S. Hrg. 118–136

ADVANCED TECHNOLOGY: EXAMINING THREATS TO NATIONAL SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON
EMERGING THREATS AND SPENDING
OVERSIGHT

OF THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 19, 2023

Available via the World Wide Web: http://www.govinfo.gov

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
53–708 PDF WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia
RICHARD BLUMENTHAL, Connecticut

RAND PAUL, Kentucky
RON JOHNSON, Wisconsin
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri
ROGER MARSHALL, Kansas

David M. Weinberg, *Staff Director*
William E. Henderson III, *Minority Staff Director*
Laura W. Kilbride, *Chief Clerk*
Ashley A. Gonzalez, *Hearing Clerk*

SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT

MAGGIE HASSAN, New Hampshire, *Chairman*

KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
JON OSSOFF, Georgia

MITT ROMNEY, Utah
JAMES LANKFORD, Oklahoma
RICK SCOTT, Florida

Jason M. Yanussi, *Staff Director*
Nick Caron, *Policy Advisor*
Scott Maclean Richardson, *Minority Staff Director*
Margaret E. Frankel, *Minority Professional Staff Member*
Kate Kielceski, *Chief Clerk*

CONTENTS

WITNESS

TUESDAY, SEPTEMBER 19, 2023

ALPHABETICAL LIST OF WITNESSES

ADVANCED TECHNOLOGY: EXAMINING THREATS TO NATIONAL SECURITY

TUESDAY, SEPTEMBER 19, 2023

U.S. SENATE,
SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT,
OF THE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:31 p.m., in room 562, Dirksen Senate Office Building, Hon. Margaret Hassan, Chair of the Subcommittee, presiding.

Present: Senators Hassan [presiding], Rosen, Romney, Lankford, and Scott.

OPENING STATEMENT OF SENATOR HASSAN[1]

Senator HASSAN. Before we get started today, I wanted to take a moment, Senator Romney, to reflect on the impact that you have had on the Senate in the time that you have been here and note how much I am going to miss working with you when you retire.

Ranking Member Romney has been an incredible partner both on this Committee and in the important bipartisan legislation that the Senate has passed in the last few years. Senator Romney, your dedication to public service is clear, and the people of Utah, Massachusetts, and the United States are better off due to your years in elected office.

Thank you for your hard work, and there is more hard work to do, so I look forward to continuing our important work for the remainder of this Congress. With that, I am going to say good afternoon to everybody and welcome our distinguished panel of witnesses.

Thank you all for appearing today to discuss potential threats to national security posed by advanced and emerging technologies, and what steps the Federal Government can take to mitigate risk and encourage the responsible development of next generation technologies.

I also want to thank Ranking Member Romney and his staff for working with us on this hearing and for our continued partnership to address emerging threats to the Nation. Today's hearing brings together a group of experts in technology policy who have previously served as government officials and who are now providing

[1] The prepared statement of Senator Hassan appears in the Appendix on page 31.

important and valued insight on the development and applications of advanced technologies.

We will hear about the potential dangers to public safety and security that may be posed by emerging technologies such as artificial intelligence (AI) and quantum technology. We will also hear about the actions that Congress and the Executive Branch can take to mitigate these risks, while still working to maintain the United States' technological innovation edge and stay ahead of our global adversaries.

Public and private investment in the United States have fueled the rapid growth and the power and availability of artificial intelligence, quantum computing, and other emerging technologies. Our nation is well positioned to benefit from the technological revolution that is already underway.

However, bad actors will also undoubtedly seek to use these powerful technologies to launch a higher volume of new and more severe attacks aimed at the American people. As we will hear today, AI and other advanced technologies pose real public safety risks, which Congress is just beginning to address.

For example, although there has been considerable congressional attention paid to many of the public safety risks posed by artificial intelligence, there has been less focus on so-called catastrophic risks posed by AI, such as the ability of AI to help terrorists develop and use unconventional weapons.

I am working on a framework to support research into safer AI that, in its fundamental design, cannot easily be abused by criminals and cannot easily behave in unexpected ways that would harm the public.

Congress needs to look closely at ways to require AI to be designed in a fundamentally safer way, and in time, require all AI hardware to be restricted to running only fundamentally safe systems.

I look forward to hearing from all of our witnesses about how Congress and the Federal Government can successfully encourage technological growth and keep the American people safe, secure, and free. I now recognize Ranking Member Romney for his opening remarks.

OPENING STATEMENT OF SENATOR ROMNEY[1]

Senator ROMNEY. Thank you, Madam Chair. I appreciate your willingness to hold this hearing. I particularly appreciate the chance to speak with these three individuals.

As you know, we have been receiving a lot of briefings from various luminaries in the technology community on matters relating to AI, but I am afraid they are not as closely involved to the nitty gritty of what is happening in the AI world as each of the three of you are, and therefore, I particularly look forward to hearing your testimony today and for our chance to ask you some questions.

I am in the camp of being more terrified about AI, than I am in the camp of those thinking this is going to make everything better for the world. Even though I know in the analysis that has been

[1] The prepared statement of Senator Romney appears in the Appendix on page 33.

done so far, that there are wonderful advances that would surely come as a result of AI.

I just saw a study, you may have seen it, with the Boston Consulting Group, where they put two different groups of consultants on various tasks. One had access to AI. The other did not. The one that had access to AI ended up producing a superior product in most cases. It is like, that will make us more productive in providing advice and counsel and doing all sorts of other procedures in the business world. I am sure government can be made more effective.

I am sure research in a whole host of areas, including medical, will be more effective. There are wonderful benefits, but at the same time, there are enormous risks to humanity at large, to our national security domestically, to jobs in the United States, to a whole host of things.

I must admit, the frightening side has the edge, at least in my own thinking. The discussions that I have heard so far about AI look at ways for us to potentially prevent some of the most severe downsides.

One is, individuals point out correctly, that we need to coordinate with other nations and perhaps have some kind of an international consortium or international agreement that relates to AI. I do not know how that would work, where it would be housed, how we would initiate that, and whether that is realistic.

There has also been discussion that we need to have a separate agency or department of the Federal Government with individuals who focus on AI and look at the companies developing it, developing strategies, and giving advice and counsel to people like the Chair and myself.

Frankly, a lot of, in my case, 76 year olds are not going to figure out how to regulate AI because we can barely use our smartphone. That is another area, which is should we have that kind of an agency, that kind of a department?

There has also been a discussion that before a new AI generation is released to the public or put on open source, that it ought to go through some trial period with individuals, experts testing it and seeing if it can be abused, and how it could be abused, and perhaps limiting its public launch until it has actually had those potential flaws corrected. Finally, a question of, how can we control the world's worst actors from having access to a technology that they could use to threaten us or threaten humanity, for that matter.

Some have suggested that because of the computing power necessary for AI systems to work, that we could manage the flow of and the presence of, if you will, large power semiconductor chips to see where they are, see who is making them, see where they go, restrict where they go. I do not know whether that is a realistic option for management of this or not, but I think, the question is, for someone like myself who is more concerned about the downside than the upside, my question is, and recognizing that this is going to be all over the world, what can we do to try and prevent as much of the downside as possible?

With that, Madam Chair, I look forward to your questions and I may have one or two myself.

Senator HASSAN. Excellent. I too am more focused on the potential downsides here, understanding that there are, of course, upsides to this emerging technology as well, including in the health care arena. But I do not think supporting the emerging positive sides of this means we should not worry about or focus on the real risks that we face, too.

Before we proceed to testimony, it is the practice of the Homeland Security and Governmental Affairs Committee (HSGAC) to swear in witnesses. If you will all please stand and raise your right hand.

Do you swear that the testimony you give before the Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. ALLEN. I do.

Dr. ALSTOTT. I do.

Dr. MURDICK. I do.

Senator HASSAN. Thank you very much. Please be seated. Our first witness today is Gregory Allen. Mr. Allen is the Director of the Wadhwani Center for AI and Advanced Technologies at the Center for Strategic and International Studies (CSIS).

Before leading the Wadhwani Center, Mr. Allen was the Director of Strategy and Policy at the Department of Defense's (DOD) Joint Artificial Intelligence Center (JAIC). In this role, he helped develop the Defense Department's AI implementation policy, as well as its standards for AI governance and ethics.

Welcome, Mr. Allen. You were recognized for your opening statement.

TESTIMONY OF GREGORY C. ALLEN,[1] DIRECTOR, WADHWANI CENTER FOR AI AND ADVANCED TECHNOLOGIES

Mr. ALLEN. Chair Hassan, Ranking Member Romney, and distinguished Members of the Subcommittee, thank you for the opportunity to testify today.

The Center for Strategic and International Studies does not take policy positions, so the views represented in my testimony are my own and should not be taken as those representing that of CSIS or the Department of Defense, where I used to work.

For my testimony today, I hope to offer a perspective regarding the national security threats of artificial intelligence and other emerging technologies, as informed by my experience serving in government, as well as my research work.

To begin, let me say that there is a broad technological trend across many fields where the cost and complexity of many technological capabilities and activities have come down significantly. In many cases, it takes less money and fewer highly trained experts staff to perform the same activity.

As a result, certain types of activities that used to be only within the reach of large government or military organizations can now be performed by individual corporations or even individual people. In general, the falling cost and complexity of technologies and the activities that they enable is good news for the global economy and society.

[1] The prepared statement of Mr. Allen appears in the Appendix on page 34.

This trend should be celebrated. However, it also poses genuine challenges for U.S. national security in areas where high cost and complexity have historically presented a barrier to malicious and dangerous activities. It is good that, for example, developing nuclear weapons is expensive and complicated.

The United States would be significantly less safe if building a functional nuclear weapon was cheap and simple. While nuclear weapons remain expensive and complicated, there are a number of areas where the cost and complexity of developing, acquiring, and employing national security relevant technologies is declining.

In some important areas, this includes placing dangerous capabilities within the reach of non-state actors that will seek to use those capabilities to threaten the United States, as well as state actors who seek to do the same. I will focus on three of these capabilities today.

The first is the reduced cost and complexity of weaponizing autonomous drones. The vast majority of non-state actors and terrorist groups throughout history have not had access to military air power for either airborne reconnaissance or for long range precision strikes.

These historically have been too expensive and complicated for insurgent groups to maintain. The rise of commercial drone aircraft has changed the story significantly. During the Battle of Mosul in 2016, the Islamic State flew more than 300 drone missions in a single month, with roughly 100 of those used to deliver explosives.

The U.S. Air Force (USAF) described this as the first time that U.S. ground forces have come under attack from enemy aircraft since the Korean War. The typical cost of these drones was $650. By comparison, the United States develops military missiles for millions of dollars per shot in some cases. While our missiles are superior to these drones, the drones are vastly more easily accessible and also much cheaper.

The second area I want to discuss is the reduced cost and complexity of developing biological pathogens. Biotechnology and bioweapons development historically was expensive.

The American bioweapons program during World War II employed roughly 4,000 people, of whom more than 500 were highly trained scientific experts. The multi-year budget was $40 million, which was about 1/20th the size of the Manhattan Project. This was a very big effort, and this was assessed at the time to be the minimum viable program size for a bioweapons program.

Decades later, in the 1990s, the Aum Shinrikyo terrorist organization in Japan attempted multiple times to develop and deploy biological weapons using anthrax and other pathogens. Thankfully, they failed.

However, the group successfully executed many steps of developing and delivering bioweapons, despite having only a handful of scientifically trained expert staff and a much smaller research and development (R&D) budget than any nation-state.

Of special note, these were folks with formal scientific training and formal affiliations with prestigious scientific research institutions who were engaged in terrorist activities. Today, the development of advanced genetic engineering technologies such as clustered regularly interspaced short palindromic repeats (CRISPR) has radically reduced the cost and complexity of gene editing to the point where even amateurs can modify the genes of viruses.

Some research organizations have previously published genetic information related to highly lethal but not highly contagious pathogens such as bird flu, and terrorist organizations following in the footsteps of Aum Shinrikyo may be able to create genetically modified pathogens that are both highly contagious and highly lethal.

The final area I want to talk about is the reduced cost and complexity of creating high quality, forged media. One of the most remarkable capabilities of AI technology is its ability to create compelling synthetic digital media.

The sort of text, photos, videos, and audio files that would have in decades past cost Hollywood hundreds of millions of dollars to develop can today be developed by amateurs working with a single smartphone or a single laptop computer.

During my time at the Department of Defense, my organization collaborated with Defense Advanced Research Projects Agency (DARPA) on technical means to detect these deepfakes or other AI enabled forgeries, but the quality and cost of producing these is radically exceeding our ability to detect them and our ability to intervene.

This is a legitimate threat to the U.S. information ecosystem and U.S. national security, and I look forward to discussing these issues with you today. Thank you.

Senator HASSAN. Thank you very much, Mr. Allen. Our next witness is Dr. Jeff Alstott. Dr. Alstott is a Senior Information Scientist at the RAND Corporation, as well as an expert for the National Science Foundation (NSF).

He has previously served in multiple national security roles in the Federal Government, including as Assistant Director for Technology Competition and Risks at the Office of Science and Technology Policy.

He also served as the Director for Technology and National Security at the National Security Council. Welcome, Dr. Alstott. You are recognized for your opening Statement.

