Statement before the House Committee on Armed Services
Subcommittee on Cyber, Information Technologies, and Innovation
On *Man and Machine: Artificial Intelligence on the Battlefield*.

AI Is a National Security Lifeline

Klon Kitchen
Senior Fellow

July 18, 2023

Opening Statement

Good morning, Chairman Gallagher, Ranking Member Khanna, and members of the committee. Thank you for the privilege of testifying.

I'd like to use my opening statement to make three points.

First, I believe artificial intelligence (AI), and particularly emerging capabilities like generative AI, are a national security lifeline for the United States. The national security community has discussed the potential of AI for years, but now it seems these technologies are finally maturing to where they can be applied at scale – with few doubting that they will soon reshape almost every part of our lives, including how we fight and win wars.

The importance of AI is felt as acutely in Beijing as it is in Washington, but until recently, I was not at all confident that the United States would hold the AI advantage. If you assume this advantage fundamentally comes down to algorithms, data, and hardware – just one year ago, I would have given the United States the advantage on algorithms, the Chinese the advantage on data, and I would have called hardware a "jump ball" between the two nations because, while the U.S. designs the most advanced semiconductors in the world, they are overwhelming produced deep within China's sphere of influence. But now I'm giving this assessment another look.

Large Language Models and other generative AIs may be moving the competition back to the American advantage. The U.S. continues to dominate the underlying computer science and algorithms giving birth to these advancements and we continue to be the location of choice for the world's most brilliant minds.

On hardware, a strong bipartisan consensus is allowing us to meaningfully constrain China's access to cutting-edge capabilities like advanced graphics processing units (GPUs) and even more can and should be done, for example, limiting Chinese cloud services would be an excellent next step.

Finally, on data, while the Chinese economy and people continue to generate a deluge of digitized data and while the Chinese Communist Party (CCP) continues to have unfettered access to these data, the fact that many of the new AI models are indexed on the open internet may blunt the CCP's advantage. It is my hope, for example, that the Chinese government's political fragility, strict content controls, and general oppression of its own people will compromise or bias much of the data that it collects, diluting its utility and ultimately limiting the development of Chinese AI. At the very least I think the United States has an opportunity to surge ahead of Beijing on AI if we properly seize this moment.

But AI offers the U.S. more than bespoke capabilities, Large Language Models and other generative technologies – if properly realized – could provide an economic base for a new era of American prosperity and security. For years, we have known that the United States is not investing in its military sufficiently to enable it to meet the demands of the nation. The truth of this has been laid bare as our defense industrial base struggles to keep up with the demand of supporting Ukraine's noble fight against Vladimir Putin illegal and evil invasion of that nation. But, according to one recent study, existing GenAI "could add the equivalent of $2.6 trillion to $4.4 trillion annually" to the global economy, and "this estimate would double if we include the impact of embedding generative AI into software that is currently used."[i]

The bottom line is this: I believe AI is offering us an opportunity to get our economic house in order, to lay a foundation for our nation's long-term prosperity, and to build a national security

enterprise that is sufficiently resourced to secure that prosperity for a generation or more.

But finally, while AI offers all this promise and more, it also has some serious national security risks – most acutely a flood of misinformation and disinformation operations and the exponential growth of conventional and novel cyber-attacks.

By now we have all seen the photos, videos, and other media generative AIs are creating and these capabilities have been almost immediately democratized. Virtually anyone, anywhere in the world, can now create and distribute synthetic media that will undoubtedly be used to undermine American confidence in our democratic institutions and free society. Similarly, generative AIs will offer hostile cyber actors potent tools for generating and automating traditional and new online attacks. In a world where we are already overwhelmed by online threats, generative AIs will soon pour gas on these fires.

There is much more that I could say on these matters, but I trust we'll cover them more fully over the course of this hearing. Thank you again for the opportunity to testify and I look forward to your questions.

