Notes: This transcription is smooth format, meaning that we do not transcribe filler words like um, er, ah, or uh huh. Nothing is rewritten or reworded. Transcriber notes such as [*cross talk*] are italicized and contained within brackets. A word that the transcriber could not understand is indicated with a six-space line followed by a time code like this \_\_\_\_\_\_ [0:22:16]. A word that the transcriber was not sure of is **bolded**. Punctuation is to the best of our ability, given that this transcript results from a conversation.

**Key:**

Inboden William Inboden, Executive Director of the Clements Center for National Security

Fenves President Gregory Fenves, The University of Texas at Austin

Burr Senator Richard Burr, Chairman of the Select Committee on Intelligence

Warner Mark Warner, Vice Chairman of the Select Committee on Intelligence

Cornyn Senator John Cornyn, Member of the Select Committee on Intelligence

Slick Moderator, Stephen Slick, Director of the Intelligence Studies Project

AQ Audience Question

Inboden: Calling the room to order. We have a real treat coming up for you here. And it is now my honor to introduce the President of UT Austin, who also happens to be my boss so, I’m doubly honored: Greg Fenves. So President Fenves is going to come on up and then introduce our next session here. [*applause*]

Fenves: All right. Well, good morning everybody. Welcome to the University of Texas. This is the fifth year that UT has hosted the Texas National Security Forum. Look at this crowd. Every year we have this event, it grows in importance, it grows in attendance, and it grows in significance. If you look at today’s program, you’ll find the names of individuals who’ve shaped policy and practice at the very highest levels of government: the Arms Forces and the intelligence community. They have dedicated their lives to protecting the American people. I’m deeply grateful for the public service and for taking time to be here in Austin with us today.

The Texas National Security Forum exists because of the vision of three UT faculty members: Will Inboden**,** Bobby Chesney, and Steve Slick, who respectively lead the Clement Center for National Security, the Strauss Center for International Security and Law, and the Intelligence Studies Project. They, along with their dedicated staff, have planned and organized and executed this event. Their hard work is evidenced by the forum every single year and the work that they put into it. So let’s have a round of applause for Bobby Chesney, Will Inboden,and Steve Slick. Thank you*.* [*applause*]

I want to thank and welcome Senator Ben Sasse of Nebraska for joining us as a keynote speaker at the forum. Senator Sasse’s résumé is deeply impressive, but the part that I think is most important is he was a faculty member here at UT in our LBJ School of Public Policy. So he may not think it this way, but we’re going to call him a Longhorn. So we welcome him back to UT.

I’d also like to thank and welcome Principal Deputy Director of National Intelligence, Sue Gordon. Thank you, Sue, for being here. She’ll be speaking later this afternoon. She is the second highest ranking official in the U.S. Intelligence Community, a former CIA officer, and former Deputy Director of the National Geo-Spatial Intelligence Agency. Director Gordon, welcome to the University of Texas, and we’re very glad to have you here. [*applause*]

Now, the keynote discussion you are about to listen to is the brain child of one person: the senior United States Senator from the State of Texas, John Cornyn. Senator Cornyn envisioned a candid conversation focusing on the Russian government’s recent actions on the world stage, actions that have threatened our democracy and brought deep concern to many within our borders and far beyond. So he called a couple of his friends: the senior U.S. Senator from North Carolina, Richard Burr, and the senior U.S. Senator from Virginia, Mark Warner, who were also Chairmen and Vice Chairmen of the Senate Select Committee on Intelligence. He asked them to come to Austin with him for this talk and thankfully, they both said yes. So this panel was thus born. So Senator Cornyn, I know I give Will, Bobby, and Steve a lot of credit for their work, but it seems you did the job for them by bringing your two colleagues here. We’re very thankful. Your **connection to the Center of Coordinates connection** with our University runs deep, and he has served the people of the great State of Texas with honor and distinction for many years. So thank you, Senator, for your service to Texas. [*applause*]

And to Senator Burr and Senator Warner, thank you for showing the entire country, in an era defined by, let’s call it some disagreements, that bipartisanship is not only possible, but can lead to tremendous progress for the American people. You, along with Senator Cornyn and Senator Sasse, represent the highest ideals of representative democracy in the United States, and it requires the freedom to learn, to understand, the passion to defend and debate, but also the sense of duty that we are in this together and we must work together, even when we disagree. So now, please welcome to the stage, Senator John Cornyn of Texas, Senator Mark Warner of Virginia, and Senator Richard Burr of North Carolina along with [**TIME CODE 0:05:00**] Steve Slick, who will moderate this discussion. [*applause*]

Slick: Thank you, President Fenves. Welcome to our guests. It’s terrific to see you here. Thanks again, Senator Cornyn, for encouraging your colleagues from the Senate to join us here today. We know he’s a hard man to say “no” to. Let me just explain to the audience here what we have in mind for this session. So I have a handful of questions that I’d like to ask the Senators. We’ll see where that discussion goes. But we’re going to break at a certain time and allow you to ask some questions and participate in the discussion. I want to say one thing about that, while you consider what you might want to ask. The investigation by the Senate Select Committee into the Russian election interference, the 2016 election and these related events, require them to work with--first off, it’s not over. We’re at an intermediate point. It also requires them to work with, what they’ll describe to you, are thousands and thousands of pages and witness interviews and highly classified material. So it may well be possible that they can’t answer a specific question that you pose to them, and we understand that. We’re grateful that you’re here, nonetheless, we’re grateful for what you’re doing for the country in the investigation; it’s that important. And I’ll say, personally, as important as the investigation itself is, to me, it’s the manner in which you’re going about it. It’s the balanced, fact-driven, methodical, bipartisan nature of all this that makes it so important, and that’s the kind of thing I want to talk about while we’re going here.

Before I get started, I’m going to steal just another minute. The moderator’s prerogative walking issue one, many of you will already know in this room that over Thanksgiving, General Michael Hayden suffered a stroke at his home in the Washington, DC area. Mike is receiving care now, but it’s a very serious matter. Michael Hayden is a tremendously important person to this community that we’re all interested in. He was the former director of the National Security Agency, the first Principal Deputy Director of National Intelligence, one of Sue’s predecessors, and then finally, the CIA Director, and he’s frankly a voice of reason out there in a pretty tumultuous time. So we’d ask you to hold Mike and his family in your thoughts and prayers. And also, I would point out to you that the family has set up a site so that you can send message of encouragement or well wishes, if you’d like, to Mike Hayden. It’s getwellgeneral, just the way it sounds, [getwellgeneeral@icloud.com](mailto:getwellgeneeral@icloud.com). So if you have a minute, send a message up there to Mike and his family.

