Stenographic Transcript
Before the

Subcommittee on Cybersecurity

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON
ARTIFICIAL INTELLIGENCE APPLICATIONS TO
OPERATIONS IN CYBERSPACE

Tuesday, May 3, 2022

Washington, D.C.

ALDERSON COURT REPORTING
1111 14TH STREET NW
SUITE 1050
WASHINGTON, D.C. 20005
(202) 289-2260
www.aldersonreporting.com

HEARING TO RECEIVE TESTIMONY ON ARTIFICIAL INTELLIGENCE APPLICATIONS TO OPERATIONS IN CYBERSPACE

Tuesday, May 3, 2022

U.S. Senate
Subcommittee on Cybersecurity
Committee on Armed Services
Washington, D.C.

The subcommittee met, pursuant to notice, at 2:43 p.m. in Room SR-232A, Russell Senate Office Building, Hon. Joe Manchin, chairman of the subcommittee, presiding.

Committee Members Present: Senators Manchin, Blumenthal, Rosen, Kelly, Rounds, Ernst, and Blackburn.

OPENING STATEMENT OF HON. JOE MANCHIN, U.S. SENATOR FROM WEST VIRGINIA

Senator Manchin: The meeting will come to order.

I want to extend a warm welcome and thanks to our distinguished witnesses today, who have all taken time out of your important duties for your companies and academic institutions to help educate all of us the Cyber Subcommittee of the Senate Armed Services Committee on the application of artificial intelligence and machine learning technology to the critical missions of offensive and defensive operations in cyberspace.

Artificial intelligence and machine learning are extremely technically complex topics so I would highly encourage our witnesses to provide as many real-world examples as they can. What I am saying is bring it down to our level, okay --

Senator Rounds: All the way to kindergarten?

Senator Manchin: Might have to -- in your answers and simplify technical concepts as much as humanly possible for the benefit of the members and the public that are viewing this hearing.

I cannot overstate our need for AI application in cyberspace operations, and I believe our witnesses' prepared statements will eloquently express your sentiments.

There is a huge shortfall of technically trained

cybersecurity personnel across the country in government and industry alike. This shortage is likely to continue to worsen, especially as cyber threats intensify in scope and scale. Keeping up with the demand of capacity in this field will therefore require massive gains in workforce productivity, which, practically speaking, means automation by computers. AI technology can power this automation and productivity growth.

Not to belabor the point but China has four times our population. There is no way we are going to win a competition in manpower, or woman power, or person power that can be dedicated to an important mission. Computer-driven automation powered by superior software innovation is the only option that we have. As Dr. Moore wrote in his prepared statement, with AI the work of 5,000 people can become the equivalent of 50,000 people.

Additionally, AI can discover subtle signals and patterns of malicious cyberattacks in a sea of noise better and faster than humans. AI can also help to automate actions to contain and eradicate cyber penetrations.

Commercial computer-aided intrusion detection technologies that are widely used today already process enormous quantities of data, provide alerts to human analysts of suspicious actions and anonymous events. But these products generate enormous numbers of false positive

-- false alarms, if you will. So many, in fact, that our analysts are overwhelmed and cannot possibly investigate them all. This is why we fail to find the genuine needles in the haystack, even when they may be noted by our security event management systems. AI, however, will increase the rate of detection of real intrusions while lowering the false alarms.

AI, in short, can enable our cyber forces to achieve scale and speed in defensive cyber operations. The flip side of this is that AI can also tremendously benefit the offensive side of cyber operations. Just as AI algorithms can scan our own networks for vulnerabilities, they can discover vulnerabilities and attack vectors and adversary networks that we can exploit.

Make no mistake. Our adversaries will capitalize on this technology, using AI to power attacks on our networks as well as increasing their ability to detect our intrusions on their networks and to respond quickly. We can use the Russian SolarWinds attack to illustrate the potential danger. The SolarWinds software supply chain operation compromised thousands of networks, but the Russians can only manually exploit a limited number of the targets they infected.

However, the use if AI technology in the future will enable Russia or China to take advantage of every target

that they compromise. It would be disastrous if we failed to be ready. Yet, while the Defense Department is developing AI applications for business efficiencies and warfighter support, I fear we are not moving at the necessary speed in cyberspace.

Commercial cybersecurity companies have, for a number of years, been developing and applying AI technology to their products, and the Department of Defense is benefitting from that investment. Microsoft's Defender product is a good example.

A direct DoD investment in cyber AI is lagging. I look forward to hearing recommendations from our witnesses on what we could be investing in and where we need to focus our attention.

So I turn now to my friend, Senator Rounds, for his remarks.

STATEMENT OF HON. MIKE ROUNDS, U.S. SENATOR FROM SOUTH DAKOTA

Senator Rounds: Thank you, Senator Manchin. First I would like to thank our witnesses for appearing at our hearing today.

The topic of today's hearing is one that is of particular interest to me. Over the last few years this subcommittee has witnessed firsthand, at our many hearings and briefings, how dynamic and rapidly evolving the cyberspace domain is. New technologies are emerging all the time, and that is a good thing, but it also poses new challenges. Malicious cyber actors have demonstrated time and time again how quickly they can exploit these new technologies to attack our systems and infrastructures. The Department of Defense must move just as quickly to understand these emerging technologies, both to provide our United States Cyber Command with cutting-edge capabilities for their cyberspace mission and also to defend against these technologies being used against our nation. I cannot think of a technology that will have a broader impact on cyberspace than the application of artificial intelligence or AI.

I would like to share an excerpt from the final report of the National Security Commission on AI -- this is the NSCAI -- which captures the landscape nicely. And I will

quote:

"AI-enhanced capabilities will be the tools of first resort in a new era of conflict as strategic competitors develop AI concepts and the technologies for military and other malign uses and cheap and commercially available AI applications, ranging from deep fakes to lethal drones, become available to rogue states, terrorists, and criminals. The United States must prepare to defend against these threats by quickly and responsibly adopting AI for national security and defense purposes.

"Defending against AI-capable adversaries operating at machine speeds without employing AI is an invitation to disaster. Human operators will not be able to keep up with or defense against AI-enabled cyber or disinformation attacks, drone swarms, or missile attacks without the assistance of AI-enabled machines. National security professionals must have access to the world's best technology to protect themselves, perform their missions, and defend us. Put simply, our adversaries are going to use AI against us, so we must use AI to defend against them."

I look forward to hearing from our witnesses today. But to begin with, I would like each witness to give a short, basic introduction to AI that will help us understanding these technologies better and help us describe these issues to our Senate colleagues so that we can have

the policy discussions that need to be completed. Please give us a short overview of the difference between a normal computer program, machine learning, artificial intelligence, and quantum computing.

Now I know that sounds like a crazy thing, but clearly if there is anybody that can do it, I would just ask you to keep down at like our kindergarten or first-grade level.

I would also like to hear from the witnesses on their perspectives of the current state of adoption of AI technologies in industry to defense against AI-capable adversaries. How are your companies leveraging AI today to defend your cyberspace infrastructure? How do you think the Department of Defense needs to leverage AI for their cyberspace missions? I would appreciate your thoughts on the best ways to leverage AI-enabled cyber defense to protect against AI-enabled cyberattacks.

Thank you again to our witnesses for coming here today. Senator Manchin.

Senator Manchin: Thank you, Senator Rounds. Before I begin I want to recognize you three for being here, and I really, really appreciate it. I think it is tremendous. It will be a tremendous hearing here.

We have Dr. Eric Horvitz. He is a Technical Fellow and Chief Scientific Officer for Microsoft. We have Dr. Andrew Lohn, who is the Senior Fellow for Security and Emerging

Technology at Georgetown University. And we have Dr. Andrew Moore. He is Vice President and Director of Google Cloud Artificial Intelligence at Google.

So we look forward to hearing your updates and we will start, Dr. Horvitz, with you.

Mr. Horvitz: Thank you. Let me first answer the overview question.

AI systems are programs, just like any other computer software, but they are special in that they are designed to emulate aspects that we would call human intelligence. So what are the capabilities we recognize as intelligence? The ability to perceive, to see and hear; the ability to reason about situations, for example, by considering multiple pieces of information or observations; the ability to make good decisions, even where uncertain; the ability to adapt to learn from experiences and information over time; the power to use and understand language; and other capabilities that are a little bit more nuanced, like the ability to generalize from specifics, to form useful abstractions about the world. So AI scientists write programs to emulate these capabilities of intelligence.

And I should say that there has been progress on all those fronts that I just mentioned, all those dimensions of intelligence. But over the last 20 years we have seen an absolute revolution in the learning part. This is the

learning part of AI and it is called machine learning. So it is a part of the larger discipline of artificial intelligence. It is one sub-area but it has come to be so important in supercharging the other areas, including computer vision, language abilities, speech recognition, and so on.

Now quantum computing is a very different thing. Quantum computers harness quantum physics to computer, that use behaviors seen on a microscope scale, behaviors discovered by physicists with interesting names like "superposition" and "entanglement." And to clean up any potential misconception, or a broad one, successes in quantum will not give us general purpose computers. A quantum computer solves special kinds of problems, like factoring large numbers, critical encryptography. So working quantum computers, when they come to be, at scale, will be able to solve extraordinarily hard problems in those areas that they are great for, thus, for example, breaking current cryptographic protections, which makes them of very deep interest for national security.

Senator Rounds: [Presiding.] On behalf of the chairman, thank you very much. I appreciate it. Did you have anything else that you wanted to add before we move forward?

Mr. Horvitz: Well, I can answer your second question.

I guess you asked a very broad question about what companies and enterprises are doing to protect themselves right now.

You know, we are building infrastructures, and I would love to see more effort in DoD and other Federal agencies, infrastructures that go from being able to sense across many computers for patterns, being able to collect that data across the world, for example, and across organizations, of course, to employ machine learning on the infrastructure, to build predictive models, and to build filters and detectors.

We have to have a great workforce of professionally trained cybersecurity experts to work with these AI systems, because despite what we think about AI, the big gain is going to be in human AI iteration and collaboration. So we need those teams, no matter how good our AI is. And lastly we need to have a system of pushing out updates quickly, to make patches and to stay in touch with end users.

Senator Rounds: Thank you. On behalf of the chairman, and he shall return very quickly. Dr. Lohn?

STATEMENT OF ANDREW LOHN, PhD, SENIOR FELLOW, CENTER FOR SECURITY AND EMERGING TECHNOLOGY, GEORGETOWN UNIVERSITY

Mr. Lohn: Thank you. I would like to start by thanking Chairman Manchin and Ranking Member Rounds and the members of the subcommittee. Thank you for inviting me to be here. I am Andrew Lohn from the CyberAI project at the Center for Security and Emerging Technology at Georgetown University. It is an honor to be here.

When we talk about AI, to answer your question, I like to use the Defense Science Board's definition. They say the capability of a computer system to perform tasks that normally require human intelligence. As an example, accounting software used to be AI when tax filing normally required humans, but now it is so common that it is no longer considered AI.

But if AI is about what software can do then machine learning and normal programs are about how that software was made. For normal programs, somebody writes all the logic themselves -- if this, then that, many times. For machine learning, nobody sets those if-then rules. The computer determines them after many examples.

Quantum computing is, as Dr. Horvitz said, kind of a different sort of process that touches a little bit on normal computer programs, machine learning, and AI, but is mostly separate.

With that background in hand, I would like to talk about three areas where AI intersects with cybersecurity: one, how AI promises to improve cyber defense; two, how AI may improve offensive cyber operations; and three, how AI is itself vulnerable.

AI for cyber defense is not a new concept. Spam and anti-phishing filter have been protecting users for many years, and AI has long been touted as a tool for companies that hunt for malware or search for intrusions. Some of these techniques have become the foundations of modern cybersecurity. But in general there is a back-and-forth. Whereas an AI learns attacker tactics, the attackers adapt their tactics to evade that AI.

To date, those attacker tactics have not relied much on AI. That is likely because so much has already been automated. A human can direct a computer to find possible targets on a network, then direct it to exploit those targets, then delist the files or folders to encrypt or extract. The human really only has to manage the system while the computers already do most of the work.

That said, there are reasons to automate attack code. In 2015, when Russia first cut power to Ukraine, the hackers had to take over the mouse and manually shut down the grid. By the next year they developed new malware that had more automation.

And an attacker may just simply want to operate a machine's speeds. In 2016, DARPA hosted the Cyber Grand Challenge, where fully automated systems competed to secure themselves while breaking into each other. These systems relied more on hard-coded rules than machine learning, but they were impressive. The winning system competed against some of the world's top humans the following day, and though it ultimately finished last there were times where it was leading some of these human teams, which is an impressive result in only its first year.

This was the first and last such challenge in the United States, but China was struck by the potential and has hosted at least seven of their own autonomous hacking challenges since. It is unclear how capable their systems are, but it is clear that both China and Russia are working to develop software that can discover vulnerabilities and in some cases run their cyber offenses more autonomously.

AI systems are technological marvels but they too are software with their own vulnerabilities. Most famously, it is easy for an attacker to change just a few pixels in an image to make a detection system to stake objects it is looking for. It is easy to imagine these techniques disguising parts of an invading force or directing drones or coastal defense systems to the wrong targets. It is even easier to envision digital decoys that overwhelm that

system. It is not clear how susceptible these systems are in the real world yet, but we may soon find out as countries rush to deploy autonomous military capabilities.

But rather than wait for our systems to be deployed, our adversaries may target the AI supply chain. Our systems are often merely adapted from existing ones that may or may not be trustworthy, and the data used to train or adapt those systems can be compromised too.

Today, most of the models, datasets, and tools are provided by trustworthy organizations such as those represented by Dr. Horvitz and Dr. Moore. But China, in particular, is making a push to provide more of these resources. If they succeed, then DoD would face an unwelcomed decision between using the most capable systems or the most trustworthy ones.

I do not wish to overstate the impact of artificial intelligence on cybersecurity nor the severity of the vulnerabilities in AI. I only hope to alert you to the potential that is being developed. Our adversaries are highly capable and grow more emboldened every year, and they have been developing increasingly autonomous attack software. Similarly, although we have seen only a few attacks directly on AI systems, the potential is no secret. Our adversaries are surely aware of the vulnerabilities, and we should expect attacks as soon as AI systems prove their

value on the battlefield.

Thank you.

[The prepared statement of Mr. Lohn follows:]

Mr. Horvitz: Senator Rounds? Just to ask courteously, I thought you were asking us to go round robin on your special questions first, but I have a prepared statement as well.

Senator Rounds: Oh. That was your question, was it not?

We will go to Dr. Moore and I will come back to you.

Mr. Horvitz: Thank you very much.

Senator Rounds: Dr. Horovitz, I am sorry.

Dr. Moore?

STATEMENT OF ANDREW MOORE, PhD, VICE PRESIDENT AND DIRECTOR OF GOOGLE CLOUD ARTIFICIAL INTELLIGENCE, GOOGLE CORPORATION

Mr. Moore: Thank you very much, Chairman Manchin and Ranking Member Rounds, and members of the committee. My name is Andrew Moore. I am Vice President and General Manager of Google Cloud AI. I most recently served as a Commissioner with Dr. Horvitz on the NSCAI, and I previously served as Dean of Carnegie Mellon University, which I cannot help but mention, won the grand challenge of which you spoke.

[Laughter.]

Mr. Moore: I really want to thank the committee's support for advancing artificial intelligence.

Chairman Manchin, you have really supported the relationship between National Science Foundation and West Virginia University. I really respect WVU, and I go there frequently. It is a really great asset.

And Dr. Rounds, as Ranking Member Rounds, thank you for your support of actually doing AI baselining at the Department of Defense. This really, really matters, so thank you for that. I greatly appreciate all the support you have given to NSCAI's recommendations as well.

My colleagues nicely defined AI. I am going to just leave it simply that AI refers to technologies that can make

decisions from billions of possible alternatives in almost real time, and modern AIs do improve themselves are they are doing this.

I want to give you a tangible example because that is what Chairman Manchin asked for. If I am lowly drone trying to attack a U.S. battle fleet -- and this is a hypothetical, non-classified example -- if I am a lowly drone trying to attack a huge battle fleet you might think I have got no chance because I am so outgunned. But suppose I can search, in the space of a second, over a trillion possible trajectories, misleading directions relative to the sun, deal with all the various possible other tricks, maybe even a flock of seagulls, at the same time. I have got this advantage that I am not fighting against a battle fleet. I am fighting against the worst-case scenario out of a trillion scenarios for that battle fleet. So that is what the power of AI is. It is where we have these supercomputers, so superhuman abilities to search lots of alternatives.

AI powers many of our products, and we are using it to help organize the world's information. For example, AI is used to help you predict the best route in Google Maps. Many of our Google Cloud solutions are used by the Department of Defense. One of my favorite examples is our partnership with the U.S. Navy, where autonomous drones are

able to take pictures of corrosion on the sides of warships and quickly and efficiently inspect what is at most danger, what needs servicing as quickly as possible. This not only saves a large amount of repair money but it helps keep us in better readiness than we would otherwise.

There are many other examples of our work with DoD, and I think it is fair to say that all the large what we call hyperscalers, the big internet companies, are proud of the opportunity to help serve the U.S. government.

Now I have got to talk about cybersecurity. Cybersecurity, as my colleagues have mentioned, is interesting because everything happens just so fast. And Google has a huge network which is being attacked all the time from huge numbers of places, including many state actors, so we have to have everything we can do to secure it.

What we have done is a pattern that I see developing in the DoD. I strongly recommend it. I am going to sort of highlight it now. There are three parts to it. The first one is using AI to defend against attacks, the other two are how we organize the data and people in the Department of Defense.

Using AI to defend against attacks, first, the most obvious one that I have already kind of illustrated is you want to be watching millions of possible attacks, known

attacks, every second, looking out for all of them. That is the basic one, and that is where you cannot possibly afford to use humans for that. Things are happening too fast.

The second one, which is interesting, is emerging attacks, people ingeniously coming up with new methods, and AIs are coming up with new methods, so you have to be learning new patterns or detecting whole new kinds of attacks in real time. This is where the full power of adversarial AI comes in.

Finally, while you are doing all of this on your perimeter you have got to be ready for the insider threat. So artificial intelligence is extremely important and it plays a large part in conjunction with the Zero Trust approach that the Department of Defense has brought in. That plays a large part in how to deal with the very real, unfortunately, insider threats, looking to see strange human patterns.

I cannot resist following up on one of Chairman Manchin's comments about we are building these AIs on the other side of building these AIs. New technologies, which I would like to make sure that the government is aware of, are things you will see, for example, in poker-playing robots. One of these championed at Carnegie Mellon University, which are using the work of mathematician John Nash to solve game theory games. And the important things about that are AI

are aware of the facts that the other person is learning from them at the same time they are taking their actions, and the AI cannot just automatically do the most obvious thing, because it actually has to conceal its activities.

So National Science Foundation is funding this kind of research into very advanced AI, and it is very important that we do not ignore that aspect.

I want to talk about the second part of all of this, which is the data inside the Department of Defense. It is not okay if there are lots of different silos of data. We need, especially in certain major scenarios, we need something to have a full understanding of what is going on, and to do that it is not okay for people to need to pick up a phone call, to phone to ask for help from a different set of sensors or a different database somewhere else.

So the notion of using concepts such as knowledge graphs to join together information from many different sources of data to form a more complete picture, extremely important. For example, I am extremely supportive of the Joint All-Domain Command and Control, JADC2, which is seeking to do this by allowing information sharing through interfaces and services across all domains.

AI without data these days is pretty worthless, and so the absolute importance of getting through the sort of social or organizational hurdles, for people to share

information about threats, is essential.

