Written Statement of Senator Rob Portman

December 6, 2023

AI Insight Forum: National Security

Introduction

Thank you for inviting me to the latest gathering of the Artificial Intelligence (AI) Insight Forum series. As the co-founder and first Republican co-chair of the Senate AI Caucus, I'm pleased to join my former colleagues to discuss AI and its national security implications. National security issues pose some of the greatest challenges and most significant opportunities for AI policymakers. It is my hope that the Senate will continue the tradition the AI caucus began of enacting substantive and bipartisan AI policy.

Senator Heinrich and I founded the AI Caucus in 2019 because we recognized the need for in-house expertise and leadership in the Senate on issues related to this emerging technology. We believed, as we do now, that without understanding and leadership in Congress, the United States risks allowing other nations to harness and build out this technology ahead of us, hurting our national competitiveness, and eroding democratic accountability on an issue which prompts equal optimism and concern from citizens.

Many of the AI Caucus proposals which have become law so far have been enacted as part of the annual *National Defense Authorization Act* (NDAA), which reveals how intertwined AI policy is with national security. Much as with previous transformative technologies—like the airplane or nuclear power—the military stands to play a uniquely influential role when it comes to AI by unlocking innovations, promoting adoption, and developing norms around safe use, all with an eye to deploying AI in ways which keep our nation safe.

At present, the Department of Defense is spending unprecedented monies towards AI research. AI also stands to improve the country's warfighting effectiveness by unlocking efficiencies in maintenance and logistics, enhancing intelligence gathering, and improving the ability to target adversaries in ways which reduce non-combatant causalities.

In addition to the military's role, AI also stands to strengthen our national security by contributing to our overall national competitiveness as we compete with countries like China and Russia. Again, questions around innovation, deployment, and safe use will be key to ensure we use AI in ways which perpetuates U.S. technological, military, and economic leadership globally. This will involve considerations of how to use AI to strengthen our industrial base, discover new innovations to give our national security agencies a further leg up in achieving their missions, and develop international AI norms with allies.

So far Congress, and especially the Senate AI Caucus, have a track record of legislative success which have played a role in the preservation of U.S. AI leadership. There is now a tradition of consistent bipartisan legislating when it comes to AI and it is important for our national competitiveness, national security, and societal trust in technology, that the Senate maintain that tradition. To that end, I propose a new framework for how to develop responsible AI policy and demonstrate how that framework applies in the national security and defense context by proposing some specific policies.

A New Era for AI Policy

During my time as co-chair of the Senate AI Caucus, AI's newness meant that legislative efforts mostly just laid the groundwork for understanding the technology and articulating the federal government's own use of AI. This meant that the laws passed in the previous two Congresses focused on promoting federal investment in cutting-edge research and creating rules for the government's (rather than the private sector's) use of AI. Alongside those efforts, and thanks to the free market, we have seen an expansion of the use of AI across the economy and society. Now, we are now entering a new phase of AI policymaking which appears to be marked by debates around more granular issues such as whether AI systems should be further regulated beyond existing laws.

But in considering whether to further regulate AI, policymakers must be careful not to stifle innovation. AI innovation is key to wringing well-being maximizing benefits from AI, as well as being itself the source of solutions to AI problems, like unfair bias. To best navigate this tension between regulation and innovation, it is important to stress that AI is not a single, monolithic technology. Rather, AI is a general-purpose technology (like steam power or electricity) given to a myriad of use cases. A single regulatory approach—such as a "Food and Drug Administration for algorithms"—treats AI like a monolith, which risks overregulation and jeopardizes innovation. It also fails to account for the existence of numerous regulatory tools and authorities already on the books.

Responsible AI policymaking must be attuned to these dynamics.

The AI Policy Cycle

To navigate this new AI moment, while avoiding a problematic and monolithic approach, policymakers would do well to consider a new conceptual framework: an AI policy cycle that policymakers can use to balance considerations of innovation and harm mitigation to develop responsible AI policies.

The cycle consists of three features: the need to *promote* AI innovation, the need to *channel* AI innovations towards productive use cases, and the need to *mitigate* harms associated with AI deployment in those use cases. Each element promotes the other. More innovation means more opportunities to use AI productively. More productive use of AI will mean the proliferation of AI throughout society for the potential benefit of our economy. And greater use may increase the risk of AI harms, which requires policies to reduce those risks. But those policies should not stymie the next round of AI innovation, which then facilitates further productive use.

So far Congress has focused mostly on promoting AI innovation. Proposals like the creation of a National AI Research Resource (NAIRR) and the National AI Initiative aim to use federal investments to complement those being spent by academia and industry in the pursuit of new AI innovations.

There are also proposals currently being debated related to the regulation of AI systems. As a threshold matter, policymakers should understand which use cases are sufficiently covered by existing regulatory authorities as to make further regulation unnecessary, burdensome, or counterproductive. Before creating something new, policymakers should first explain why existing regulatory authorities are insufficient at guarding against AI harms. Consideration should also be given to whether a better approach might be needed to ensure that existing agencies have the authorities, resources, and technical talent they need.