So Mr. Chairmen, I want to just get off to a fast start here. Quickly, set the stage for the committee’s work. You all started looking into the Russian interference matter early 2017, shortly after the Intelligence Community issued its ICA, the Intelligence Community Assessment, providing the intelligence view of what Russia’s involvement had been, and also after the new president was inaugurated. You and the Vice Chairmen, Senator Warner, have been out a couple of times, reluctantly, it looked like to me. But you’ve been out to talk to the press and update folks on what you had in mind and an intermediate point on what kind of progress you’re making. So in terms of deliverables, from what I can tell, you’ve certainly written and spoken as a committee on the ICA, itself. I think you agreed that it was a sound intelligence product, which is important to put that to rest. And then, you also issued a written report on Russian involvement probing in state election systems, which was very timely, obviously, given the bi-election that we just held. So here we are. We’re not done yet. There’s a lot of work to do. I wanted to give you the chance to describe and we’ll let Senator Warner talk about it as well. Where are you? What comes next? What should we expect? What challenges do you foresee?

Burr: How long you got?

Slick: In three minutes or less.

Burr: Thanks for the opportunity to be here. I’d say, the first thing is, that we don’t do anything that the two of us don’t agree on, and that’s really the way the committee should be set up. We made a decision very early **[TIME CODE 0:10:00]** on that we would operate the investigation with as much transparency for the American people that we could provide, given the unprecedented access to the most sensitive information, and the means with which we acquire that information. To date, I think we’ve done a fairly good job at maintaining the integrity of the information, the sources of the information, and for the most part I think we’ve lived up to our obligation to be as transparent with the American people as we could be do this point.

We’ve had over 11 open hearings. They’ve been televised. Some of you probably watched them. That’s not our normal operating atmosphere. The Intelligence Committees were never designed to function in public. They were designed to assure 85 other members of the Senate and the American people, that everything that happens within our Intelligence Community that there are 15 people that certify they live within the letter of the law or the authority of the President. Up until this point, with few exceptions, the American people and our colleagues have accepted that. It’s made it extremely challenging on our part to go through what is now a two-year investigation, interview over 200 witnesses, the press focused on everything that Mark and I say, do, where we go from the time we hit Capitol Hill until the time we leave, and maintain some degree of privacy for nine members of our staff who have conducted this investigation. We haven’t asked for extra money, we haven’t gone outside and hired other people, because quite honestly had we done that, it would have taken them two years to understand the intelligence products that they were provided to try and do an investigation from.

So for two years, nine people have carried on their day job and an investigation. In many cases, it means if there was a Republican professional staff in charge of the CIA and a Democrat staff were assigned to the CIA, if one or the other was on the investigation it meant that the other one was doing 100% of the duty because we trust each other’s staffs just as much as we trust each other. I think it is impossible for a committee like that to operate if, in fact, we have any partisan line that exists, other than the fact that I’ve got one more member than him, it does me absolutely no good because I never have looked at the Committee and said an 8 to 7 vote should ever happen in the Committee. It’s not to say we’re always unanimous. We may not come to a unanimous conclusion at the end of the investigation. But this investigation was never for us to have a vote on; it was for us to present to the American people the facts in whatever context we could, and for you to make up your mind from what we have been able to accumulate.

Let me just draw one quick distinction, then I’ll turn it to Mark. I don’t want you to get us mixed up with Bob Mueller’s Special Prosecutor investigation. We have no criminal responsibilities. If we identify a crime in our investigation that has been committed, we refer it to the Special Prosecutor. I won’t tell you the number of times, but we have made referrals to the Special Prosecutor. One instance, just highlighted of late, is that the Special Prosecutor made an indictment yesterday using the transcripts of interviews we have done in our Committee to indict somebody for lying to Congress. It’s a loud message to everybody that is interviewed by our Committee, regardless of where that prosecution comes from. If you lie to us, we’re going to go after you. Our mandate is, at the end of this, to get as close to the clear truth as we possibly can, and we can’t do it on conjecture; we’ve got to do it on facts. So everything that we try to do is rooted in “show us the factual information that substantiates the claim that we’re making.” That’s not always the fastest process, but we think it’s the best.

Warner: First of all, and I made this comment at a classified setting earlier, and I don’t want to break too much news at the beginning, top of this presentation, but truth is, while we don’t always agree, we actually like each other and can work together. [*applause*] I appreciate John inviting us down. **[TIME CODE 0:15:00]** Richard and I have had a great partnership. I would reinforce everything he said in terms of the quality of our staff, the enormous work that’s been done, the fact that we’ve got this tension of protecting sources and methods, as well as making sure that we provide deliverables to the American public so that at the end of the day, while the press attention may be focused on was there collusion, not collusion, equally important, if not more important, is how do we make sure that when a foreign nation attacked us with a whole new set of tools that it doesn’t happen again in the future?

Let me briefly go through--Steve, you kind of hit it, but I’d like to go through a little more detail in the four areas where I think we are almost done and have virtual unanimity. You made mention of the fact that the Intelligence Community did an assessment that came out in January of ‘17, basically said Russians have massively interfered in our elections. They did it with the goal of helping Mr. Trump and hurting Mrs. Clinton, and they were using tools that frankly, caught all of us off guard. We spent a year going back, talking to everybody who put together that report from all of the component parts of the IC, and confirmed that that was a good intelligence product, as you said.

Second is, and this took some push and pull--and again, want to give Richard some credit on this, and John credit on this--to get DHS not in a partisan way, but DHS to come more clean on the fact that at least 21 of our states’ electoral systems had been touched or tampered with. No votes had been changed, but we exposed a set of vulnerabilities that, quite candidly, I don’t think we fully appreciated at the outset. I would argue, while we don’t have the perfect legislative solution yet, we’ve got bipartisan legislation out there; the Congress has committed $375 million to upgrade the security in our state systems, and many of the state top election officials, who were nervous about federal government intervention, realize now, the vulnerabilities they face going forward, and the fact that we all have to up our game. Because, while it may have been Russia in 2016, it could be a host of other countries on a going forward basis.