The final thing I want to quickly mention is humans and machines working together. I know that there are bills which advocate for a cyber reserve unit, for example, and thank you for those. I strongly support that. As it comes in, the people that we are putting on the frontlines with AI need powerful tools designed for humans to work with machines. And many of us in industry are working incredibly hard at the moment to make sure that those tools are usable by folks trained up to become an AI force as easily as possible. So we have put lots of effort into AI platforms which help guide users to quickly be able to respond and work on new and important AI issues as they come up.

Let me be clear about what I mean here. If we get a threat, some major, new attacks surfaces, and we have to get together a whole bunch of people to deal with it, that is done in an hour or so, at the very latest, and you immediately have people with the tools, who know how to use them, to combine the data to build a system against some new threat in ideally less than a day, and within a week or two all you are doing is double-checking the patches and doing postmortems to make sure it never happens again.

The nightmare for me is if, instead, the U.S. government ever found itself in a position it said, "Hey, this is not really working. We better start a procurement

process to find a contractor to bid on solving this thing." I strongly believe you actually need people in the Armed Services with the capabilities to get on this stuff right away.

So with that I again want to express my appreciation. I have a lot more thoughts on this.

Senator Manchin: We are going to have questions for you too, Doctor. We are going to have a lot of questions for you.

Mr. Moore: Great. So thank you for the opportunity, and I look forward to helping continue work with Congress on this issue.

[The prepared statement of Mr. Moore follows:]

Senator Manchin: [Presiding.] Thank you, sir. Thank you.

Dr. Horvitz, I am sorry we misinterpreted. I thought that is where Mike was coming.

Mr. Horvitz: Yeah, so did I.

Senator Rounds: What were you thinking?

Senator Manchin: His intro was so profound that I thought, well, here we go.

STATEMENT OF ERIC HORVITZ, PhD, TECHNICAL FELLOW AND CHIEF SCIENTIFIC OFFICER, MICROSOFT CORPORATION

Mr. Horvitz: So Chairman Manchin, Ranking Member Rounds, and members of the subcommittee, thanks for inviting us today to testify on this important topic. I am Eric Horvitz. I currently serve as the Chief Scientific Officer of Microsoft.

AI researchers and engineers work to automate tasks that are typically associated, as I mentioned earlier, with human cognition, such as perception, pattern recognition, prediction, reasoning, and learning. We are seeing developments in AI now at a pace we could not have predicted just a few years ago.

I will focus my remarks today on three areas that lie at the intersection of AI and cybersecurity" number one, advancing our cybersecurity with AI; number two, malicious uses of AI to power cyberattacks; and three, an interesting area evolving quickly, attacks on AI systems themselves.

First, using AI in cyber defense. It is an exciting area and it is being used today to detect attacks and respond to attacks in real time, at scales that would be nearly impossible with manual techniques. These methods can recognize pattern of activity associated with attacks, they can adapt to new attacks, and detect attacks never seen before by identifying subtle similarities and signals that

adversaries try hard to hide.

AI methods help cybersecurity teams to scale their efforts, which is critically important when there is a global deficit of nearly three million cybersecurity professionals and when cybersecurity job opportunities are projected to grow 33 percent over the next decade.

Second, AI-powered cyberattacks, that is using AI on the offense, is an important area of concern. To date, there is scarce information on the active us of AI in cyberattacks. It is expected, though, that AI technologies will be used to scale cyberattacks and increase their efficacy, and the power of offensive AI, we will call it, has been demonstrated by red teams and a growing community of researchers. So given the pace of AI, we have to prepare ourselves.

Offensive AI spans several areas. Researchers have demonstrated the ability to efficiently guess passwords, to attack industrial control systems, to create malware that can evade detection.

Another form of attack uses AI methods for social engineering. This is aimed at the soft, human side of cybersecurity. The work includes impressive formal demonstrations that show how AI can be used to ultra-personalize phishing attacks on individuals, generating content that compels people, even security experts, to click

on links that emit malware.

Finally, another rising concern is attacks on AI systems themselves, what we call -- and you will hear this over the years -- adversarial AI. These attacks use AI techniques to disrupt the operation of target AI systems or gaining access to their data or processes.

Here is an example about how AI attackers have used AI techniques to fool AI systems, causing the system to fail dramatically. In stunning demonstrations, researchers can make a stop sign look like a yield sign by injecting patterns of dots too fine to be seen by human eyes, into an image. The stop signs look the same but they look differently to the AI system.

The same kind of thing has been done with stealthy audio signals embedded in voice commands, where a speech recognition system hears the commands that the attacker wishes to execute, not what the owner says or hears.

Other types of attacks include methods that steal secrets about the operation of the AI system or the proprietary data that was used to train the system. In another attack, adversaries poisoned the AI systems by injecting erroneous or biased training data into the system.

So to conclude I will highlight five recommendations for you to consider.

One, we need to invest in core R&D on harnessing AI to

push ahead on the frontier of defense and to better understand offenses that will be on the horizon. This includes red-teaming. This is imagining what adversaries can do and developing strategies to protect our systems in advance.

We need to incentivize the creation of cross-sector partnerships to promote sharing and collaboration around data, experiences, best practices, and research.

Three, we need to ensure that AI systems are designed with awareness and best understandings about handling these special adversarial attacks.

Four, we need to develop training programs to educate cybersecurity and AI workforce teams on the special security vulnerabilities of AI systems and their components.

And finally, we need to ensure that DoD and Federal AI agency systems are developed in a secure manner across the lifecycle of these projects to protect the data, protect the executables, and the programs.

Thank you again for your leadership on this important topic and for giving me the opportunity to testify today. I look forward to hearing your questions.

[The prepared statement of Mr. Horvitz follows:]

Senator Manchin: First of all, thank you all so much.

We are going to do rounds of 7 minutes. Being it is just the three of us, I think we will not --

Senator Rosen: My favorite subcommittee.

Senator Manchin: I know it is. I can tell. I mean, Jackie --

Senator Rosen: You are talking my language.

Senator Manchin: Let me tell you one thing. She is ready to -- she might take more than 7. It will be all right with me. But she is ready to go.

Senator Rosen: I have got all the questions.

Senator Manchin: I want to thank all three of you.

I am going to start with simply an overview. We have been hearing an awful lot about artificial intelligence and machine learning. Are they one in the same? That is one thing. You can maybe answer very quickly.

I really want to know, and Mike and I both serve on Armed Services -- this is a subcommittee of Armed Services that all three of us serve on -- where are we in the pecking order of what is going on in this unbelievable world that you are explaining to us? Are we behind? Are we in the hunt? Are we on the cutting edge? What more can we do besides, we know, investing? But we want to invest in the right places to get the best results.

So is the private sector, are you moving us to a

position to where -- I will use the whole SpaceX program, what they have been able to do in the private sector for the defense of our country and the amount of money we have saved because of the efficiency of the private sector? Can that be duplicated here, in artificial intelligence and machine learning, better invested in? Because we are contracting, as the Federal Government, for our defense programs, with SpaceX, putting different types of articles that we need in space, as you know.

So with that, we can start, and we will start, Dr. Moore, if you can, and keep them fairly concise, if you can, in your answer, because everyone has an awful lot of interesting questions.

Mr. Moore: Thank you, Chair Manchin. Yes, I will be concise. Artificial intelligence without machine learning gave us things like Deep Blue, where the American IBM computer Deep Blue beat the Russian chess master Kasparov, Gary Kasparov, back in the 1990s. We were all so happy about that in the AI world.

But these systems did not adapt over time, and so that is why machine learning, in the early 2000s, has come in and made AI much more powerful than it was in the days of Deep Blue.

Senator Manchin: So basically it has been integrated into one? It is all one, AI and machine learning is now

integrated as one?

Mr. Moore: That is right. In the old days you could have AI without machine learning. These days you always want AI with machine learning.

Senator Manchin: And on the other, real quickly, on the other, where do we rank? Just give me a ranking. You do not have to name countries, but are we behind in the hunt or are we on the cutting edge?

Mr. Moore: We are ahead. We are losing ground. I am most worried about our structures. Bringing in massive scale, super-human automation means changing organizational structures and change management. That is what I believe companies are really quite good at.

Senator Manchin: You all can do it better than we can do it in the government, is what you are saying, and we can contract out in a very secure situation, like we do with some of our defense. Okay.

Mr. Moore: Perhaps, yes.

Senator Manchin: Dr. Lohn?

Mr. Lohn: Thank you, Senator Manchin. I would like to concur with Dr. Moore that AI is like a broader umbrella that has machine learning within it as a component. Now I understand the confusion because those two terms have become almost synonymous because almost all of the AI that we talk about today is machine learning, but in the past there were

other techniques that were not machine learning, so right now they are basically the same thing. And it may be that machine learning will not be the same as AI in the future, but right now they are basically the same thing, and now machine learning is a small subset of AI.

With respect to are we ahead or behind --

Senator Manchin: Can you evaluate what is going on? I am sure you all have interaction with your colleagues around the world, in different countries, whether they are adversaries or allies. The scientific world seems to cross over pretty -- I wish we could do as well as you all do in that arena.

Mr. Lohn: Yes.

Senator Manchin: How do you evaluate it?

Mr. Lohn: I have tried to study this directly, and U.S. is ahead. China has been gaining. We still have an innovation lead, I am confident to say, and we also have companies like those represented here that give us a huge leg up.

What I would like to point out, from a DoD perspective, is that the DoD has an opportunity to step ahead of industry in the adversarial context. A lot of the time my co-panelists here are developing products that do not have a natural adversary trying to mess with them, but the DoD does. And so that is a place where we really need to focus

a little bit further on what is somebody going to do to subvert our systems as we deploy them.

Senator Manchin: Dr. Horvitz?

Mr. Horvitz: First let me say that the people in the other fields of AI love machine learning but they have all existed side by side since 1956, when the first proposal was written about using the phrase "AI" for the first time. Machine learning has gained but it is simply -- well, I should not say "simply" because it is important -- a part of AI. It is not separate. It is one of the important disciplines within AI. That is the way AI researchers view machine learning.

Now it has grown up to be a very big discipline because almost every other discipline leverages the advances in that field, which are moving very quickly.

The U.S. is leading in science at the core principles and creative applications, from my point of view. That said, these days technical advances spread around the world like lightning. So at the scientific frontiers of IC scientists really keeping pace with one another around the world, there are issues around who has the right resources to do the computation that is needed, because these models are getting bigger and bigger and they are showing with getting bigger, that we do not see any leveling off just yet. You need tremendous amounts of compute for that kind

of thing. There are probably two places in the United States that can compute like that and a couple in China right now.

So thinking about the resource constraints, especially on academic researchers, to push on the research is a very, very important direction.

The private sector is kind of like SpaceX in some ways. Microsoft, for example, is building platforms and tools, and it is working with customers in the Federal Government as well as in civil society and the private sector to understand what it takes to field these applications and technologies.

The one place that I worry about Federal applications in DoD is integrating in these scientific achievements into real-world workflows. I think the devil is in the details there. It gets into lots of engineering, human AI, human factors and human AI collaborative approaches. We need to get our hands dirty and work hard and then share ideas and insights across the sectors.

Senator Manchin: Thank you all so much. And then just one final one. I will say, respectfully, all three of you are working with Federal Government and with the Department of Defense and being able to harden, basically making sure that we are not going to be hacked or the information we have is being protected. I would assume you all have done

that, and we will talk about that more too. But I just wanted to make sure about that.

Senator Rounds.

Senator Rounds: Thank you, Mr. Chairman. Look, first of all, let me just say thank you very much for taking the time to come in and visit with us today. I think part of the challenge we have here is trying to explain and to express to other members here in the Senate just how serious the threats are but also how great the opportunities are, and the recognition that AI is not something that is 10 years away. It is here, has been here, and it is embedded in a lot of the things that we do right now.

Dr. Moore, I direct this question to you, due to your experience as the Dean at Carnegie Mellon University, but welcome all panelists to respond.

According to an article dated April 13, 2021, in The New York Times, a majority of the AI engineers working in the United States are from China and studied in China. I understand that some of the best programs in AI are at universities in China and they are graduating students at record rates. How can we replicate the same types of success at U.S. universities, especially in places like South Dakota, where we have Dakota State University and others that really do have experience in cyber but they want to continue and grow it? How do we take the next steps to

really develop that capability here?

Mr. Moore: Thank you. A very important question, and I think there is some good news, that for us in the cloud sector the democratization of AI, so that we can have large groups of students learning about it all throughout the United States, has been a major part of our roadmaps. It actually does not work to anyone's interest in the United States for it to only be this small group of like 100 PhDs each year who come out with these skills.

So we are all in the commercial sector working on making it faster and faster and easier for folks to get up the training so that they can use AI usefully in their own jobs. I see it as being incredibly important for the work that we are doing with things like reserve programs and information technology or Cyber Reserve Corps for us to be taking those programs, to train people up using these democratized AI tools.

Senator Rounds: Thank you. Dr. Lohn?

Mr. Lohn: Thank you. I would like to maybe make two points, is that AI and cybersecurity are both getting easier to learn. When I started, not that long ago, it was very difficult. You had to go through a lot of math and build things out all from scratch. But now there are many tools and many learning resources available. And so I think that we have an opportunity to pull people through our industry

giants but also to bring people through armed services, in the enlisted ranks as well as the officer corps, I think we can push for the development there and create these opportunities for servicemembers to have those skills while they are in service and then also to take them elsewhere.

Senator Rounds: Thank you. Dr. Horvitz.

Mr. Horvitz: First let me say that I am proud that this country is still the world's talent magnet. We have built our country on that and it is fabulous we continue to act in that way and to serve in that role.

That said, we can do a lot better with educating our folks. Community college programs are really fabulous and they can use investment, fabulous faculty, and tools from industry and academia. There is a great deal we could do all the interesting skilling programs that are post-graduate skilling programs, online coursework we can invest in. The tools are becoming more usable and many companies are providing beautiful self-help, self-learning programs to use the tools.

I would like to say that we have new applications of AI even. For example, Microsoft has in private preview a project called Copilot that helps developers learn to code, gain insights about coding, and also having an AI coding companion. We are seeing it in private preview how much this is helping coders right now move ahead and become

better as a team with the AI system.

So I think that I am optimistic, but I think we can do better.

Senator Rounds: Thank you. Just a question. With regard to the Department of Defense, if you were to grade the Department of Defense in terms of their ability so far and where we are at with regard to the application of AI in multiple application opportunities, what grade would you give the Department of Defense in their implementation and utilization of AI today?

Mr. Horvitz: Can I just say that I would give most of this country a D, maybe a C minus, given the potential of what can be done. I think about health care and how AI is a sleeping giant for health care, whether it be VA system or other venues.

Senator Rounds: Is it fair to say we could find cures for cancer within 5 years if we would fully implement AI?

Mr. Horvitz: Well, let me just say that advances like AlphaFold and RoseTTAFold are really helping us jump forward in the understanding, for example, of sale of machinery. So I am optimistic. I cannot give you a time that we will understand cancer one day, as a running computer program.

But let me back up a bit and talk a little bit about the possibilities for the Department of Defense. We often think about AI, even in your opening comments, which were

fabulous, as on the battlefield, as kinetics. But DoD is a huge operation, in peacetime and in war. The logistics, planning, predictive models, employment, back to health care, the VA system all can benefit greatly by even basic applications of machine learning, predictions, diagnoses, and planning.

So I do not want to call out the DoD as failing when I see them doing fabulous work and really working to get on board quickly and doing some of the most enthusiastic and energetic catch-up right now of any organization. But this whole country can do better.

Senator Rounds: I enjoy it when you say the basic application of machine learning. Dr. Lohn?

Mr. Lohn: I am not quite as pessimistic as Dr. Horvitz, although he certainly has reason to be. I hesitate to give a letter grade but I would not put it quite as low as a D. I think that, as you mentioned at the end of your answer, that they have been doing a great job of catch-up. They have been very enthusiastic within the DoD to adopt and develop technologies and have been trying things and fielding them quickly.

I would like to point out also they have a difficult situation as compared to many other people trying to field AI because of the adversarial and permissive environment that they are trying to do it in.

Senator Rounds: Thank you. Dr. Moore, I am out of time but do you want to try to give me a quick shot on it?

Mr. Moore: I will give you a super-quick answer. the way that we are structured with such brilliant individuals within the U.S. military who are willing to try new things is fantastic. But I am really, really worried if I do not see a concerted effort but instead just lots of talk.

I was very encouraged by the creation of the new Chief Data and Analytics Officer under Deputy Secretary Hicks. I wish that person great success. This is how we are going to succeed is by having a centralized effort to put an artificial intelligence strategy across the whole DoD.

What I worry about, frankly, and what I would be really worried about for this individual is whether they are going to get enough support from the government and from the center of DoD to actually make changes that are needed, because you cannot just magic AI on top of existing systems. You have to think about how you are going to change operations. So please give support to your central AI leaders.

Senator Rounds: Thank you. Thank you, Mr. Chairman.

Senator Manchin: Thank you, Senator. Senator Rosen.

Senator Rosen: Well I have been so excited to sit here and listen to all of this because as a former coder I started in the '70s, '80s, and '90s, I wrote a lot of if-

then code, so I think it is a good thing that we have moved a little bit forward.

To Senator Rounds, how do we get people going? We have got to start K-12 as early as possible, like my Building Blocks of STEM Act that was passed into law. You have got to start the pipeline as early as you can to excite people about these jobs.

And Dr. Moore, all of you, thank you for mentioning my Cyber Ready Reserve Act, my Cyber Ready Workforce. How do we surge up the resources from public-private partnerships like we do with our other military reserves? And, of course, we started the Junior ROTC. We are giving them a STEM track as well, so young kids in high school can see themselves doing this and serving in the military.

So I appreciate that, and I do think our challenge is to be sure that we bring these very complex ideas down to something tangible that people can really understand, because they are very, very complex and it is important that we all have a platform, a shared platform, to talk about them in the same way. And that is our challenge today.

But I want to talk just a little bit about international partnerships, because we do have to maintain our technological edge. We have to advance our competitiveness in relation to China and others, and we must act -- well, we have to act yesterday. I mean, time is

moving. And so as the National Security Commission on Artificial Intelligence pointed out we have to leverage all of this.

I did join Senators Rubio, Cantwell, and Blackburn in introducing the U.S.-Israel AI Center Act, and that is bipartisan legislation to create that artificial intelligence collaboration between the U.S. and Israel, and Israel is an emerging hub for these technologies.

Dr. Horvitz, can you talk about how we can work with our international partners, because this does not happen in a vacuum? You mentioned silos across DoD or private-public and other countries. We know that this quantum computing, these complex problems are best when data is not siloed.

Mr. Horvitz: In the National Security Commission on AI we focused a bit of our time on opportunities for international coordination among allies and like-minded nations, including sharing technologies, data, both in research and engineering as well as for operations. Lots to be said about that and I am very excited about the possibilities there.

There is particular interest, for example, in some of the work that is going on in companies as well as was pointed out on the National Security Commission also on the JAIC, the Joint AI Center in DoD, on responsible development and fielding of AI technologies, fielding technologies that

are resonant with the United States' democratic values and principles. It turns out that AI can act in different ways in the world. Bias can be unexplainable. Its use can be a challenge to civil liberties. And the U.S. can be a leader among nations in thinking through how do we actually field these technologies in a way that resonates and is in accordance with our approach to democracy, human rights, rule of law?

Senator Rosen: Thank you. I want to continue to build on that, so for Dr. Horvitz and then Dr. Moore, you both served on these commissions. And the National Security Commission on AI called for a $20 million increase to DARPA for AI-enabled cyber defenses. So I know how AI can be applied to detect malware and pattern recognition. Can you talk about how that really works? So right now we see the conflict in Ukraine with Russia. We are bracing ourselves for shields up, as CISA is telling us, for cyberattacks. So can you just try to explain to everybody here a little bit how that pattern recognition works?

Mr. Horvitz: I can jump in on a recent situation in Ukraine.