TESTIMONY OF JEFF ALSTOTT, PH.D.,[1] SENIOR INFORMATION SCIENTIST, RAND CORPORATION

Dr. ALSTOTT. Chair Hassan, Ranking Member Romney, and Members of the Subcommittee, good afternoon and thank you for the opportunity to testify. Progress in AI has advanced rapidly in recent years, leading to expanded debate among experts about its potential risks.

Although AI has the potential to transform entire industries, it could also pose novel threats to national defense and homeland security. AI developers are racing to build increasingly advanced systems, and the drivers of AI progress, including algorithms, hardware, workforce, and investment, continue to advance.

Despite this rapid progress, the sciences of interpreting and explaining AI behavior, assessing powerful AI for dangerous capabilities, and designing appropriate guardrails to mitigate harms are all

[1] The prepared statement of Dr. Alstott appears in the Appendix on page 44.

efforts that are still in their infancy. Existing safeguards are still imperfect, and AI released by leading U.S. companies today can and do still exhibit unsafe and unanticipated behaviors long after they are trained and released. Unless society puts in effective guardrails, broadly capable AI systems could hasten the design and proliferation of bioweapons, cyber weapons, nuclear weapons, progressively more general intelligence, and other threats not yet conceived.

If such systems proliferate, it will be very difficult to put the genie back in the bottle, potentially causing irreversible damage. One particular area of concern is the relationship of advanced AI development with biosecurity.

Existing AI is already capable of assisting non-state actors with biological attacks that would cause pandemics, including the conception, design, and implementation of such attacks. Without safeguards, the development of ever more advanced AI systems will bring ever greater reductions to the barriers to launch such attacks, until we are at the point in which a lone actor can cause a pandemic killing millions.

This change is occurring at the same time as gene synthesis machines are decreasing in cost and proliferating more widely, increasing the number of actors who have the necessary access and ability to create and release new diseases. Effective oversight of increasingly powerful AI and its potential threats will require visibility into the full AI development lifecycle.

This lifecycle begins with large concentrations of AI hardware, with thousands of advanced chips performing a training run costing millions or soon billions of dollars. Once the AI is fully trained, it is made available to the public through a controlled Internet interface or by being published online in its entirety, at which point proliferation essentially cannot be stopped.

Oversight of each of these stages, AI hardware, training, and release will be necessary to ensure our national security. These efforts will not come at the cost of U.S. innovation but will bolster U.S. competitiveness by ensuring the reliability of leading U.S. products and establishing the United States as the responsible market leader. In addition, domestic oversight, although essential, will not be sufficient alone.

We must cooperate with our allies and partners, and communicate responsibly with our competitors and adversaries, to ensure the safe development of these technologies at the global level. I will highlight six actions that the Federal Government could take to mitigate these threats.

First, require that large computing clusters that could be used to train powerful AIs, for example, high performance computers with over 10,000 advanced AI chips, be reported to the government, have adequate cybersecurity, and have know-your-customer processes for anyone doing a very large computation on them.

Two, require those making powerful AIs to maintain responsible security procedures during and after the training process to prevent U.S. made models from being stolen or leaked. The threshold for this requirement could be frontier models trained to be several times larger than any AI system made today and should cover both those handling the code and those handling the hardware.

Three, ensure that these frontier AI development efforts also undergo an independent assessment to determine whether the AI or its proliferation would be a threat to national security, similar to how rocket launches are reviewed by the Federal Aviation Administration (FAA). This should include risk assessments prior to model training, at regular intervals throughout the training run, and just prior to model deployment.

AI that is determined to be insufficiently safe could be held from further development and release until safety and security issues are adequately resolved. Conducting evaluations in each major stage of the AI development process would help companies detect safety problems early on, when issues are less costly to fix, reducing security risks, while saving companies time and money.

Four, create a safe harbor information sharing environment for the private and public sectors to share safety and security problems from their AIs as they identify them and then create solutions together.

Five, establish know your customer requirements for the providers of gene synthesis services and gene synthesis devices.

Six, require that genetic material synthesized over at threshold length be screened for pathogenic potential. This should include supporting the development and adoption of a universal gene synthesis screening mechanism, which would decrease costs for U.S. companies and maintain U.S. competitiveness in the global bioeconomy. I thank the Subcommittee for the opportunity to testify. I look forward to answering your questions.

Senator HASSAN. Thank you very much, doctor. Our third witness is Dr. Dewey Murdick. Dr. Murdick is the Executive Director at Georgetown's Center for Security and Emerging Technology.

Before moving to the Georgetown Center, Dr. Murdick served in both the public and private sector, including the Chief Analytics Officer and Deputy Chief Scientist of the Department of Homeland Security (DHS). He also stood up in office at the Intelligence Advanced Research Projects Activity focused on anticipatory intelligence.

Welcome, Dr. Murdick. You are recognized for your opening statement.

TESTIMONY OF DEWEY MURDICK, PH.D.[1] EXECUTIVE DIRECTOR, CENTER FOR SECURITY AND EMERGING TECHNOLOGY

Dr. MURDICK. Chair Hassan, Ranking Member Romney, and honorable Senators, thank you so much for the opportunity to chat. As you are keenly aware, the attention of elected officials and public servants is a precious commodity, and advanced technology threats are calling now.

As such, I would like to make three suggestions. First, prioritize your attention and consider key criteria when evaluating threats. Focus on actionable steps that lay foundations for the most pressing concerns. Three, enable an adaptive approach to policymaking so we can simultaneously act and learn.

Expanding on point one, prioritizing your attention requires knowledge of potential threat actors, a clear way to estimate threat

[1] The prepared statement of Dr. Murdick appears in the Appendix on page 49.

severity, and an ability to estimate how much time we have to plan.

For many Homeland Security missions, AI is changing the threat landscape now because it could lower the barriers of entry for novice criminals to do harm, like set fires, or steal cars, or whatever.

It can magnify the effectiveness of disinformation and targeted phishing attacks by nation-states, or human traffickers who can use new tactics to exploit victims and their families. It can also help advanced criminals evade law enforcement alerts, such as with sophisticated methods to avoid detection in meth making ingredients' acquisition at scale.

Other technologies are harder to plan for because we are still trying to figure them out. Consider the prospect of super intelligent AI systems that theoretically operate across both digital and physical worlds with some kind of agency.

They do not currently exist, and we do not really know how to build them. However, we still need rigorous research and monitoring systems to flag when the critical developments might change our threat mitigation planning.

Likewise, we anticipate quantum computers may someday break advanced encryption algorithms. Despite uncertainties about when and if this will all play out, we need to prepare for this threat and update how we protect our nation's secrets today.

Some advancements may not be as transformative as we thought. For example, some have expressed concerns, and we just heard a very well laid out concern about the chat bots and other kinds of tools lowering the information hurdles for creating dangerous biological agents and pathogens. However, the information barrier is already extremely low and other interventions are probably actually, of higher relative priority.

For example, you heard the screening of Deoxyribonucleic acid (DNA) sequences and improving our country's management of large amounts of genomic data. Furthermore, in this prioritization thinking, if an advanced technology threat is not prioritized today, we need to be systematically monitored so we do not forget about it, and we can track it.

Point two, a strong foundation for addressing the most pressing threats requires all our talent, every types of it, no matter their backgrounds, no matter in technical, non-technical, and we need to adapt to changes in the domestic and international workforce landscape.

We need to assess existing tech relevant authorities that we have within the government and adapt them to leverage our national strengths. There are advocates who speak of today's threats, observed threats, and then there are those who are concerned about anticipated existential risks. I think we need to find a common ground between these two communities.

How we address immediate threats shapes how we respond to long term concerns. We are still learning and need to adapt our plans as new information arrives. Gathering new information from—and potentially creating new bodies is something that we need to think about, specifically for specific gaps.

For AI, we need to actively gather information on AI harms through voluntary and mandatory incident reporting. We need to also enhance the quality and security of our resources. We also need potentially new oversight organizations which can oversee where gaps are in existing sector specific agencies, see where they are being applied, and be the first to deal with problems.

In conclusion, my last point, our approach must be agile, adaptive, and ever vigilant to global shifts. Our policies and our organizations need flexibility to gain these new insights. It is not just about immediate action, but a continuous cycle of small, informed steps backed by robust analytics that help us learn from new advancements and respond to what is working best. This is more than just tactical advice.

It is a call to significantly bolster analytic capabilities in the United States with better data and more effective monitoring system, we can make timely and informed decisions. This is not just policy. It is a playbook for navigating the current and future tech age. Thank you.

Senator HASSAN. Thank you very much, all three, for such thoughtful testimony. I am going to start with a round of questions and then go to Senator Romney. We may have other Members in and out. There is a lot of activity in the Senate this afternoon, so we will see if others join us for questioning.

I am going to start with a question to you, Dr. Alstott. At last week's AI forum here in the Senate, an AI researcher told Senators that his team was able to get Meta's AI system to provide instructions for how to develop a biological weapon. According to the researcher, all it took was $800 and a few hours of work.

This is an example of a jailbreak which bad actors such as terrorists can use to evade the safeguards in AI systems. Is there risk of bad actors using AI to develop modified biological or chemical weapons? How can we mitigate any public safety risks from these kinds of jailbreaks?

Dr. ALSTOTT. Yes, there is a risk. We are in the process of identifying what the size of that risk is today. We know that the risk will increase over time. At RAND, we are running an experiment, along with colleagues, of really doing the bake off between teams that do and do not have today's AIs to see how quickly they can design a biological weapon. That experiment is not done. Can't comment on the intermediate results.

However, we know that as the technology continues to change, that the information barriers will continue to come down. Those have been the last barriers when it comes to biological weapons. Unlike, say, nuclear weapons, where once you know how to make a bomb, you still have to go get the fissile material, all of our cells are the factories for a pandemic.

The fundamental physics of making an attack for a pandemic, as opposed to, say, anthrax or another form of bioweapon, is really not in our favor. Protecting that sort of exquisite technical information that would enable a non-state actor to make such attacks is really critical for national security.

Senator HASSAN. Are there steps we can take to mitigate?

Dr. ALSTOTT. The first step, as Dr. Murdick described, is to have vigilance of what exactly are the threats that are coming in and characterize them at a technical level to be able to identify if a certain model, certain AI really would accelerate people. Then there would be the sort of all of society saying, that is not a tool that we want to have in our society's toolkit.

I spoke during my testimony about different mechanisms that government could employ to say, all right, these are the models that we are going to check to see whether or not there is a problem, and then if there is a problem, we can give a green light or a red light to saying whether or not that should go out.

Senator HASSAN. Thank you. Another question for you, Dr. Alstott. The public safety risk from these so-called jailbreaks also extends to the fentanyl crisis. This Committee has worked on ways to combat the opioid epidemic and stay in front of the changing tactics of transnational criminal organizations (TCOs) who fuel the crisis.

As illegal fentanyl creation and distribution has soared, the development of new fentanyl analogs has posed unique challenges for law enforcement, not only in the testing for fentanyl, but also in enforcing existing laws that have struggled to keep up with the rapid creation and evolution of fentanyl analogs.

Can you comment on the risk posed by bad actors who could use AI to develop drug analogs that could potentially skirt existing laws and interdiction efforts?

Dr. ALSTOTT. That is an area where I myself only have adjacent knowledge. I can tell you that the overall notion of using machine learning models, be that today's large language models or other things that are more specialized for chemistry, would indeed be tools that anyone would want to have in their pocket for developing those analogs.

Senator HASSAN. OK. Something we will have to figure out how to develop a response to. Dr. Murdick, I want to take a moment to consider some of the very serious risks posed by artificial intelligence. As we heard earlier, AI can be susceptible to jailbreaks that disable guardrails and create enormous potential for dangerous outcomes.

Similar catastrophic risks could come from powerful AI systems that might behave in unintended ways, such as future AI systems that manage critical infrastructure. To comprehensively address these kinds of risks in the long run, we have to strive to make AI fundamentally safe, meaning it cannot easily be abused by criminals and cannot easily behave in unexpected ways that harm the public.

Instead of relying on AI systems to make values based decisions from training models or data sets, we need to ensure that AI systems can only be run on hardware that has intrinsic protections to prevent AI from acting in a harmful or malicious manner.

This requires significant research and developing safeguards for systems that can ensure that AI will not be used to harm individuals or communities. Dr. Murdick, is research and development into technology that makes AI fundamentally safe an area that would benefit from sustained and focused Federal investment?

Dr. MURDICK. Yes. All the components that are part of safe AI, everything from responsible or traceable systems, robust systems, there is a lot of wonderful, very meaningful words that are associated with this whole community. It is a fairly new community.

There is not a lot of cohesion yet, and the terminology is still in flux in some ways. Now, I am less concerned about that terminology than the actual impact that you are trying to lay out. But it is a sign that it is still a fairly new community that needs a lot of attention to figure out how to buildup these capabilities.

Some of the specifics that you mentioned about being able to put controls in hardware to be able to stop it from running if it is running something troublesome, to my knowledge, today there is no clear direction of how that could even be implemented.