Third thing, and this has not received as much attention, but it’s, I think, very important: What did the Obama Administration do right and what did they get wrong? Some of this stuff should have been higher priority earlier in the 2016 election cycle. The various agencies that we worked with, which ones did their jobs, which ones, particularly in terms of the counter-intelligence efforts, need to improve their game? We’ll have some very serious recommendations on that topic.

The fourth, and this is one probably that we all learned a lot about, and again, I think, with my good friend, Sue Gordon here, respectfully, the Intelligence Community was a little caught off-guard on was the ability for a foreign entity to massively use social media to manipulate news, to pit Americans against each other. And while we initially thought that it was the obvious effort of Russian or Russian agents buying paid political advertising, that was the just the tip of the spear. The real issue was the ability to create fake personas and create followers, not on politics, but a site that might promote Texas football or gardening, and then draw folks in and then start to see political malfeasance. We’re still, I think, wrestling with how we put some guardrails in place on a going forward basis.

And then, obviously, the final piece, which we’ve still got to work through is, with some of the contacts and connections, what did happen with Russians and some of the campaigns? But those first four pieces are really, really important and I guess one of the things that I think we all feel is that this is not going to be a one and off. This is going to have be an ongoing part of our oversight because, the one thing we’ve discovered is, I think Sue’s boss, Dan Coates, went to a NATO function recently and was asking all the countries how many of them had seen Russian intervention in their political process. Everybody raised their hands, 29 NATO nations.

And the remarkable thing, and from a National Security standpoint, last comment I want to make on the outset is that it’s been pretty well-documented what the Russians did in the French elections. Actually, Facebook took down 30,000 accounts. So far, in America, they only took down 470 directly-related Russian accounts. But French government was actually a little ahead of us **[TIME CODE 0:20:00],** but they were further down the process. The Brits, who had first thought there was no Russian involvement inBrexit now acknowledge there was plenty of Russian involvement in Brexit and their own parliamentary inquiry is proceeding ahead.

If you just take the Russian investments in disrupting our election, the French election, and the British election and add it all up, it’s less than the cost of one new F35 airplane. So I worry, from a National Security standpoint, I don’t want us just buying 20th Century stuff when I think a lot of conflict in the 21st Century is going to be in the cyber domain and the misinformation/disinformation domain. We’ll have more to say about it, but it is where the front line of conflict in the 21st Century will evolve.

Slick: Senator Cornyn, I want to circle back to you in just a second because you have some very unique perspectives on this, but could I just follow up briefly, Mr. Chairman? You mentioned that the issue of unanimity and consensus, and I went back and looked at some of the earlier press briefings that you did, and you really set a high bar for yourselves on this. We know how hard this is. These are controversial topics, but you said that’s what you were headed for and you thought that the work of the Committee and the report of the Committee would be, obviously, less impactful and degraded if you couldn’t achieve it. How do you feel now, about two years in, some of these controversial topics, like the Obama Administration’s response to the intelligence, like possible relationship between Russia and the Trump Campaign? Are you more or less confident that you can bring the Committee around to signing the same report?

Burr: Steve, I always base that on the fact that if we stayed focused on facts that members could find agreement. If we stray from that, it makes it tougher, like any good potential scandal or issue, the media doesn’t necessarily make our life easy because, in many cases, their 15 stories a day, three of them are true and 12 of them are questionable. But that sets how people look at what we do and it impacts internally what we’re forced to look at.

I would probably say this: if you asked me what’s different today than it was two years ago when we started this? I think Mark and I would tell you, we had expectations we’d be done, and we’re not. We never dreamed that we would find as coordinated, complicated, focused effort by Russia globally to utilize technological tools that today, allow them to meddle anywhere. It’s particularly difficult to the United States because we have this thing called the First Amendment. So when we sit and look for solutions to what we perceive the biggest problem to be, we keep bumping up against the First Amendment, and it limits then how you can construct a solution. So I would tell you that our Committee will have years of work, probably continual, on a whole different mission outside of what we have historically looked at, not one that we’ve been tasked with by the Intelligence Community, but one of oversight about these things that are going on in the world that are threats to us. Technology is a wonderful thing. It provides us the ability to communicate in a different way and it provides somebody the ability to meddle in a different way. We don’t have an architecture in the United States of government that’s ready to handle that. So ours is not just the challenge of coming up with a solution, here it is; it’s changing the entire architecture to recognize the fact that we’re in the 21st Century, and not the 20th Century, and that’s not just government; it’s how we integrate that architecture into the private sector.

Slick: Senator Cornyn, you seem to me to have two, at least two, very unique perspective on this. You’re a member of this Committee, have been throughout this investigation, but you’re also part of the majority party’s leadership team. So I’d ask you to go back early 2017. There were a lot of decisions to be made about how the Congress was going to investigate or react to the claims that were appearing in the media and elsewhere about Russian interference. There were lots of good ideas. I think you called it at one of your press conferences “lots of talking heads out there,” special commissions, joint committees, all sorts of alternatives for how the Congress could do that. That’s an historic precedent as well. But you and the majority leader went with the regular order. You decided **[TIME CODE 0:25:00]** send this to the Intelligence Committee, two years down. Can you take us back there? What were the considerations and what does it look like from your chair on the Committee?

Cornyn: Steve, I think the sort of confidence that the majority leader had and the Democratic leader, the minority leader, Senator Schumer had in our Senate Select Committee on Intelligence, and Chairman Burr and Vice Chairman Warner, and the members as a non-partisan Committee that would do our work, sometimes unglamorous, always behind closed doors where we can’t really share it with the public. I think it was an indication of the confidence they had on a bipartisan basis that the committee would do exactly what it has done under Chairman Burr and Vice Chairman Warner’s leadership. It’s easy for things to spin out of control. You might have noticed, in the other House, things were handled a little differently. So I take that as a point of pride in the great work that Mark and Richard have done.