Senator Rosen: Thank you.

Mr. Horvitz: Microsoft detected, with a neural net model, a piece of malware that was related to a known piece of malware, attributed to a group that we refer to as

Iridium -- it is also called Sandworm by other teams -- based in Russia, that put on machines in Ukraine software called wiper software, that wipes the drives clean.

We detected this and immediately dispatched patch and alerts to the Ukraine to protect their systems. And interestingly, what we are seeing in Ukraine -- we just fielded a report a week and a half ago on what we are picking up from our signals in Ukraine -- interesting signs of where the world is going with hybrid warfare, with coordinated attacks, kinetics plus cyber, that are not just associated in time but they are planful, where there will be an announcement about dissatisfaction with disinformation, machines being locked out in a broadcasting station in Kyiv, and then missiles hitting that station. Hybrid warfare, planful and deliberate. We have to look out for that and begin to plan for it.

Senator Rosen: And so that, of course, goes to the workforce because you need people, not just coders, not just engineers, you need a really robust workforce in every area of the network to do that -- oh, I have just about a minute -- so that goes to the cyber workforce shortage. We really have to do a lot. It is a huge spectrum. Most people do not understand. They see your PhDs and they wonder what are the 2-year degree or certificate or apprenticeship jobs.

So can you talk about the jobs, the 600,000 jobs that

are open in cybersecurity now, the kinds of things that somebody who is looking for a new job now, or maybe somebody coming out of high school even, can go and begin to get into this field at that level? Maybe you could speak to that.

Mr. Moore: Absolutely. If a student at a community college starts to just learn Python or one of the sorts of basic languages of data science, and then starts to play around with data analysis on projects like that, immediately they are going to find that consulting companies, the big internet companies, and startups are going to be really interested in their skills. And having that applied experience, just downloading from some of the cloud networks, simple AI systems, where you can get up and running in a matter of hours in writing your own machine learning recognition system for computer vision or something.

So I want to see Python taught, followed by a data science class taught, and at that point that person is already very well distinguished for joining an organization which will train them further.

Senator Rosen: Thank you. I think that really is our task, to try to help everybody understand. 600,000 jobs open. Over 3,500 in my state, just in cybersecurity. What does that mean, because I want to plug people into the way that they can do that. So we will speak offline and maybe

some good ways --

Mr. Horvitz: Senator, just to make a comment. About a year and a half ago we opened up LinkedIn courseware to the world, including really rich sets of classes on

cybersecurity, promoted by the (ISC) group, the cybersecurity professional organization, and saw I think nearly three million engagements with the courseware.

So let's think through how we can creatively use our platforms to bring people into the fold and get on the path to becoming cybersecurity professionals.

Senator Rosen: I want people to see that these jobs are for them, not for somebody else. They can all do them. Thank you.

Senator Manchin: Thank you, Senator. Senator Kelly.

Senator Kelly: I see 7 minutes on the clock. Is this a new thing we are doing?

Senator Manchin: If more people come in it will not be.

Senator Kelly: Doctor, Doctor, Doctor, thank you all for joining us.

Dr. Lohn, in 2020, you contributed to a RAND study on the military application of artificial intelligence in which it was stated, and this is a quote, "There is also growing interest in the potential for machines that can find and patch vulnerabilities in friendly systems or find and attack

vulnerabilities in enemy systems. But these applications still cannot perform these tasks at the level of experienced humans." And Dr. Horvitz mentioned dispatching patches and alerts to Ukraine. I imagine that was done with people.

So understanding that this technology is constantly evolving and maturing, are we any closer to leveraging AI to assess and either patch or exploit vulnerabilities in friendly or enemy cyber systems?

Mr. Lohn: We are somewhat closer. Certainly the technology continues to progress and there are new research papers. I think that there is opportunity for us to advance at a faster rate with appropriate funding. As I discussed earlier, we have gone away from the Cyber Grand Challenge model and our adversaries have adopted it, and I think we might consider whether we would want to push to accelerate these technologies faster.

Senator Kelly: What is appropriate funding?

Mr. Lohn: Appropriate funding? I am not sure. I would say in the tens of millions of dollars would let us continue the Cyber Grand Challenge effort.

Senator Kelly: And if we were to do that, how does this whole world look in, let's say, a decade from now?

Mr. Lohn: A decade from how is difficult to say, of course. But what I would say is that the patching of the vulnerabilities is one aspect that is very important, but we

already today have a lot of our patches known before we disclose that this vulnerability exists.

The real big push that we need to make on is incorporating the patches. It is a challenge for a lot of companies to take a patch that exists and put it into their systems, knowing that it might break their systems, they might encounter downtimes.

And so these technologies that are developing vulnerabilities, are developing the patches, are making progress. Where we need to put more progress is in deploying those patches. If we do not progress in the deployment of the patches we could actually end up in a more dangerous situation, where the world is flooded with vulnerabilities, and even though we know how to patch them we have not been able to slip them into our code to make the protection.

Senator Kelly: How about the other side of this, which is the exploitation of our enemies systems?

Mr. Lohn: The exploitation of our enemy systems is kind of on that same bend. As we exist today, you can spread these exploits very quickly. The way it works is somebody finds a vulnerability, and then they will develop some attack code for that vulnerability, and then they can post it on the internet or into offensive hacking toolkits. And it just downloads automatically into your toolkit and

now you can push a button and go sometimes. That can happen very, very quickly.

And so I think there is actually more opportunity for us to make progress on the defensive side, where we are slow today. I think the offensive side is already relatively quick. And so we have some opportunities to advance there but I would really like to focus on the defensive side. I think that is where the biggest gains are to be made.

Senator Kelly: And Dr. Horvitz or Dr. Moore, where do you see us in about 10 years on this run?

Mr. Horvitz: One comment is I see tremendous opportunity to automate. When I say that, that does not mean workforce issues go away. I think we need people to be shifting over to doing more intensive, creative work in this space, and we will have plenty of that need arising.

One of the problems with automation right now is false positives. More accurate AI systems that can do better at reducing false positives and false negatives, which will come with more training data over time, will be helpful. Also the whole idea of coming up with strategies, for example, like I will accept, in this setting, higher false positives for shutdown that will be frustrating to protect me in this situation that I am in right now, sort of context-sensitive control of thresholds on automation.

To date, when it comes to an important alert, the AI is

helping humans triage through thousands of alerts coming in. I think that will get better and better as we get better and better AI systems.

Senator Kelly: How far are we away from -- go ahead, Dr. Moore.

Mr. Moore: I just wanted to add, it is not going to get automated to the extent that we will need fewer cyber warriors on the U.S. side. You will get hopefully a larger workforce using vastly more powerful tools. So one person does the work of 10,000 people in 2022, but it will still have to be quite an army of humans.

Senator Kelly: How far away are we from having an artificial intelligence system being able to write really powerful code to exploit vulnerabilities with little input, like just giving some AI code, like a set of requirements, we want you to do this. You know, here are the requirements and just hit a button and the code is written.

Mr. Horvitz: Let me say that the concern with using Copilot, which I mentioned earlier, a system that uses a large-scale, what is called a language model chain on large amounts of code to look at prompts of code being written and writing code for you, can generate all sorts of interesting offense cybersecurity as well as cyber offense and cyber defense code. The study we did of Copilot, pre-general availability, was to make the system safer in that regard.

So to answer your question, automated code-writing systems, given prompts and constraints, are surprisingly real these days. How should we field tools to the general public, how they should be used, different questions?

Senator Kelly: Thank you.

Senator Manchin: Thank you. I have just got a couple of quick questions. Do you want another round? We are going to a real quick 5-minute round. So I will just start with this one.

When you look and see the superiority that we do have, or the advancements that you think that we may be, how did the Colonial Pipeline happen, that we were not able to detect that? How are we not able to send a very strong signal -- and Russia seems to be prolific. I mean, they just made a business out of this whole hacking and hostage-taking, if you will, for profit. And the other countries that have joined. You know, I am understanding that our country is more hacked than any other country in the world, on a minute-by-minute basis.

How can we not be able to stop that and be able to send a signal strong, or shut some of these rogue actors down? Whoever wants to start?

Mr. Horvitz: Go ahead, Andrew.

Mr. Moore: Not all of our own computer systems are created equally, so it is extremely important --

Senator Manchin: What now? I am sorry. I did not --

Mr. Moore: Not all of our U.S. computer systems are created equally. We have a legacy of many systems developed over the last 20, 30, 40 years which have existed with some serious security holes, and it is very hard to manage systems built on on-prem large legacy systems of perhaps some computers from 15 years ago, some from 10, some from 5.

So the more sort of continued modernization of software, whereby software is run on very boringly sensible, secure, small pieces of infrastructure, this is the approach that clouds have adopted, means that is much safer for securing infrastructure than if you are having to remember to deal with hundreds, or actually tens of thousands of different old models and operating systems from the distant past.

One of the reasons I was so attracted to the cloud is because of this extra layer of standardization you get from just using modern, constantly patched systems instead of legacy bits of hardware.

Senator Manchin: So I am going to jump into technology for a second and raise the prospect that colleagues have discussed over the last maybe 4 or 5 years, which is whether there should be new international laws and norms and practices regarding attack of civilian infrastructure -- hospitals, pipelines, energy. One of the efforts has been

called "digital Geneva Convention." Let's thing about that, think through that. Do we need new kinds of conventions and new kinds of laws and practices, internationally?

Mr. Lohn: And I will add on just a little bit. I would like to accentuate that not all computer systems are created equally and some of these ones that are legacy are very difficult to patch, and it might not be easy for us to make those adjustments. So we might need to have more protections on the outside and we might need to have higher standards for what we expect of a company to protect themselves, and we might need to communicate which things are unacceptable for other countries to do to us.

Senator Manchin: You would think that, like our grid system, you know, that could be absolutely a tremendous, tremendous challenge for all of us but also a horrible situation if they shut it down. And we have different carriers, different transmission in different parts of the country. I do not even know if they are interconnected. I do not know if they are talking to each other. I really do not know.

Do you know, first of all, if that is being done, and if it is not being done, should it be done? Food supply. The food chains, our basic infrastructure, our water, just the things that we depend on, take for granted every day. I would think that if we are not secure, if they were able to

get to Colonial Pipeline and almost shut down tremendous flow of our transportation mode, that would have given them --

Mr. Horvitz: Yeah. Let me play red team for a bit and imagine the future. And Mr. Kelly is not with us right now but to further answer his question, we can imagine AI technologies being used adversarially to think through not just a single Colonial Pipeline but a multi-pronged attack, a hybrid attack -- going back to my comments about Ukraine, what we saw there -- that look across multiple systems and sequences of attack and use the AI technology to optimize the plan and to carry it out.

I think we need to start thinking through -- this is called red-teaming -- in a creative way to prepare for those kinds of futures, to be proactive, to disrupt them before them happen. It is going to take a lot of work.

Mr. Lohn: And with just the last couple of seconds I would like to say that our grid operators took note, in 2015 and 2016, when Russia shut down the grid, but that it still scares me.

Senator Manchin: Senator Rounds?

Senator Rounds: Thank you, Mr. Chairman. I would agree with you. I think one of the nice things about it right now is that we have multiple grids out there, and they can take one but they would have to basically take multiples

in order to get the entire country. But grid by grid, yeah, they are vulnerable.

I am just curious. The NSCAI Commission, of which two of you were members, in your final report you stated that the expanding application of existing AI cyber capabilities will make cyberattacks more precise and tailored, further accelerate and automate cyber warfare, enable stealthier and more persistent cyber weapons, and make cyber campaigns more effective on a larger scale.

I would like to hear your perspectives with regard to the threat assessment today, where we are today, with regard to AI-enabled cyberattacks on the DoDIN and on the individual businesses within the United States? Where are we at today?

Mr. Lohn: As I mentioned in my comments, there is scarce evidence of adversaries using advanced AI methods for attacks these days, but most everybody believes that the demonstrations that we have seen, for example, in cybersecurity competitions, team-on-team, have led to lots of learnings. And we know that one of the DARPA Grand Challenge competitions in cybersecurity, which had this gaming going on, was picked up by China, who took quite a bit of interest that we did that and has been holding more of those kinds of competitions and looking at their results than the United States.

Mr. Moore: Yeah, if I could add, if you look at where folks like myself and Dr. Horvitz are deploying engineers, even within an artificial intelligence group, which you might think is a bunch of mathematicians, a large fraction of all the work is on security, so perhaps these novice engineers who we were talking about earlier who are building AI systems, built on platforms with security guarantees underneath the platforms.

The word "platform" is an incredibly boring word to use. It makes people think of really boring computer science. But it is really important, the notion that a few places, places with resources like Google, are able to put huge amounts of effort into making these Lego blocks to build information systems where we have had the opportunity to put in every single piece of security, which hundreds of thousands of human engineer years of thought have gone into.

So although I love startups, mom-and-pop shops for all kinds of areas, I would like to see the Department of Defense, as it is building its systems it needs to build them not on my cloud, necessarily, but on a secure cloud, not to try to do it as sort of on legacy bits of hardware. It is really, really important. The government needs secure cloud.

Senator Rounds: Dr. Lohn?

Mr. Lohn: I will just add a little bit along the lines

of Dr. Moore, is that in addition to the tools and resources being provided by the tech companies that are represented here, there is a lot being done in the open-source community as well. And people will build a model or release a dataset or create some tool and then that is downloaded and used by these relative novices -- not you -- novices that he was referring to, and those may or may not have the same sort of security that we are expecting from our tech companies. There is an opportunity to help fund them, to do the hygiene and clean up their code as well.

Senator Rounds: And one last thought that I have to ask, and that his, when we talk about AI and we are looking at the power it takes, are the existing platforms that are out there, are the existing hardware systems, is the AI dependent on the capability, the power of the computing capability of the actual hardware itself, to an extreme basis, or is it being able to utilize an existing power source or computing capability to a greater extent by using the AI concept?

Mr. Moore: The good news is there are two lines working, fully supporting each other. Hardware miniaturization is working extremely effectively at the moment, but the software folks are also figuring out new ways to take advantage of all the bits of technology. So that is an area where everything is advancing. And if I

told you what was happening today it would be different from 3 months ago.

Mr. Horvitz: To build the largest models, as we call them, that are showing some of these interesting emergent properties right now, where there is a great deal of interest, it is taking specialized hardware, and a lot of it, and a lot of energy.

Senator Rounds: Anything else?

Mr. Lohn: I would just like to add that the ability to keep on that trajectory is starting to look less promising because it requires so much.

Senator Rounds: Thank you. Thank you, Mr. Chairman.

Senator Manchin: Senator Blackburn.

Senator Blackburn: Thank you, Mr. Chairman. I appreciate that.

Let me stay with that AI, because there should be some practical applications that come forward. One of the things that has been of concern to me, as we have done our combatant command hearings, is looking at human capital and the workforce and retaining individuals that can solve some of these complex issues and problems, address these problem sets. So when you look at the utilization of AI you should be able to push forward with problem-solving in the absence of individuals, by having the brainpower that is there to distill what you are hearing.

Dr. Horvitz, I think it would come to you. Talk to me a little bit about how you are using this, the distillation from AI, to help solve some of these problems of malign activity, business processes. And I would like to hear that from each of you, because that is how we are going to stay in the game when it comes to great power competition.

Mr. Horvitz: And when you say malign, can you clarify what you mean?

Senator Blackburn: Adverse bad actors, trying to do bad things to us --

Mr. Horvitz: Oh, in the world.

Senator Blackburn: -- in order to thwart some of our positive activity, carry out malign influence campaigns, things of that nature.

Mr. Horvitz: I see. Well, as I mentioned in my written testimony, one of the concerns with the rise of power AI technologies is the ability to generate content, for AI systems to generate deep fakes, for example. And we are going to be in a place where humans nor AI will be able to detect and discriminate a deep fake from a real scene, a real event in the world. And so we need technologies for that, and we described at least one technology called digital content provenance, which, in some ways the way I like to describe it is glass-to-glass, can you cryptography to certify this is non-AI technology, dealing with an AI

outcome or capability, which is deep fakes, to certify that every time hitting this camera surface is represented by a pixel on display, and no one has changed anything, and you can actually track all the edge in between. So we can imagine working on that. That is an interesting front.

More generally, there is opportunity to study large datasets, and I think in our NSCAI report we talked about this idea of having new kinds of centers that would think through, collect data and do research and R&D on malign information campaigns, their source, how they spread and diffuse, how we might address them ideally.

Senator Blackburn: Okay. Dr. Lohn?

Mr. Lohn: Yes. I would like to expand just a little bit on Dr. Horvitz's discussion. Not only is there technology for creating fake images but it can create fake text, and that text can be very convincing. We did a study that found that it could convince people, American population, to oppose Chinese sanctions or to support or oppose the withdrawal from Afghanistan, either way.

But what I would like to kind of point out is that the dichotomy between the amount of skills required. So to build these models that can generate that text requires many, many geniuses, but to use it, not so much. All you have to do is type a couple of words, hit stop, go run, and then it fills out the rest. There is no real programming

expertise required.

And so we need really smart people to build some of these technologies, but to use them, to build companies out of them or to defend ourselves, or the adversaries to come after us sometimes requires very little expertise. And that it both an opportunity and a threat.

Senator Blackburn: And that is why -- and I appreciate the mention of our civilian cyber force, which would help with that early response, have people there that are able to utilize some of these technologies when we do not have individuals, enough people to do the work that we need to do. We can kind of bring them in an as-needed basis. I think that is a good and positive step, and I appreciate you all mentioning that in the opening.

Dr. Moore?

Mr. Moore: Thank you. Your question is very on point, and thank you for bringing it up. This notion that folks can actually poison our own systems was kind of science fiction-y 5 years ago but it has happened to me, and I have been on the front lines of dealing with this, and attacks against Google systems. So, as you can imagine, that is now a major aspect of defense.

One thing I would like to mention is we at Google Cloud have partnered with the Defense Innovation Unit to stand up their secure cloud management solution, to be ready for

these second-, third-, and fourth-level attacks, where everyone is looking above and beyond what each other are doing. It is absolutely the place where the battle is being fought at the moment.

Senator Blackburn: Okay. Thank you all for that.

Dr. Horvitz, Microsoft, what have they learned from, I think it is the Hafnium Project. Could you talk to me just a little bit about what the lessons learned are from that and then how you plan to use that information.

Mr. Horvitz: The main lesson for the world is on-prem is not as secure as cloud. On-prem requires having your own machines. It might seem like I have my data and it is protected here but the amount of updates that are required to keep up with old software, for example, especially in small and medium-sized businesses that do not have IT teams, for example, it is challenging.

We recommend, for the top-notch security, move to the cloud and let the big tech companies take their best resources and ongoing surveillance and cybersecurity software, let them do the work for the businesses. That was the main finding, from my point of view.

Senator Blackburn: Okay. Dr. Moore, I see you shaking your head. Anything to add to that?

Mr. Moore: [Inaudible.]

Senator Blackburn: Okay. Well, thank you all. I know

my time has expired, but to your answer I think the prevailing and unanswered question for the 21st century is who owns the virtual you, which is you and your presence online, and being able to distill some of this information and be able to decide what is real, what is fake, what is a misrepresentation is one that we are going to have to continue to work through.

Thank you all for your time.

Senator Manchin: Thank you, Senator.

Let me just again thank all of the witnesses. Thank you all for being here and sharing with us your knowledge and forecasts and what we need to do and how we need to all work together. I tell you, we are mostly committed to that. Artificial intelligence development and the applications to national security and our everyday lives has the potential, really, to revolutionize our lives, and we understand that, and most importantly, our society. But Congress and the Federal Government must be prepared to prioritize -- and I have heard it loud and clear -- prioritize the necessary investments now.

So I know Senator Rounds and I share the priority and I look forward to working together on implementing what we have learned today and continuing to work with you all.