None of which is to say that there is no need for new approaches: some of the challenges posed by AI may not be well-covered by existing authorities and may require more tailored approaches. This could include the need to clarify the application of legal liability where AI is involved. Or whether to require AI tools and services to be clearly labeled as such. Or creating structures to monitor and manage novel risks from the most advanced AI systems. But policymakers proposing new regulatory authorities for AI should first provide justification by demonstrating how existing authorities fall short of mitigating AI harms. By identifying potential gaps in authorities, policymakers can develop bespoke, targeted authorities which mitigate harms while reducing damage to innovation.

So far, less work has been done to channel AI to productive use cases. There is little value to using AI to improve the social media experience—more targeted cat videos do not enhance societal well-being. But there are great benefits to be gleaned from the deployment of AI in sectors of the economy often not affiliated with technology, like manufacturing, logistics, healthcare, and national security. For instance, doctors are now using AI to review mammograms 30 times faster and with 99 percent accuracy.

Policymakers should investigate any current barriers to widespread adoption of AI in those sectors with an aim to safely remove those barriers. The AI policy cycle offers a means by which policymakers can understand how different AI issues—innovation, productivity, and mitigation—mesh together. Keeping all these elements in balance ensures that AI policy is responsible and its outcomes valuable to the citizens it is designed to benefit. The goal of AI policy is to maximize its benefits and reduce its harms, which in doing so maximizes well-being for citizens.

Application to the National Security Context

I share this conceptual framework not only because it is a valuable guide for AI policymaking overall, but also because national security offers a useful example to show how the framework leads to responsible outcomes. Moreover, the fact that much AI legislation has become law under the aegis of national security in the annual defense authorization bills makes clear that regardless of topic or use case, AI issues never stray very far from fundamental issues of national security and national competitiveness. So how does the three-part AI policy cycle manifest in the national security context?

Promote AI Innovation

AI innovation is core to our national security and national competitiveness. Innovation is critical to national power, as our adversaries are aware. China intends to be the world's dominant AI power by 2030 and is making investments to achieve that aim. As of 2019, China had 515 Key State Laboratories, entities equally critical to China's military and commercial technology ambitions.[1]

To ensure that the United States remains the world's dominant AI power well past the end of the decade, Senator Heinrich and I led the effort to the establish the NAIRR, or National AI Research Resource.[2] Signed into law by President Trump, and prioritized by President Biden, the NAIRR will be a national network of the AI research tools—including serious compute power—needed to supercharge AI innovation. There are smart researchers across America, and they should not have to work for a Big Tech firm to get access to the infrastructure needed to pursue promising AI ideas. By democratizing access to these resources, the NAIRR leverages our country's unique talent base to keep our foot on the AI innovation gas pedal.

The original NAIRR concept was developed by the National Security Commission on AI (NSCAI), one of their many recommendations to Congress which have since become law. Continuing the effort to finally establish the NAIRR—which a new bipartisan bill by Senators Heinrich, Young, Booker, and Rounds would do—would be one of the single best things Congress could do to bolster our national competitiveness.

Channel Towards Productive Use Cases

[1] Emily Weinstein, Daniel Chou, Channing Lee, Ryan Fedasiuk, and Anna Puglisi, *China's State Key Laboratory System: A View into China's Innovation System*, Center for Security and Emerging Technology (2022), https://cset.georgetown.edu/publication/chinas-state-key-laboratory-system.

[2] *See* section 5106 of P.L.116-283.

Given the high stakes associated with the nation's security, policymakers should want to channel AI into the use cases which will yield the most value for our security, defense, and competitiveness. One high-value use case is predictive maintenance. By using AI to manage the maintenance cycles of our warships, aircraft, and vehicles, our military can improve their effectiveness and reduce the time those assets are off the battlefield. In the cybersecurity context, AI systems can augment human defenders as well as bolster our offensive capabilities by helping to locate new network vulnerabilities in real time.

National security agencies also possess a tremendous amount of information and intelligence—AI can augment human experts to make better decisions, more quickly. The same can be said of using AI to improve military logistics to get warfighters the resources they need more efficiently. And more broadly, AI can help experts more deeply scrutinize critical supply chains for vulnerabilities. Identifying supply chain chokepoints and dependencies gives policymakers the information they need to build resilience against natural and man-made threats.

With respect to our national competitiveness, policymakers can enable productive AI use cases by setting global rules which benefit U.S. firms and help promote our values abroad.

Sensible AI standards make it easier for firms to channel AI into productive uses globally and promotes U.S. technology exports. However, entities affiliated with China have become quite active in global and international standards setting bodies. This poses risks—such as the normalization of opinions and rules about the use of AI-enabled surveillance technologies—which undermines U.S. technology equities abroad.[3] For these reasons, additional engagement by U.S. entities at standards setting bodies is vital.