That is not to say it is impossible, but a lot of the questions need some pretty fundamental research to open that up, and they are basic research questions that need to be explored. I think the point about baking in our values AI systems, most of the AI systems that I foresee coming in the next period of time—it is really hard to forecast the future, so just take that with a grain of salt—are ones that are human, machine teaming based.

The AI system should not have agency at a level that we see in movies, right. It is going to have the capability to respond very helpfully and very usefully to human prompts.

I think at this next phase, there is a lot of AI safety work that is baked into that human-machine teaming process, and there are a lot of opportunities to explore and implement licensing. For example, I drive a car. I am licensed to drive a car, and I know, I have general qualifications.

You could imagine for someone having access to a certain type of model, then likewise having a license of some form where they have learned how to work with that system. They know when to believe it, when not to believe it, and how to work it effectively.

That kind of human-machine team, that is within present day regulatory capabilities. We know how to do those kind of things. Those are examples of things that could happen now. Then there is long term research.

Senator HASSAN. Thank you very much. I am going to turn now to Senator Romney for his questions.

Senator ROMNEY. If the objective of this hearing was to calm our nerves and give us more confidence that everything is fine, it has not done that. It has underscored the fright that exists in my soul that this is a very dangerous development.

I realize, it is not like overnight we clicked on a switch and now we have AI, and we have machine learning, and before we did not. We have been having machine learning, but it has now reached a level with generative AI that is in many respects quite different than what we have known in the past.

Each of you have suggested some of the ways we might be able to safeguard against the worst kind of outcomes in the respective areas that have been described. The challenge that comes to mind is, one, as I listen to your recommendations, I understand about half. Maybe that is an overstatement.

But in terms of, you describe the various stages, we need to put safeguards here, safeguards there. I am not sure I understand what the stages are. I do not know what is involved in them. The likelihood that Senators are going to be able to figure that out and draft a bill that focuses on this area, it just strikes me as being not reasonable. It is just not going to happen.

Not in the House, not in the Senate. I look for your counsel or your thinking on how do we get from where we are, which is no safeguards at all, to the safeguards you would recommend, or others.

I can tell you that were I the Chief Executive Officer (CEO) of the country or the Chief Executive Officer of a corporation, let us say I was a CEO of a major corporation, and I had two or three areas, let us say the head of a bank, two or three areas I am really concerned about, quantum computing being able to break into our systems to move money around and so forth. What I would do is I would first decide who I want to put in charge.

There is going to be someone in charge of our effort to combat these threats, all of the threats. It might be an agency. It might be a department. But I am going to put someone in charge.

Then, I am going to say to them, you are going to need to hire the expertise in each one of those threats or opportunities, and either hire someone to oversee each of those—and then, they may need to hire outside people who have expertise there or multiple outside people, or perhaps hire their own staff, but we are going to have to take this apart piece by piece and solve it piece by piece.

Am I wrong in that assessment? If I am right, where should this be—who should be responsible? Dr. Murdick, was in Homeland Security. Should we task this with Homeland Security. They have so much on their plate right now. It is like, oh, gosh, here is one more thing, Secretary Mayorkas, that we can criticize you for.

Do we set up a new agency, a new department? I do not know if you know where this all resides right now, but what is the process? How do we get from where we are, to actually putting in place these safeguards? That is the question.

How much time do we have to do it? With that, maybe in the order of those who offered testimony, you might just go down the row and give any thoughts you have about how we do what you recommended.

Mr. ALLEN. Senator, thank you for expressing your concerns. I am sorry that our solutions were not adequately—— [Laughter.]

Senator ROMNEY. It was not your job, that is all right.

Mr. ALLEN. But if I could offer one potential source of optimism, think about the difference in safety from a fire safety perspective of a candle and an electric light bulb. I think everyone in this room would say if this place burned down, it would be much more likely to have happened from a candle than from an electric light bulb.

But that was not such an obvious distinction when electricity was first invented. When electricity was first invented, it was a safety disaster. It was the constant source of fires. It was the constant source of the electrocution deaths of electrical workers.

Electricity is not inherently safe. The companies and the government agencies of this country made it safe through deliberate effort over time. AI right now is not inherently safe, but it is also not inherently dangerous. It will depend upon the work that we do in the coming years. There is a lot of incredibly important work to be done.

Now, one problem that you identified, which is the capacity of the government, you pointed out the capacity in the Senate to understand these issues. Jeff and I just got out of government not that long ago, and there was a dramatic shortage of AI talent on these issues. There is a significant shortage of biosecurity talent.

That is not to mean that there are not smart, hardworking people on these issues. But if you were asking me to design the program to address these problems and compare it against the current skill sets and numbers of individuals serving in government, we just do not have enough.

We must think of a program that would actually result in the outcomes that we want. For example, my own prior organization, the Joint Artificial Intelligence Center, was given the authority to have 100 civil servant or military personnel staff. But the result there was that military personnel were assigned to our organization.

They may or may not have had prior understanding or expertise in AI, and there was not an existing program that they could be sent to, to sort of give them a crash course on AI. These are all structures that are going to have to be created to increase the bureaucratic capacity of the U.S. Government, and that is some of the most important work that can be done.

In terms of what can be done from a regulatory perspective, I would argue that we should think about the levers in the system where there might be a high return on investment. We want to make it hard for accidents to happen if they are catastrophic. We want to make it hard for malicious activity to happen.

But we do not want to ban all of these good activities as well. For example, biosecurity as an example, the mechanism of the problem that your question was about, Senator Hassan, was, why is it a challenge? Why does AI make it easier to make bioweapons?

Part of it is the nature of existing regulations. The current biosecurity system is primarily a list based system. If you want to get access to anthrax pathogen, that is on a list. It is regulated because it is on a list. The challenge with AI systems is that they could assist in the development of novel pathogens that are not on a list anywhere.

We must think OK, if DNA synthesis companies are going to need the ability to detect that something is a pathogen, even if it has never been created anywhere before and never been tested for pathogenic properties, how are we going to ensure that those companies have that capability?

That is some of the most promising research that the government could invest in. How do we identify the risk of malicious use for things that are not currently on a list somewhere?

Dr. ALSTOTT. Senator Young, my fellow Hoosier, said recently that his analysis was that for the vast majority of issues that AI touches, there is already some part of government that has authority and responsibility to deal with it, and I agree with this. Self-driving cars, Department of Transportation (DOT). AI in medical context, Department of Health and Human Services (HHS).

Most of AI can in principle be handled by the current setup of government, with a few exceptions. One is that if someone is making or deploying an AI that is predictably going to get millions of people killed, there is no part of government that has clear authorities and responsibility for addressing that, and so that needs to be created.

There are several places that it would be logical to create it. An independent agency is one. DHS, which this Committee works with, is another. There is also the Department of Commerce, particularly the Bureau of Industry and Security (BIS). There is also Department of Energy (DOE), which has a lot of existing relevant authorities that could synergize there.

Wherever it is that the Congress chooses to put it, it needs to have the authorities to be able to say, this is a problem, and we are not going to let that AI go out and needs to have the responsibility to understand this at a technical level.

Thankfully, no part of government has to work alone. First, they have all the rest of government to work with, but also all of American society. Any part of government that has this responsibility should be trying to solve the talent problem by making friends.

Whether they are working in government or working in industry, there are multiple mechanisms to reach technical experts.

Senator ROMNEY. Thank you.

Dr. MURDICK. Great. I think there is a few things. The threats are overwhelming. If you focus on what could kill you, I do think it is a little paralyzing, but I do think there is a very clear set of actions that are necessary, that have been used before, and the first up is information gathering.

Mandatory and voluntary incident reporting is an incredibly useful way, both within specific sectors and across, to be able to get evidence of what is breaking. It is unfortunate, but sometimes you need a little bit more oomph to actually get action and having evidence of harm is really helpful in being able to do that.

I think information gathering is extremely important. Two, to strengthen that information gathering, we need to strengthen our auditing community. That could be at the Government Accountability Office (GAO), that could be private sector, that could be any civil society organization that has a concern. But strengthening, raising the bar of that auditing community, developing those skills—there is a bit of investment that could go there.

There is a bit more standard, I know, community development. There is a lot of things that could go in that space. Third, as Jeff was just mentioning, and we heard other times, there is a lot of agencies that have authorities that are very germane to the question at hand, the Federal Trade Commission (FTC), FAA, and the alphabet soup that I will not repeat, but these are really important roles.

I think there is some tweaking. I think we first need to do a catalog of what authorities they have that are relevant to AI and figure out if they are adequate. Do they need small adjustments? If so, let us figure out how to do that to empower them.

We have biological conventions and other things, if there is actually a harm that is being engineered, we have agreements across nations to be able to track some of these things. I am not saying they are perfect, but we have those. We might want to look at them and see if there is some updates.

I think there will be across nations to strengthen some of those ideas. I have talked about info gathering, auditing, and some who of existing agencies. I do think if you start considering future organizations, my thing has been new organizations.

Starting up at Intelligence Advanced Research Projects Activity (IARPA) and in the private sector, and watching DHS startup, there is lessons learned there. If you drop a ton of cash on a new organization, it is really easy to make mistakes. But just giving them a little bit, and then forgetting about them, and never increasing their budget is another problem.

I do not actually know how to do that, but I think it has to be some kind of mechanism where you stage funding and you expand it with some kind of very clear waypoints and you do not just dump in because it stresses out government officials to execute that money and do it all right, and their oversight is super high when you have $1 billion in your pocket as opposed to a smaller amount.

Anyway, this is not my expertise. I think you need a very carefully stage that growth because as we learned—lastly, and I mentioned this over and over in my opening comments, I will not belabor it now, but we do learn. We need a set of agile systems to be able to pick up information and learn how to address and how to collect information from industry.

We do not know really how to do that. What questions should we ask to understand the level of threat? How do we update that thinking? How do we continue that integration? How do we avoid regulatory capture by that process of becoming too close to industry? These are things we do not know, but if we set it up to pick that up and gradually grow and learn, I think it is really important.

The last thing, you asked about how much time do we have? I think in some cases we have no time. Information gathering on harms that are happening—every day we delay is less information we have. There is things like Skynet in its super empowered system of working across physical and digital worlds, I think we got some time there.

But, I am not trying to minimize that threat, but we need to start taking these very clear steps long before that. To avoid getting overwhelmed, I think we need to think of it as a very staged process. Hopefully that is helpful.

Senator HASSAN. Thank you. That is a great overview, I think. What I think I will do now, I want to follow up with one or two questions and then turn to Senator Lankford, and we will again go back and forth.

As Senator Romney was asking kind of this overall, how do we begin to think about this from our perspective, which is how do we establish the capacity, and then what kind of authorities do we need, I want to try to focus in some of my questions on particular risks, because I think one of the jobs of all of us moving forward is going to be to figure out how to prioritize what we work on first.

Let me start, Mr. Allen, another question to you. In Russia's war on Ukraine, we have seen unmanned aerial systems (UAS) shape the battlefield and allow small military units or even individual soldiers to conduct aerial warfare.

As the war has progressed, tutorials for utilizing civilian drones for military purposes have spread widely, and nearly anyone can now find directions for dropping explosives from a drone with just a quick online search.

Additionally, more advanced drones have clear potential for dangerous use, such as an agricultural sprayer drone that could deliver a biochemical agent with virtually no additional modifications.

Unmanned aerial systems are widely available in the United States and available to purchase at a relatively low price point. Mr. Allen, do you think that the Federal Government is investing enough in the technology needed to prepare for drone based threats to the United States?

Mr. ALLEN. Thank you for raising this question. It is an area that I spent a lot of time thinking about when I was in the Department of Defense. I will say that good work on this issue is being done in both the Department of Defense and the Department of Homeland Security.

But I would say the war in Ukraine sort of raises a new risk factor in this story. Namely that countermeasures for drone based warfare and especially cheap commercial based drones is in the stocks of the U.S. Army. It is in the stocks of the Department of Homeland Security.

But many of these countermeasures specifically target the communications link between the remote operator and the drone itself. As this has become widespread practice in the war in Ukraine, both sides in that conflict are increasingly resorting to more autonomous systems that do not have a communications link between the operator and the aircraft itself.

What this means is that many of the defenses that the United States and DHS in particular have been amassing will not work in specifically interrupting these types of threats.

This is sort of a gap in our defensive capabilities, specifically within DHS. While we have good measures in place for the remotely operated aircraft, I would say we need to do significantly more with related to autonomous systems.

Senator HASSAN. Thank you. I am going to ask one more question, this one to Dr. Murdick, because I would like to turn now to a discussion of threats that may be posed by a different technology, which is quantum technology.

Quantum and its impacts are further down the road than some of the other technologies we have discussed today. However, the applications of quantum technology in the hands of our adversaries could pose a significant threat to national and homeland security.

Much of the public discussion around quantum technology is centered on the need to protect sensitive and private information from quantum computers capable of breaking our current encryption standards.

While Congress has begun to address this issue, there are still other threats from quantum technology that have received less public attention. For example, quantum sensors could be extremely effective at detecting even the smallest changes in the environment, rendering some stealth aircraft obsolete.

Dr. Murdick, what can Congress do now to ensure that the Federal Government is planning for the risks posed by developments in quantum technology, especially quantum technologies that have gotten less attention, such as quantum sensors?