With that the meeting is adjourned.

[Whereupon, at 4:05 p.m., the hearing was adjourned.]

WORD INDEX

< $ >
$20 44:*12*

< 1 >
10 36:*10* 50:*10* 53:*7*
10,000 51:*10*
100 37:*8*
13 36:*16*
15 53:*7*
1956 34:*6*
1990s 31:*18*

< 2 >
2 47:*4*
2:43 1:*11*
20 9:*24* 53:*4*
2000s 31:*21*
2015 13:*22* 55:*18*
2016 14:*2* 55:*19*
2020 47:*21*
2021 36:*16*
2022 1:*4* 51:*10*
21st 64:*2*
2-year 45:*24*

< 3 >
3 1:*4* 59:*2*
3,500 46:*23*
30 53:*4*
33 27:*6*

< 4 >
4 53:*22*
4:05 64:*25*
40 53:*4*

< 5 >
5 39:*17* 53:*7*, *22* 62:*19*
5,000 3:*15*
50,000 3:*16*
5-minute 52:*8*

< 6 >
600,000 45:*25* 46:*22*

< 7 >
7 30:*2*, *9* 47:*15*
70s 41:*25*

< 8 >
80s 41:*25*

< 9 >
90s 41:*25*

< A >
abilities 10:*5* 19:*18*
ability 4:*17* 9:*12*, *14*, *15*, *18* 27:*17* 39:*6* 59:*9* 60:*17*
able 7:*13* 10:*17* 11:*5*, *6* 20:*1* 23:*12* 31:*2* 35:*23* 49:*15* 51:*13* 52:*12*, *13*, *20* 54:*25* 57:*12* 58:*17* 59:*23* 60:*19* 62:*9* 64:*4*, *5*
absence 59:*23*
absolute 9:*25* 22:*24*
Absolutely 46:*5* 54:*14* 63:*3*
abstractions 9:*19*
academia 38:*14*
academic 2:*6* 35:*5*
accelerate 48:*15* 56:*7*
accentuate 54:*5*
accept 50:*21*
access 7:*17* 28:*6*
accounting 12:*13*
accurate 50:*17*
achieve 4:*8*
achievements 35:*14*
act 38:*10* 42:*5*, *9*, *25* 43:*5* 44:*2*
actions 3:*20*, *24* 22:*2*
active 27:*9*
activities 22:*4*
activity 26:*23* 60:*4*, *13*
actors 6:*12* 20:*15* 52:*21* 60:*9*
actual 58:*16*
adapt 9:*15* 13:*12* 15:*7* 26:*24* 31:*20*
adapted 15:*6*
add 10:*23* 51:*6* 54:*4* 57:*1*, *25* 59:*9* 63:*23*
addition 58:*1*
Additionally 3:*17*
address 59:*21* 61:*11*
adjourned 64:*24*, *25*
adjustments 54:*8*
adopt 40:*19*
adopted 48:*14* 53:*11*
adopting 7:*9*
adoption 8:*9*
advance 29:*5* 42:*23* 48:*11* 50:*6*
advanced 22:*6* 56:*16*
advancements 52:*11*
advances 34:*14*, *18* 39:*18*
advancing 18:*14* 26:*16* 58:*25*
advantage 4:*25* 19:*14* 58:*24*
adversarial 21:*9* 28:*4* 29:*11* 33:*22* 40:*24*
adversarially 55:*7*
adversaries 4:*15* 7:*11*, *19* 8:*11* 15:*5*, *19*, *24* 27:*1* 28:*21* 29:*3* 33:*10* 48:*14* 56:*16* 62:*4*
adversary 4:*13* 33:*24*
Adverse 60:*9*
advocate 23:*4*
afford 21:*2*
Afghanistan 61:*19*
agencies 11:*4*
agency 29:*16*
ago 26:*13* 37:*21* 45:*7* 47:*3* 53:*7* 59:*2* 62:*19*
agree 55:*23*
ahead 29:*1* 32:*9* 33:*6*, *16*, *21* 38:*25* 51:*4* 52:*23*
AI 2:*22* 3:*7*, *15*, *17*, *19* 4:*5*, *8*, *10*, *11*, *16*, *24* 5:*3*, *7*, *11* 6:*22*, *24* 7:*4*, *5*, *9*, *12*, *20*, *23* 8:*9*, *11*, *13* 9:*8*, *20* 10:*1* 11:*11*, *12*, *13*, *14* 12:*9*, *13*, *15*, *16*, *24* 13:*2*, *3*, *4*, *6*, *8*, *12*, *13*, *15* 14:*18* 15:*5*, *18*, *23*, *25* 18:*7*, *20*, *24*, *25* 19:*17*, *20*, *21* 20:*20*, *23* 21:*9*, *25* 22:*3*, *6*, *23* 23:*6*, *10*, *11*, *13* 26:*8*, *12*, *15*, *16*, *17*, *18*, *19* 27:*2*, *7*, *9*, *10*, *12*, *14*, *16*, *20*, *23* 28:*2*, *4*, *5*, *7*, *8*, *13*, *19*, *21*, *25* 29:*9*, *13*, *14*, *15* 31:*19*, *22*, *25* 32:*3*, *4*, *21*, *24* 33:*3*, *5* 34:*5*, *7*, *10*, *11* 35:*16*, *17* 36:*10*, *17*, *19* 37:*4*, *12*, *17*, *20* 38:*20*, *23* 39:*1*, *7*, *10*, *13*, *17*, *25* 40:*24* 41:*17*, *19* 43:*5*, *14*, *24*, *25* 44:*2*, *12*, *13* 46:*13* 48:*6* 50:*17*, *25* 51:*3*, *15* 55:*6*, *11* 56:*5*, *16* 57:*7* 58:*12*, *14*, *19* 59:*16*, *22* 60:*3*, *17*, *18*, *19*, *25*
AI-capable 7:*11* 8:*10*
AI-enabled 7:*14*, *16* 8:*15*, *16* 44:*13* 56:*12*
AI-enhanced 7:*2*
aimed 27:*21*
AI-powered 27:*7*
AIs 19:*2* 21:*6*, *19*, *20*
alarms 4:*1*, *7*
alert 15:*18* 50:*25*
alerts 3:*23* 45:*5* 48:*4* 51:*1*
algorithms 4:*11*
alike 3:*2*
All-Domain 22:*20*
allies 33:*10* 43:*16*
allowing 22:*21*
AlphaFold 39:*19*
alternatives 19:*1*, *19*
American 31:*16* 61:*17*
amount 20:*4* 31:*3* 61:*21* 63:*13*
amounts 34:*25* 51:*21* 57:*13*
analysis 46:*8*
analysts 3:*24* 4:*2*
Analytics 41:*9*
Andrew 8:*24* 9:*1* 12:*1*, *6* 18:*1*, *6* 52:*23*
announcement 45:*12*
anonymous 3:*24*
answer 9:*6* 10:*25* 12:*9* 30:*16* 31:*12* 40:*18* 41:*3* 52:*1* 55:*6* 64:*1*
answers 2:*18*
anti-phishing 13:*7*
anybody 8:*6*
anyone's 37:*7*
appearing 6:*4*
application 2:*9*, *22* 6:*21* 39:*7*, *8* 40:*13* 47:*22* 56:*5*
APPLICATIONS 1:*2* 5:*3* 7:*6* 34:*17* 35:*11*, *13* 38:*20* 40:*5* 48:*1* 59:*17* 64:*14*
applied 44:*14* 46:*11*
applying 5:*7*
appreciate 8:*14*, *21* 10:*22* 18:*22* 42:*15* 59:*15* 62:*7*, *13*
appreciation 24:*5*
apprenticeship 45:*24*
approach 21:*14* 44:*7* 53:*10*
approaches 35:*17*
appropriate 48:*12*, *17*, *18*
April 36:*16*
area 26:*18*, *20* 27:*8* 45:*19* 58:*25*
areas 10:*4*, *18* 13:*2* 26:*14* 27:*16* 57:*18*
arena 33:*12*
arising 50:*15*
Armed 1:*8* 2:*8* 24:*2* 30:*18* 38:*1*
army 51:*11*
article 36:*16*
articles 31:*8*
ARTIFICIAL 1:*1* 2:*9*, *12* 6:*21* 8:*3* 9:*3* 10:*2* 15:*16* 18:*2*, *14* 21:*12* 30:*14* 31:*5*, *15* 41:*12* 43:*2*, *6* 47:*22* 51:*13* 57:*3* 64:*14*
asked 11:*1* 19:*5*
asking 17:*2*
as-needed 62:*12*
aspect 22:*7* 48:*25* 62:*22*
aspects 9:*10*
assess 48:*7*
assessment 56:*11*
asset 18:*18*
assistance 7:*16*

associated 26:*9, 23* 45:*11*
assume 35:*25*
attack 4:*13, 19* 6:*14* 13:*21* 15:*21* 19:*6, 8* 27:*18, 20* 28:*21* 47:*25* 49:*23* 53:*24* 55:*8, 9, 11*
attacked 20:*13*
attacker 13:*12, 14* 14:*1, 20* 28:*16*
attackers 13:*12* 28:*7*
attacks 4:*16* 7:*15* 15:*23, 25* 20:*20, 23, 25* 21:*1, 5, 8* 23:*15* 26:*18, 20, 21, 23, 24* 27:*24* 28:*2, 4, 18* 29:*11* 45:*10* 56:*17* 62:*20* 63:*1*
attention 5:*14*
attracted 53:*16*
attributed 44:*25*
audio 28:*15*
automate 3:*19* 13:*21* 26:*8* 50:*12* 56:*7*
automated 13:*16* 14:*3* 51:*7* 52:*1*
automatically 22:*3* 49:*25*
automation 3:*6, 7, 13* 13:*25* 32:*11* 50:*16, 24*
autonomous 14:*13* 15:*3, 21* 19:*25*
autonomously 14:*17*
availability 51:*25*
available 7:*5, 7* 37:*24*
aware 15:*24* 21:*21* 22:*1*
awareness 29:*10*
awful 30:*14* 31:*12*

< B >
back 17:*7* 31:*18* 39:*23* 40:*3* 55:*9*
back-and-forth 13:*11*
background 13:*1*
bad 60:*9, 10*
based 45:*2*
baselining 18:*20*
basic 7:*23* 21:*2* 40:*4, 12* 46:*7* 54:*23*
basically 31:*24* 33:*2, 4* 35:*23* 55:*25*
basis 52:*19* 58:*17* 62:*12*
battle 19:*6, 8, 14, 16* 63:*3*
battlefield 16:*1* 40:*1*
beat 31:*17*
beautiful 38:*18*
becoming 38:*17* 47:*10*
behalf 10:*21* 11:*17*
behaviors 10:*9*
belabor 3:*9*
believe 2:*23* 24:*2* 32:*12*
believes 56:*17*
bend 49:*20*
benefit 2:*20* 4:*10* 40:*4*
benefitting 5:*8*
best 7:*17* 8:*15* 19:*22* 29:*8, 10* 30:*24* 36:*19* 43:*13* 63:*18*
better 3:*18* 7:*24* 20:*5* 23:*25* 29:*1* 31:*6* 32:*14* 38:*11* 39:*1, 3* 40:*11* 50:*17* 51:*2, 3*
beyond 63:*2*
Bias 44:*3*
biased 28:*22*
bid 24:*1*
big 11:*12* 20:*8* 34:*13* 46:*9* 49:*3* 63:*18*
bigger 34:*23, 24*
biggest 50:*8*
billions 19:*1*
bills 23:*3*
bipartisan 43:*6*
bit 9:*18* 12:*23* 34:*1* 39:*23* 42:*2, 21* 43:*15* 44:*18* 54:*4* 55:*4* 56:*23* 57:*25* 60:*2* 61:*14* 63:*8*
bits 53:*19* 57:*21* 58:*24*
Blackburn 1:*15* 43:*4* 59:*13, 14* 60:*9, 12* 61:*12* 62:*7* 63:*5, 22, 25*
Blocks 42:*5* 57:*13*
Blue 31:*16, 17, 23*
Blumenthal 1:*15*
board 40:*9*
Board's 12:*10*
boring 57:*9, 10*
boringly 53:*9*
bracing 44:*16*
brainpower 59:*24*
break 49:*6*
breaking 10:*18* 14:*4*
briefings 6:*9*
brilliant 41:*4*
bring 2:*15* 38:*1* 42:*16* 47:*9* 62:*12*
Bringing 32:*10* 62:*17*
broad 10:*12* 11:*1*
broadcasting 45:*13*
broader 6:*20* 32:*21*
brought 21:*14*
build 11:*9* 23:*19* 37:*22* 44:*9* 57:*14, 19* 58:*4* 59:*3* 61:*22* 62:*2, 3*
Building 1:*12* 11:*3* 21:*19, 20* 35:*8* 42:*4* 57:*6, 19*
built 38:*9* 53:*6* 57:*7*
bunch 23:*16* 57:*4*
business 5:*3* 52:*15* 60:*4*
businesses 56:*13* 63:*15, 20*
button 50:*1* 51:*17*

< C >
call 9:*10* 20:*7* 22:*14* 27:*12* 28:*3* 40:*7* 59:*3*
called 10:*1* 38:*22* 44:*12* 45:*1, 3* 51:*20* 54:*1* 55:*14* 60:*22*
camera 61:*2*
campaigns 56:*8* 60:*13* 61:*10*
cancer 39:*17, 22*
Cantwell 43:*4*
capabilities 6:*17* 7:*2* 9:*11, 17, 21* 15:*3* 24:*3* 56:*5*
capability 12:*11* 37:*1* 58:*15, 16, 18* 61:*1*
capable 14:*14* 15:*14, 20*
capacity 3:*4*
capital 59:*19*
capitalize 4:*15*
captures 6:*25*
care 39:*13, 14* 40:*4*
Carnegie 18:*9* 21:*23* 36:*14*
carriers 54:*17*
carry 55:*12* 60:*13*
cases 14:*17*
catch-up 40:*10, 18*
causing 28:*8*
CENTER 12:*1, 7* 41:*16* 43:*5, 24*
centers 61:*8*
central 41:*19*
centralized 41:*11*
century 64:*2*
certain 22:*11*
certainly 40:*15* 48:*9*
certificate 45:*24*
certify 60:*25* 61:*1*
chain 4:*20* 15:*5* 51:*20*
chains 54:*23*
Chair 31:*14*
chairman 1:*13* 10:*22* 11:*17* 12:*4* 18:*4, 15* 19:*5* 21:*18* 26:*3* 36:*4* 41:*21* 55:*22* 59:*12, 14*
Challenge 14:*3, 11* 18:*10* 36:*7* 42:*15, 20* 44:*4* 48:*13, 20* 49:*4* 54:*15* 56:*21*
challenges 6:*12* 14:*14*
challenging 63:*16*
championed 21:*23*
chance 19:*9*
change 14:*20* 32:*12* 41:*18*
changed 61:*3*
changes 41:*16*
changing 32:*11*
cheap 7:*5*
chess 31:*17*
Chief 8:*24* 26:*2, 6* 41:*8*
China 3:*9* 4:*25* 14:*12, 15* 15:*11* 33:*16* 35:*2* 36:*18, 20* 42:*24* 56:*22*
Chinese 61:*18*
CISA 44:*17*
civil 35:*10* 44:*4*
civilian 53:*24* 62:*8*
clarify 60:*7*
class 46:*18*
classes 47:*4*
clean 10:*11* 45:*3* 58:*10*
clear 14:*15* 15:*1* 23:*14* 64:*19*
clearly 8:*5*
click 27:*25*
clock 47:*15*
closer 48:*6, 9*
Cloud 9:*2* 18:*2, 7* 19:*23* 37:*3* 46:*12* 53:*16* 57:*20, 23* 62:*23, 25* 63:*11, 18*
clouds 53:*11*
coastal 14:*24*
code 13:*21* 38:*22* 42:*1* 49:*15, 23* 51:*14, 15, 17, 21, 22, 24* 58:*10*
coder 41:*24*
coders 38:*25* 45:*18*
code-writing 52:*1*
coding 38:*23*
cognition 26:*10*
collaboration 11:*13* 29:*7* 43:*7*
collaborative 35:*17*
colleagues 7:*25* 18:*24* 20:*11* 33:*8* 53:*21*
collect 11:*6* 61:*9*
college 38:*12* 46:*6*
Colonial 52:*12* 55:*1, 8*
combatant 59:*19*
combine 23:*19*
come 2:*3* 10:*3, 16* 17:*7* 23:*13* 31:*21* 36:*6* 37:*9* 47:*17* 50:*19* 59:*17* 60:*1* 62:*4*
comes 21:*9* 23:*5* 50:*25* 60:*6*
coming 8:*17* 21:*5, 6* 25:*4* 46:*3* 50:*20* 51:*1*
Command 6:*17* 22:*20* 59:*19*
commands 28:*15, 16*
comment 47:*2* 50:*11*
comments 21:*19* 39:*25* 55:*9* 56:*15*
Commercial 3:*21* 5:*6* 37:*10*
commercially 7:*5*
Commission 6:*24* 43:*1, 14, 23* 44:*12* 56:*3*
Commissioner 18:*8*

commissions 44:*11*
committed 64:*13*
Committee 1:*8*, *14* 2:*8* 18:*5*
committee's 18:*13*
common 12:*14*
communicate 54:*11*
community 27:*13* 38:*12* 46:*5* 58:*3*
companies 2:*6* 5:*6* 8:*11* 11:*1* 13:*8* 20:*8* 32:*13* 33:*18* 38:*17* 43:*22* 46:*9*, *10* 49:*5* 58:*2*, *8* 62:*3* 63:*18*
companion 38:*24*
company 54:*10*
compared 40:*23*
compels 27:*25*
competed 14:*3*, *6*
competition 3:*11* 60:*6*
competitions 56:*19*, *21*, *24*
competitiveness 42:*24*
competitors 7:*3*
complete 22:*18*
completed 8:*1*
complex 2:*13* 42:*16*, *18* 43:*13* 59:*21*
component 32:*22*
components 29:*14*
compromise 5:*1*
compromised 4:*21* 15:*8*
computation 34:*22*
compute 34:*25* 35:*2*
Computer 3:*12* 8:*3* 9:*8* 10:*5*, *8*, *14* 12:*11*, *20*, *24* 13:*16* 31:*17* 39:*22* 46:*15* 52:*24* 53:*2* 54:*5* 57:*10*
computer-aided 3:*21*
computers 3:*7* 10:*8*, *13*, *16* 11:*6* 13:*20* 53:*7*
computing 8:*4* 10:*7* 12:*22* 43:*12* 58:*15*, *18*
conceal 22:*4*
concept 13:*6* 58:*19*
concepts 2:*19* 7:*4* 22:*16*
concern 27:*8* 28:*2* 51:*18* 59:*18*
concerns 60:*16*
concerted 41:*7*
concise 31:*11*, *15*
conclude 28:*23*
concur 32:*21*
confident 33:*17*
conflict 7:*3* 44:*16*
confusion 32:*23*
Congress 24:*11* 64:*17*
conjunction 21:*13*
consider 28:*24* 48:*15*
considered 12:*15*
considering 9:*13*
constantly 48:*5* 53:*18*
constraints 35:*4* 52:*2*
consulting 46:*9*
contain 3:*20*
content 27:*25* 60:*17*, *23*
context 33:*22*
context-sensitive 50:*24*
continue 3:*2* 24:*11* 36:*25* 38:*9* 44:*9* 48:*20* 64:*7*
continued 53:*8*
continues 48:*10*
continuing 64:*23*
contract 32:*16*
contracting 31:*6*
contractor 24:*1*
contributed 47:*21*
Control 22:*20* 27:*18* 50:*24*
Convention 54:*1*
conventions 54:*2*
convince 61:*17*
convincing 61:*16*
coordinated 45:*10*
coordination 43:*16*
Copilot 38:*22* 51:*19*, *24*
core 28:*25* 34:*16*
CORPORATION 18:*3* 26:*2*
Corps 37:*15* 38:*2*
corrosion 20:*1*
countries 15:*2* 32:*7* 33:*9* 43:*12* 52:*16* 54:*12*
country 3:*1* 31:*3* 38:*8*, *9* 39:*12* 40:*11* 52:*18* 54:*18* 56:*1*
couple 35:*2* 52:*6* 55:*17* 61:*24*
course 11:*8* 42:*12* 45:*17* 48:*24*
courseware 47:*3*, *7*
coursework 38:*16*
courteously 17:*1*
crazy 8:*5*
create 27:*18* 38:*3* 43:*6* 58:*5* 61:*15*
created 52:*25* 53:*3* 54:*6*
creating 61:*15*
creation 29:*6* 41:*8*
creative 34:*17* 50:*14* 55:*14*
creatively 47:*8*
criminals 7:*7*
critical 2:*10* 10:*15*
critically 27:*3*
cross 33:*10*
cross-sector 29:*6*
cryptographic 10:*19*
cryptography 60:*24*
cures 39:*16*
curious 56:*3*
current 8:*9* 10:*19*
currently 26:*6*
customers 35:*9*
cut 13:*22*
cutting 30:*22* 32:*8*
cutting-edge 6:*17*
Cyber 2:*7* 3:*3*, *20* 4:*8*, *9*, *11* 5:*11* 6:*12*, *17* 7:*14* 8:*15* 13:*3*, *4*, *6* 14:*2*, *17* 23:*4* 26:*19* 36:*24* 37:*15* 42:*9* 44:*13* 45:*10*, *21* 48:*8*, *13*, *20* 51:*7*, *23* 56:*5*, *7*, *8* 62:*8*
CyberAI 12:*6*
cyberattacks 3:*18* 8:*16* 26:*17* 27:*7*, *10*, *11* 44:*17* 56:*6*, *12*
Cybersecurity 1:*7* 3:*1* 5:*6* 11:*11* 13:*2*, *11* 15:*17* 20:*10*, *11* 26:*15*, *16* 27:*2*, *4*, *5*, *22* 29:*13* 37:*20* 46:*1*, *23* 47:*5*, *6*, *10* 51:*23* 56:*19*, *21* 63:*19*
CYBERSPACE 1:*2* 2:*11*, *23* 5:*5* 6:*10*, *18*, *21* 8:*12*, *14*