Background

Artificial Intelligence (AI), particularly generative AI (GenAI), offers a substantial opportunity for the United States to reclaim its technological and economic upper hand on the global stage. By deploying AI power, the U.S. can accelerate innovation, encourage economic growth, and sustain its leadership in the technology sector – all of which facilitate the nation's security interests.

GenAI holds the potential to reshape various industries, including healthcare, finance, manufacturing, and entertainment. Advanced AI models, like OpenAI's GPT, can create realistic text, images, and even music. This paves the way for creative applications, content creation, and personalized user experiences. With GenAI, American companies can craft innovative products and services that meet evolving market demands, which would foster economic growth and create new jobs.

For example, according to a recent McKinsey and Company study, GenAI "could add the equivalent of $2.6 trillion to $4.4 trillion annually" to the global economy, and "this estimate would double if we include the impact of embedding generative AI into software that is currently used."[ii]

AI-driven automation can also boost productivity and efficiency across sectors, enabling American businesses to compete on the global stage. Intelligent automation can enhance operations, optimize supply chains, and improve decision-making processes. This can result in cost savings, increased output, and improved competitiveness for American industries.

Here again, McKinsey's study concludes, "Current generative AI and other technologies have the potential to automate work activities that absorb 60-70 percent of employees' time today." It adds that "…half of today's work activities could be automated between 2030 and 2060, with a midpoint in 2045, or roughly a decade earlier than in our previous estimates."[iii]

The U.S.' potential to reclaim its competitive advantage is evident in the wealth of talent and expertise in the AI field. American universities and research institutions have led AI research, producing pioneering advancements and cultivating a skilled workforce. Furthermore, the U.S.

hosts a dynamic ecosystem of AI startups and technology companies that are driving innovation and attracting global investments. For example, American companies have led breakthroughs in machine learning, computer vision, natural language processing, and other AI disciplines. These advancements have yielded transformative technologies like voice assistants, autonomous vehicles, and personalized recommendations. The U.S. has also led in deploying AI technologies across sectors, including finance, healthcare, and e-commerce, driving significant economic growth.

It is also important to underscore how much American policymakers are united in their understanding of the strategic importance of AI and have actively supported its development. The U.S. government has invested in AI research, encouraged academia-industry collaborations, and promoted the adoption of AI technologies in public sectors. These initiatives reveal a commitment to fostering an AI-driven economy and maintaining American leadership in the global technology landscape.

AI, particularly GenAI, presents a remarkable opportunity for the U.S. to reclaim its technological and economic dominance. By exploiting AI's transformative potential, investing in research and development, and nurturing talent, the U.S. can accelerate innovation, create jobs, and sustain its leadership in the global AI landscape. The country's historical successes, along with its robust AI ecosystem and supportive policies, position it favorably to seize this opportunity and secure its technological and economic future.

This new efficiency and prosperity should be the backbone of a renewed American military and national security enterprise that is resourced to meet our nation’s global interests and priorities. But, even if the U.S. does everything right, many of our partners are approaching AI and other technologies in ways that will constrain—or even imperil—our shared security concerns.

Military Interoperability

The U.S. and its allies should pursue complementary approaches to AI and other emerging technologies, considering the private sector’s critical role in AI and related technologies.

Indeed, the significant role of the private sector in GenAI development is a key reason for focusing on regulatory interoperability. Private companies are leading AI innovation, investing heavily in research and development. Their expertise and resources centrally position them to shape the trajectory of AI technologies. As the private sector operates globally, regulatory interoperability becomes crucial for effective engagement and collaboration between companies across different countries and, more importantly, for the interoperability of military capabilities.

The ability for allied forces to seamlessly collaborate is essential for joint missions and coalition efforts. Specifically, aligning regulations, standards, and ethical frameworks among allies is crucial to ensure smooth coordination and information sharing.

Military interoperability is particularly important in the context of GenAI. GenAI technologies, with their potential for autonomous decision-making and advanced capabilities, require close coordination and trust among allied forces. By adopting complementary approaches, the U.S. and its allies can establish common guidelines and principles for the development, deployment, and use of GenAI in military applications. This ensures that AI systems adhere to shared ethical norms, respect international humanitarian law, and are compatible with each other, enabling effective joint operations. But some of our allies appear not to understand this.