If I could just tack onto just one thing that Mark was saying about the Active Measures Campaign; I keep thinking back at what our friend, Bobby Inman, said after 9/11, that it was a failure of imagination. So what the Russians did is really not new, in a sense, but what they did is take their cyber capability, their ability to steal information online, they added to that their propaganda effort through Russia today, through Sputnik in particular, compounded that with the social media phenomenon that we’re all still trying to come to grips with, and then the mainstream media, at a certain point, you go on your Twitter feed and see what is trending--well, reporters all look at that and they think, “Well, maybe I need to report that,” \_\_\_\_\_\_\_\_\_[0:27:14] before they’ve really been able to confirm the information in an appropriate way, using what I would call traditional journalistic standards. There’s always a rush to be the first to report it, and that actually plays right into the Russian playbook, in terms of sowing discord and producing disinformation that causes us difficulties as a nation.

Burr: I think one of the challenges is, when something like this happens, you always try to look for “what’s the intent?” I would tell you, this is where we have to from the 21st Century back to the 20th Century. It seems that Russia still looks at the world and says, “If it’s bad for America, it must be good for us.” So you don’t need to look real deep to say, “Well, what is it they were exactly trying to do?” They just perceived that if it was bad for us, it’s got to be good for them.

Warner: To build on that, it’s easy, in retrospect, but the Russians are pretty clear about this. Their equivalent of their Chairman of Joint Chief of Staff, General **Geramazov**, in 2011 wrote the modern Russian military doctrine that basically said, Russia couldn’t keep up with the West in tanks and trucks and planes and guns, but in the realm of cyber or misinformation/disinformation, it could. And I think they’ve gone about. They didn’t try it. We weren’t the first subject. Their own people: Ukraine, the Baltic nations. They tried all these tactics out in other nations.

Two quick points on what John said: one, there’s a nascent industry now of social media experts. One of the guys, John Kelly, who we’ve had testify in public for us, has indicated that--and I don’t know if his numbers are completely right--but that the vast majority of political content on the far left and the far right that still goes on in our country, is not actually generated by Americans, but generated by foreign-based bots. Now, to a degree maybe, that makes me feel good there’s not as many crazies in our country. But the fact that we don’t even know, and social media companies haven’t been willing to share how many bots versus human beings, it’s one of the points of ongoing discussion.

The other point I want to make, that John said, and this is where I fear where we’re headed, John indicated in 2015, 2016 when the Russians were doing this, they kept their cyber activities, hack into the DNC, hack into Podesta, leak that, separate from their social media. Let’s create fake identities. **[TIME CODE 0:30:00**] What I predict 2020 will be, or somewhere this will happen in the coming two years, will be they will marry cyber and disinformation. What do I mean by that? They will go out and use cyber tools to hack into an entity, like an Equifax company, that has troves of personal information on lots of Americans, get that personal information, contact us with the personal information that would make you think, “Oh, my gosh, I should open this because they know my mom’s maiden name or they know my Social Security,” and then, what they will see will not be a printed message from somebody that says, “It’s Richard Burr,” but actually, “Sergey in St. Petersburg.” You’ll see what’s called the next generation of this, called deep fake technology, where you’ll see a visual image of Richard Burr’s face and his voice communicating with you on a virtual YouTube attempt. But that won’t be Richard at all. So this combination of misinformation with cyber is, I think, where the frontier’s headed.

Burr: We’re very anxious to watch the Ukrainian elections to see what Russia might do in Ukraine, which would give us an indication as to how their capabilities have changed from ’16 to that point.

Slick: Important. Can I move to the issue of follow up? So I started to quiz you, Senator Warner, over in the corner on this. In the course of this investigation, your staff’s becoming incredibly well-informed, expert. Your membership is, as well, on some really hard problems. As you said, they’re not going anywhere. The question is, how to translate that into legislation, statute, policy, rules, and practices that will help us avoid it in the future. I’m thinking of the 9/11 Commission here, which also did seminally important work. They had findings of fact, they had recommendations on policy, and they had a clear strategy to drive these, even after the Commission submitted its report, resulted in the 2004 Intelligence Reform Legislation. So my question for you all is, as leadership, as a Committee, how do you translate that expertise, wisdom, some of the recommendations you’ll agree on and make that into policy?

Warner: First of all, and I want to give, again, Richard credit on this. I’d had some of the tech background before I got in the political side, but he worked really hard, we worked really hard to try to make sure the Committee got educated about bots, about social media. I remember when Zuckerberg first came and I was really upset that he wasn’t coming to our Committee. Rick said, “No, Mark, don’t work.” Man, I was so glad he didn’t come to our Committee, but we didn’t look nearly as stupid as some of our colleagues. [*laughter*] Amend that to ill-informed.

So we went through an education process. When we had a hearing recently, our Committee members weren’t talking about **politicalization** and algorithms; they were asking real questions of Facebook and Twitter about what they could do. I think figuring out, and as Richard mentioned, you do have First Amendment challenges, and I think around election security, we’ve at least come together on some ideas. James Langford from our Committee and Amy \_\_\_\_\_\_\_\_[0:33:35] Kamala Harris have got a very good piece of legislation out there.

On the social media area, I’ve tried to put out a series of ideas; I’ve tried to go pretty deep in this field, and I think there are buckets of areas where we could do either legislation or guard rails. One area is around identity validation on the Internet. There a host of questions that raises there. There should be some low-hanging fruit. Should we at least know when we’re being talked to by a human being versus a bot? Should we have geo coding? Should there be **estonious** move to actual identification? It maybe makes sense in America but maybe it doesn’t make sense for a female journalist in Egypt.

There’s privacy issues that the Europeans and frankly, I think the European model is a little too clunky, but there a host of privacy related concerns, and there’s a menu of eight or 10 ideas there. But also, I think where we may be able to find some commonality, can we add more competition into the field in social media? Can we get more transparency? Three quick ideas. I was a telecom guy, and it used to be really hard to move from one telephone company to another until you had number portability. Maybe there ought to be data portability, so you can move all of your Facebook activities, including your cat videos to another platform, if you don’t like the privacy or protections you’re getting. Should you actually have transparency on the data they’re collecting? **[TIME CODE 0:35:00]** If Americans think this stuff is free, it’s not free. Facebook, Twitter, Google--I’m not criticizing them, but if everybody here realized how many single points of information these companies have on us, they have much more than the United States government has on any individual here.