Dr. MURDICK. Great. To first talk about quantum computing, I know that is kind of—but I do think that there is a very clear path.

We do not know exactly when quantum computers will become a reality, but there is a very clear path for the post quantum cryptography approach.

I think this is extremely high priority. Yes, it might be 20 years before it is all in place, but it is going to take us a number of years to get these kind of quantum resistant algorithms in place.

I wanted to say that because it is really important. Quantum sensors that detect gravitational field variance and other kinds of things are super interesting research. Even in quantum computing, there are some really near term capabilities that are hybrids between quantum and classical computers that are super interesting.

Now, they are mostly research toys right now, and I think even some of the quantum sensors, the noise that is part of our life overwhelms most quantum things. A lot of research.

I still am in the camp that there is a lot of research to be done here. The thing that is helpful, though, is looking at that research from a threat perspective. Researchers typically do not do that. They are trying, it depends on the grant language. Usually it is opportunity based.

I think employing the type of individuals who are actually tearing apart the technology, maybe not as the primary researcher but analytically, and developing the way points of like this stage of development would mean that this capability is now possible, by establishing those maps and those roadmaps, you get a lot of insights.

Some of them, if possible, making them open is really helpful because it provides for a much more collective hive mind kind of criticism and optimism thinking. Sometimes people get really obsessed with threats and that is all they can see. They do not actually see some of the other benefits.

I would suggest if there is opportunities to do more analysis and developing monitoring systems for watching these types of technologies, I think that is where we are at right now due to some of the fundamental technical challenges.

Senator HASSAN. Thank you very much. Senator Lankford, if you are ready with questions, I will turn it over to you.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. I am. Thank you. Thanks for holding the hearing. Obviously, we have a lot we have to learn because we have to figure out how to not limit this technology but to manage its use. My question, I have asked just about everybody, I want to start with you all.

Define the phrase responsible AI for me, because everyone seems to throw around, we want to make sure we have a responsible AI. But this is not a trick question. I am really trying to figure out how is that defined—what does that mean, responsible AI? How do we start to define that?

Because we cannot just throw that around. We have to actually get a definition for what that means. If anybody wants to jump in. Again, not trying to have a trick question. We just have to be able to narrow that list. Ready, set, go.

Dr. ALSTOTT. All right, I will take the bait. The issue with the phrase responsible AI, trustworthy AI, etcetera, is that it is like saying responsible cars, or responsible rocket ships, or so on. You have to get more technically precise about what are the harms or benefits that you care about and how do you tradeoff between them.

In our testimonies today, we talked about various fairly specific threats that can come from AI in particular. I use the analogy of the FAA approving rocket launches and I think that this is particularly relevant. We do not have responsible rocket launches as a thing within physics.

We have the idea that we do not want the rocket to fall on people's houses, so we will only approve launches that point away from people's houses.

Senator LANKFORD. Right.

We do not want F–35s landing on their house either, but that is a whole different issue for the day.

Dr. ALSTOTT. Exactly. Similarly, you can have these principles for AI. You can say that we are going to prioritize the largest national security and public safety threats, and that these are the sort of logical equivalents of point the AI away from people's houses before you launch it, please. This is an example of the kind of technical detail that you——

Senator LANKFORD. I get it. But we have to put something in statutory language at some point to be able to say this is off limits, this is limits. Then to also say there is much of AI that we do not know what that is.

Quite frankly, for me, it is setting the value set to say yes, no, this is a value set, and then go build on it rather than putting a fence around it to say you cannot go beyond here, if that makes sense.

Dr. ALSTOTT. Absolutely.

Senator LANKFORD. Any ideas, thoughts that you have as you gather with other folks to talk about this, we have to be able to build on a value set of what is responsible AI, and then work from there.

I am not looking for a final answer today, but I am looking to spark a conversation that we have got to have in a larger community because that value piece is still not established for us. Does that make sense? But I am glad to engage. Let me throw a dozen other things at you real quick.

This whole concept of machine learning, obviously, we have had a lot of questions that come out because the government is the largest holder of data in many areas. Everyone that is involved in AI right now is coming to the government and saying, hey, would you give us this section of data?

We will protect private information, but we need your data, otherwise we are harvesting this off the Internet and we want to be able to get your data for x. There are lots of issues that are unresolved, so, for the Federal Government and for national security. Let me give you one of them.

If we are dealing with, let us say, port security. We obviously have done a lot of screening at Transportation Security Administration (TSA), a lot of port security. We have a lot of vehicles that we have scanned. All those different technologies are out there to actually scan vehicles, scan people, scan for fentanyl, whatever it may be.

If we are going to upload that data to any one of these private entities, the question then becomes, once we hand data over for machine learning—we have handed a lot of data over. Who owns that data? Where does that data go?

How could that data actually be used? Could that then be resold for all that data to go somewhere else? If there is a problem with it, at the end, that ends up being a national security issue.

Liability issues then start to be able to fall into—you see what I am talking about? This gets into the weeds of actual practical applications of how AI is used and how the interchange is happening right now on national security.

Thoughts and ideas on that, on that data? When they actually come to the Federal Government, we are going to protect privacy as well. We constitutionally must and should, but how do you manage ownership of privacy, ownership of data, and private entities trying to build some of this for national security?

Dr. MURDICK. Since Jeff took the last one out, I will start here. Greg, feel free to jump in if you want otherwise. A connection between those two last questions I think is really interesting.

Responsible AI, one of the most potent counter questions or companion questions that goes with is, what are you trying to accomplish? That totally changes and clarifies a very nebulous question to something very specific, because policy implementation actually is what matters.

This concept of data governance, I think at the very high level is all about trust. We have to create structures that people trust. Trust in government is fairly low. I do not know if it is an all-time low, but it is, I do not know, somewhere around 25 percent of the population or something.

Trust in corporations goes up and down and is generally pretty low. Whatever structure we do, we have to protect this information. It has a lot of very personal information about individuals and handing it over to a corporation.

For example, there was a DHS system that I used to work with that for some reason whoever wrote the contract never bothered to include that the government had ownership of the data.

Extracting data actually cost money every time. It was a horrible contract. I think we have to write these kind of agreements that make sure that that data is the people's data. Obviously, we cannot make the people data, public data——

Senator LANKFORD. Right.

Dr. MURDICK. But it is data. I think the concept of trust, and I am going to—mash two words together.

If you design a data trust where that trust has, whoever is overseeing it has trust like responsibilities, fiduciary responsibilities to act in the interest of the people who are in that data set or in the American people, I think that kind of structure, however you do it, whether it is within the government, whether it is outside the government, it needs to have that kind of trust baked into it that allows people to see, these people, their sole responsibility is to make sure that this data is being used and leveraged and stored and moved and shared with another company or not shared by the company in the interest of the people.

I think some kind of transparent mechanism, and I am sorry, I do not have more detail on that, but if it was some kind of transparent mechanism that implements that, and I borrow language from the trusts because it is a very easy connection to make in my mind, but I think it is a really useful framing.

Mr. ALLEN. Regarding your question about data, Senator, I could give you multiple examples in which it makes sense for the government to closely guard its data and share it with almost no one.

I can give you examples where it makes sense to give it away freely. I can give you examples where it makes sense to share it with a select group of folks, perhaps contractors working on a specific project.

I would say that the sort of specific advice that the government needs to follow with regards to data strategy is probably not something that would be a good target for a legislative outcome. What I would say is that government employees need to have training on sort of what data strategy really looks like for a given end use.

People who are writing acquisition contracts, for example, need to understand under what circumstances would it make sense for the government to retain the data as a proprietary asset, and under what circumstances might they want to release that under a license to a contractor, and so on.

If you go to Silicon Valley and you talk to anybody in the corporate strategy departments of these various companies and you ask them what is their data strategy, you will find many different companies pursuing many different types of data strategies, but all with very deliberate thought and reasoning for why they are sharing and when they are sharing, and how it makes sense to their corporate bottom line.

My point is that the government bureaucracies need the flexibility and the expertise to make those same kind of decisions.

Senator LANKFORD. This is a body that is not super excited about bureaucratic flexibility because that can be used in all kinds of different ways. I am going to speak for the other folks in the dais for me, but the concept of bureaucratic flexibility makes the hair on the back of my neck stand up because I can really go sideways in a hurry.

Let me just give you this thought on this, and I want to get out the way because I do not want to occupy all the time. When data is released and a corporate entity then owns that data and is using that data for whatever it may be for that software, then they continue to be able to use that data for something else, and then someone else buys into the company, or someone else also buys that resource, only they have access to that data, and all that has been gained from us, it does not take long on a national security level to be able to understand we have a risk that gets involved based on if a Chinese subsidiary ends up buying into one of these companies or getting access to data. I have a great deal of trust for picking up my cell phone and making a call.

But I am also keenly aware that my cell phone provider also provides that metadata out on the open market, and that if people can track me based on having enough data points to be able to personally identify my location. That is not my intent with it.

To go back to determining what we are going to do with data based on the intent and what it was actually designed for, Facebook was designed for college students to speak to each other. That is what it was originally designed for, and that is certainly not what its full usage is.

My concern on any of this, on how we are building systems is, how do we build a value set without restricting the technology, because the technology is the technology. But how do we build a value set? How do we engage in such a way to protect national security, national security data, and systems, not knowing how a system will eventually be used or where that data will go in the days ahead?

I want our screening to be better at the border. We have a lot of data on a lot of vehicles. We can make our screening better. But where else does that data go, how does that go, and what is the risk that we have to take with that? I appreciate your mercy here. Letting me go a couple of minutes over on that. I appreciate that very much. Thank you.

Senator HASSAN. Senator Romney, do you have other questions?

Senator ROMNEY. I took up more than my fair share already.

Senator HASSAN. Then I have about three or four more. The last one, to give you all a heads up, is really kind of a wrap up. What didn't you get to talk about today? Or are there things that one of you said or one of us said that you want to comment on?

But let me start with a question about the use of advanced technologies by non-state actors. This goes to all three of you. Here is a two part question about potential risks posed by the proliferation of advanced technologies.

Because the first computers were complicated and expensive, only governments and large companies could use them, and we have already talked about that. However, today, hundreds of millions of people use their smartphones, tiny, powerful computers all across the world, and previously inaccessible technologies are becoming available to more and more people.

This proliferation of technology has empowered terrorists and dangerous non-state actors, allowing them to create, for instance, cell phone triggers for roadside bombs or use the Internet to radicalize lone wolf attackers in faraway places.

In short, dangerous groups have proved adept at adopting new technologies. We have been discussing risks from developing and existing advanced technologies, so I would like to start by asking, are there technologies that you believe are particularly prone to use by dangerous non-state actors that we have not discussed yet or we should discuss further?

Second, does the Federal Government have the resources and necessary expertise to successfully counter these threats? I will start with you, Mr. Allen.

Mr. ALLEN. Thank you. The technology capability that I like to dwell upon that we did not spend a great deal of time on in today's session relates to deepfakes. This is the use of AI to generate synthetic media that is extremely realistic and compelling.

My point here is that the tools for this have really brought down the costs of creating high quality things. If you look at a deepfake that I could create on my laptop using an open source software package, it is superior to Hollywood movies that spent hundreds of millions of dollars on their computer-generated imagery (CGI) budgets 20 years ago.

This is coming in really strong. I would say that even though the politically motivated deepfake attacks that we have seen so far have been clumsy. For example, Russia's release of a Deepfake where President Zelensky of Ukraine surrendered and stated that all his forces should lay down their arms.

This was a really low quality deepfake that was clumsily executed. But I draw almost no comfort from that fact because we should expect malicious actors to grow in sophistication and we should expect the tools to grow in sophistication.

Think about, for example, the 2015 attempted coup in Turkey. The specific turning point in that coup was when the Turkish President did an interview on live television holding up his iPhone to the camera to do a face time interview in which he called upon the people of Turkey to go out into the streets and protest the military takeover.

My point is that the right media, deployed at the right political moment can have transformative consequences. Because Russia is bad at it today, just because China is bad at it today, does not mean they will be bad at it 2 years from now, and we should expect them to be thinking long and hard about how to pull off these types of attacks.

The intervention that I think could be useful in this regard relates to the tools for deepfake creation. Right now, I am technically qualified to download a package of software to create deepfakes. I am not technically qualified to create that package of software.

If the U.S. Government were, for example, to require that the makers of this type of software embed characteristics in the media files that allow them under technical analysis to be revealed as AI enabled forgeries, this would raise the cost and complexity of executing these types of forged media political interventions.

As I said before, our goal is not to make everything impossible, but our goal is to make malicious activity more difficult and more complicated, while allowing deepfakes for Hollywood movies or other types of entertainment applications to proceed.

To give you just one example. Under a camera, you can do computer analysis of a video recording of a person that allows you to observe that person's pulse, literally the blood flushing into their face with every heartbeat. Now, my eyes cannot detect that in either, anybody's face over there.

But a computer analysis of a video can observe this. My point is, if we were to prohibit, for example, deepfake video from replicating this blood flush phenomenon, then there would be something where for an entertainment application, it is indistinguishable to the human eye, but under technical analysis, it reveals itself as an AI generated forgery.