Regulatory Interoperability

Unfortunately, many of our closest partners, especially in Europe, are pursuing policies that risk stifling innovation and creating barriers to market entry for American companies. The European Union's proposed AI Act, along with other technology regulations targeting American tech companies, are already negatively impacting both the American tech industry and the global technology landscape.

The AI Act introduces strict rules and requirements for AI systems, including "high-risk" applications. While these regulations aim to ensure ethical and responsible AI deployment, the Act's provisions are overly prescriptive and hinder innovation. The compliance costs and regulatory complexities may disproportionately impact smaller tech companies, including startups, limiting their ability to compete and thrive in the European market. And this is broadly recognized even among European technology companies.

For example, recently more than 150 European companies issued a public letter criticizing the AI Act, arguing that the EU's heavy-handed approach is threatening EU digital sovereignty and calling for active industry involvement from companies on both sides of the Atlantic. "Such regulation," the letter warns, "cold lead to highly innovative companies moving their activities abroad, investors withdrawing their capital from the development of the European Foundation Models and European AI in general."[iv] But this is not the only challenge.

The EU's focus on data localization and data sovereignty further exacerbates the potential negative impact on American tech companies. The proposed regulations aimed at promoting the storage and processing of data within the EU would limit the ability for American tech companies to efficiently operate and deliver services in the European market. These regulations not only create an uneven playing field that may favor domestic European competitors, but it also disrupts the seamless exchange of data needed to address common global challenges, such as privacy, cybersecurity, and the responsible deployment of AI.

Adopting complementary approaches to AI and emerging technologies allows the US and its allies to leverage their collective strengths. Each country brings unique expertise, resources, and perspectives to the table. By working together, they can share best practices, collaborate on research and development, and jointly tackle common challenges.

Beyond helping our friends assume a more productive posture on AI and emerging technologies, the U.S. should also prepare for how our adversaries might seek to use these capabilities to subvert the American people and our national interests.

Foreign AI Threats

The rapid advancement of GenAI poses a significant near-term threat concerning its potential use against us by foreign adversaries. One of the most concerning aspects is the exponential growth of traditional cyber threats in both speed and scale. The convergence of GenAI and cyberattacks magnifies the potential risks and challenges faced by nations, governments, and individuals in defending against these threats.

Foreign adversaries leveraging GenAI can significantly increase the speed at which cyberattacks are executed. AI-powered systems can autonomously scan and exploit vulnerabilities in

computer networks and software at an unprecedented pace. This acceleration allows adversaries to infiltrate systems rapidly, extract sensitive information, or disrupt critical infrastructure. With the ability to quickly automate and execute attacks, the response time for defenders becomes increasingly limited, amplifying the potential damage caused by cyberattacks.

The scalability of GenAI-driven cyber threats is another alarming aspect. Adversaries can utilize AI-powered bots and algorithms to orchestrate large-scale attacks, overwhelming networks and systems. Distributed denial-of-service (DDoS) attacks, for example, can be amplified through AI-controlled botnets, causing severe disruptions to online services and critical infrastructure. The ability to orchestrate simultaneous attacks on multiple targets with minimal human intervention increases the potential for large-scale cyber disruptions and undermines the stability of nations and economies.

Moreover, GenAI enhances the sophistication and effectiveness of cyber threats. AI algorithms can learn and adapt to defensive measures, making attacks more evasive and difficult to detect. Adversaries can leverage AI's ability to analyze vast amounts of data to identify patterns, exploit weaknesses, and craft customized attacks. By constantly learning and evolving, GenAI-powered cyberattacks become more sophisticated, resilient, and capable of bypassing traditional security measures.