And the third would be, if we actually **knew** price transparency. If we knew that John’s data was worth $25 a month to Facebook, and mine was worth $18, and Richard’s was worth $35, there might be intermediaries that would come in and say, “Well, how do we disaggregate that a little bit and create some more competition?” So I think there may be buckets of areas. What I’m hopeful is, none of this falls on the normal liberal conservative continuum. It really is, can you be forward leaning or not? I think our Committee has done some pretty good forward leaning work.

Burr: Did you really say cat video?

Warner: I did say--I didn’t say what you wanted me to say. [*laughter*]

Slick: Senator Cornyn, Mr. Chairman.

Cornyn: I was just going to say, I don’t disagree with anything Mark just said. But let me just express a note of skepticism when you asked about legislation that Congress could pass. The technology’s moving so fast that I don’t want us to be an impediment, but rather, I think the best role of the Congress is to provide tools, like the 702 re-authorization of the Foreign Intelligence Surveillance Act, like the reform of the Committee on Foreign Investment in the United States to look at foreign direct investment in ways that countries like China get access to our intellectual property and the know-how, and just part of their China 2025 Project, take it over and make it in China and put us out of business.

The one thing I’ve learned since I’ve been part of the federal government is, the federal government does not innovate. That is the antithesis of what the federal government does, is innovate. So we need to let the innovators innovate and we need to make sure we’re doing the oversight of the Intelligence Community and challenge them to be the nimble ones to meet the challenges of the developing technology in these new circumstances that we might not have even thought of just a year or two ago.

Warner: Let me just quickly jump in here, though. I would argue that you’d never have the Internet if there hadn’t been some set of rules. I would also argue that we’ve constantly reached out to the companies and said, “Help us, because if you leave it just to us, we might screw it up.” But their willingness to engage in a meaningful way has been--there was that empty chair for Google to come and they didn’t even come. I would argue, there are a variety of models out there. My fear though is, if America gives up its leadership position on setting these guardrails, and I don’t want to knee cap these great American tech companies and have them replaced by Ali Baba \_\_\_\_\_\_\_\_\_\_[0:38:00]. I don’t want to cut back on innovation. But if we give up our ability to set the framework, which America has always led around technology, it’s going to happen by the Europeans or it’s going to happen on a state-by-state basis, the way California already has. I think you need the lightest touch possible, and there may even be models the way where you have even an industry funding the way in the financial section, you’ve got \_\_\_\_\_\_\_\_\_[0:38:26], but I think there’s going to have to be some guardrails here, or as the Chairman often points out, I’m not sure these companies can control their behavior without some of those guardrails.

Burr: On the technology piece, I think it’s important that everybody understand there is no Committee of Technology in Congress and there is no Agency of Technology in Washington, nor do you want one. So when you look for solutions, solutions, Steve, are not always legislative. I think John hits on a point that I think you would find complete agreement on in Washington, that technology and innovation are speeding up at a pace where what we’ve got this year and what we buy next year will be so totally different in its capabilities that it’s hard for me to believe that you could put something in statute that doesn’t deter the ability for the deployment of that technology 12 months from now. What we’re really looking at is, one, how we change the architecture of government; and, two, how do we set up a new type of collaboration between government and the private sector? If we can successfully figure out how to create that collaboration--and I would say that that collaboration has to have the trust that Bobby, that the Intelligence Community and the agencies have, where we can share information and they can have a real **[TIME CODE 0:40:00]** understanding of the threat that’s out there, then their willingness to work with us on what they could do with us to overcome the threat is a much better approach to do it, because it means you can change it on a dime, and it’s not reliant on Mark and I to go legislatively. Our Committee has no jurisdiction in cyber security. Three years ago, Diane Feinstein and I wrote the Cyber Security Act. It’s not perfect, and it’s voluntary, but it’s hoped for business and government to create a communications link that didn’t exist and couldn’t exist. So we don’t rule out legislation, we just want to begin to understand the total landscape better.

Slick: You also described it as something of a continuing care issue, that the Committee’s not going to be able to just sign off on a report and move on to other business; you’re going to have to stay \_\_\_\_\_\_ [0:40:55, *cross talk]*

Burr: Well, I would tell you that we’ve discovered things specifically as it relates to the Russian effort that extends far outside of what we’re looking at in our investigation, and this will be of great interest, as I like to say. I think we’ll have a Committee that has red teams that look at certain things for maybe the next decade. I think one can anticipate that the problems that we see generated by Russia meddling in the United States’ elections, we have to expect by the time we get to 2020 there will be other players out there that we’ve got to be just as concerned with because their intent and their capabilities are the same. So this is not a rifle shot solution; more of a warning bell.

Slick: Senator, I’m sorry, I cut you off.

Cornyn: No, you didn’t. I was just going to make the point that Richard was eluding to that the Intelligence Committee doesn’t have jurisdiction over a lot of these matters, but we do have some of the expertise and thanks to our IC, we get some information that, frankly, we can’t share broadly. But that’s the reason why, for example, there is a reserved seat for a member of the judiciary committee in both the majority and minority. I happen to occupy that seat of the majority, Senator Feinstein for the minority. Same for Armed Services, Foreign Relations Committee. We bring all that background and that additional fire power to bear. Getting the information is part of our oversight responsibilities, but then we can take that back to our other committees and develop the tools, the authorizations that are needed for the Intelligence Committee as a result of that collaboration between different committees. So it’s not just the Intelligence Committee, is the point I’m trying to make. I thought that was a point worth making.

Slick: Terrific one, with respect to these crossover memberships that allow you to have reach based on your access to sensitive information. I want to pull the camera back a little bit. I’m sure the questioners are going to take us back into the Russia morass, but more generally, the topic of our conference today, of course, is the return of great power competition. So I want to talk a little bit about priorities, I want to talk about threats and get each of you to comment on that. So maybe there should be a question mark after the title when we say the return of great power competition, or maybe there is no question. But the issue is this: with respect to the Intelligence Community, I know each year you all hold a hearing. I’m not sure if yours is one of the ones done in open or done in closed session, worldwide threat where the director and some of the agency heads come down and essentially give you a list of dangerous situations, threats out there that the community is monitoring. That’s good and important, useful for the public to see their Intelligence leaders and to see you all doing oversight. But the fact of the matter is, making a list of threats is not the same as making priorities. What’s more serious than another threat? Where are you going to invest? Where are you going to spend your time? Where are you going to hire professional expertise? That’s harder, and it seems to be absolutely necessary, and that’s what we’re talking about during the rest of this conference is, where should America have is national security? In your case, it’s intelligence-focused. What can we not afford to get wrong? So if I could just get from each of you what should we be thinking about? What should we, as I say, not be sleeping on? What’s more important than something else?