Similarly, strong digital trade rules—such as those which were included in the U.S.-Mexico-Canada Agreement (USMCA)—represent valuable tools to promote U.S. values abroad with respect to technology, boost American AI exports, and improve the productive use of AI domestically, such as in smart manufacturing. Therefore, it is concerning that the U.S. Trade Representative recently withdrew longstanding U.S. digital trade proposals from negotiation at the World Trade Organization (WTO). Walking away from strong digital trade rules undermines U.S. technology leadership and cedes that leadership position to China. Instead, the United States should negotiate assertively to promote the adoption of rules which strengthen our competitive position such as by promoting a technology ecosystem conducive to the productive adoption of AI.

Mitigate Harms

Widespread deployment of AI will, by its nature, increase individual's potential exposure to AI harms. Because AI is not monolithic, mitigating those harms is best done on a use case by use case basis. Moreover, the federal government already possesses numerous regulatory authorities which might be helpful in addressing AI harms. Before rushing to create new authorities, policymakers should ensure agencies have the proper resources and expertise to respond to the AI moment responsibly and effectively.

In the national security context, this includes ensuring quality AI training for our servicemembers and military leadership. Senator Heinrich and I passed three bills dealing with AI training for the military,

[3] Press Release, U.S. Senate, Portman, Warner, Bipartisan Colleagues Express Concern About China's Use of Artificial Intelligence-Based Technologies to Oppress Uyghur Muslims, Urge Secretary Pompeo to Work With Allies to Prevent Its Spread Internationally (March 12, 2020), https://www.warner.senate.gov/public/index.cfm/2020/3/portman-warner-bipartisan-colleagues-express-concern-about-china-s-use-of-artificial-intelligence-based-technologies-to-oppress-uyghur-muslims-urge-secretary-pompeo-to-work-with-allies-to-prevent-its-spread-internationally.

but there is always more to be done, including passing unenacted recommendations proposed by the NSCAI.[4] Another law, which I passed with Senator Peters, will provide training to procurement officers across the government to give them the knowledge necessary to successfully procure quality and safe AI systems.[5]

A unique harm posed by generative AI are the risks associated with targeted and widespread disinformation, including deepfakes. For most of human history seeing meant believing. Combined with the network effects created by social media, fake videos or pictures can travel around the world in an instant, tricking citizens. I proposed the *Deepfake Task Force Act* with Senator Peters to develop digital content provenance rules to expose and track deepfakes across the internet and help content creators authenticate their work.[6] By making progress to develop standards, we can help companies, tech platforms, journalists, and all Americans can better track and authenticate content. This law was passed out of the Homeland Security and Governmental Affairs Committee twice with bipartisan support but has yet to be considered this Congress.

Lastly, Congress must ensure that investments in AI research and innovation do not fall into the hands of our adversaries, like Russia and China. Stronger rules are needed to blunt the infiltration of the U.S. research base by foreign "talent recruitment programs." I introduced the *Safeguarding American Innovation Act* (SAIA) with Senator Carper in 2020 after a two-year investigation as Chairman of the Permanent Subcommittee on Investigations. Starting in the late 1990s through its talent recruitment programs, China began recruiting U.S.-based scientists and researchers to transfer U.S. taxpayer-funded intellectual property for China's military and economic gain. In particular, SAIA includes a provision requested by the administrations of Presidents Trump and Biden to give the Department of State authority to deny visas to those seeking to enter the country to steal emerging technology, like artificial intelligence. Although SAIA passed the Senate as part of the *U.S. Innovation and Competition Act*, it has yet to become law.

Conclusion

There is no doubt about the transformational power of AI. But whether the United States can meet the AI moment in ways responsible and effective is an open question. A responsible approach recognizes the need for balance between innovation and regulation as well as the importance of channeling AI into use cases prone to generate benefits and enhance well-being. In doing so, policymakers should be cognizant of the value of existing tools and be precise in explaining the instances where those tools are insufficient enough—or where AI is unique enough—to merit the creation of bespoke new regulatory authorities.

As a conceptual framework, the AI policy cycle is a guide for policymakers as they meet the AI moment. The cycle is a feedback loop of three components: promoting AI innovation, channeling AI into productive use cases, and mitigating AI harms. While the fruits of the AI policy cycle help strengthen national security by promoting a healthy AI ecosystem overall, this discipline can also be used to navigate national security specific use cases. AI, and innovation broadly, represents a key source of national power—one which the United States uniquely possesses. To sustain and improve that source, it is my hope that the Senate continues its bipartisan tradition of vigorous, but careful and responsible AI policymaking.

[4] *See* section 228 of P.L.117-81 (AI for the Military Act), sections 1751 and 594 of P.L.116-283 (AI for the Armed Forces Act), and sections 230 and 231 of P.L. 116-92 (Armed Forces Digital Advantage Act).

[5] *See* P.L.117-207 (AI Training Act).

[6] *See* S. 2559, Deepfake Task Force Act, https://www.congress.gov/bill/117th-congress/senate-bill/2559.