Finally, there is also the potential for foreign adversaries to leverage GenAI for social engineering and psychological manipulation. AI algorithms can analyze and understand human behavior patterns, preferences, and vulnerabilities, enabling adversaries to tailor attacks with precision. By leveraging this technology, adversaries can craft convincing phishing emails, generate realistic deep fake videos, or manipulate public opinion through targeted disinformation campaigns. The combination of GenAI's computational power and psychological insights can exponentially amplify the impact of such attacks, posing significant risks to national security and social cohesion.

To address this near-term threat, it is essential for governments, cybersecurity experts, and technology companies to collaboratively develop robust defenses against GenAI-powered cyber threats. This includes leveraging AI and machine learning technologies to enhance threat detection, automate responses, and mitigate the risks posed by AI-driven attacks.

International cooperation is also crucial in establishing norms, agreements, and frameworks to address the malicious use of AI technologies. Encouraging information sharing, promoting transparency, and establishing guidelines for responsible AI development can help mitigate the risks posed by foreign adversaries. Additionally, fostering public-private partnerships is vital to exchange knowledge, resources, and best practices in addressing the evolving cyber threat landscape. But there are other near-term threats beyond traditional cybersecurity.

The arrival of GenAI also introduces the potential for low-friction misinformation and disinformation operations that pose significant challenges to democratic institutions in the U.S. Specifically, GenAI's ability to rapidly generate and disseminate vast amounts of convincing content can amplify the spread of misinformation, degrade trust in institutions, and undermine democratic processes reliant on informed decision-making and an educated citizenry.

One of the key implications of GenAI-enabled misinformation and disinformation operations is the speed and scale at which false or misleading information can be generated and disseminated. AI algorithms can swiftly produce and distribute content that appears legitimate, making it

increasingly difficult for users to distinguish between real and fake information. This allows malicious actors to manipulate public opinion, exploit existing biases, and intensify societal divisions with minimal effort and cost.

Moreover, GenAI can generate highly personalized and targeted content, designed to exploit individuals' vulnerabilities and preferences. By analyzing vast amounts of data, AI algorithms can understand users' interests, beliefs, and behaviors, enabling the creation of hyper-targeted misinformation campaigns. This level of personalization enhances the persuasive power of disinformation, making it more likely for individuals to be influenced and reinforce echo chambers that undermine public discourse.

Furthermore, GenAI-powered disinformation campaigns can influence electoral processes, threatening the integrity of democratic elections. Malicious actors can leverage AI algorithms to amplify divisive narratives, suppress voter turnout, or manipulate public opinion to favor specific candidates or causes. The proliferation of misinformation can create an environment where the truth becomes obscured, and electoral outcomes are skewed, compromising the legitimacy and fairness of democratic processes.

Ultimately, the widespread dissemination of misinformation and disinformation erodes trust in democratic institutions. When false or misleading information proliferates unchecked, public trust in media, government, and other authoritative sources can diminish. This undermines the foundation of democratic societies, as citizens rely on accurate information to make informed decisions, hold elected officials accountable, and engage in meaningful political discourse.

Addressing the challenges posed by GenAI-enabled misinformation and disinformation requires a multi-faceted approach. It involves collaboration among governments, technology companies, civil society, and the public. Efforts should focus on developing robust fact-checking mechanisms, promoting media literacy, and improving digital literacy among citizens. Technology companies should enhance their algorithms and platforms to detect and counteract the spread of false information. Governments can play a role by implementing legislation that promotes transparency, accountability, and the responsible use of AI technologies.

While cybersecurity and misinformation and disinformation will be critical near-term challenges, advancing AI will also provoke more systemic and strategic challenges for national security leaders over the long-term. Specifically, we will need to navigate the unprecedented level of knowledge AI can provide, the opacity of AI decision-making processes, the authority granted to AI systems, and the potential for lethal autonomy.

Long-Term Challenges of AI

As aforementioned, one of the premiere challenges of AI is its acquisition of knowledge at an unprecedented scale and speed. AI algorithms can process vast amounts of data, analyze patterns, and derive insights that surpass human capabilities. This knowledge can be immensely valuable for a range of applications, from scientific discoveries to business insights. However, as we accumulate more knowledge, it becomes increasingly challenging to manage and interpret this information effectively. The sheer volume and complexity of AI-generated knowledge require careful navigation and the development of robust frameworks for verification, validation, and interpretation.