< D >
D.C 1:*9*
DAKOTA 6:*2* 36:*23*
danger 4:*20* 20:*2*
dangerous 49:*13*
DARPA 14:*2* 44:*12* 56:*20*
data 3:*23* 11:*6* 15:*7* 20:*21* 22:*9*, *10*, *18*, *23* 23:*19* 28:*6*, *20*, *22* 29:*8*, *17* 41:*9* 43:*13*, *17* 46:*7*, *8*, *17* 50:*19* 61:*9* 63:*12*
database 22:*15*
dataset 58:*4*
datasets 15:*9* 61:*7*
date 13:*14* 27:*8* 50:*25*
dated 36:*16*
day 14:*7* 23:*20* 39:*22* 54:*24*
days 22:*23* 31:*22* 32:*2*, *3* 34:*18* 52:*3* 56:*17*
deal 19:*12* 21:*15* 23:*16* 38:*14* 53:*13* 59:*5*
dealing 60:*25* 62:*20*
Dean 18:*9* 36:*14*
decade 27:*6* 48:*22*, *23*
decide 64:*5*
decision 15:*14*
decisions 9:*15* 19:*1*
decoys 14:*25*
dedicated 3:*12*
deep 7:*6* 10:*20* 31:*16*, *17*, *22* 60:*18*, *20* 61:*1*
defend 6:*18* 7:*8*, *19*, *20* 8:*12* 20:*20*, *23* 62:*4*
Defender 5:*9*
Defending 7:*11*
Defense 5:*2*, *8* 6:*15* 7:*10*, *14* 8:*10*, *13*, *15* 12:*10* 13:*3*, *6* 14:*24* 18:*21* 19:*24* 20:*22* 21:*14* 22:*9* 26:*19* 29:*1* 31:*3*, *7* 32:*17* 35:*23* 39:*5*, *6*, *9*, *24* 51:*24* 57:*19* 62:*22*, *24*
defenses 44:*13*
defensive 2:*11* 4:*9* 50:*4*, *7*
deficit 27:*4*
defined 18:*24*
definition 12:*10*
degree 45:*24*
deliberate 45:*15*
delist 13:*18*
demand 3:*4*
democracy 44:*7*
democratic 44:*1*
democratization 37:*4*
democratized 37:*17*
demonstrated 6:*12* 27:*13*, *17*
demonstrations 27:*23* 28:*9* 56:*18*
Department 5:*2*, *8* 6:*15* 8:*13* 18:*21* 19:*24* 20:*21* 21:*14* 22:*9* 35:*22* 39:*5*, *6*, *9*, *24* 57:*18*
depend 54:*24*
dependent 58:*15*
deploy 15:*3* 34:*2*
deployed 15:*4*
deploying 49:*11* 57:*2*
deployment 49:*12*
Deputy 41:*9*
describe 7:*24* 60:*24*
described 60:*22*
designed 9:*9* 23:*7* 29:*9*
despite 11:*12*
details 35:*15*
detect 4:*17* 26:*20*, *24* 44:*14* 52:*13* 60:*20*
detected 44:*23* 45:*4*
detecting 21:*7*
detection 3:*21* 4:*6* 14:*21* 27:*19*
detectors 11:*9*
determines 12:*21*
develop 7:*4* 14:*16* 29:*12* 37:*1* 40:*20* 49:*22*
developed 13:*24* 15:*19* 29:*16* 53:*3*
developers 38:*22*
developing 5:*3*, *7* 15:*21* 20:*17* 29:*4* 33:*23* 49:*8*, *9*

development 38:*3* 43:*24* 64:*14*
developments 26:*12*
devil 35:*15*
diagnoses 40:*5*
dichotomy 61:*21*
difference 8:*2*
different 10:*7* 12:*23* 22:*10*, *14*, *15*, *17* 31:*8* 33:*9* 44:*2* 52:*4* 53:*14* 54:*16*, *17* 59:*1*
differently 28:*13*
difficult 37:*22* 40:*22* 48:*23* 54:*7*
diffuse 61:*11*
digital 14:*25* 54:*1* 60:*23*
dimensions 9:*23*
direct 5:*11* 13:*16*, *17* 36:*13*
directing 14:*23*
direction 35:*6*
directions 19:*11*
directly 15:*23* 33:*15*
Director 9:*2* 18:*2*
dirty 35:*18*
disaster 7:*13*
disastrous 5:*1*
discipline 10:*2* 34:*13*, *14*
disciplines 34:*11*
disclose 49:*2*
discover 3:*17* 4:*13* 14:*16*
discovered 10:*10*
discriminate 60:*20*
discussed 48:*12* 53:*22*
discussion 61:*14*
discussions 8:*1*
disguising 14:*23*
disinformation 7:*14* 45:*12*
dispatched 45:*4*
dispatching 48:*3*
display 61:*3*
disrupt 28:*5* 55:*15*
dissatisfaction 45:*12*
distant 53:*14*
distill 59:*25* 64:*4*
distillation 60:*2*
distinguished 2:*5* 46:*19*
Doctor 24:*8* 47:*19*
DoD 5:*11* 11:*4* 15:*13* 20:*6*, *18* 29:*15* 33:*20*, *21*, *24* 35:*14* 40:*1*, *7*, *19* 41:*12*, *16* 43:*11*, *24*
DoDIN 56:*12*
doing 11:*2* 18:*20* 19:*3* 21:*10* 23:*21* 37:*14* 40:*8*, *9*, *18* 42:*14* 47:*16* 50:*14* 63:*3*
dollars 48:*19*
domain 6:*10*
domains 22:*22*
dots 28:*11*
double-checking 23:*21*
downloaded 58:*5*
downloading 46:*12*
downloads 49:*25*
downtimes 49:*7*
Dr 3:*14* 8:*23*, *24* 9:*1*, *5* 11:*18* 12:*22* 15:*11* 17:*7*, *9*, *10* 18:*8*, *19* 25:*3* 31:*10* 32:*19*, *21* 34:*3* 36:*13* 37:*18* 38:*6* 40:*13*, *14* 41:*1* 42:*8* 43:*9* 44:*10* 47:*21* 48:*3* 50:*9* 51:*5* 57:*2*, *24* 58:*1* 60:*1* 61:*12*, *14* 62:*15* 63:*6*, *22*
dramatically 28:*9*
driven 3:*13*
drives 45:*3*
drone 7:*15* 19:*5*, *7*
drones 7:*6* 14:*23* 19:*25*
due 36:*13*
duplicated 31:*5*
duties 2:*6*
dynamic 6:*9*

< E >
earlier 26:*9* 48:*13* 51:*19* 57:*6*
early 31:*21* 42:*4*, *6* 62:*9*
easier 14:*25* 37:*11*, *20*
easily 23:*10*
easy 14:*20*, *22* 54:*7*
edge 30:*22* 32:*8* 42:*23* 61:*4*
educate 2:*7* 29:*12*
educating 38:*11*
effective 56:*9*
effectively 58:*22*
efficacy 27:*12*
efficiencies 5:*3*
efficiency 31:*4*
efficiently 20:*2* 27:*17*
effort 11:*4* 23:*11* 41:*7*, *11* 48:*20* 57:*13*
efforts 27:*3* 53:*25*
either 48:*7* 61:*19*
eloquently 2:*24*
embedded 28:*15* 36:*11*
emboldened 15:*20*
emergent 59:*4*
emerging 6:*10*, *16* 8:*25* 12:*2*, *7* 21:*4* 43:*8*
emit 28:*1*
employ 11:*8*
employing 7:*12*
employment 40:*3*
emulate 9:*10*, *20*
enable 4:*8*, *25* 56:*7*
encounter 49:*7*
encourage 2:*14*
encouraged 41:*8*
encrypt 13:*18*
encryptography 10:*15*
enemies 49:*18*
enemy 48:*1*, *8* 49:*19*
energetic 40:*10*
energy 53:*25* 59:*7*
engagements 47:*7*
engineer 57:*16*
engineering 27:*21* 35:*16* 43:*18*
engineers 26:*8* 36:*17* 45:*19* 57:*2*, *6*
enjoy 40:*12*
enlisted 38:*2*
enormous 3:*23*, *25*
ensure 29:*9*, *15*
entanglement 10:*11*
enterprises 11:*2*
enthusiastic 40:*9*, *19*
entire 56:*1*
environment 40:*24*
envision 14:*25*
equally 52:*25* 53:*3* 54:*6*
equivalent 3:*16*
era 7:*3*
eradicate 3:*20*
Eric 8:*23* 26:*1*, *5*
Ernst 1:*15*
erroneous 28:*22*
especially 3:*3* 22:*11* 35:*4* 36:*22* 63:*14*
essential 23:*1*
evade 13:*13* 27:*19*
evaluate 33:*7*, *14*
event 4:*5* 60:*21*
events 3:*24*
everybody 44:*18* 46:*22* 56:*17*
everyday 64:*15*
evidence 56:*16*
evolving 6:*9* 26:*18* 48:*6*
example 5:*10* 9:*13* 10:*18* 11:*7* 12:*12* 19:*4*, *7*, *21* 21:*22* 22:*19* 23:*4* 28:*7* 35:*8* 38:*21* 39:*20* 43:*21* 50:*21* 56:*18* 60:*18* 63:*14*, *16*
examples 2:*15* 12:*21* 19:*24* 20:*6*
excerpt 6:*23*
excite 42:*6*
excited 41:*23* 43:*19*
exciting 26:*19*
executables 29:*18*
execute 28:*17*
exist 49:*20*
existed 34:*6* 53:*4*
existing 15:*6* 41:*17* 56:*5* 58:*13*, *14*, *17*
exists 49:*2*, *5*
expand 61:*13*
expanding 56:*5*
expect 15:*25* 54:*10*
expected 27:*10*
expecting 58:*8*
experience 36:*14*, *24* 46:*12*
experienced 48:*2*
experiences 9:*16* 29:*8*
expertise 62:*1*, *5*
experts 11:*11* 27:*25*
expired 64:*1*
explain 36:*7* 44:*18*
explaining 30:*21*
exploit 4:*14*, *22* 6:*13* 13:*17* 48:*7* 51:*14*
exploitation 49:*18*, *19*
exploits 49:*21*
express 2:*24* 24:*5* 36:*8*
extend 2:*4*
extent 51:*7* 58:*18*
extra 53:*17*
extract 13:*19*
extraordinarily 10:*17*
extreme 58:*16*
extremely 2:*13* 21:*12* 22:*18*, *19* 52:*25* 58:*22*
eyes 28:*11*

< F >
fabulous 38:*9*, *12*, *13* 40:*1*, *8*
face 15:*13*
fact 4:*1*
factoring 10:*15*
factors 35:*17*
facts 22:*1*
faculty 38:*13*
fail 4:*3* 28:*8*
failed 5:*1*
failing 40:*7*
fair 20:*7* 39:*16*
fairly 31:*11*
fake 60:*20* 61:*15* 64:*5*
fakes 7:*6* 60:*18* 61:*1*
false 3:*25* 4:*1*, *7* 50:*16*, *18*, *21*
famously 14:*19*
fantastic 41:*6*
far 39:*6* 51:*4*, *12*
fast 20:*12* 21:*3*
faster 3:*19* 37:*11* 48:*12*, *16*
favorite 19:*24* 30:*4*
fear 5:*4*
Federal 11:*4* 29:*15* 31:*7* 35:*9*, *13*, *22* 64:*18*
Fellow 8:*23*, *25* 12:*1* 26:*1*

fewer 51:*7*
fiction-y 62:*19*
field 3:*4* 34:*15* 35:*11* 40:*23* 44:*5* 46:*4* 52:*3*
fielded 45:*7*
fielding 40:*21* 43:*25*
fields 34:*5*
fighting 19:*14*, *15*
figuring 58:*23*
files 13:*18*
filing 12:*13*
fills 61:*25*
filter 13:*7*
filters 11:*9*
final 6:*23* 23:*2* 35:*21* 56:*4*
Finally 21:*10* 28:*2* 29:*15*
find 4:*3* 13:*16* 15:*2* 24:*1* 39:*16* 46:*9* 47:*24*, *25*
finding 63:*21*
finds 49:*22*
fine 28:*11*
finished 14:*8*
First 6:*3* 7:*2* 9:*6* 13:*22* 14:*10*, *11* 17:*3* 20:*19*, *23* 26:*19* 30:*1* 34:*4*, *6*, *7* 36:*4* 38:*7* 54:*21*
first-grade 8:*7*
firsthand 6:*8*
five 28:*23*
fleet 19:*6*, *8*, *14*, *16*
flip 4:*9*
flock 19:*13*
flooded 49:*13*
flow 55:*2*
focus 5:*13* 26:*14* 33:*25* 50:*7*
focused 43:*15*
fold 47:*9*
folders 13:*18*
folks 23:*10* 37:*11* 38:*12* 57:*2* 58:*23* 62:*17*
followed 46:*17*
following 14:*7* 21:*18*
follows 16:*3* 24:*13* 29:*22*
Food 54:*22*, *23*
fool 28:*8*
force 14:*23* 23:*10* 62:*8*
forces 4:*8*
forecasts 64:*12*
form 9:*19* 22:*18* 27:*20*
formal 27:*22*
former 41:*24*
forward 5:*12* 7:*21* 9:*4* 10:*24* 24:*11* 29:*21* 39:*19* 42:*2* 59:*17*, *23* 64:*22*
fought 63:*4*
found 23:*24* 61:*17*
Foundation 18:*16* 22:*5*
foundations 13:*10*
four 3:*9* 29:*12*
fourth-level 63:*1*
fraction 57:*4*
frankly 41:*13*
frequently 18:*18*
friend 5:*15*
friendly 47:*25* 48:*8*
front 61:*5* 62:*20*
frontier 29:*1*
frontiers 34:*19*
frontlines 23:*6*
fronts 9:*23*
frustrating 50:*22*
full 21:*8* 22:*12*
fully 14:*3* 39:*17* 58:*21*
fund 58:*9*
funding 22:*5* 48:*12*, *17*, *18*
further 34:*1* 46:*20* 55:*6* 56:*6*
future 4:*24* 33:*3* 55:*5*
futures 55:*15*

< G >
gain 11:*12* 38:*23*
gained 34:*8*
gaining 28:*6* 33:*16*
gains 3:*5* 50:*8*
game 21:*24* 60:*6*
games 21:*25*
gaming 56:*22*
Gary 31:*18*
general 10:*13* 13:*11* 18:*6* 52:*3*
generalize 9:*19*
generally 61:*6*
generate 3:*25* 51:*22* 60:*17*, *18* 61:*22*
generating 27:*24*
Geneva 54:*1*
geniuses 61:*23*
genuine 4:*3*
Georgetown 9:*1* 12:*2*, *7*
getting 22:*24* 34:*23*, *24* 37:*20*
giant 39:*14*
giants 38:*1*
give 7:*22* 8:*2* 10:*13* 19:*4* 32:*6* 33:*18* 39:*9*, *11*, *21* 40:*16* 41:*2*, *3*, *19*
given 18:*23* 27:*14* 39:*12* 52:*2* 55:*2*
giving 29:*20* 42:*12* 51:*15*
glass-to-glass 60:*24*
global 27:*4*
go 11:*5* 17:*2*, *7* 18:*17* 25:*8* 30:*10* 37:*22* 46:*3* 50:*1*, *13* 51:*4* 52:*23* 61:*24*
goes 45:*17*, *21*
going 3:*10* 7:*19* 11:*13* 18:*24* 20:*18* 22:*12* 24:*7*, *8* 30:*2*, *13*, *20* 33:*7* 34:*1* 35:*24* 41:*10*, *14*, *18* 42:*3* 43:*22* 45:*9* 46:*9*, *10* 51:*6* 52:*8* 53:*20* 55:*9*, *16* 56:*22* 60:*5*, *19* 64:*6*
good 5:*10* 6:*11* 9:*15* 11:*14* 32:*13* 37:*3* 42:*1* 47:*1* 58:*20* 62:*13*
Google 9:*2*, *3* 18:*2*, *7* 19:*22*, *23* 20:*13* 57:*12* 62:*21*, *23*
government 3:*1* 20:*9* 21:*21* 23:*24* 31:*7* 32:*15* 35:*9*, *22* 41:*15* 57:*22* 64:*18*
grade 39:*5*, *8* 40:*16*
graduating 36:*20*
Grand 14:*2* 18:*10* 48:*13*, *20* 56:*20*
granted 54:*24*
graphs 22:*17*
great 10:*18* 11:*10* 18:*18* 24:*10* 36:*9* 38:*14* 40:*18* 41:*10* 59:*5* 60:*6*
greater 58:*18*
greatly 18:*22* 40:*4*
grid 13:*23* 54:*13* 55:*18*, *19* 56:*1*
grids 55:*24*
ground 32:*9*
group 37:*8* 44:*25* 47:*5* 57:*3*
groups 37:*5*
grow 15:*20* 27:*6* 36:*25*
growing 27:*13* 47:*23*
grown 34:*13*
growth 3:*8*
guarantees 57:*7*
guess 11:*1* 27:*17*
guide 23:*12*