I do not claim that this is the perfect example, but my point is that we should be hunting for these kinds of examples that make malicious activity hard——

Senator ROMNEY. Let me just ask, well and good. Let us say we prohibit that in the United States from all the U.S. providers of this technology. But 5 years from now, or 2 years from now, the Chinese will have the capacity, the Russian synthetic capacity, the Iranians. We cannot prevent them from putting a flush on the face.

Mr. ALLEN. Yes, you are absolutely right. What you have to think about is the scale of the intervention that you are doing and what actors you are preventing. Somebody who has an unlimited research and development budget is much harder to stop than somebody who is an amateur cyber-criminal.

My point is there are certain types of interventions that we could put in right now that would effectively be costless to the entertainment or research community but would present a high barrier for low technical sophistication actors.

As we think about the sort of high sophistication threats coming from foreign intelligence services, those are obviously going to require more sophisticated interventions than what I described.

Senator HASSAN. Let us go to Dr. Alstott, and then Dr. Murdick, about the same question. I want to think about the non-state actor question in particular, if we can, too.

Dr. ALSTOTT. Non-state actors, terrorists, and others have attempted to use bioweapons, cyber weapons, and nuclear weapons in the past. For different threats, sometimes the barrier has been information and expertise, and sometimes it has been physical material.

Over the decades, we have, unfortunately, in multiple instances, seen non-state actors attempt to use bioweapons that really have strategic scale to them. Fortunately, they have never succeeded. Unfortunately, the barriers are going down and we have had fairly recent close-ish calls within the classified record.

This is a place that I would direct the majority of my attention because of the low barriers on the physical side. However, cyber weapons, nuclear weapons are two obvious cases in which a non-state actor could cause a great deal of trouble. But there are other threats not yet conceived.

What we need to make sure exists is a function that is able to identify these threats as they are coming in and as they are identified, right, so that if we identify that AI will help a non-state actor use some category of weapon that we are not even talking about today, that we are able to move to address that problem at a faster Observe, Orient, Decide, Act (OODA) loop than we are today.

Senator HASSAN. Thank you. Dr. Murdick.

Dr. MURDICK. Yes. You have heard it said that necessity is the mother of invention, and I think for non-state actors, they are running generally on fairly small budgets, and they want to get more resources.

They need to get information out. They need to get recruits. They need to get disruption, whatever their mission is. I think in the space where there are more tools available, there are a lot of creativity that is going to be coming out.

I think from my perspective, there is some great examples here. I do think cybersecurity, especially the attack surface has increased because of the number of information systems that we are using. For example, AI itself is all mediated through computer systems.

You have just increased the attack surface. You are disruptive—your people with your bent forks that can do weird things to systems is where I think you are going to see your type of threats, and I think cybersecurity is just where a lot of those threats will be realized—particularly in the disruptive goal.

Senator HASSAN. If we are looking at where to invest in talent and resources, that would be one of the areas that you would start with, assuming that as talented and good as a lot of the people we have are, we do not have enough given this landscape.

Dr. MURDICK. The neat thing about this area is it does not require your most technical Ph.D. individuals. The people who are most skilled with the bent forks—pardon me, I do not know where that analogy came from, but are your people who are living in the applied world, and so it is a class of talent that we really need to leverage that many people would call non-technical talent.

Senator HASSAN. OK. A couple of more questions, and bear with me, because Senator Romney, you were getting at the state actors, the China and Russia, and the technology.

Mr. Allen, I want to follow up a little bit because as China, Russia, and other foreign adversaries look to develop their own advanced technologies or versions of them, it is really important that we are going to be able, the United States, to take steps to protect our intellectual property and technological edge.

In the spring, the Biden Administration announced new controls to prevent the exportation of certain advanced semiconductor manufacturing equipment to China. This is an important step that will hopefully slow down Chinese development of the types of chips needed to produce powerful artificial intelligence systems.

However, these controls would have been far less effective if the Dutch and Japanese had not also added export limits for similar technologies because of their roles as market leaders alongside the United States.

Can you speak to the importance of multilateral cooperation in slowing the proliferation of advanced technologies to our adversaries?

Mr. ALLEN. Thank you. I think you made the exact right point about the need for multilateral cooperation on this issue.

The technological competition that we face with China is extremely different than that with the Soviet Union in the Cold War, both because of the depth of our trading relationship with China, and also because on a relative basis, the United States economy is smaller in global terms.

Right after World War II, we alone were more than 50 percent of global gross domestic product (GDP), and that is not the case today. There are a lot of other places in the world that possess extraordinary technological capability that is relevant to great power competition, including that with China.

The October 7th export controls that the Biden Administration adopted to restrict the sale of advanced AI chips and advanced chipmaking equipment to China, I believe, was one of the two most important decisions the Biden Administration made in foreign policy last year. Other than Russia's war in Ukraine, that was probably the most important thing that happened. It really did fundamentally change our relationship with China for a long period of time.

I would say the challenge is that export controls are not a foolproof solution. One Chinese company, Yangtze Memory Technologies Co (YMTC), which is a memory chip producing company, reportedly in 2021, had had 800 people employed full time for more than 2 years trying to develop alternatives to American technology in order to avoid export controls.

The entire U.S. Export Control Agency is only 300 people. Actually, in inflation adjusted terms, their budget is headed for a cut this year. After the United States Federal Government put export controls at the center of U.S. foreign policy, both in our response to Russia's invasion of Ukraine and also in our artificial intelligence competition with China, we are actually degrading our own ability to enforce these export controls and to assess where export control restrictions would have our intended consequences, and I think that is a grave error on the part of the U.S. Government.

Senator HASSAN. Thank you. One more question, if you have the patience for it too, Senator Romney, and then the wrap up question that I talked about. To Dr. Alstott, as research institutions, private companies, and nations rapidly develop artificial intelligences of increasing power, the severity of the risks associated with these systems also increases.

Earlier, I asked a question, and we talked about the utility of AI to dangerous non-state actors, but this risk could be mitigated by developing AI that cannot take harmful actions in the first place.

As we develop powerful artificial intelligence and it becomes even more integrated into our daily lives, I think there need to be safeguards that protect the lives of Americans. What specific research questions do we need to ask and have answered to develop AI that is fundamentally safer and either cannot be exploited or at least is much harder to exploit for dangerous uses?

Dr. ALSTOTT. There are a variety of technical bets out there, and different technical experts have different takes on this.

However, an example of a particular technical direction that has broad buy in is about the interpretability of what is going on inside the AI—mechanistic interpretability is a particular term of art these days.

This is very much like doing neuroscience except on an AI, where you are able to look inside the AI as it is doing things and understand how its concepts are represented, how the concepts interact, how it makes decisions, how it does planning and so on, which is exactly the sort of view that you need in order to make strong claims about what this AI will and will not do under different circumstances.

Now, I am a lapsed neuroscientist myself, so I can tell you that neuroscience is pretty hard. But this should be easier in the case of AI because we have visibility into the internals of the AI. We do not have to do surgery on it, no skulls need to be cut, etcetera. This is an example of just one technique.

This technique and many other techniques have a sort of fundamental strategic issue with them, which is that it needs to be the case for them that as the AI is increasing in complexity and power, that your safety techniques keep up.

If it is lagging behind, this will not work over the long term. You need your interpretability, or whatever techniques you would like, to be matching or exceeding as the AI grows in power and complexity.

Senator HASSAN. Thank you for that. That is helpful. We have discussed a pretty broad range of topics. I have found it very helpful.

We obviously cannot cover all potential threats to national security in one short hearing, but I did want to give each of you a chance to share any final thoughts on topics that we maybe have not sufficiently addressed already.

I will start with Dr. Murdick and go down to the table. Thank you all for being here. Dr. Murdick, any final thoughts?

Dr. MURDICK. I have really appreciated this conversation. It is such a rich discussion. Just very briefly, three things that I do not think we talked much about. This first one is relevant to your last question, software liability.

Procedural changes have had huge impact in how systems are deployed. A Senate body cannot respond to everything directly, but by figuring out software liability questions, I think there is a huge opportunity to change the landscape of innovation and the threat space because you get lots of people empowered to start to adjust the landscape.

Second, talent, I think, is so important. We did talk about it a lot. I think it is extremely important for AI literacy, for Science, technology, engineering, and mathematics (STEM) talent, for nontechnical talent. It is going to take all of us to be able to do this.

Making it clear that you do not have to be a Ph.D. in whatever to be participating in this discussion is extremely important. Then last, whatever we design, ultimately know the apparatus is to protect us. There is a desire, because we want everything to start with a complex system, but only in Greek mythology do complex systems spring into existence.

I think we have to start with very simple systems that work, have a very clear mission, and then they get expanded in a very judicious way. I think we have to resist the urge to try to solve all your values based questions and get very focused ones, and then build from there. That way, we will get complex systems that work.

Senator HASSAN. Thank you. Dr. Alstott.

Dr. ALSTOTT. I second the idea of having a clear mission. As I said earlier, we do not currently have a function within government that has clear authorities and responsibilities on the issue of broadly capable AI and the threats that it could pose.

As Senator Lankford was describing, this is in part a values question of what are the things that we need a bureaucracy empowered to address. The virtue of the United States is that we have a lot of diversity in values, which I at least personally enjoy.

But one thing that there is a lot of agreement on is national security and public safety, so that seems like a top candidate for a place that a clear mission could start. Possibly other things could also be included, but this would seem to be a place that there be a lot of agreement.

Senator HASSAN. Thank you. Mr. Allen.

Mr. ALLEN. Thank you so much for the opportunity to testify today. I think my closing remarks will principally be an apology to Senator Romney, because you asked a bunch of questions that I feel like we did not quite answer. I am going to use my closing remarks to do my best to answer them.

You asked do we need an international consortium? Is that realistic, or how do we control the world's worst actors? Before I answer those, I want to talk about what I view as the problem that we are trying to solve, and it is split into two areas vis a vis AI.

When I was working in the United States Department of Defense, we were principally focused on application specific AI. These are machine learning systems, and they learn from data. If you want to generate an AI system that can recognize cats, you need a bunch of pictures of cats.

If you want to generate an AI system that can recognize military vehicles from satellite imagery, you need a lot of satellite images. These are application specific AI systems, and I believe the existing United States regulatory framework is pretty good at handling application specific AI systems.

What I have just described is really the AI revolution from the year 2012 to around 2020 or 2022. The challenge that we have now is there are these increasingly general AI systems. If you talk to Chat Generative Pre-trained Transformer (ChatGPT), it will give you advice for how to design a nuclear submarine, and it will give you medical advice, and it will give you financial advice.

These are no longer application specific systems because the training data is not a large library of cats, the training data is almost the entire Internet. It is such a general system that it is not a good fit for the existing regulatory structure—or at least in some instances, it is not a good fit for the regulatory structure.

The second challenge we have is that these systems continue to get better at an exponential rate. I am sure both of you are familiar with Moore's Law, which is the phenomenon that computers get twice as fast for the same price or perhaps even a lesser price every 2 years.

What that means is that in 20 years, AI systems will not be 20 times better, they will be 1,000 times better, and that is if they proceed at the Moore's Law pace. Over the past 10 years, AI research has radically exceeded the pace of Moore's Law in terms of the pace of technological progress.

We must conceive now of regulatory structures that would be useful and relevant to AI systems that are not a little bit better than the astonishingly capable systems we have today, but a lot better than the astonishingly capable systems we have today. That is what I think the challenge is to solve.

From that perspective, I do think that it is worth the U.S. Government's time to consider creating a new Federal agency or creating a new organization within a Federal agency that is specifically working on this problem.

I have just recently hired staff to come up with a detailed proposal on this issue, and so I would hesitate to give you a detailed proposal today, but that is what I view as the problem that demands some kind of new type of action.

International collaboration will be required on this issue, but we should think about developing mechanisms that are also useful in the event that international collaboration fails. For example, when I was in the United States Department of Defense, we put forth multiple requests for dialog with the People's Liberation Army to discuss military AI risk reduction so that we do not go to war accidentally, and all of those requests were refused.

I do think it is worth us thinking about structures that can work even in the event that international collaboration does not go the way we hoped. Thank you both.

Senator HASSAN. Thank you all three for really not only excellent testimony but sharing your expertise with us so thoughtfully and so broadly. Again, just to thank you, too, for what you have already contributed to our nation's security.

We really appreciate it. I look forward to continuing this conversation with my colleagues and my constituents. I know that you gave us a lot of ideas. You gave us some new problems to try to solve.

I look forward to continuing the work with all of you and with my colleagues. The hearing record will remain open for 15 days until 5.00 p.m. on October 4th for submissions of statements and questions for the record. The hearing is now adjourned.

[Whereupon, at 3:59 p.m., the hearing was adjourned.]

APPENDIX

Opening Statement as Prepared for Delivery by Chair Maggie Hassan
Emerging Threats and Spending Oversight Subcommittee Hearing:
"Advanced Technology: Examining Threats to National Security"
September 19, 2023

Before we get started today, I wanted to take a moment to reflect on the impact that Ranking Member Romney has had on the Senate in his time here, and note that I will miss working with him when he retires.

Ranking Member Romney has been an incredible partner both on this committee and in the important bipartisan legislation that the Senate has passed in the last few years.

