pose significant risks to the national security of the United States;

(F) identification of the top methods that can be used to disrupt advanced artificial intelligence projects of the People's Republic of China and an assessment of their efficacy and limitations;

(G) an assessment of efforts originating in the People's Republic of China to acquire technology and information from entities operating within the United States or other nations to advance progress toward advanced artificial intelligence, including advanced semiconductors, research findings, or insights relating to training or inference; and

(H) a comparative assessment of efforts in the People's Republic of China and United States to characterize and mitigate security risks from advanced artificial intelligence systems, including an evaluation of how leading researchers and policymakers in each country conceptualize the national security risks posed by uncontrolled or misaligned advanced artificial intelligence.

(6) In consultation with the Director of National Intelligence and the Secretary of Homeland Security, assess the security capabilities of leading

United States artificial intelligence developers, with a focus on their ability to protect advanced artificial intelligence systems, model weights, and key insights from the People's Republic of China and other highly resourced adversaries.

(7) Assess the national security risks posed by uncontrolled or misaligned advanced artificial intelligence. The assessment, focusing on the People's Republic of China and the United States, shall include—

(A) an examination of emerging capabilities relevant to misaligned or uncontrolled artificial intelligence, including automated artificial intelligence research, recursive self-improvement, ability to deceive humans, agentic capabilities, and other capabilities or processes that could undermine robust or trustworthy human oversight;

(B) a review of research on AI misalignment, alignment faking, deception, and other related areas in which artificial intelligence systems appear to act in ways that diverge from the intentions or values of their developers or in ways that diverge from United States values or interests;

(C) an assessment of current capabilities within the United States Government to detect and monitor the threats described above, including evaluations of the ability to identify early warning signs or imminent threats relating to recursive self-improvement, offensive cyber use, alignment faking, or other system misbehavior;

(D) recommendations for improving the identification, mitigation, and response to risks from uncontrolled or misaligned artificial intelligence systems, with particular attention to interagency coordination and collaboration with the private sector, academic institutions, and allied governments; and

(E) implications for the Department of Defense's approach toward adopting or deploying advanced artificial intelligence.

(8) Create materials and prepare plans to address acute national security risks or crises involving advanced artificial intelligence, including risks from uncontrolled or misaligned advanced artificial intelligence systems, which shall include—

(A) developing and conducting unclassified and classified scenario exercises, wargames, ta-

bletop exercises, and other similar efforts to understand how advanced artificial intelligence capabilities could present acute national security risks or crises or pose a risk to existing operational plans of the Department of Defense;

(B) developing preparedness plans detailing governmental response strategies to scenarios described in subparagraph (A), including detailed information describing how the Department of Defense would coordinate with relevant entities of the United States (such as advanced artificial intelligence developers, compute cluster providers, and government officials) in the event of an acute national security risk or crisis; and

(C) identifying potential gaps in the Department of Defense's authorities, relationships, personnel, or other factors that could affect the Department's ability to address scenarios described in subparagraph (A) or execute strategies described in subparagraph (B).

(9) Develop potential strategies and recommendations to prevent adversaries from acquiring advanced artificial intelligence that would pose a grave national security threat if acquired or stolen.

As part of this effort, the Secretary shall assess the potential of a hypothetical centralized, highly secure, Department of Defense-led project to securely develop advanced artificial intelligence. This evaluation shall consider factors including the governance structure, cybersecurity and physical security protocols, counterintelligence and antiespionage measures against the People's Republic of China and other foreign adversaries, chain-of-command, size and location of the project, resources and personnel required, contingency and emergency response plans, geopolitical considerations, and other elements to ensure that the project supports United States national security objectives. Additional strategies may include export controls, counterespionage measures, and approaches for protecting sensitive information relevant to national security or advanced artificial intelligence development and deployment.

(10) Provide policy and resourcing recommendations to the Secretary of Defense, the President, and Congress relating to the topics covered by the Initiative.

(d) REPORTS AND BRIEFINGS.—

(1) INITIAL REPORT AND BRIEFING.—Not later than 90 days after the date of the enactment of this Act—

(A) the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report detailing the organizational structure, staffing requirements, and initial objectives of the Initiative; and

(B) provide to the Committees a briefing on the matters set forth in the report.

(2) ANNUAL REPORTS AND BRIEFINGS.—Not later than 180 days after the submission of the initial report under paragraph (1), and every 180 days thereafter, the Secretary of Defense shall—

(A) submit to the Committees on Armed Services of the Senate and the House of Representatives a report on the activities carried out under the Initiative since the date of the last report under this subsection, including any findings, assessments, and recommendations with respect to the national security implications of advanced artificial intelligence; and

(B) provide to the Committees a briefing on the matters set forth in the report.

(e) SUNSET.—The authority to carry out this section shall terminate 10 years after the date of the enactment of this Act.

(g) DEFINITIONS.—In this section:

(1) The term ''artificial intelligence'' has the meaning given that term in section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. note prec. 4061).

(2) The term ''advanced artificial intelligence'' means artificial general intelligence and other advanced artificial intelligence systems at the frontier of performance, including systems that match or exceed human expert performance in key skills, tasks, or knowledge areas, such as in the areas of chemical, biological, radiological, and nuclear capabilities, cyber offense, model autonomy, persuasion, research and development, self-improvement, or military strategy.