Burr: Well, my day starts probably a lot like Sue’s does, reading the overnight Intelligence reports that used to take maybe 30 minutes on a really bad day, focused on one continent, maybe a little leakage over to another continent, one or two primary targets, and now takes somewhere between an hour and a half and two hours, **[TIME CODE 0:45:00]** deals with every continent in the world and multiple players. So I’m not sure that, in the world I’m looking at, we have the capability right now, or that we have the luxury, I guess I would say, of boiling it down and saying, “We can focus on this one, number one, this one, number two.” If I ranked them, every week, they’d change. One night I go to bed and I’m really worried about what is going to happen the next day in North Korea and the next day, all of a sudden, it changes to somebody else somewhere else in the world. So we’ve got a host of adversaries that, based upon what we do and what they do, changes their concern on our threat list.

Slick: So it’s an agile, a flexible community.

Burr: This is a very challenging time to be in the Intelligence Community and also to be at a place like the Defense Department, where you’re tasked to have a contingency plan for the hot spots, and everywhere is a hot spot.

Warner: I don’t disagree with Chairman, but I’d take it slightly different. I think you nailed the topic. I think that we, appropriately, post 9/11 have been focused on the threat of terrorism, we’ve been focused on rogue states, and there’s been a re‑emergence of our near peer adversaries in Russia and China. To a degree, we took our eye off the ball on both of those nations. In many ways, and I’m not always a keen fan of this Administration, but they have, I think, made some movement in cyber. I would argue, last three administrations, Democratic and Republican alike, have allowed these near peer adversaries, Russia and China, particularly in the cyber domain or the intellectual property theft domain to attack us without any response. We had no cyber doctrine. If anything, our technological advantage made us afraid of using our tools in terms of potential technological escalation. Moscow goes without power for 24 hours, it’s a challenge; New York goes without power for 24 hours, it’s a meltdown. I think there’s a growing sense that re‑engaging and looking at the re‑emergence of these nations, and I would agree with Richard that Russia still has this “us bad, them good.” One of our earlier sessions today was on the enormous challenge that China poses. Their goal is not economic equivalency and technological equivalency; it is economic and technological advantage over not just us, but the whole West.

I come back to my earlier question about, the issue I think we’ve got to grapple with is, we just spent $716 billion on defense and we’ve got great leaders of our military here. We’ve got an awful lot of that in Texas, Virginia, and North Carolina. Russia’s spending $70 billion, and they’re not the same kind of economic power, but in the realm of cyber and misinformation, they are our peer. China’s roughly spending a couple hundred billion, and my fear, particularly vis-à-vis China is, the delta between our spend and their spend on defense, they are investing in artificial intelligence, next generation computing, quantum computing, 5G technology, and America’s technological lead that we have maintained for at least in every field post-World War II, is very much in jeopardy right now, and that is a level of a threat that I think we have potentially a special ability to observe, and I think part of our challenge is to engage with the Defense Community, the IC Community, and frankly, the business community to recognize and have doctrines to **counter some of this.**

Slick: So we have an incredibly well-resourced Intelligence Community and, thanks to you, for a lot of that, and completely necessary. On the other hand, there are limits. There are choices to be made. You can’t be good on everything every day. Senator Cornyn, do you have a sense of how to think and rack and stack these?

Cornyn: I can’t do any better than Senator Burr and Senator Warner, but I did have a thought. My favorite response--somebody asked General Mattis, “What keeps you awake at night?” He says, “Nobody. I keep *them* awake at night.” I like that a lot. [*laughter*] But I was thinking a little bit about, I had the chance to visit some of our national labs **[TIME CODE 0:50:00**] recently: Los Alamos and Sandia and go to the Nevada nuclear test site. The last time we tested nuclear weapons was 1992, but it’s fascinating places. But just to reflect on the fact that we beat Germany and Japan and everybody else to develop an atomic weapon and, of course, used it in Hiroshima and Nagasaki to end World War II. But isn’t it remarkable that since that time, there has not been a nuclear weapon discharged? That’s because of mutual assured destruction, because we’ve dealt mainly with rational actors who’ve had nuclear weapons. We try to keep them from proliferating. But really, to me, one of the biggest concerns that I have is, of course, nuclear weapons in the hands of non-rational actors, like Iran and North Korea. So to me, those really percolate to the top of the list, thought they were worth mentioning.

Slick: Terrific. Thanks for that. Okay. Time for questions. Here’s how I think we’d like to handle this. If you raise your hands, we’ll call on you; stand, wait for microphone, tell us who you are, make sure there’s a question mark at the end of your speech, and we’ll try to get as many in as we can before we run out of time. Sir, you were first. Is there a microphone coming? Great.

AQ: Hi, Shane Harris from the Washington Post. Thanks for being here with us. I wonder if I can pull you back into the Russia investigation a little bit. Can you respond to Mr. Cohen’s guilty plea this week, and specifically, how that might change the thrust of the investigation? Will you be going back and looking at other statements that people from the Trump Organization, for instance, may have made about their efforts to pursue a project in Russia and how long that went on? And if I may, in a broader sense, too, Chairman Burr, you noted that at the end of this investigation you may not come to a unanimous conclusion on all of the points that you’re looking at. Can you give us some sense of where there might be differences of interpretation between the Republicans and the Democrats?

Burr: Well, given that we’re not finished, I think it’s impossible for me to try to point those out to you, but I think, like any issue of this complexity, I reserve the fact that somebody may be in disagreement with what the facts show. Relative to yesterday’s announcement, I think the myth out there is that we did interviews and never read them. We continually go back and look at the testimony we’ve been given and we weigh it against any new information that might be out there, that either a reporter has been able to get a comment from an individual, or colleagues in the House. We have shared, when permission has been given by those that we interview, interview notes with the Department of Justice, and specifically, with the Special Prosecutor.