Senator Romney, your dedication to public service is clear, and the people of Utah, Massachusetts, and the United States are better off due to your years in elected office.

Thank you for your hard work, I look forward to continuing our important work for the remainder of this Congress.

Good morning, and welcome to our distinguished panel of witnesses.

Thank you for appearing today to discuss potential threats to national security posed by advanced and emerging technologies, and what steps the federal government can take to mitigate risk and encourage the responsible development of next-generation technologies.

I also want to thank Ranking Member Romney and his staff for working with us on this hearing, and for our continued partnership to address emerging threats to the nation.

Today's hearing brings together a group of experts in technology policy who have previously served as government officials, and who are now providing important and valued insight on the development and applications of advanced technologies.

We will hear about the potential dangers to public safety and security that may be posed by emerging technologies – such as artificial intelligence and quantum technology.

We will also hear about the actions that Congress and the Executive branch can take to mitigate these risks while still working to maintain the United States' technological innovation edge and stay ahead of our global adversaries.

Public and private investment in the United States have fueled the rapid growth in the power and availability of artificial intelligence, quantum computing, and other emerging technologies, and our nation is well positioned to benefit from the technological revolution that is already underway.

However, bad actors will also undoubtedly seek to use these powerful technologies to launch a higher volume of new and more severe attacks aimed at the American people.

As we will hear today, AI and other advanced technologies pose real public safety risks, which Congress is just beginning to address.

For example - although there has been considerable Congressional attention paid to many of the public safety risks posed by artificial intelligence, there has been less focus on so-called "catastrophic" risks posed by AI – such as the ability of AI to help terrorists develop and use unconventional weapons.

I'm working on a framework to support research into safer AI that – in its fundamental design – cannot easily be abused by criminals, and cannot easily behave in unexpected ways that harm the public.

Congress needs to look closely at ways to require AI to be designed in a fundamentally safer way, and – in time – require all AI hardware to be restricted to running only fundamentally safe systems.

I look forward to hearing from all of our witnesses about how Congress and the federal government can successfully encourage technological growth and keep the American people safe, secure, and free.

Opening Statement
Ranking Member Mitt Romney

U.S. SENATE SUBCOMMITTEE ON
EMERGING THREATS AND SPENDING OVERSIGHT
- *"ADVANCED TECHNOLOGY: EXAMINING THREATS TO NATIONAL SECURITY"*
SEPTEMBER 19, 2023

Thank you, Chair Hassan, for holding a hearing on this important topic. I look forward to this discussion about risks to national security from advanced technology such as AI and examining how the United States can best mitigate those risks.

Technological innovation is a pillar of American strength. We must keep in mind the role that the private sector plays in creating and maintaining America's competitive advantage, especially as China seeks to gain supremacy in technology.

At the same time, AI is rapidly advancing, all the while becoming increasingly integrated into daily life. While AI can be used for good, it also has a concerning potential for misuse. Many in the tech community have acknowledged "profound risks to society and humanity" posed by AI.

Experts say it can be weaponized by bad actors. Perhaps AI could be used to build biological or chemical weapons, or to launch cyber-attacks against critical infrastructure like the electric grid.

AI systems often lack "explainability." In other words, AI developers don't fully understand how outcomes are reached. If they don't fully understand, how can we expect Congress to?

And yet, we hear a chorus of voices from experts and industry calling for Congress to act. At the Senate AI forum last week, there was "universal agreement" among participants that government needs to do something.

Today, I'm interested in hearing your views on some big questions:

1. Should the U.S. consider a licensing regime to prevent the most advanced AI models from amplifying these risks? If so, who should be doing the licensing and who should be subject to it?

2. How do we protect U.S. technology and our lead in AI over China? What more can do we to strengthen and enforce export controls?

3. From a national security perspective, should we be allowing the proliferation of open-source AI models? Does the Chinese government support open-source models?

4. What more can we do to responsibly bolster U.S. national security capabilities in the AI space?

Thank you, Madam Chair.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Statement before the

Senate Homeland Security and Governmental Affairs

Subcommittee on Emerging Threats and Spending Oversight

"Advanced Technology: Examining Threats to National Security"

A Testimony by:

Gregory C. Allen

Director, Wadhwani Center for AI and Advanced Technologies, CSIS

Tuesday, September 19, 2023

562 Dirksen Senate Office Building

Chair Hassan, Ranking Member Romney, and distinguished members of the Subcommittee, thank you for inviting me to testify today. The Center for Strategic and International Studies (CSIS) does not take policy positions, so the views represented in this testimony are my own and should not be taken as representing those of my current or former employers.

I currently serve as the director of the Wadhwani Center for AI and Advanced Technologies at CSIS, where I lead a team conducting policy research at the intersection of technology, economics, and national security. Prior to CSIS, I spent three years working at the U.S. Department of Defense Joint Artificial Intelligence Center, where I most recently served as the director for strategy and policy.

For my testimony today, I hope to offer a perspective regarding the national security threats of artificial intelligence (AI) and other emerging technologies that is informed by my experience serving in government as well as my research work since leaving government.

An Overarching Trend: Reduced Cost and Complexity

To begin, let me say that there is a broad technological trend across many fields where the cost and complexity of many technological capabilities and activities have come down significantly. In many cases, it takes less money and fewer highly trained expert staff to perform the same activity.

As a result, certain types of activities that used to be only within the reach of large governments or military organizations can now be performed by individual corporations or even individual people. Take, as just one illustrative example, orbital space launch. Prior to SpaceX's successful launch of the Falcon 1, developing a new orbital space launch vehicle typically cost billions of dollars and required thousands or tens of thousands of employees. SpaceX developed the Falcon 1, which successfully launched in 2008 for only $90 million dollars. At the time of the launch, SpaceX had a staff of only around 500 people.[1]

In general, the falling cost and complexity of technologies and the activities they enable is good news for the global economy and society. This trend should be celebrated. However, it also poses genuine challenges for U.S. national security in areas where high cost and complexity have historically presented a barrier to dangerous activities. It is good that, for example, developing nuclear weapons is expensive and complicated. The United States would be significantly less safe if building a functional nuclear weapon was cheap and simple.

While nuclear weapons remain expensive and complicated, there are a number of areas where the cost and complexity of developing, acquiring, and employing national security-relevant technologies is declining. In some important areas, this includes placing certain dangerous

[1] NASA, *Commercial Market Assessment for Crew and Cargo Systems* (Washington, DC: April 2011), https://www.nasa.gov/sites/default/files/files/Section403(b)CommercialMarketAssessmentReportFinal.pdf.

capabilities within the reach of non-state actors that will seek to use those capabilities to threaten the United States. I will focus on three in particular today.

1) Reduced Cost and Complexity of Weaponizing Autonomous Drones

To provide a simple example, the vast majority of non-state terrorist groups and insurgents throughout history have not had access to military air power for either airborne reconnaissance or long-range precision strike unless they are being directly supported with military aid from a foreign government.[2] Otherwise, aircraft are typically too expensive and difficult to maintain.

The rise of commercial drone aircraft, however, has changed this story significantly. During the Battle of Mosul in 2016, the Islamic State flew more than 300 drone missions in a single month, with roughly 100 of those used for delivering explosives.[3] The U.S. Air Force described this as the first time that U.S. ground forces had come under attack from enemy aircraft since the Korean War. The typical drone used by the Islamic State during this period was a commercial model purchased for roughly $650 and then modified to carry explosives.

The trend of commercial drones being adapted for military applications now extends to both sides in the war in Ukraine, where Ukrainian forces have used commercial drones to drop explosives on Russian tanks, destroying Russian vehicles costing hundreds of thousands or millions of dollars for the price of a $100 grenade and a $1,000 drone.[4]

The drones being used in the war in Ukraine are generally remotely piloted and travel relatively short distances, but this may change as improved technology becomes more widely available. Russian forces have already used kamikaze drone weapons in Ukraine with autonomous navigation capability,[5] and in early 2023, the leader of a Russian private military corporation stated the group's intention to test an AI-enabled autonomous tank weapons system in active combat, though this may have been an exaggeration to attract attention.[6]

The basic trend of increasingly capable, increasingly autonomous drones that deliver military-relevant capabilities at a fraction of the cost of traditional military systems is highly likely to

[2] John G. Bunnell, "From the Underground to the High Ground: The Insurgent Use of Air Power," Air War College, Air University, February 16, 2011, https://apps.dtic.mil/sti/pdfs/AD1018700.pdf.

[3] Mark Pomerleau, "How $650 drones are creating problems in Iraq and Syria," C4ISRNET, January 5, 2018, https://www.c4isrnet.com/unmanned/uas/2018/01/05/how-650-drones-are-creating-problems-in-iraq-and-syria/.

[4] Gregory C. Allen, "Across Drones, AI, and Space, Commercial Tech Is Flexing Military Muscle in Ukraine," CSIS, *Commentary*, May 13, 2022, https://www.csis.org/analysis/across-drones-ai-and-space-commercial-tech-flexing-military-muscle-ukraine.

[5] Gregory C. Allen, "Russia Probably Has Not Used AI-Enabled Weapons in Ukraine, but That Could Change," CSIS, *Commentary*, May 26, 2022, https://www.csis.org/analysis/russia-probably-has-not-used-ai-enabled-weapons-ukraine-could-change.

[6] Samuel Bendett, "Bureaucrat's Gambit: Why Is Dmitry Rogozin Sending Russian Uncrewed Ground Vehicles to Ukraine—And Does It Matter?," Modern War Institute at West Point, February 10, 2023, https://mwi.usma.edu/bureaucrats-gambit-why-is-dmitry-rogozin-sending-russian-uncrewed-ground-vehicles-to-ukraine-and-does-it-matter/.

continue. At present, the United States does not have a significant challenge with drone-based terrorist attacks, whether AI-enabled or not. However, the relevant technological pieces are in place for such a threat to emerge. In the past, some types of malicious activity, such as ransomware, were technologically viable for a long period of time before they became a widespread cybercrime tactic.[7]

2) Reduced Cost and Complexity of Developing Biological Pathogens

Biotechnology is a clear case where the cost and complexity of dangerous activities have been declining for decades. The American bioweapons program during World War II employed roughly 4,000 people, of whom more than 500 were technical experts. Its multi-year budget totaled roughly $40 million ($690 million in 2023).[8] This was assessed at the time to be roughly the minimum viable program size for a bioweapons research and development effort.[9]

Decades later, in the 1990s, the Aum Shinrikyo terrorist organization in Japan attempted multiple times to develop and deploy biological weapons using botulinum and anthrax. Thankfully, Aum Shinrikyo's bioweapons efforts failed. However, the group successfully executed many steps of developing and delivering bioweapons despite having only a handful of technical expert staff and a much smaller research and development budget than any nation state.[10] Of special note, Aum Shinrikyo had members with education from and ties to legitimate academic research organizations working in biology and medicine.

Today, the development of advanced genetic engineering technologies such as CRISPR has radically reduced the cost and complexity of gene editing to the point where even amateurs can modify the genes of viruses.[11] Some research organizations have previously published genetic information related to highly lethal (but not highly contagious) pathogens such as bird flu.[12] Terrorists and terrorist organizations following in the footsteps of Aum Shinrikyo may be able to create genetically modified pathogens that are both highly contagious and highly lethal. The U.S.

[7] "History of Ransomware," Crowdstrike, October 10, 2022, https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/.

[8] Lt. Comdr. William B. Sarles, "Report of Meeting, 28 December 1944" (Washington, DC, December 28, 1944), RG 160, NM-25 12, Box 77, National Archives at College Park, MD.

[9] William F. Vogel, "'The Mighty Microbe Can Go to War': Scientists, Secrecy, and American Biological Weapons Research, 1941–1969," (PhD dissertation, University of Minnesota, November 2021), https://conservancy.umn.edu/bitstream/handle/11299/226425/Vogel_umn_0130E_22969.pdf.

[10] Richard Danzig et al., *Aum Shinrikyo: Insights into How Terrorists Develop Biological and Chemical Weapons* (Washington, DC: Center for a New American Security, December 2012), https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/CNAS_AumShinrikyo_SecondEdition_English.pdf.

[11] Heidi Ledford, "Biohackers gear up for genome editing," *Nature* 524 (2015): 398–399, https://www.nature.com/articles/524398a.

[12] Nell Greenfieldboyce, "Scientists Publish Recipe For Making Bird Flu More Contagious," NPR, April 10, 2014, https://www.npr.org/sections/health-shots/2014/04/10/301432633/scientists-publish-recipe-for-making-bird-flu-more-contagious.

Intelligence Community specifically called out this bioweapons proliferation threat in a previous report to Congress.[13]

3) Reduced Cost and Complexity of High-Quality Forged Media

One of the most remarkable capabilities of modern AI technology is its ability to generate compelling synthetic digital media—text, photos, videos, and audio files—that can realistically imitate or depict real people in appropriate contexts. Today, many of these AI-enabled media forgery capabilities, commonly referred to as deepfakes, are realistic enough that they can routinely fool the untrained eye and ear and sometimes even the trained eye and ear. Moreover, these tools are increasingly available not only to advanced computer scientists, but to essentially anyone with a computer or smartphone.