The second challenge arises from the opacity of AI decision-making processes. As AI systems

become more sophisticated, they employ complex algorithms that can yield accurate results but may not provide explainable or interpretable rationales. In certain cases, AI can produce correct outcomes without us fully understanding how it arrived at those conclusions. This lack of explainability can be problematic, especially in critical domains where transparency and accountability are essential. It raises concerns about biases, ethical implications, and the potential for unintended consequences. Striking a balance between the accuracy and explainability of AI systems is an ongoing challenge that requires careful consideration and research.

The third challenge is related to the authority granted to AI systems. As AI algorithms demonstrate impressive performance and accuracy, there is a tendency to rely heavily on their decisions and recommendations. However, AI systems are not infallible and can make errors or encounter scenarios outside their training data. The challenge lies in discerning when AI is authoritative and when human judgment should prevail. It requires understanding the limitations of AI systems, designing appropriate checks and balances, and establishing clear boundaries for human oversight and intervention. Striking the right balance between human judgment and AI authority is crucial to ensure responsible and accountable decision-making.

The fourth, and perhaps most contentious challenge, is the emergence of lethal autonomy. Lethal autonomous systems refer to AI-powered machines or weapons that can independently identify and engage targets without direct human control. The development of such systems raises ethical and legal questions, as it has the potential to be abused or create unintended consequences. The challenge lies in determining the appropriate policies, regulations, and safeguards to ensure that lethal autonomous systems adhere to international humanitarian law, ethical principles, and the principles of proportionality and distinction in armed conflict. It requires international cooperation, robust ethical frameworks, and clear guidelines to prevent the escalation of conflicts or the loss of human control over life-and-death decisions.

Addressing these challenges requires a comprehensive and multidisciplinary approach. It involves collaboration among policymakers, researchers, industry leaders, and civil society to develop ethical guidelines, regulatory frameworks, and technical solutions. Transparency and accountability in AI systems are paramount, necessitating efforts to enhance explainability and interpretability. Ongoing research in AI ethics, fairness, and bias mitigation is crucial to ensure that AI is deployed responsibly and does not perpetuate or amplify existing societal inequities.

Moreover, as has been reiterated throughout my testimony, international cooperation is essential in addressing the challenges posed by AI technologies. Establishing global norms and agreements can help guide the development, deployment, and use of AI in a manner that respects human rights, privacy, and security. It can also promote cooperation in areas such as data sharing, research collaboration, and the prevention of malicious uses of AI.

In conclusion, as AI continues to advance, there are inherent challenges that we need to navigate. These challenges include managing an unprecedented level of knowledge, addressing the opacity of AI decision-making processes, determining the appropriate balance between AI authority and human judgment, and grappling with the potential implications of lethal autonomy. Addressing these challenges requires multidisciplinary collaboration, transparency, accountability, and ongoing research and innovation. By proactively tackling these challenges, we can harness the potential of AI while ensuring its responsible and beneficial integration into our society.

Again, I thank the committee for the opportunity to share these observations and I look forward to your questions.

[i] McKinsey and Company. *The economic potential of generative AI: The next productivity frontier.* 14 June 2023.<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of generative-ai-the-next-productivity-frontier#introduction>.

[ii] McKinsey and Company. *The economic potential of generative AI: The next productivity frontier.* 14 June 2023.<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of generative-ai-the-next-productivity-frontier#introduction>.

[iii] Ibid.

[iv] Butcher, Mike. *European VCs and tech firms sign open letter warning against over-regulation of AI in draft EU laws*. 30 June 2023.<https://techcrunch.com/2023/06/30/european-vcs-tech-firms-sign-open-letter-warning-against-over-regulation-of-ai-in-draft-eu-laws/>.