I won’t get into the numbers, but we have made referrals from our Committee to the Special Prosecutor for prosecution. In a lot of cases, those might be tied to lying to us. My message yesterday was, if you lie to us, we’re going to catch you and we’re going to prosecute you. Period, end of sentence.

When Mark and I started this investigation, we went for almost five months where when we invited somebody in to interview, they came in and we didn’t have to deal with a bunch of lawyers. When the Special Prosecutor was set up, the next day, every person who was on our deck of interest had a lawyer. So for the last year and a half, we’ve had to deal through lawyers to get to people. But I will say this, we’ve interviewed over 200 people. I don’t think just a handful of those were compelled to come in because of a subpoena. We have not held anybody in contempt to this point. I’m not sure I’ll be able to finish it and say that, but our congressional tools are limited; they’re not as extensive as a Special Prosecutor’s got. But I would remind everybody, ours is not to search out a criminal act; ours is a counter-intelligence function. So we’re focused on a particular area and we try not to drift over into the other, but we’re certainly not scared to refer something that we believe is criminal, and lying to Congress is right at the top of that. **[TIME CODE 0:55:00]**

Slick: Terrific. I’m looking for a student. Please, ma’am.

AQ: Hi, I’m Jillian Smith, and I am a student here at UT. I was wondering, in regards to building up a cyber doctrine and keeping a technical advantage over Russia and China, how can y’all in Congress still build that cyber doctrine while still protecting the public good from big tech companies and social media companies as they expand?

Warner: Great question. I think Richard mentioned the First Amendment concern, John’s mentioned the question of, would you stall innovation? I was in the technology business longer than I’ve been in politics. I get the fact that government can screw it up. But we’ve got a lot of things to balance here, and that’s why I do think, and I think if history is any guide, there’s never been an industry that has had this much concentration as quickly as the data business. There’s never been a business model where every time you interact with these companies, if data’s the new oil, you give them new oil. So that’s a fundamentally different business model than before. So I come back to again, thinking at some point, we’re going to have to come up with some guardrails that, as much as possible, do not limit innovation; but I’d rather have America setting those guardrails than others in the world.

On the question about cyber doctrine, though, I think it’s going to have to be done in concert with other nations in the world. I don’t want to completely make the nuclear weapons analogy, maybe better as the chemical weapons or landmines, where at some point, there were certain tools that were just beyond where “civilized nations” would be. And there may be certain cyber tools shutting down a water system, polluting a water system, cutting off the grid, that there could be commonality amongst many nations in the world that say, “If you do that kind of activity, we’re going to punch you back, and we’re going to punch you back with a lower level of attribution than we have perhaps right now.” There has to be some consequences for the rising nation states, but also for the one-off actors, because this is such an asymmetrical battle.

Burr: I might add to that that our friends around the world look to us for leadership. I’m not going to say that they don’t act, but they would prefer to be in concert with us. So Europe’s out ahead of us on data. We don’t necessarily fully agree with where they are, but we’ve got an opportunity. It was John Cornyn that led the changes toCFIUS, Foreign Investment in the United States, and our friends in Europe, they were dying for this to happen so that they could know what to initiate in parliament. All of these issues, cyber security, 5G, it’s our partners around the world that are looking to us to set the framework for them to implement exactly what we did. There’s an advantage to that for us, globally, if it all looks the same.

Warner: Just one last quick--truth is, without strong, more American leadership, economically, militarily, morally, the rest of the world wanders.

Slick: Terrific. Gentleman over there, please. He’s coming up behind you.

AQ: Hi. James **Arshay**. On the private sector side, in cyber security and financial services, given the theme of partnership, what would you like to see more of from the private sector and/or conversely less of, other than from the peer tech companies? Is it knowledge transfer to help committee staffs to get current on what companies they’re seeing? Is it advisory or focus grouping to come up with things like, say, a national weather service for cyber threat indicators, where private sector people could subscribe to some sort of scrubbed IOCs and provide that back to the government? What would you guys like to see more of?

Warner: Well, I actually think we need--this is again, one of those things where we all can improve. We all need to improve our cyber hygiene. \_\_\_\_\_\_\_\_\_\_[0:59;48] Basic, small things and make that much more the rules of the road. We’ve been doing a bit of a road show **[TIME CODE 1:00:00]** with different business groups around the country about the real challenges posed by an emerging China, and their willingness to frankly, beg, borrow, or steal technology from our companies or make the price--the fact that American and Western companies will give up their source codes to get into China? They would not do that for any other admission into any other country in the world, and we’re not going to be able to do this on a one-off basis. We’re going to need to work with business on that. I think we’re making some progress, for example, on that front. Richard and I have been trying to deal with the Telecom companies and making sure that we don’t allow, as a former wireless guy, 5G standards to be driven by the Chinese. The **wahways** and CTs of the world that, I think we will say, or at least I would feel, are a national security threat. So we’re going to need that collaboration back and forth and, candidly, things like a national weather service around cyber? We need your good ideas, because those innovative ideas probably won’t be birthed--Chris is not here--out of DHS.

Burr: I would say we’re also trying to look at what the collaborative model looks like in the future. I would suggest to you that we’re far enough along that real collaboration in the future is going to be a partnership of government academia in the private sector, which is a fascinating combination where we’re bringing it all together. Geographical locations like Austin, Texas and Raleigh, North Carolina, and Charlottesville, Virginia--

Warner: Or Blacksburg, Virginia, take your pick!

Burr: --are going to be very advantageous to that, but I think it’s safe to say, governments never felt really comfortable being in the room. We’d fund something at academia, but we didn’t want to be in the room. Business really didn’t want to be in the room with government, but they would give us suggestions. When I talk about collaboration of government, academia, and business, the first thing that you have to agree to when you walk in the door, nobody holds intellectual property. Nobody walks out of the room and says, “This is mine.” When you change that dynamic at the start, in the models that we’ve tried it, it is amazing what you can accomplish when you bring the bench strength of academia, the expertise and focus of government, and the capabilities of the private sector together, it’s been somewhat amazing.

Cornyn: Can I just…?

Slick: Of course.