< H >
hacked 35:*24* 52:*18*
hackers 13:*22*
hacking 14:*13* 49:*24* 52:*15*
Hafnium 63:*7*
half 45:*7* 47:*3*
hand 13:*1*
handling 29:*10*
hands 35:*18*
happen 43:*10* 50:*1* 52:*12* 55:*16*
happened 62:*19*
happening 21:*3* 59:*1*
happens 20:*12* 23:*22*
happy 31:*18*
hard 10:*17* 23:*9* 27:*1* 35:*18* 53:*5*
hard-coded 14:*5*
harden 35:*23*
hardware 53:*19* 57:*21* 58:*14*, *16*, *21* 59:*6*
harness 10:*8*
harnessing 28:*25*
haystack 4:*4*
head 63:*23*
health 39:*13*, *14* 40:*3*
hear 8:*8* 9:*12* 28:*3* 56:*10* 60:*4*
heard 64:*19*
HEARING 1:*1* 2:*21* 5:*12* 6:*5*, *6* 7:*21* 8:*22* 9:*4* 29:*21* 30:*14* 59:*25* 64:*25*
hearings 6:*8* 59:*19*
hears 28:*16*, *17*
help 2:*7* 3:*19* 7:*23*, *24* 18:*10* 19:*21*, *22* 20:*9* 22:*14* 23:*12* 27:*2* 46:*22* 58:*9* 60:*3* 62:*8*
helpful 50:*19*
helping 24:*11* 38:*25* 39:*19* 51:*1*
helps 20:*4* 38:*22*
hesitate 40:*15*
Hey 23:*24*
Hicks 41:*9*
hide 27:*1*
high 42:*13* 46:*3*
higher 50:*21* 54:*9*
highlight 20:*19* 28:*23*
highly 2:*13* 15:*20*
hit 51:*17* 61:*24*
hitting 45:*14* 61:*2*
holding 56:*23*
holes 53:*5*
Hon 1:*12* 2:*1* 6:*1*
honor 12:*8*
hope 15:*18*
hopefully 51:*8*
horizon 29:*2*
Horovitz 17:*9*
horrible 54:*15*
Horvitz 8:*23* 9:*5*, *6* 10:*25* 12:*22* 15:*11* 17:*1*, *8* 18:*8* 25:*3*, *5* 26:*1*, *3*, *6* 29:*22* 34:*3*, *4* 38:*6*, *7* 39:*11*, *18* 40:*15* 43:*9*, *14* 44:*10*, *20*, *23* 47:*2* 48:*3* 50:*9*, *11* 51:*18* 52:*23* 55:*4* 57:*2* 59:*3* 60:*1*, *7*, *11*, *15* 63:*6*, *10*
Horvitz's 61:*14*
hospitals 53:*25*
hostage 52:*15*
hosted 14:*2*, *13*
hour 23:*17*

hours 46:*14*
hub 43:*8*
huge 2:*25* 19:*8* 20:*13*, *14* 33:*18* 40:*2* 45:*22* 57:*13*
human 3:*23* 7:*13* 9:*10* 11:*13* 12:*12* 13:*16*, *19* 14:*9* 21:*16* 26:*10* 27:*21* 28:*11* 35:*16*, *17* 44:*7* 57:*16* 59:*19*
humanly 2:*19*
humans 3:*19* 12:*14* 14:*7* 21:*3* 23:*2*, *7* 48:*3* 51:*1*, *11* 60:*19*
hundreds 53:*13* 57:*15*
hunt 13:*9* 30:*22* 32:*7*
hurdles 22:*25*
hybrid 45:*9*, *14* 55:*9*
hygiene 58:*9*
hyperscalers 20:*8*
hypothetical 19:*6*

< I >
IBM 31:*16*
IC 34:*19*
idea 50:*20* 61:*8*
ideally 23:*20* 61:*11*
ideas 35:*18* 42:*16*
identifying 26:*25*
if-then 12:*20*
ignore 22:*7*
illustrate 4:*19*
illustrated 20:*24*
image 14:*21* 28:*12*
images 61:*15*
imagine 14:*22* 48:*4* 55:*5*, *6* 61:*5* 62:*21*
imagining 29:*3*
immediately 23:*18* 45:*4* 46:*8*
impact 6:*20* 15:*16*
implement 39:*17*
implementation 39:*9*
implementing 64:*22*
importance 22:*24*
important 2:*6* 3:*12* 10:*4* 21:*12*, *25* 22:*6*, *19* 23:*13* 26:*5* 27:*3*, *8* 29:*19* 34:*9*, *10* 35:*6* 37:*2*, *13* 42:*18* 48:*25* 50:*25* 52:*25* 57:*11*, *22*
importantly 64:*17*
impossible 26:*22*
impressive 14:*6*, *9* 27:*22*
improve 13:*3*, *4* 19:*2*
Inaudible 63:*24*
incentivize 29:*6*
include 28:*18*
includes 27:*22* 29:*3*
including 10:*4* 20:*14* 43:*17* 47:*4*
incorporating 49:*4*
increase 4:*5* 27:*11* 44:*12*
increasing 4:*17*
increasingly 15:*21*
incredibly 23:*8* 37:*13* 57:*9*
individual 41:*14* 56:*13*
individuals 27:*24* 41:*4* 59:*20*, *24* 62:*11*
industrial 27:*18*
industry 3:*2* 8:*10* 23:*8* 33:*21* 37:*25* 38:*14*
infected 4:*23*
influence 60:*13*
information 9:*14*, *16* 19:*21* 22:*17*, *21* 23:*1* 27:*9* 35:*24* 37:*15* 57:*14* 61:*10* 63:*9* 64:*4*
infrastructure 8:*12* 11:*8* 53:*10*, *12*, *24* 54:*23*
infrastructures 6:*14* 11:*3*, *5*
ingeniously 21:*5*
injecting 28:*10*, *22*
innovation 3:*13* 33:*17* 62:*24*
input 51:*14*
inside 22:*9*
insider 21:*11*, *16*
insights 35:*19* 38:*23*
inspect 20:*2*
institutions 2:*7*
integrated 31:*24* 32:*1*
integrating 35:*14*
INTELLIGENCE 1:*1* 2:*9*, *12* 6:*21* 8:*3* 9:*3*, *10*, *11*, *21*, *24* 10:*3* 12:*12* 15:*17* 18:*2*, *14* 21:*12* 30:*14* 31:*5*, *15* 41:*12* 43:*2*, *7* 47:*22* 51:*13* 57:*3* 64:*14*
intensify 3:*3*
intensive 50:*14*
interaction 33:*8*
interconnected 54:*18*
interest 6:*7* 10:*20* 37:*7* 43:*21* 47:*24* 56:*23* 59:*6*
interested 46:*11*
interesting 10:*10* 20:*12* 21:*4* 26:*17* 31:*13* 38:*15* 45:*8* 51:*22* 59:*4* 61:*5*
interestingly 45:*6*
interfaces 22:*22*
international 42:*22* 43:*10*, *16* 53:*23*
internationally 54:*3*
internet 20:*8* 46:*10* 49:*24*
intersection 26:*15*
intersects 13:*2*
intro 25:*7*
introducing 43:*5*
introduction 7:*23*
intrusion 3:*21*
intrusions 4:*6*, *17* 13:*9*
invading 14:*23*
invest 28:*25* 30:*23* 38:*16*
invested 31:*6*
investigate 4:*2*
investing 5:*13* 30:*23*
investment 5:*9*, *11* 38:*13*
investments 64:*20*
invitation 7:*12*
inviting 12:*5* 26:*4*
Iridium 45:*1*
ISC 47:*5*
Israel 43:*7*, *8*
issue 24:*12*
issues 7:*25* 23:*13* 34:*21* 50:*13* 59:*21*
iteration 11:*13*
its 14:*10* 22:*4* 44:*3* 57:*19*

< J >
Jackie 30:*6*
JADC2 22:*20*
JAIC 43:*24*
job 27:*5* 40:*18* 46:*2*
jobs 37:*13* 42:*7* 45:*24*, *25* 46:*22* 47:*11*
Joe 1:*12* 2:*1*
John 21:*24*
join 22:*17* 43:*4*
joined 52:*17*
joining 46:*19* 47:*20*
Joint 22:*20* 43:*24*
jump 39:*19* 44:*20* 53:*20*
Junior 42:*12*

< K >
K-12 42:*4*
Kasparov 31:*17*, *18*
keep 7:*13* 8:*7* 20:*4* 31:*11* 59:*10* 63:*14*
Keeping 3:*4* 34:*20*
Kelly 1:*15* 47:*14*, *15*, *19* 48:*17*, *21* 49:*17* 50:*9* 51:*4*, *12* 52:*5* 55:*5*
kids 42:*13*
kind 12:*22* 20:*24* 22:*5* 28:*14* 34:*25* 35:*7* 49:*20* 61:*20* 62:*12*, *18*
kindergarten 2:*17* 8:*7*
kinds 10:*14* 21:*7* 46:*1* 54:*2*, *3* 55:*15* 56:*24* 57:*18* 61:*8*
kinetics 40:*1* 45:*10*
know 8:*5* 11:*3* 23:*3*, *18* 30:*5*, *17*, *23* 31:*9* 43:*12* 44:*13* 49:*14* 51:*16* 52:*17* 54:*14*, *18*, *19*, *20*, *21* 56:*20* 63:*25* 64:*21*
knowing 49:*6*
knowledge 22:*16* 64:*11*
known 20:*25* 44:*24* 49:*1*
Kyiv 45:*13*

< L >
lagging 5:*11*
landscape 6:*25*
language 9:*17* 10:*5* 30:*7* 51:*20*
languages 46:*7*
large 10:*15* 20:*4*, *7* 21:*13*, *15* 37:*4* 51:*20* 53:*6* 57:*4* 61:*6*
larger 10:*2* 51:*8* 56:*9*
large-scale 51:*20*
largest 59:*3*
lastly 11:*14*
latest 23:*17*
Laughter 18:*12*
law 42:*5* 44:*8*
laws 53:*23* 54:*3*
layer 53:*17*
lead 33:*17*
leader 44:*4*
leaders 41:*20*
leadership 29:*19*
leading 14:*9* 34:*16*
learn 9:*16* 37:*21* 38:*22* 46:*6*
learned 63:*6*, *8* 64:*23*
learning 2:*9*, *12* 8:*3* 9:*25* 10:*1* 11:*8* 12:*17*, *20*, *24* 14:*5* 21:*7* 22:*1* 26:*11* 30:*15* 31:*6*, *15*, *21*, *25* 32:*3*, *4*, *22*, *25* 33:*1*, *3*, *5* 34:*5*, *8*, *12* 37:*5*, *24* 40:*5*, *13* 46:*15*
learnings 56:*20*
learns 13:*12*
leave 18:*25*
led 56:*19*
leg 33:*19*
legacy 53:*3*, *6*, *19* 54:*6* 57:*21*
legislation 43:*6*
Lego 57:*13*
lesson 63:*10*
lessons 63:*8*
lethal 7:*6*
letter 40:*16*
level 2:*16* 8:*7* 46:*4* 48:*2*
leveling 34:*24*
leverage 8:*13*, *15* 43:*2*
leverages 34:*14*
leveraging 8:*11* 48:*6*
liberties 44:*4*
lie 26:*14*

lifecycle 29:*17*
lightning 34:*19*
like-minded 43:*16*
limited 4:*22*
lines 57:*25* 58:*20* 62:*20*
LinkedIn 47:*3*
links 28:*1*
listen 41:*24*
little 9:*18* 12:*23* 34:*1* 39:*23* 42:*2*, *21* 44:*18* 51:*14* 54:*4* 57:*25* 60:*2* 61:*13* 62:*5* 63:*8*
lives 64:*15*, *16*
locked 45:*13*
logic 12:*18*
logistics 40:*2*
Lohn 8:*25* 11:*18* 12:*1*, *3*, *6* 16:*3* 32:*19*, *20* 33:*13*, *15* 37:*18*, *19* 40:*13*, *14* 47:*21* 48:*9*, *18*, *23* 49:*19* 54:*4* 55:*17* 56:*15* 57:*24*, *25* 59:*9* 61:*12*, *13*
long 13:*8* 37:*21*
longer 12:*15*
look 5:*11* 7:*21* 9:*4* 24:*11* 28:*10*, *12* 29:*21* 36:*4* 45:*15* 48:*22* 51:*21* 52:*10* 55:*10* 57:*1* 59:*10*, *22* 64:*22*
looking 14:*22* 21:*1*, *16* 46:*2* 56:*24* 58:*12* 59:*19* 63:*2*
losing 32:*9*
lot 24:*6*, *8* 30:*14* 31:*12* 33:*22* 36:*12* 37:*22* 38:*11* 41:*25* 45:*22* 49:*1*, *4* 55:*16* 58:*3* 59:*6*, *7*
lots 19:*18* 22:*10* 23:*11* 35:*16* 41:*7* 43:*18* 56:*19*
loud 64:*19*
love 11:*4* 34:*5* 57:*17*
low 40:*16*
lowering 4:*6*
lowly 19:*5*, *7*

< M >
machine 2:*9*, *12* 7:*12* 8:*3* 10:*1* 11:*8* 12:*16*, *19*, *24* 14:*5* 30:*15* 31:*5*, *15*, *21*, *25* 32:*3*, *4*, *22*, *25* 33:*1*, *3*, *5* 34:*5*, *8*, *12* 40:*5*, *13* 46:*14*
machinery 39:*20*
machines 7:*16* 23:*3*, *8* 45:*2*, *13* 47:*24* 63:*12*
machine's 14:*2*
magic 41:*17*
magnet 38:*8*
main 63:*10*, *21*
maintain 42:*22*
major 22:*11* 23:*15* 37:*6* 62:*22*
majority 36:*17*
making 15:*12* 35:*23* 37:*11* 49:*9* 57:*13*
malicious 3:*18* 6:*12* 26:*16*
malign 7:*5* 60:*3*, *7*, *13* 61:*9*
malware 13:*9*, *24* 27:*18* 28:*1* 44:*14*, *24*, *25*
manage 13:*19* 53:*5*
management 4:*5* 32:*12* 62:*25*
Manager 18:*7*
Manchin 1:*13*, *14* 2:*1*, *3*, *18* 6:*3* 8:*18*, *19* 12:*4* 18:*4*, *15* 19:*5* 24:*7* 25:*1*, *7* 26:*3* 30:*1*, *5*, *8*, *12* 31:*14*, *24* 32:*5*, *14*, *19*, *20* 33:*7*, *14* 34:*3* 35:*20* 41:*22* 47:*14*, *17* 52:*6* 53:*1*, *20* 54:*13* 55:*21* 59:*13* 64:*9*
Manchin's 21:*19*
manner 29:*16*
manpower 3:*11*
manual 26:*22*
manually 4:*22* 13:*23*
Maps 19:*22*
marvels 14:*18*
massive 3:*5* 32:*10*
master 31:*17*
math 37:*22*
mathematician 21:*24*
mathematicians 57:*4*
matter 11:*14* 46:*14*
matters 18:*21*
maturing 48:*6*
mean 23:*14* 30:*5* 42:*25* 46:*24* 50:*13* 52:*14* 60:*8*
means 3:*6* 32:*11* 53:*11*
medium-sized 63:*15*
meeting 2:*3* 64:*24*
Mellon 18:*9* 21:*23* 36:*14*
Member 12:*4* 18:*5*, *19* 26:*3*
Members 1:*14* 2:*20* 12:*5* 18:*5* 26:*4* 36:*8* 56:*4*
mention 18:*10* 23:*2* 62:*8*, *23*
mentioned 9:*23* 20:*11* 26:*9* 40:*17* 43:*11* 48:*3* 51:*19* 56:*15* 60:*15*
mentioning 42:*8* 62:*14*
merely 15:*6*
mess 33:*24*
met 1:*11*
methods 21:*5*, *6* 26:*22* 27:*2*, *20* 28:*18* 56:*16*
microscope 10:*9*
Microsoft 8:*24* 26:*2*, *7* 35:*8* 38:*21* 44:*23* 63:*6*
Microsoft's 5:*9*
MIKE 6:*1* 25:*4* 30:*17*
military 7:*4* 15:*3* 41:*5* 42:*11*, *14* 47:*22*
million 27:*4* 44:*12* 47:*7*
millions 20:*25* 48:*19*
miniaturization 58:*22*
minus 39:*12*
minute 45:*20*
minute-by-minute 52:*19*
minutes 30:*2* 47:*15*
misconception 10:*12*
misinterpreted 25:*3*
misleading 19:*11*
misrepresentation 64:*6*
missile 7:*15*
missiles 45:*14*
mission 3:*12* 6:*18*
missions 2:*10* 7:*18* 8:*14*
mistake 4:*15*
mode 55:*2*
model 44:*24* 48:*14* 51:*20* 58:*4*
models 11:*9* 15:*9* 34:*22* 40:*3* 53:*14* 59:*3* 61:*22*
modern 13:*10* 19:*2* 53:*18*
modernization 53:*8*
mom-and-pop 57:*17*
moment 23:*9* 58:*23* 63:*4*
money 20:*4* 31:*3*
months 59:*2*
Moore 3:*14* 9:*2* 15:*11* 17:*7*, *10* 18:*1*, *4*, *6*, *13* 24:*10*, *13* 31:*11*, *14* 32:*2*, *9*, *18*, *21* 36:*13* 37:*2* 41:*1*, *3* 42:*8* 44:*10* 46:*5* 50:*9* 51:*5*, *6* 52:*24* 53:*2* 57:*1* 58:*1*, *20* 62:*15*, *16* 63:*22*, *24*
mouse 13:*23*
move 6:*15* 10:*23* 38:*25* 63:*17*
moved 42:*1*
moving 5:*4* 30:*25* 34:*15* 43:*1*
multiple 9:*13* 39:*8* 55:*10*, *24*
multiples 55:*25*
multi-pronged 55:*8*

< N >
name 18:*6* 32:*7*
names 10:*10*
Nash 21:*24*
nation 6:*19*
National 6:*24* 7:*9*, *16* 10:*20* 18:*16* 22:*5* 43:*1*, *14*, *23* 44:*11* 64:*15*
nations 43:*17* 44:*5*
natural 33:*24*
nature 60:*14*
Navy 19:*25*
nearly 26:*22* 27:*4* 47:*7*
necessarily 57:*20*
necessary 5:*5* 64:*19*
need 2:*22* 5:*13* 8:*1* 11:*14*, *15* 22:*11*, *13* 23:*7* 24:*2* 28:*25* 29:*6*, *9*, *12*, *15* 31:*8* 33:*25* 34:*25* 35:*17* 45:*18*, *19* 49:*3*, *10* 50:*13*, *15* 51:*7* 54:*2*, *8*, *9*, *11* 55:*13* 60:*21* 62:*2*, *11* 64:*12*
needed 34:*22* 41:*16*
needles 4:*3*
needs 8:*13* 20:*3* 57:*19*, *22*
negatives 50:*18*
net 44:*23*
network 13:*17* 20:*13* 45:*20*
networks 4:*12*, *14*, *16*, *18*, *21* 46:*13*
neural 44:*23*
never 23:*22* 26:*24*
New 6:*10*, *11*, *13* 7:*3* 13:*6*, *24* 21:*5*, *6*, *7*, *20* 23:*13*, *15*, *19* 26:*24* 36:*17* 38:*20* 41:*5*, *8* 46:*2* 47:*16* 48:*10* 53:*23* 54:*2*, *3* 58:*23* 61:*8*
news 37:*3* 58:*20*
nice 55:*23*
nicely 6:*25* 18:*24*
nightmare 23:*23*
noise 3:*18*
non-AI 60:*25*
non-classified 19:*7*
normal 8:*2* 12:*17*, *18*, *24*
normally 12:*12*, *13*
norms 53:*23*
note 55:*18*
noted 4:*4*
notice 1:*11*
notion 22:*16* 57:*11* 62:*17*
novice 57:*5*
novices 58:*6*
NSCAI 6:*25* 18:*8* 56:*3* 61:*7*
NSCAI's 18:*23*
nuanced 9:*18*
number 4:*22* 5:*6* 26:*15*, *16*
numbers 3:*25* 10:*15* 20:*14*