During my time at the Department of Defense, my organization collaborated with DARPA on an effort to detect deepfake media using technical analysis. Similar efforts to develop digital forensics tools to detect AI-generated media are now widespread in the private sector and academia.[14]

However, work on such tools is not preventing deepfakes from featuring increasingly prominently in cybercrime and disinformation attacks. For example, in July 2019, Symantec reported that it was aware of three cases in which deepfake audio was used as part of a criminal operation to impersonate corporate CEOs in which company employees were tricked into transferring funds totaling millions of dollars.[15] More recently, deepfakes have been used as part of false kidnapping scams and other types of crime.[16]

Beyond criminal theft, deepfakes are also increasingly likely to feature in politically motivated disinformation efforts. In March 2022, a deepfake video—presumably created by the Russian government—depicted Ukrainian president Volodymyr Zelenskyy surrendering to Russia and instructing Ukrainian forces to stop fighting.[17] The quality of this particular deepfake was quite low, and the Ukrainian government had been warning its citizens to expect manipulated videos. As a result, few were fooled. Pro-Chinese propaganda organizations have also recently used

[13] James R. Clapper, "Worldwide Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, February 9, 2016, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

[14] Matthew Hutson, "Detection Stays One Step Ahead of Deepfakes—for Now: The spread of AI-generated content is keeping the tech designed to spot it on its toes," IEEE Spectrum, March 6, 2023, https://spectrum.ieee.org/deepfake.

[15] "Fake voices 'help cyber-crooks steal cash'," BBC, July 8, 2019, https://www.bbc.com/news/technology-48908736.

[16] Faith Karimi, "'Mom, these bad men have me': She believes scammers cloned her daughter's voice in a fake kidnapping," CNN, April 29, 2023, https://www.cnn.com/2023/04/29/us/ai-scam-calls-kidnapping-cec/index.html.

[17] James Pearson and Natalia Zinets, "Deepfake footage purports to show Ukrainian president capitulating," Reuters, March 17, 2022, https://www.reuters.com/world/europe/deepfake-footage-purports-show-ukrainian-president-capitulating-2022-03-16/.

deepfake media as part of an online disinformation effort.[18] This was also a low-quality effort with minimal impact.

However, these examples should not lead anyone to conclude that future deepfake disinformation campaigns will continue to be equivalently clumsy and ineffective. Many early cyberattacks were also clumsy and ineffective, but the field improved dramatically over time. Moreover, important events in recent world history have frequently hinged upon disseminating the right media at the right time. For example, the 2015 attempted coup in Turkey was prevented in part because the Turkish president conducted a live TV interview via video call in which he successfully encouraged Turkish citizens to protest the coup.[19] Had that news broadcast been coopted by a deepfake disinformation attack, perhaps the events that day might have taken a different course.

Governance of Artificial Intelligence

In 2012, a revolution in the application of deep neural networks and GPU processors to image recognition kicked off a decade of revolutionary progress in AI technology. In just the past year, a second equally extraordinary AI revolution has begun with the application of generative AI models. These two major milestones in AI over the last 15 years have considerably expanded the scale and scope of AI's applications across the global economy, civil society, and international security. Generative AI has the potential to disrupt industries, driving large gains in efficiency and quality, but will also raise difficult questions about workforce displacement, education, intellectual property rights, and responsible use. People and organizations of all sizes are already using AI to advance labor productivity and drive anti-inflationary growth, develop more sustainable products, cure diseases, feed a growing population, and address climate change. In the future, AI has the potential to transform the way societies learn, work, innovate, and address global challenges.

Like any technology, AI presents risks. AI can be maliciously used for harm, such as the previously mentioned disinformation attacks, and can also be a source of unintentional harm through technical or managerial failures.

There is no inherent trade-off between mitigating AI risks and pursuing the benefits of increased adoption. We can pursue both goals simultaneously. AI regulation and frameworks must be well balanced, ethically designed, and part of an internationally interoperable framework.

Many uses of AI are already regulated today when AI is used in a regulated application. For example, a bank using AI as part of a consumer lending decision would still be subject to the relevant regulations, such as non-discrimination. Any use of machine learning in an aircraft would still be subject to U.S. air safety regulations.

[18] Graphika Team, "Deepfake It Till You Make It, Pro-Chinese Actors Promote AI-Generated Video of Fictitious People in Online Influence Operation," Graphika, February 2023, https://public-assets.graphika.com/reports/graphika-report-deepfake-it-till-you-make-it.pdf.

[19] Kieran Healy, "Turkey Coup: How Facetime and social media helped Erdogan foil the plot," Vox, July 16, 2016, https://www.vox.com/2016/7/16/12206304/turkey-coup-facetime.

A key challenge for regulators, however, is the fact that AI systems are becoming both increasingly powerful and increasingly generalized. Many large language models, for example, can expound on topics ranging from medical advice, to engineering assistance, to military strategy.

These models currently suffer from "hallucinations" and other reliability problems that limit the willingness of most customers to deploy them in mission- and safety-critical applications without appropriate guardrails in place. Sector-specific regulations are still useful and appropriate, but there is also an opportunity for more general regulations that would be helpful, particularly for the largest and more advanced models.

More generalized regulations in support of AI safety should take the form of a licensing regime for the most advanced AI models and a Know Your Customer requirement for cloud companies that are supporting the development and use of advanced AI models.

Artificial Intelligence and Semiconductor Export Controls

AI powered by machine learning is a general-purpose technology, analogous to electricity or digital computers. When first invented during World War II, computers had only a handful of important military applications, such as code breaking. Today, nearly every military technology involves computers to some greater or lesser extent, whether that is radio communications or missile guidance systems. Even military items that do not have any computers, such as boots or bullets, were nonetheless designed on computers.

Military AI is in a similar situation today as computers were in the 1940s and 1950s. There are a handful of applications where the use of AI is already delivering significant military benefit—such as satellite imagery analysis. Over the next several decades, AI technology will be involved in a rapidly growing share of military activities. The senior military leadership of both the United States and China believe that AI will be foundational to the future of military and economic power.

In some areas, AI will genuinely revolutionize how military operations and warfighting are conducted. The Department of Defense's Replicator Initiative, which seeks to field thousands of AI-enabled and attritable autonomous drones within the next 24 months, is one example.

AI development is not merely an issue of software. All software has to run on semiconductor chip hardware somewhere, and that hardware, and the software architectures that run on top of it, are areas in which the United States and allied countries have a significant technological edge.

On October 7, 2022, the Biden administration adopted a new export controls policy designed to severely restrict China's access to American semiconductor technology, including chips, chipmaking equipment, chip design software, and equipment components.[20] This was a genuine landmark in the history of U.S.-China relations.[21]

The four chokepoints mentioned above are not all alike in the case of enforcement. Chipmaking equipment, which is large, expensive, and produced in limited quantities, is easiest to enforce prior to sale and—to a lesser extent—even after sale. However, from China's perspective, the most direct path to AI progress is simply continuing to use American chips. It is at this first and crucial chokepoint that China most flagrantly attempts to evade our export controls—and too often succeeds.

The Bureau of Industry and Security (BIS) at the Department of Commerce oversees most export controls. Unfortunately, BIS is increasingly challenged by worldwide smuggling and export control evasion networks, especially those that are supported by Russia and China. For example, investigators have examined the wreckage of downed Russian weapons systems in Ukraine and found that they contain U.S. and allied components, including electronics that were manufactured years after the implementation of the 2014 Russia export controls.[22]

As our geopolitical rivals pursue increasingly aggressive and better-resourced means of obtaining critical technology, BIS must use every tool available to increase capacity and productivity for effective enforcement. At a time when the need for robust U.S. export controls is more strategically critical than at any time since the end of the Cold War, BIS's enabling technology is in a poor state.

The cause is simple: decades of underinvestment. Current and former BIS staff have told CSIS in interviews that the major government databases that they use to monitor trade flows and identify suspicious activity can perform only a fraction of the needed functionality and crash routinely. Instead of knowledge graph databases and machine learning—capabilities that have revolutionized both the private sector and other federal agencies with similar missions—BIS analysts often perform their work primarily using Google searches and Microsoft Excel.

Modern, data-driven digital technologies utilizing AI and machine learning can and should play an integral role in enhancing BIS export control enforcement capabilities. Relatively modest investments could lead to significant improvements in analyst productivity. Despite the increasingly pressing need to invest in these new enforcement capabilities, the budget of BIS has not increased commensurate with the increased number of export-controlled items, the evolving threat landscape, and the growing pressure from an increasingly sophisticated evasion regime.

[20] Gregory C. Allen, *Choking off China's Access to the Future of AI* (Washington, DC: CSIS, October 2022), https://www.csis.org/analysis/choking-chinas-access-future-ai.

[21] Gregory C. Allen, *China's New Strategy for Waging the Microchip Tech War* (Washington, DC: CSIS, May 2023), https://www.csis.org/analysis/chinas-new-strategy-waging-microchip-tech-war.

[22] Jeanne Stars and Stripes, June 16, 2022, https://www.stripes.com/theaters/us/2022-06-15/us-electronic-chips-russian-military-6356609.html.

The current international momentum behind U.S.-led export controls presents a unique opportunity both to help solve a pressing problem—responding to Russia's invasion of Ukraine—and to advance the adoption of digital technology by U.S. government agencies for mission impact. A changed geopolitical landscape demands reinvigorated U.S. government export controls capacity, and this cannot be done without additional resources. CSIS analysis of relevant, comparable data-driven digital technology modernization efforts by other U.S. government agencies with similar mission requirements suggests that this could be accomplished with an additional appropriation for technology modernization at BIS of roughly $25 million annually for five years.

This funding would allow BIS to better ingest, connect, and analyze hundreds of billions of records from both government and open-source data. By applying modern data science and machine learning techniques, BIS could increase productivity across all its processes, such as automatically detecting that a purported Eastern European "tractor manufacturer" has the same phone number as a supplier of engines to the Russian military. This figure accounts for opportunities at BIS to improve collaboration with other U.S. government agencies and the need to prevent unnecessary duplication of effort.

However, a more productive enforcement analysis community will identify more entities as likely shell companies engaging in illicit transactions. This will in turn increase the need for enforcement agents to conduct site inspections or criminal investigations of these identified entities. Despite the severe current technological limitations on the efficacy of the analytic community, its work is already identifying enough candidate entities for inspection to more than fully consume the capacity of the current staff. Therefore, in addition to the $25 million annual increase for five years to support new technology and staff for BIS analytical capabilities, BIS will also require an additional $18.4 million and 48 positions annually for the Export Enforcement organization as well as another $1.2 million for additional classified facility space for these individuals to support the classified aspects of their work. Thus, the total size of the recommended additional BIS budget appropriation is $44.6 million annually.

In terms of return on investment, this increase in BIS's budget by $44.6 million annually is likely to be one of the best opportunities available anywhere in U.S. national security. The U.S. government is currently spending tens of billions to assist Ukraine in destroying the weapons of Russia's military, which too often are powered by U.S. technology. Providing a few tens of millions of dollars annually to BIS to modernize the technology that enables export controls enforcement and increase their staff would go a long way toward ensuring that far fewer Russian and Chinese weapons using U.S. technology are built in the future.

Conclusion

AI and biotechnology, together with other emerging technologies, are among the most exciting developments occurring anywhere in the global economy. While I have focused my testimony on the risks and challenges that these technologies present for U.S. national security, I want to emphasize again that emerging technologies have enormous positive potential. The United States government should pursue accelerated adoption of these technologies in areas where they have the potential to make a positive impact, while also pursuing regulatory and other mechanisms that can improve the safety and security of the United States.

Thank you for the opportunity to testify today, and I look forward to your questions.

Testimony

JEFF ALSTOTT

Preparing the Federal Response to Advanced Technologies

CT-A2953-1

Testimony presented before the U.S. Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Emerging Threats and Spending Oversight, on September 19, 2023

For more information on this publication, visit www.rand.org/t/CTA2953-1.

Testimonies

RAND testimonies record testimony presented or submitted by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies.

Published by the RAND Corporation, Santa Monica, Calif.

Preparing the Federal Response to Advanced Technologies

Testimony of Jeff Alstott[1]
The RAND Corporation[2]

Before the Committee on Homeland Security and Governmental Affairs
Subcommittee on Emerging Threats and Spending Oversight
United States Senate

September 19, 2023

Chair Hassan, Ranking Member Romney, and members of the subcommittee: Good afternoon, and thank you for the opportunity to testify today. I am a senior information scientist with the RAND Corporation, a nonprofit and nonpartisan research organization. Before RAND, I served at the White House as assistant director for technology competition and risks at the Office of Science and Technology Policy and as director for technology and national security at the National Security Council. I also spent time in the intelligence community as a program manager at the Intelligence Advanced Research Projects Activity, with a portfolio that included artificial intelligence (AI), analytic methods, biosecurity, and science and technology forecasting.

For the past 75 years, RAND has conducted research in support of U.S. national security and domestic policy. We manage four federally funded research and development centers for the government focused on national and homeland security. Today, I will focus my comments on

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of the RAND Corporation or any of the sponsors of its research.