Cornyn: I would say, to answer your question, all of the above. We need all of the above. But as we’ve said, we don’t need government to be stifling innovation; we need the private sector to be responsive to the needs of the country and the government. This was mentioned, a discussion about rising China and the threat that China poses economically, and from a National Security perspective. Some of the companies we were talking to this morning asked, “Well, how do I vet my workforce? We assume that when you issue a visa, somebody comes into the United States, the government’s okay on that person if they’re a, let’s say, a nuclear physicist.” Well, no, we haven’t vetted that person. Or they’re studying or working at one of our research institutions. Sue Gordon made, I thought, a really good point. The Intelligence Community has learned how to deal with the insider threat, which is the same thing we’re talking about when it comes to academic institutions, when we’re talking about industry. So there’s also, not just a way we can learn, the government can learn from the private sector; the government, particularly the Intelligence Community can help the private sector deal with this insider threat in ways that will, I think, create a lot of new products and services and create a lot of new great opportunities.

Warner: This is another one of my hot buttons, echoing if we’re going to have these collaborations, and Sue has been the lead on this is, you can’t have a security clearance reform--you can’t have a secure clearance process that has a 700,000 person backlog. That is a national security threat. There are smarter ways to change that paradigm, and Sue has been leading on that. I know this afternoon, she’s going to tell us what number that backlog is going to be down to by the first half of next year. You got it? It’ll be the number we discussed. **[TIME CODE 1:05:00]**

Burr: And if you haven’t caught on, Sue’s a very, very important person.

Slick: Okay, terrific. Who do we have? The gentleman in the back, there. Blue blazer. You, yep.

AQ: Thank you, Senators. My name is Anthony. My question is, going back to your comments that we need a business to innovate to counter these things, my question is, how can we rely on business to innovate and counter untruthful news and headlines that sow discord when, in a lot of ways, they are not incentivized to do so because it seems like businesses actually want those headlines there because those **click bait-y**, politicized, untruthful headlines seem to bring them a lot of profits. So that’s actually what they’re going for in a lot of sense, and care more for. Thank you.

Warner: Well, this is where again, we may agree to disagree, but if stories were trending based on actual humans posting as opposed to bots, that might--now again, it’s easy to say, it’s harder to do. California tried. But there are ways that we can, short of a government censor, or for that matter, a Facebook censor, try to bring a little more transparency to the process. I think driving down the news feeds on the algorithms with the bots would be one; having the idea around data transparency and pricing transparency. If John Cornyn’s data’s worth $30 a month, and somebody could take $3 of that a month and say, “I’m going to end up helping to screen the news or helping to get rid of the spam,” that might be a value proposition for a new company. Matter of fact, in California this year, and this is going to scare the dickens out of some of the social media companies, but this is why I think it’s better to do it perhaps national, than state by state, there’s going to be a legislation proposed that says, “You are the customer. That would never allow you to give up all your rights, no matter how many times you clicked ‘I agree,’ and the bill would legislate that Facebook, Google, and Twitters would have to give 25% of all the profits they made off of you back to you. Now, that may be a little heavy-handed, but it’s going to get their attention. The point I keep trying, my frustration, again, as somebody who spent longer in technology than I have in politics, I beg them to work with us in a meaningful way, because we need their expertise to try to get it right.

Burr: I’m not sure that we see that there’s going to be a technology company going forward that sets up its whole revenue system off of the ability to take people’s data that they control and use that data to be their revenue stream. So as they begin to change it, it gets into either paying for the use of my data or it gets into creating a different revenue stream. It’s just telling us that those technology models are going to look different in the future, and it’s not because of what we’re doing; it’s because of what your demands are about your data and the protection of it. So we really don’t want to be the ones that manipulate it. We want to make sure that individuals have that input.

Warner: You should see, this is one of those areas where we can agree to disagree. I think there’s somewhere between manipulate and transparency where there might be some agreement. I don’t think transparently, if we could roll back the clock 25 years, 30 years in the healthcare field and actually have built-in real price transparency 25 years ago in healthcare, our system would be a hell of a lot better. We’re at the beginnings, as wild as the data business is right now, it’s exponentially growing. If we can build some transparency into that right now, I just think at the end of the day, sunshine is a good thing to bring to any business process.

Slick: A rare sentiment from the Senate Select Committee on Intelligence. Little transparency, little daylight, happy port. Admiral Lindman*.* [*laughter*] He doesn’t really need that thing.

Warner: This is an admiral. You need to recognize, you are the first questioner that actually gets to hold the mic on their own.

Slick: You’ve sussed out our MO. Good point.

AQ: You might expect, that it’s more advice than question. [*laughter*] **[TIME CODE 1:10:00]** In reflecting back when oversight of the Intelligence Community began, we had to get away from all the public hearings, the church committee time, and go back to recognizing that we were protecting sources and methods. Closed hearing was critical. Listening to this, there isn’t a technology committee, and there’s no other group that has assembled the knowledge you already have about a lot of these issues. Corporations have proprietary reasons. Intelligence Community, it sources methods, and the private sector it’s the proprietor. So a suggestion to you: closed session, but one-on-one with a clear understanding what you need from them, are suggestions. Knowing their technology. How can you get at making changes? I think you have a better prospect of getting useful information with that. The public hearings that show the empty seat with the name on it are great media coverage, but they don’t advance it. So just my gut instinct from now, 35 years in the private sector is, you’re going to have to establish that you will protect the proprietary data in order to get them to share with you the way the Intelligence Community \_\_\_\_\_\_\_\_\_\_\_\_[1:11:26]. I’d say to the audience, we constantly hear the public’s right to know, but the reality is, in the ability to learn what’s going on in the rest of the world, very fragile sources and methods are at risk. It’s only the oversight--you are the substitute for the fourth state, in making sure that things are done legally, right, quickly, but you can’t share them, the details or how, or else we’ll lose the ability to access. That’s hard to get across in this current world: the right to know I would put up against the right to be protected. I wish you great good luck in your ongoing efforts. [*applause*]

Senators: Thank you.

Slick: Before we wrap this up and say thank you to our guests, I just want to give everybody a logistical reminder. The program asks that you please relatively quickly move back out of the auditorium to the left, grab your lunch, bring it back to the table, because we’re going to start promptly at 12:45 with the next session. So please join me in thanking our guests. [*applause*]

[*End of Recording*]