< O >

objects 14:*21*
observations 9:*14*
obvious 20:*24* 22:*3*
offense 27:*8* 51:*23*
offenses 14:*17* 29:*2*
offensive 2:*10* 4:*11* 13:*4* 27:*12, 16* 49:*24* 50:*5*
Office 1:*12*
Officer 8:*24* 26:*2, 6* 38:*2* 41:*9*
offline 46:*25*
Oh 17:*5* 45:*20* 60:*11*
okay 2:*16* 22:*10, 13* 32:*17* 61:*12* 63:*5, 22, 25*
old 32:*2* 53:*14* 63:*14*
ones 15:*6, 15* 54:*6*
ongoing 63:*19*
online 38:*16* 64:*4*
on-prem 53:*6* 63:*10, 11*
open 46:*1, 23*
opened 47:*3*
OPENING 2:*1* 39:*25* 62:*14*
open-source 58:*3*
operate 14:*1*
operating 7:*11* 53:*14*
operation 4:*20* 28:*5, 19* 40:*2*
OPERATIONS 1:*2* 2:*11, 23* 4:*9, 11* 13:*4* 41:*19* 43:*18*
operators 7:*13* 55:*18*
opportunities 27:*5* 36:*9* 38:*4* 39:*8* 43:*15* 50:*6*
opportunity 20:*9* 24:*10* 29:*20* 33:*21* 37:*25* 48:*11* 50:*3, 12* 57:*14* 58:*9* 61:*6* 62:*6*
oppose 61:*18, 19*
optimistic 39:*2, 21*
optimize 55:*11*
option 3:*14*
order 2:*3* 30:*20* 56:*1* 60:*12*
organization 40:*10* 46:*19* 47:*6*
organizational 22:*25* 32:*11*
organizations 11:*7* 15:*10*
organize 19:*21* 20:*21*
outcome 61:*1*
outgunned 19:*9*
outside 54:*9*
overstate 2:*22* 15:*16*
overview 8:*2* 9:*7* 30:*13*
overwhelm 14:*25*
overwhelmed 4:*2*
owner 28:*17*
owns 64:*3*

< P >
p.m 1:*11* 64:*25*
pace 26:*12* 27:*14* 34:*20*
panelists 33:*23* 36:*15*
papers 48:*11*
part 9:*25* 10:*1, 2* 21:*13, 15* 22:*8* 34:*9* 36:*6* 37:*6*
particular 6:*7* 15:*12* 43:*21*
partnered 62:*24*
partners 43:*10*
partnership 19:*25*
partnerships 29:*7* 42:*10, 22*
parts 14:*23* 20:*19* 54:*17*
passed 42:*5*
passwords 27:*17*
patch 45:*4* 47:*25* 48:*7* 49:*5, 14* 54:*7*
patched 53:*18*
patches 11:*16* 23:*21* 48:*3* 49:*1, 4, 9, 11, 12*
patching 48:*24*
path 47:*9*
pattern 20:*17* 26:*10, 23* 44:*14, 19*
patterns 3:*18* 11:*6* 21:*7, 17* 28:*11*
peacetime 40:*2*
pecking 30:*19*
penetrations 3:*20*
people 3:*15, 16* 20:*21* 21:*5* 22:*13, 25* 23:*6, 16, 18* 24:*2* 27:*25* 34:*4* 37:*16, 25* 38:*1* 40:*23* 42:*3, 6, 17* 45:*18, 22* 46:*24* 47:*9, 11, 17* 48:*4* 50:*13* 51:*10* 57:*10* 58:*4* 61:*17* 62:*2, 9, 11*
perceive 9:*12*
percent 27:*6*
perception 26:*10*
perform 7:*18* 12:*11* 48:*2*
perimeter 21:*11*
permissive 40:*24*
persistent 56:*8*
person 3:*11* 22:*1* 41:*10* 46:*18* 51:*9*
personalize 27:*24*
personnel 3:*1*
perspective 33:*20*
perspectives 8:*9* 56:*10*
pessimistic 40:*14*
PhD 12:*1* 18:*1* 26:*1*
PhDs 37:*8* 45:*23*
phishing 27:*24*
phone 22:*14*
phrase 34:*7*
physicists 10:*10*
physics 10:*8*

pick 22:*13*
picked 56:*22*
picking 45:*8*
picture 22:*18*
pictures 20:*1*
piece 44:*24* 57:*15*
pieces 9:*14* 53:*10*
pipeline 42:*6* 52:*12* 55:*1, 8*
pipelines 53:*25*
pixel 61:*3*
pixels 14:*20*
place 33:*25* 35:*13* 60:*19* 63:*3*
places 20:*14* 30:*24* 35:*1* 36:*22* 57:*12*
plan 45:*16* 55:*12* 63:*9*
planful 45:*11, 15*
planning 40:*3, 6*
platform 42:*19* 57:*9*
platforms 23:*11* 35:*8* 47:*9* 57:*7, 8* 58:*13*
play 46:*7* 55:*4*
plays 21:*13, 15*
Please 8:*1* 41:*19*
plenty 50:*15*
plug 46:*24*
plus 45:*10*
point 3:*9* 33:*20* 34:*17* 40:*22* 46:*18* 61:*20* 62:*16* 63:*21*
pointed 43:*2, 23*
points 37:*20*
poison 62:*18*
poisoned 28:*21*
poker-playing 21:*22*
policy 8:*1*
population 3:*10* 61:*18*
poses 6:*11*
position 23:*24* 31:*1*
positive 3:*25* 60:*13* 62:*13*
positives 50:*17, 18, 22*
possibilities 39:*24* 43:*20*
possible 2:*19* 13:*16* 19:*1, 10, 12* 20:*3, 25* 23:*11* 42:*4*
possibly 4:*2* 21:*2*
post 49:*24*
post-graduate 38:*15*
postmortems 23:*22*
potential 4:*19* 10:*12* 14:*12* 15:*19, 23* 39:*12* 47:*24* 64:*15*
power 3:*7, 11* 4:*16* 9:*17* 13:*22* 19:*17* 21:*8* 26:*17* 27:*12* 58:*13, 15, 17* 60:*6, 17*
powered 3:*13*
powerful 23:*7* 31:*22* 51:*9, 14*

powers 19:*20*
practical 59:*17*
practically 3:*6*
practices 29:*8* 53:*24* 54:*3*
precise 56:*6*
predict 19:*22*
predicted 26:*12*
prediction 26:*11*
predictions 40:*5*
predictive 11:*9* 40:*3*
pre-general 51:*24*
prepare 7:*8* 27:*14* 55:*14*
prepared 2:*23* 3:*15* 16:*3* 17:*3* 24:*13* 29:*22* 64:*18*
presence 64:*3*
Present 1:*14*
President 9:*2* 18:*1, 6*
presiding 1:*13* 10:*21* 25:*1*
pretty 22:*23* 33:*11*
prevailing 64:*2*
preview 38:*21, 24*
previously 18:*8*
principles 34:*16* 44:*2*
prioritize 64:*18, 19*
priority 64:*21*
private 30:*25* 31:*2, 4* 35:*7, 10* 38:*21, 24*
private-public 43:*11*
proactive 55:*15*
probably 35:*1*
problem 59:*21*
problems 10:*14, 17* 43:*13* 50:*16* 59:*21* 60:*3*
problem-solving 59:*23*
process 3:*22* 12:*23* 24:*1*
processes 28:*6* 60:*4*
procurement 23:*25*
product 5:*9*
productivity 3:*6, 8*
products 3:*25* 5:*8* 19:*20* 33:*23*
professional 47:*6*
professionally 11:*10*
professionals 7:*17* 27:*5* 47:*10*
profit 52:*16*
profound 25:*7*
program 8:*3* 31:*1* 39:*22*
programming 61:*25*
programs 9:*8, 20* 12:*17, 18, 24* 29:*12, 18* 31:*7* 36:*19* 37:*14, 16* 38:*12, 15, 16, 18*
progress 9:*22* 48:*10* 49:*10, 11* 50:*4*
project 12:*6* 38:*22* 63:*7*
projected 27:*6*
projects 29:*17* 46:*8*

prolific 52:*14*
promises 13:*3*
promising 59:*10*
promote 29:*7*
promoted 47:*5*
prompts 51:*21* 52:*2*
properties 59:*5*
proposal 34:*6*
proprietary 28:*20*
prospect 53:*21*
protect 7:*18* 8:*16* 11:*2* 29:*4, 17* 45:*5* 50:*22* 54:*10*
protected 35:*25* 63:*13*
protecting 13:*7*
protection 49:*16*
protections 10:*19* 54:*9*
proud 20:*8* 38:*7*
prove 15:*25*
provenance 60:*23*
provide 2:*14* 3:*23* 6:*16* 15:*12*
provided 15:*10* 58:*2*
providing 38:*18*
public 2:*20* 52:*4*
public-private 42:*10*
pull 37:*25*
purpose 10:*13*
purposes 7:*10*
pursuant 1:*11*
push 15:*12* 29:*1* 35:*5* 38:*3* 48:*15* 49:*3* 50:*1* 59:*23*
pushing 11:*15*
Put 7:*19* 23:*11* 40:*16* 41:*11* 45:*2* 49:*5, 10* 57:*12, 15*
putting 23:*6* 31:*8*
Python 46:*6, 17*

< Q >
quantities 3:*23*
quantum 8:*4* 10:*7, 8, 13, 14, 16* 12:*22* 43:*12*
question 9:*7* 10:*25* 11:*1* 12:*9* 17:*5* 36:*13* 37:*2* 39:*4* 52:*1* 55:*6* 62:*16* 64:*2*
questions 17:*3* 24:*7, 8* 29:*21* 30:*11* 31:*13* 52:*4, 7*
quick 41:*2* 50:*6* 52:*7, 8*
quickly 4:*18* 6:*13, 15* 7:*9* 11:*15, 18* 20:*2, 3* 23:*2, 12* 26:*18* 30:*16* 32:*5* 34:*15* 40:*9, 21* 49:*21* 50:*2*
quite 32:*13* 40:*14, 16* 51:*11* 56:*22*
quote 7:*1* 47:*23*

< R >
R&D 28:*25* 61:*9*
raise 53:*21*
RAND 47:*21*
ranging 7:*6*
rank 32:*6*
Ranking 12:*4* 18:*5, 19* 26:*3* 32:*6*
ranks 38:*2*
rapidly 6:*9*
rate 4:*6* 48:*12*
rates 36:*21*
readiness 20:*5*
ready 5:*2* 21:*11* 30:*9, 10* 42:*9* 62:*25*
real 4:*6* 15:*2* 19:*2* 21:*8, 15* 26:*21* 32:*5* 49:*3* 52:*3, 8* 60:*20, 21* 61:*25* 64:*5*
really 8:*21* 13:*19* 18:*13, 15, 17, 18, 21* 23:*25* 30:*17* 32:*13* 33:*25* 34:*20* 36:*24* 37:*1* 38:*12* 39:*19* 40:*8* 41:*6, 13* 42:*17* 44:*15* 45:*19, 21* 46:*10, 21* 47:*4* 50:*7* 51:*13* 54:*19* 57:*10, 11, 22* 62:*2* 64:*16*
real-world 2:*14* 35:*15*
reason 9:*12* 40:*15*
reasoning 26:*11*
reasons 13:*21* 53:*16*
RECEIVE 1:*1*
recognition 10:*5* 26:*10* 28:*16* 36:*10* 44:*14, 19* 46:*15*
recognize 8:*20* 9:*11* 26:*23*
recommend 20:*18* 63:*17*
recommendations 5:*12* 18:*23* 28:*23*
record 36:*21*
red 27:*13* 55:*4*
red-teaming 29:*3* 55:*14*
reducing 50:*18*
refer 44:*25*
referring 58:*7*
refers 18:*25*
regard 39:*5, 7* 51:*25* 56:*10, 11*
regarding 53:*24*
related 44:*24*
relation 42:*24*
relationship 18:*16*
relative 19:*11* 58:*6*
relatively 50:*5*
release 58:*4*
relied 13:*14* 14:*5*
remarks 5:*16* 26:*14*
remember 53:*12*
repair 20:*4*
replicate 36:*21*
report 6:*23* 45:*7* 56:*4* 61:*7*
represented 15:*11* 33:*18* 58:*2* 61:*2*
require 3:*5* 12:*12*
required 12:*14* 61:*21* 62:*1* 63:*13*
requirements 51:*15, 16*
requires 59:*11* 61:*22* 62:*5* 63:*11*
research 22:*6* 29:*8* 35:*5* 43:*18* 48:*10* 61:*9*
researchers 26:*8* 27:*14, 16* 28:*9* 34:*11* 35:*5*
reserve 23:*4* 37:*14, 15* 42:*9*
reserves 42:*11*
resist 21:*18*
resonant 44:*1*
resonates 44:*6*
resort 7:*3*
resource 35:*4*
resources 15:*13* 34:*21* 37:*24* 42:*10* 57:*12* 58:*1* 63:*19*
respect 18:*17* 33:*6*
respectfully 35:*21*
respond 4:*18* 23:*12* 26:*21* 36:*15*
response 62:*9*
responsible 43:*24*
responsibly 7:*9*
rest 61:*25*
result 14:*10*
results 30:*24* 56:*24*
retaining 59:*20*
return 11:*18*
revolution 9:*25*
revolutionize 64:*16*
rich 47:*4*
right 11:*2* 24:*3* 30:*10, 24* 32:*2* 33:*1, 4* 34:*21* 35:*3* 36:*12* 38:*25* 40:*10* 44:*15* 50:*16, 23* 55:*5, 24* 59:*5*
rights 44:*7*
rise 60:*16*
rising 28:*2*
roadmaps 37:*6*
robin 17:*2*
robots 21:*22*
robust 45:*19*
rogue 7:*7* 52:*21*
role 38:*10*
Room 1:*12*
Rosen 1:*15* 30:*4, 7, 11* 41:*22, 23* 44:*9, 22* 45:*17* 46:*21* 47:*11*
RoseTTAFold 39:*19*
ROTC 42:*12*
round 17:*2* 52:*7, 8*
Rounds 1:*15* 2:*17* 5:*15* 6:*1, 3* 8:*19* 10:*21* 11:*17* 12:*4* 17:*1, 5, 9* 18:*5, 19* 25:*6* 26:*4* 30:*2* 36:*3, 4* 37:*18* 38:*6* 39:*4, 16* 40:*12* 41:*1, 21* 42:*3* 55:*21, 22* 57:*24* 58:*11* 59:*8, 12* 64:*21*
route 19:*22*
Rubio 43:*4*
rule 44:*8*
rules 12:*20* 14:*5*
run 14:*17* 50:*10* 53:*9* 61:*24*
running 39:*22* 46:*14*
rush 15:*3*
Russell 1:*12*
Russia 4:*25* 13:*22* 14:*15* 44:*16* 45:*2* 52:*14* 55:*19*
Russian 4:*19* 31:*17*
Russians 4:*21*

< S >
safer 51:*25* 53:*11*
sale 39:*20*
sanctions 61:*18*
Sandworm 45:*1*
saved 31:*3*
saves 20:*4*
saw 47:*6* 55:*10*
saying 2:*15* 32:*15*
says 28:*17*
scale 3:*4* 4:*9* 10:*9, 16* 27:*2, 11* 32:*11* 56:*9*
scales 26:*21*
scan 4:*12*
scarce 27:*9* 56:*16*
scares 55:*20*
scenario 19:*15*
scenarios 19:*16* 22:*11*
scene 60:*20*
school 42:*13* 46:*3*
Science 12:*10* 18:*16* 22:*5* 34:*16* 46:*7, 18* 57:*11* 62:*18*
Scientific 8:*24* 26:*2, 6* 33:*10* 34:*19* 35:*14*
scientists 9:*20* 34:*20*
scope 3:*3*
scratch 37:*23*
sea 3:*18*
seagulls 19:*13*
search 13:*9* 19:*9, 18*
second 10:*25* 19:*10* 21:*1, 4* 22:*8* 27:*7* 53:*21* 63:*1*
seconds 55:*17*
secret 15:*23*
Secretary 41:*9*
secrets 28:*19*
sector 30:*25* 31:*2, 4* 35:*7,*