[2] The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. RAND's mission is enabled through its core values of quality and objectivity and its commitment to integrity and ethical behavior. RAND subjects its research publications to a robust and exacting quality-assurance process; avoids financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursues transparency through the open publication of research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. This testimony is not a research publication, but witnesses affiliated with RAND routinely draw on relevant research conducted in the organization.

how the federal government can respond to emerging threats to national security and public safety posed by broadly capable AI systems, including how they intersect with biosecurity.[3]

Progress in AI has advanced rapidly in recent years, leading to expanded debate among experts about its potential risks. Although AI has the potential to transform entire industries, it could also pose novel threats to national defense and homeland security. AI developers are racing to build increasingly advanced systems, and the drivers of AI progress—including more-efficient algorithms, more-efficient hardware, a better trained and more capable workforce, and greater investment—continue to increase exponentially. Despite this rapid progress, the sciences of interpreting and explaining AI behavior, assessing powerful AI for dangerous capabilities, and designing appropriate guardrails to mitigate harms are all efforts that are still in their infancy. Existing safeguards are still imperfect, and AI models released by leading U.S. companies today can and do still exhibit unsafe and unanticipated behaviors long after they are trained and released. Unless society puts in effective guardrails, broadly capable AI systems could hasten the design and proliferation of bioweapons, cyberweapons, nuclear weapons, progressively more general intelligence, and other threats not yet conceived. If such systems proliferate, it will be very difficult to put the genie back in the bottle, potentially causing irreversible damage.

One particular area of concern is the relationship of advanced AI development with biosecurity. Existing AI models are already capable of assisting nonstate actors with biological attacks that would cause pandemics, including the conception, design, and implementation of such attacks. Without safeguards, the development of ever-more-advanced AI systems will bring ever-greater reductions to the barriers to launch such attacks, until we are at the point in which a lone actor can cause a pandemic, killing millions. This change is occurring at the same time that gene synthesis machines are decreasing in cost, improving in quality and reliability, and proliferating more widely, increasing the number of actors who have the necessary access and ability to create and release new diseases.

Effective oversight of increasingly powerful AI and its potential threats will require visibility into the full AI development lifecycle. This lifecycle begins with large concentrations of AI hardware, with thousands of advanced chips performing a training run costing millions or soon billions of dollars. Once the AI is fully trained, it is made available to the public through a controlled internet interface or by being published online in its entirety, at which point proliferation essentially cannot be stopped. Oversight of each of these stages—AI hardware, training, and release—will be necessary to ensure our national security. These efforts will not come at the cost of U.S. innovation but will bolster U.S. competitiveness by ensuring the safety and reliability of leading U.S. AI products and establishing the United States as a responsible market leader. In addition, domestic oversight, although essential, will not be sufficient alone. We must cooperate with our allies and partners—and communicate responsibly with our competitors—to ensure the safe development of these technologies at the global level.

I will highlight six actions that the federal government could take to mitigate these threats:

[3] This testimony builds on previous testimony provided to Congress by RAND's president and chief executive officer. See, for example, Jason Matheny, *Advancing Trustworthy Artificial Intelligence,* RAND Corporation, CT-A2824-1, 2023, https://www.rand.org/pubs/testimonies/CTA2824-1.html.

1. Require that large computing clusters that could be used to train powerful AIs (e.g., high-performance computers with >10,000 advanced AI chips) be reported to the government, have adequate cybersecurity, and have know-your-customer processes for anyone doing a very large computation on them that may be a training run for a powerful AI.
2. Require those making powerful AIs to maintain responsible security procedures during and after the training process to prevent U.S.-made models from being stolen or leaked. The threshold for this requirement could be frontier models trained with >10^26 operations, several times larger than any AI system made before, and should include both those handling the code and those handling the hardware infrastructure.
3. Ensure that these frontier AI development efforts also undergo an independent assessment to determine whether the AI or its proliferation would be a threat to national security, similar to how rocket launches are reviewed by the Federal Aviation Administration. This should include risk assessments prior to model training, safety evaluations and red team tests at regular intervals throughout the training run, and rigorous safety reviews prior to model deployment. Models that are determined to be insufficiently safe could be held for further development and release until safety and security issues are adequately resolved. Conducting safety evaluations in each major stage of the AI development process would help companies detect safety problems early on, when issues are less costly to fix, reducing security risks while saving U.S. companies time and money.
4. Create a safe harbor information-sharing environment for both the private and public sectors to share safety and security problems from their AIs as they identify them and then create solutions.
5. Establish know-your-customer requirements for the providers of gene synthesis services (including cloud laboratory services) and gene synthesis devices (including benchtop synthesizers) to reduce growing biosecurity threats.
6. Require that genetic material synthesized over a threshold (e.g., fragments of >50 base pairs) be screened for pathogenic potential. This should include supporting the development and adoption of a universal, secure, and continuously updated gene synthesis screening mechanism, which would reduce urgent biosecurity threats while decreasing costs for U.S. companies and maintaining U.S. competitiveness in the global bioeconomy.

I thank the subcommittee for the opportunity to testify, and I look forward to answering your questions.

CSET CENTER *for* SECURITY *and* EMERGING TECHNOLOGY

Written testimony of Dr. Dewey Murdick
Executive Director
Center for Security and Emerging Technology, Georgetown University

For a Senate Homeland Security and Governmental Affairs Subcommittee on Emerging Threats and Spending Oversight hearing on Advanced Technology: Examining Threats to National Security

September 19, 2023

Chairwoman Hassan, Ranking Member Romney and honorable Senators of the Emerging Threats and Spending Oversight Subcommittee, thank you for the opportunity to discuss the increasingly vital topic of how emerging advanced technologies are affecting our national security. Many of the ideas I will discuss are motivated by the data-driven, tech-policy analysis from Georgetown's Center for Security and Emerging Technology. Others come from my own experience working within government departments and agencies, a couple years living and working in Silicon Valley, and academic experiences.

Key Questions About Emerging Technology Threats

Elected officials and public servants are continuously bombarded with warnings about looming threats or game-changing technologies, all demanding urgent action and investment. Many of these warnings and promises are based on something real, but how do we decide which are most relevant and deserve the most attention and resources? There are three important questions that I think all policymakers should ask when considering various emerging technologies, proposals to address their threats, and recommendations for capitalizing on their potential. These questions can help prioritize our attention and national resources toward the most urgent and transformational efforts and include the following:

1. **What technologies are most timely (i.e., exist now or will exist soon) and have the most significant impact on our national security, economic competitiveness, and societal well-being?**

   Many of today's emerging technologies require urgent action, a demand that this body is rightfully working to meet. For example, AI could improve a terrorist's target reconnaissance and attack planning, allow an adversary to generate more and better disinformation or phishing attacks, guide criminals on the best way to acquire chemicals for meth production without triggering law enforcement alerts, or assist human traffickers in developing more convincing pitches to manipulate victims or their families.

   Others, such as the threats from superintelligent AI systems, are more nebulous, often because we don't yet understand enough about the potential or limitations of the technology involved. I am no expert in quantum computing implementation, but CSET staff have talked with experts and concluded that the practical ability to break through protections and read messages encrypted by modern algorithms, a key application area, remains potentially as far as decades away. As of now, existing quantum computers have nowhere near the scale and capacity required to tackle these challenges.

And still others may not be as transformative as we might think. Recent coverage of how AI chatbots could potentially assist non-experts in dangerous scientific endeavors such as creating pandemics, sparked by a recent preprint article, may exaggerate the threat. An individual motivated to cause harm could already access a wealth of scientific information and protocols online just like the MIT class in this article did. They could learn basic lab techniques from YouTube tutorials, guided by the help of an animated beaver, or even order high-school level kits (in magenta no less) designed to teach bacterial engineering. Open scientific learning and discovery is a very good thing, so I am not advocating that this be curtailed; however, the information barrier for bad actors is not as high as it might appear, and chatbots at this stage serve more as a convenient tool that brings together information in context rather than a game-changing enabler.

In the case of large language models, it doesn't seem that advances here are as relevant to competition with China as we may initially think. Given the Chinese Communist Party's penchant for tight control over the domestic information environment, unpredictable generative AI that might generate responses on Tiananmen Square or images of Winnie the Pooh are unlikely to be a priority. Instead, their efforts are more inclined toward surveillance technologies, such as computer vision methods used for monitoring the face or walking style of tracked individuals.

2. **Do we have the plans, authorities, and tools necessary to mitigate the threat or capitalize on the opportunity? If not, what can we easily update?**

In the short term, there are steps we can take to promote the development of AI that aligns with U.S. values. We should find ways to get the information we need to make better decisions by:

- Tracking AI harms in incident reporting (including voluntary and required reporting);
- Examining the data and models used in existing widespread applications to increase accountability (e.g., sentencing algorithms);
- Encouraging the development of the third-party auditing and red teaming ecosystem; and
- Improving the quality and security of resources, including training and pretrained models that form the backbone of many of today's AI systems.

As we look forward into the near future, it is crucial to **take stock of our existing relevant authorities** that apply to new application areas and leverage the existing strengths of our nation. Understanding and effectively using these existing authorities and abilities will help us move forward and determine which areas require updates or additional focus. To my knowledge, these assessments have not yet been completed.

In the longer term, additional authorities — or even a new agency — may be needed to lead coordination, develop a critical mass of expertise, or improve oversight. A new agency could:

- Check how AI is being used in and overseen by existing agencies;
- Be the first to deal with problems, directing those in need to the right solutions; and
- Fill gaps that existing sector-specific agencies don't cover.

However, Congress should be cognizant of the time and money it will require to stand up a new agency, let alone allow it to gain its political footing in the D.C. bureaucracy. This doesn't mean it shouldn't be done, but it also shouldn't hold us up from taking other action now.

In the case of biotechnology, the primary concern should not be the ease of information access facilitated by chatbots, but rather on strengthening biosecurity regulations that govern physical experimentation and tangible materials, including access to tools and resources like custom mail-order DNA. Currently, DNA synthesis providers are not required to screen orders for sequences of concern, allowing bad actors to obtain materials with minimal oversight. The 2010 Health and Human Services Screening Framework Guidance offers voluntary guidelines for DNA synthesis providers, but adoption remains optional. A more effective approach to risk mitigation would be to mandate screening protocols for all DNA synthesis providers, thereby directly addressing the foundational risk pointed out by the MIT experiment.

Additionally, we can and should develop emerging technology-aware talent. Doing so will take time, but we cannot afford to underutilize our human capital and it is this long horizon that requires us to act now. Congress can help right away by facilitating a targeted high-skilled immigration program and incentivize efforts to advance general AI literacy, grow more STEM talent, and promote certification programs within the United States. While most of these ideas are focused on AI, many of these same principles apply to cybersecurity talent and the broader biotechnology workforce.

3. **Are our plans, authorities, and tools easily adaptable if and when the landscape changes? Do we have the information necessary to know when that adaptation needs to happen?**

Finally, we need to be prepared to adapt these plans as technological breakthroughs occur or as the threat environment changes. In order to adapt to new information and update our priorities based on changing landscapes, we need a dedicated monitoring capability that tracks emerging technology developments, both here and abroad. A well-funded, decision support capability (see an early proposal) using publicly available information can tell us things like:

- Who has essential capabilities in vital research and the transformative knowledge poised to change the emerging technology landscape;

- What problems our adversaries and competitors are funding and trying to solve and what this tells us about their strategies and priorities;
- Where new technologies are being applied, such as the use of AI in genetics or other fields, where risks might be particularly concerning;
- Talent development trends, including what fields are attracting talent and where those skilled workers are going to work after they receive their education and training, both in the United States and abroad; and
- The makeup of supply chains and any associated checkpoints that jeopardize our security or that we can leverage toward others.

Then we need to be able to effectively coordinate information sharing and policy adaptations across agencies, based on the information provided above. This requires resourcing and expertise embedded in core government functions, as opposed to being only run by time-bound political appointees.

Finally, asking these questions is not a static exercise and constant reevaluation is needed. What may be lower priority today can easily jump toward the top of the list next month or in two years. Given the sensitive and often long-lasting nature of government communications, it is prudent to continue the transition to data encryption methods that cannot be easily cracked by quantum computers and ensure that the attention paid is proportional to realistic assessments of opportunity and risk.

For this and other topics not prioritized today, the technology monitoring mechanism can ensure we are tracking technological progress and limit the possibility that we are surprised by major breakthroughs.

Conclusion: Agility and Vigilance is Key

In conclusion, our approach to emerging technologies and their impact on national security must be agile, adaptive, and action-oriented. We can't afford a "set and forget" mindset; we must be prepared to continually adjust our strategies as technologies evolve and the global threat landscape shifts. Different nations and actors have unique motivations, which could influence technological developments in ways distinct from our own. We need to be vigilant in monitoring these variances and ready to prioritize and de-prioritize as things shift.

A practical way forward is adopting an iterative strategy: take small steps, evaluate their effectiveness, learn from the results, and then take the next steps. This is not just an operational recommendation but a call to invest in analytics. Better data and insights will allow us to make more informed and timely decisions, effectively allocate resources, address regulatory gaps and build a robust talent base.

By committing to a continuous learning process, we ensure that our approach remains nimble and responsive to the rapid developments in technology that we're bound to face.

Thank you.