10 37:*4*, *10*
sectors 35:*19*
secure 14:*3* 20:*15* 29:*16* 32:*16* 53:*10* 54:*25* 57:*20*, *22* 62:*25* 63:*11*
securing 53:*12*
security 4:*4* 6:*24* 7:*10*, *16* 8:*25* 10:*20* 12:*2*, *7* 27:*25* 29:*13* 43:*1*, *14*, *23* 44:*11* 53:*5* 57:*5*, *7*, *15* 58:*8* 63:*17* 64:*15*
see 9:*12* 11:*4* 20:*17* 21:*16*, *22* 34:*24* 37:*13* 40:*8* 41:*7* 42:*13* 44:*15* 45:*23* 46:*17* 47:*11*, *15* 50:*10*, *11* 52:*10* 57:*18* 60:*15* 63:*22*
seeing 26:*11* 38:*24* 45:*6*
seeking 22:*21*
seen 9:*24* 10:*9* 15:*22* 26:*24* 28:*11* 56:*18*
self-help 38:*18*
self-learning 38:*18*
Senate 1:*6*, *12* 2:*8* 7:*25* 36:*8*
SENATOR 2:*1*, *3*, *17*, *18* 5:*15* 6:*1*, *3* 8:*18*, *19* 10:*21* 11:*17* 17:*1*, *5*, *9* 24:*7* 25:*1*, *6*, *7* 30:*1*, *4*, *5*, *7*, *8*, *11*, *12* 31:*24* 32:*5*, *14*, *19*, *20* 33:*7*, *14* 34:*3* 35:*20* 36:*3*, *4* 37:*18* 38:*6* 39:*4*, *16* 40:*12* 41:*1*, *21*, *22*, *23* 42:*3* 44:*9*, *22* 45:*17* 46:*21* 47:*2*, *11*, *14*, *15*, *17*, *19* 48:*17*, *21* 49:*17* 50:*9* 51:*4*, *12* 52:*5*, *6* 53:*1*, *20* 54:*13* 55:*21*, *22* 57:*24* 58:*11* 59:*8*, *12*, *13*, *14* 60:*9*, *12* 61:*12* 62:*7* 63:*5*, *22*, *25* 64:*9*, *21*
Senators 1:*14* 43:*4*
send 52:*13*, *20*
Senior 8:*25* 12:*1*
sense 11:*5*
sensible 53:*9*
sensors 22:*15*
sentiments 2:*24*
separate 12:*25* 34:*10*
sequences 55:*11*
serious 36:*8* 53:*5*
serve 20:*9* 26:*6* 30:*17*, *19* 38:*10*
served 18:*7*, *9* 44:*11*
service 38:*5*
servicemembers 38:*4*
Services 1:*8* 2:*8* 22:*22* 24:*3* 30:*18* 38:*1*
servicing 20:*3*
serving 42:*14*
set 22:*14* 51:*15*
sets 12:*20* 47:*4* 59:*22*
setting 50:*21*
seven 14:*13*
severity 15:*17*
shaking 63:*22*
share 6:*23* 22:*25* 35:*18* 64:*21*
shared 42:*19*
sharing 22:*21* 29:*7* 43:*17* 64:*11*
shields 44:*17*
shifting 50:*14*
shops 57:*17*
short 4:*8* 7:*23* 8:*2*
shortage 3:*2* 45:*21*
shortfall 2:*25*
shot 41:*2*
show 27:*23*
showing 34:*23* 59:*4*
shut 13:*23* 52:*21* 54:*16* 55:*1*, *19*
shutdown 50:*22*
side 4:*10*, *11* 21:*20* 27:*21* 34:*6* 49:*17* 50:*4*, *5*, *7* 51:*8*
sides 20:*1*
sign 28:*10*
signal 52:*14*, *21*
signals 3:*17* 26:*25* 28:*15* 45:*8*
signs 28:*12* 45:*8*
siloed 43:*13*
silos 22:*10* 43:*11*
similarities 26:*25*
Similarly 15:*22*
simple 46:*13*
simplify 2:*19*
simply 7:*19* 14:*1* 18:*25* 30:*13* 34:*8*, *9*
single 55:*8* 57:*15*
sir 25:*1*
sit 41:*23*
situation 32:*16* 40:*23* 44:*20* 49:*13* 50:*23* 54:*16*
situations 9:*13*
skilling 38:*15*, *16*
skills 37:*9* 38:*4* 46:*11* 61:*21*
sleeping 39:*14*
slip 49:*15*
slow 50:*4*
small 33:*5* 37:*8* 53:*10* 63:*15*
smart 62:*2*
social 22:*25* 27:*20*
society 35:*10* 64:*17*
soft 27:*21*
software 3:*13* 4:*20* 9:*9* 12:*13*, *16*, *17* 14:*16*, *19* 15:*22* 45:*2*, *3* 53:*9* 58:*23* 63:*14*, *20*
SolarWinds 4:*19*, *20*
solution 62:*25*
solutions 19:*23*
solve 10:*17* 21:*24* 59:*20* 60:*3*
solves 10:*14*
solving 24:*1*
somebody 12:*18* 34:*1* 46:*2* 47:*12* 49:*22*
somewhat 48:*9*
soon 15:*2*, *25*
sorry 17:*9* 25:*3* 53:*1*
sort 12:*23* 20:*18* 22:*24* 50:*23* 53:*8* 57:*21* 58:*7*
sorts 46:*6* 51:*22*
sounds 8:*5*
source 58:*18* 61:*10*
sources 22:*18*
SOUTH 6:*1* 36:*23*
space 19:*10* 31:*9* 50:*15*
SpaceX 31:*1*, *8* 35:*7*
Spam 13:*6*
spans 27:*16*
speak 46:*4*, *25*
speaking 3:*6*
special 9:*9* 10:*14* 17:*3* 29:*11*, *13*
specialized 59:*6*
specifics 9:*19*
spectrum 45:*22*
speech 10:*5* 28:*15*
speed 4:*9* 5:*5*
speeds 7:*12* 14:*2*
spoke 18:*11*
spread 34:*18* 49:*21* 61:*10*
SR-232A 1:*12*
stake 14:*21*
stand 62:*24*
standardization 53:*17*
standards 54:*10*
start 9:*5* 12:*3* 23:*25* 30:*13* 31:*10* 42:*4*, *6* 52:*8*, *22* 55:*13*
started 37:*21* 41:*25* 42:*12*
starting 59:*10*
starts 46:*6*, *7*
startups 46:*10* 57:*17*
state 8:*9* 20:*14* 36:*23* 46:*23*
stated 47:*23* 56:*4*
STATEMENT 2:*1* 3:*15* 6:*1* 12:*1* 16:*3* 17:*3* 18:*1* 24:*13* 26:*1* 29:*22*
statements 2:*24*
States 6:*17* 7:*7*, *8* 14:*12* 35:*2* 36:*18* 37:*6*, *8* 44:*1* 56:*13*, *25*
station 45:*13*, *14*
stay 11:*16* 59:*16* 60:*5*
steal 28:*18*
stealthier 56:*7*
stealthy 28:*14*
STEM 42:*5*, *13*
step 33:*21* 62:*13*
steps 36:*25*
stop 28:*10*, *12* 52:*20* 61:*24*
strange 21:*16*
strategic 7:*3*
strategies 29:*4* 50:*20*
strategy 41:*12*
strong 52:*13*, *21*
strongly 20:*18* 23:*5* 24:*2*
struck 14:*12*
structured 41:*4*
structures 32:*10*, *12*
student 46:*5*
students 36:*20* 37:*5*
studied 36:*18*
study 33:*15* 47:*21* 51:*24* 61:*6*, *16*
stuff 24:*3*
stunning 28:*9*
sub-area 10:*3*
Subcommittee 1:*7*, *11*, *13* 2:*8* 6:*8* 12:*5* 26:*4* 30:*4*, *18*
subset 33:*5*
subtle 3:*17* 26:*25*
subvert 34:*2*
succeed 15:*13* 41:*11*
success 36:*22* 41:*10*
successes 10:*12*
sun 19:*11*
supercharging 10:*4*
supercomputers 19:*18*
superhuman 19:*18*
super-human 32:*11*
superior 3:*13*
superiority 52:*10*
superposition 10:*11*
super-quick 41:*3*
supply 4:*20* 15:*5* 54:*22*
support 5:*4* 18:*14*, *20*, *22* 23:*5* 41:*15*, *19* 61:*18*
supported 18:*15*
supporting 58:*21*
supportive 22:*19*
suppose 19:*9*
sure 21:*21* 23:*9*, *22* 33:*8* 35:*23* 36:*2* 42:*16* 48:*18*
surely 15:*24*
surface 61:*2*
surfaces 23:*15*
surge 42:*10*
surprisingly 52:*2*

surveillance 63:*19*
susceptible 15:*1*
suspicious 3:*24*
swarms 7:*15*
synonymous 32:*24*
system 11:*15* 12:*11* 13:*19* 14:*6*, *21* 15:*1* 23:*19* 28:*8*, *13*, *16*, *19*, *20*, *22* 39:*1*, *14* 40:*4* 46:*15* 51:*13*, *19*, *25* 54:*14*
systems 4:*5* 6:*14* 9:*8* 11:*11* 14:*3*, *4*, *14*, *18*, *24* 15:*1*, *4*, *5*, *8*, *14*, *23*, *25* 26:*18* 27:*18* 28:*3*, *5*, *8*, *21* 29:*4*, *9*, *14*, *16* 31:*20* 34:*2* 41:*17* 45:*5* 46:*13* 47:*25* 48:*1*, *8* 49:*6*, *18*, *19* 50:*17* 51:*3* 52:*2*, *24* 53:*2*, *3*, *6*, *14*, *18* 54:*5* 55:*10* 57:*7*, *14*, *19* 58:*14* 60:*18* 62:*18*, *21*

< T >
tactics 13:*12*, *13*, *14*
tailored 56:*6*
take 4:*25* 13:*23* 20:*1* 30:*9* 36:*25* 38:*5* 49:*5* 54:*24* 55:*16*, *25* 58:*24* 63:*18*
taken 2:*5*
takes 35:*11* 58:*13*
talent 38:*8*
talk 12:*9* 13:*1* 20:*10* 22:*8* 32:*24* 36:*1* 39:*23* 41:*7* 42:*19*, *21* 43:*9* 44:*15* 45:*25* 58:*12* 60:*1* 63:*7*
talked 61:*7*
talking 30:*7* 54:*19* 57:*6*
tangible 19:*4* 42:*17*
target 4:*25* 15:*5* 28:*5*
targets 4:*22* 13:*17*, *18* 14:*24*
task 46:*22*
tasks 12:*11* 26:*8* 48:*2*
taught 46:*17*, *18*
tax 12:*13*
team 39:*1* 55:*4*
team-on-team 56:*19*
teams 11:*14* 14:*9* 27:*2*, *13* 29:*13* 45:*1* 63:*15*
tech 58:*2*, *8* 63:*18*
technical 2:*19* 8:*23* 26:*1* 34:*18*
technically 2:*13*, *25*
techniques 13:*10* 14:*22* 26:*22* 28:*5*, *8* 33:*1*
technological 14:*18* 42:*23*
technologies 3:*22* 6:*10*, *14*, *16*, *19* 7:*4*, *24* 8:*10* 18:*25* 21:*20* 27:*10* 35:*12* 40:*20* 43:*8*, *17*, *25* 44:*6* 48:*16* 49:*8* 55:*7* 60:*17*, *21* 62:*3*, *10*
technology 2:*10* 3:*7* 4:*16*, *24* 5:*7* 6:*20* 7:*18* 9:*1* 12:*2*, *7* 37:*15* 48:*5*, *10* 53:*20* 55:*11* 58:*24* 60:*22*, *25* 61:*15*
tell 30:*5*, *8* 64:*13*
telling 44:*17*
tens 48:*19* 53:*13*
terms 32:*23* 39:*6*
terrorists 7:*7*
testify 26:*5* 29:*20*
TESTIMONY 1:*1* 60:*16*
text 61:*16*, *22*
Thank 6:*3*, *4* 8:*17*, *19* 9:*6* 10:*22* 11:*17* 12:*3*, *5* 16:*2* 17:*8* 18:*4*, *13*, *19*, *22* 23:*5* 24:*10* 25:*1* 29:*19* 30:*1*, *12* 31:*14* 32:*20* 35:*20* 36:*4*, *5* 37:*2*, *18*, *19* 38:*6* 39:*4* 41:*1*, *21*, *22* 42:*8* 44:*9*, *22* 46:*21* 47:*13*, *14*, *19* 52:*5*, *6* 55:*22* 59:*12*, *14* 62:*16*, *17* 63:*5*, *25* 64:*8*, *9*, *10*
thanking 12:*4*
thanks 2:*4* 26:*4*
theory 21:*25*
thing 6:*11* 8:*5* 10:*7* 22:*4* 23:*2* 24:*1* 28:*14* 30:*8*, *16* 33:*2*, *4* 35:*1* 42:*1* 47:*16* 54:*1* 62:*23*
Things 21:*3*, *22*, *25* 31:*16* 36:*12* 37:*14*, *23* 40:*20* 41:*5* 46:*1* 54:*11*, *24* 55:*23* 59:*17* 60:*10*, *14*
think 6:*20* 8:*12*, *21* 11:*12* 19:*8* 20:*7* 30:*3* 35:*15* 36:*6* 37:*3*, *24* 38:*2* 39:*2*, *13*, *25* 40:*17* 41:*18* 42:*1*, *15* 46:*21* 47:*6*, *8* 48:*11*, *14* 50:*3*, *5*, *8*, *13* 51:*2* 52:*11* 54:*2*, *13*, *25* 55:*7*, *13*, *23* 57:*4*, *10* 60:*1* 61:*7*, *8* 62:*13* 63:*7* 64:*1*
thinking 25:*6* 35:*4* 44:*5* 55:*13*
third 63:*1*
thought 17:*2* 25:*3*, *8* 57:*16* 58:*11*
thoughts 8:*14* 24:*6*
thousands 4:*21* 51:*1* 53:*13* 57:*16*
threat 21:*11* 23:*15*, *20* 56:*11* 62:*6*
threats 3:*3* 7:*9* 21:*16* 23:*1* 36:*9*
three 8:*20* 13:*2*, *4* 20:*19* 26:*14*, *17* 27:*4* 29:*9* 30:*3*, *12*, *19* 35:*21* 47:*7*
thresholds 50:*24*
thwart 60:*12*
time 2:*5* 6:*11*, *12*, *13* 9:*16* 19:*2*, *13* 20:*14* 21:*8* 22:*2* 26:*21* 31:*20* 33:*22* 34:*7* 36:*6* 39:*21* 41:*2* 42:*25* 43:*15* 45:*11* 50:*19* 61:*2* 64:*1*, *8*
times 3:*9* 12:*19* 14:*8* 36:*17*
today 2:*5* 3:*22* 6:*5* 7:*21* 8:*11*, *17* 15:*9* 26:*5*, *14*, *20* 29:*20* 32:*25* 36:*6* 39:*10* 42:*20* 49:*1*, *20* 50:*5* 56:*11*, *14* 59:*1* 64:*23*
today's 6:*6*
told 59:*1*
tool 13:*8* 58:*5*
toolkit 49:*25*
toolkits 49:*24*
tools 7:*2* 15:*9* 23:*7*, *9*, *18* 35:*8* 37:*17*, *23* 38:*13*, *17*, *19* 51:*9* 52:*3* 58:*1*
top 14:*7* 41:*17*
topic 6:*6* 26:*5* 29:*20*
topics 2:*13*
top-notch 63:*17*
touch 11:*16*
touches 12:*23*
touted 13:*8*
track 42:*13* 61:*4*
train 15:*7* 28:*20* 37:*16* 46:*20*
trained 2:*25* 11:*11* 23:*10*
training 28:*22* 29:*12* 37:*12* 50:*19*
trajectories 19:*11*
trajectory 59:*10*
transmission 54:*17*
transportation 55:*2*
tremendous 8:*21*, *22* 34:*25* 50:*11* 54:*14*, *15* 55:*1*
tremendously 4:*10*
triage 51:*1*
tricks 19:*12*
tried 33:*15*
trillion 19:*10*, *16*
Trust 21:*13*
trustworthy 15:*7*, *10*, *15*
try 27:*1* 41:*2*, *5* 44:*18* 46:*22* 57:*21*
trying 19:*5*, *7* 33:*24* 36:*7* 40:*20*, *23*, *25* 60:*9*
Tuesday 1:*4*
turn 5:*15*
turns 44:*2*
two 13:*3* 20:*20* 23:*20* 26:*16* 32:*23* 35:*1* 37:*19* 56:*3* 58:*20*
type 61:*24*
types 28:*18* 31:*8* 36:*21*
typically 26:*9*

< U >
U.S 1:*6* 2:*1* 6:*1* 19:*6*, *25* 20:*9* 23:*23* 33:*16* 34:*16* 36:*22* 41:*5* 43:*7* 44:*4* 51:*8* 53:*2*
U.S.-Israel 43:*5*
Ukraine 13:*22* 44:*16*, *21* 45:*2*, *5*, *6*, *8* 48:*4* 55:*9*
ultimately 14:*8*
ultra 27:*23*
umbrella 32:*21*
unacceptable 54:*12*
unanswered 64:*2*
unbelievable 30:*20*
uncertain 9:*15*
unclear 14:*14*
underneath 57:*8*
understand 6:*16* 9:*17* 29:*2* 32:*23* 35:*11* 36:*19* 39:*22* 42:*17* 45:*23* 46:*22* 64:*16*
understanding 7:*24* 22:*12* 39:*20* 48:*5* 52:*17*
understandings 29:*10*
unexplainable 44:*3*
unfortunately 21:*16*
unit 23:*4* 62:*24*
United 6:*17* 7:*8* 14:*12* 35:*1* 36:*18* 37:*6*, *7* 44:*1* 56:*13*, *25*
universities 36:*20*, *22*
University 9:*1* 12:*2*, *8* 18:*9*, *17* 21:*23* 36:*14*, *23*
unwelcomed 15:*14*
updates 9:*4* 11:*15* 63:*13*
usable 23:*9* 38:*17*
use 4:*18*, *24* 7:*19*, *20* 9:*17* 10:*9* 12:*10* 21:*3* 23:*18* 28:*4* 31:*1* 37:*12* 38:*13*, *18* 44:*3* 47:*8* 55:*11* 57:*10* 61:*23* 62:*3* 63:*9*
useful 9:*19*
usefully 37:*12*
users 11:*16* 13:*7* 23:*12*
uses 7:*5* 26:*17* 27:*20* 51:*19*
utilization 39:*10* 59:*22*
utilize 58:*17* 62:*10*

< V >
VA 39:*14* 40:*4*
vacuum 43:*11*

value 16:*1*
values 44:*1*
various 19:*12*
vastly 51:*9*
vectors 4:*13*
venues 39:*15*
Vice 9:*2* 18:*1, 6*
view 34:*11, 17* 63:*21*
viewing 2:*20*
VIRGINIA 2:*2* 18:*17*
virtual 64:*3*
vision 10:*5* 46:*15*
visit 36:*6*
voice 28:*15*
vulnerabilities 4:*12, 13* 14:*16, 19* 15:*18, 24* 29:*14* 47:*25* 48:*1, 7, 25* 49:*9, 14* 51:*14*
vulnerability 49:*2, 22, 23*
vulnerable 13:*5* 56:*2*

< W >
wait 15:*4*
want 2:*4* 8:*20* 14:*1* 18:*13* 19:*4* 20:*25* 22:*8* 23:*2* 24:*5* 30:*12, 17, 23* 32:*4* 36:*24* 40:*7* 41:*2* 42:*21* 44:*9* 46:*17, 24* 47:*11* 48:*15* 51:*16* 52:*7*
wanted 10:*23* 36:*2* 51:*6*
wants 52:*22*
war 40:*2*
warfare 45:*9, 14* 56:*7*
warfighter 5:*4*
warm 2:*4*
warriors 51:*8*
warships 20:*1*
Washington 1:*9*
watching 20:*25*
water 54:*23*
way 2:*17* 3:*10* 34:*11* 38:*10* 41:*4* 42:*20* 44:*6* 46:*24* 49:*21* 55:*14* 60:*23* 61:*19*
ways 8:*15* 35:*7* 44:*2* 47:*1* 58:*24* 60:*23*
weapons 56:*8*
week 23:*20* 45:*7*
welcome 2:*4* 36:*15*
well 4:*17* 10:*25* 17:*4* 18:*23* 25:*8* 33:*11* 34:*8* 35:*10* 38:*2* 39:*18* 41:*23* 42:*13, 25* 43:*18, 22* 46:*19* 51:*23* 58:*4, 10* 60:*15* 63:*25*
WEST 2:*2* 18:*16*
widely 3:*22*
willing 41:*5*
win 3:*10*
winning 14:*6*
wiper 45:*3*
wipes 45:*3*
wish 15:*16* 33:*11* 41:*10*
wishes 28:*17*
withdrawal 61:*19*
witness 7:*22*
witnessed 6:*8*
witnesses 2:*5, 14, 23* 5:*12* 6:*4* 7:*21* 8:*8, 17* 64:*10*
woman 3:*11*
won 18:*10*
wonder 45:*23*
word 57:*9*
words 61:*24*
work 3:*15* 11:*11* 13:*20* 20:*6* 21:*24* 23:*7, 13* 24:*11* 26:*8* 27:*22* 35:*18* 37:*7, 13* 40:*8* 43:*9, 22* 50:*14* 51:*10* 55:*16* 57:*5* 62:*11* 63:*20* 64:*7, 13, 23*
workflows 35:*15*
workforce 3:*5* 11:*10* 29:*13* 42:*9* 45:*18, 19, 21* 50:*13* 51:*9* 59:*20*
working 10:*16* 14:*15* 23:*3, 8, 25* 35:*9, 22* 36:*17* 37:*10* 40:*8* 58:*21, 22* 61:*5* 64:*22*
works 44:*15, 19* 49:*21*
world 9:*20* 11:*7* 15:*2* 30:*20* 31:*19* 33:*9, 10* 34:*18, 21* 44:*3* 45:*9* 47:*4* 48:*22* 49:*13* 52:*18* 60:*11, 21* 63:*10*
world's 7:*17* 14:*7* 19:*21* 38:*8*
worried 32:*10* 41:*6, 14*
worry 35:*13* 41:*13*
worsen 3:*3*
worst-case 19:*15*
worthless 22:*23*
write 9:*20* 51:*13*
writes 12:*18*
writing 46:*14* 51:*22*
written 34:*7* 51:*17, 21* 60:*16*
wrong 14:*24*
wrote 3:*14* 41:*25*
WVU 18:*17*

< Y >
Yeah 25:*5* 55:*4* 56:*1* 57:*1*
year 13:*24* 14:*10* 15:*20* 37:*9* 47:*3*
years 5:*7* 6:*7* 9:*24* 13:*8* 26:*13* 28:*4* 36:*11* 39:*17* 50:*10* 53:*4, 7, 22* 57:*16* 62:*19*
yesterday 42:*25*
yield 28:*10*
York 36:*17*
young 42:*13*

< Z >
Zero 21:*13*