Steve Clemons:
Is this the establishment intelligence for you to come to intimidate me? Everybody—George Little, you know, he’s a spokesman for the CIA, Pentagon. You know. You’re not going to intimidate me.

George Little: OK.
[laughter]

Steve Clemons: Maybe him.

Rep. Will Hurd: Why is he sitting right in front of me, too?
[laughter]

Steve Clemons: I know. Yeah, yeah.


Steve Clemons: Oh, congressman, it’s great to be with you again. I walked in, and I was talking to Gus from Accenture this morning, saying I’m fairly depressed about this topic, in the sense that in the many years that I’ve had the privilege of interviewing you or talking about the cyber health of the country and what’s going on, you just read every day another shocking revelation. The North Koreans just stole the war plans from the U.S. government and the South Korean government about what we might do. The Securities and Exchange Commission hacked—doesn’t tell anybody for two years. There’s a lot—you know, Equifax. There’s a lot of things going on. And I’m just interested in—I mean, you’re the cyber guy, the cyber diva in Congress.

0:01:05
Rep. Will Hurd: I don’t know how I feel about that title, but…
[laughter]

Steve Clemons: In my world, it’s a compliment.


[laughter]

Steve Clemons:
But I would tell you that—I want to just get a sense from you, because you’re trying to fix things.


Steve Clemons: And you have a lot of Republican colleagues and Democratic colleagues, and I just wonder what is your own assessment, when you get up every morning and say, “Crap, another big company went down” or “The U.S. government got hacked”? Rep. Will Hurd: So I’m hopeful that we can get it right, because most of these major attacks are not zero day exploits. Zero day exploits being something that’s previously
unknown. So it’s not like these are incredibly sophisticated attacks. It is people—the
defenders not doing basic stuff that is going when it comes to digital system hygiene. So if
you patch your software, if you have strong passwords, if you make sure that folks don’t
have—that people’s permissions to data is right, you can defend against 85 percent of the kind of
attacks that are happening.

0:02:17
But that’s why it also makes this issue so frustrating, is because if you do the basics, you
should be defending your digital infrastructure. And because we’re not doing the basics, that’s
why we have the OPM hack. That’s why we have Equifax as a problem. So that’s how I
would look at the state of things.

Steve Clemons:
So we’re 17 years into the 21st century, and I
remember the year 2000, Andy Grove, the
former chairman and CEO of Intel, was lobbying
Congress about the concerns about Y2K, and
about the vulnerabilities we had there. It seemed
like we met that challenge and have gone to
time for 15 years. Tom Udall just gushed praise
on you—this is a Democratic senator gushing
praise on you and what you did with modernizing
government, getting more resources and
awareness.

0:03:07
Why is the system so slow? Why has it taken 17
years for Will Hurd to come in and say, “We
need to modernize our government systems and
to be smarter on IT?” I mean just what’s going
on?

Rep. Will Hurd:
Well, I think there needs to be an improved
common body of knowledge, not only in
Congress, but in the executive branch as well,
recommending and understanding the threats.

Steve Clemons:
Tell me what that means. An improved body of
knowledge. I don’t get it.

Rep. Will Hurd: So look, many of my
colleagues think the dark web is the—is direct
messaging within Twitter, right?

[laugh]

Steve Clemons: Or WhatsApp.


Steve Clemons: Yeah.

Rep. Will Hurd:
So it’s some basic things like that, that we need
to improve. We need to make sure that agency
heads are responsible for cybersecurity. We’re
seeing that trend change in the private sector,
where this is no longer just seen as a cost
center—cybersecurity, that is.

0:04:00
It is something that’s invaluable to the basic
operations of a company. And that’s why you
have CIOs and CISOs report directly to CEOs,
so they’re considered to be part of the C-suite.
We need to have that same kind of mentality
and culture here in the government. There are
still I believe 14 of the—so there’s 24 CFO
agencies. These are the big agencies in the
federal government. I think 14 still have a CIO
that doesn’t report to the deputy agency head or
the agency head. And so you have to make
sure that culture is there. And what we’ve
tried—what I’ve tried to do is just be persistent.
Continue to shine a light on the problem. Bring
people back in, over and over, and make them
answer these questions.

Steve Clemons:
I know you’ve been thinking a lot about
personnel. If I were a graduate of MIT today, in
some very sophisticated stuff in the IT world,
and I had a couple of piercings and tattoos and
you know, just stayed up all night, slept during
the day, wore a lot of black—if I get offered a
fortune to go work for Intel, and I can be who I
am, versus going to work for the U.S.
government, that represents a fork in the road.
And what I think you’ve been worried about—the absence of really competent talent going into the U.S. government and being drawn into the private sector. So where does my creative, MIT, digital horizon go? And how do you deal with that?

Rep. Will Hurd:
Look, we need that person to continue going into industry. We need that person to be a white hat hacker. We need—that community is important to our digital ecosystem. But what the government needs to accept is that we’re never going to compete with the private sector for jobs. And that’s OK. But how can we compete? And the concept, and what I’m working on, is this thing called the cyber national guard.

Steve Clemons: Right.

Rep. Will Hurd: If you’re a kid and you want to go…

Steve Clemons: Is that hashtag cyber national guard?

Rep. Will Hurd:
Hashtag cyber national guard. You heard it here first. If you’re in high school, and you want to go to college in something around cybersecurity, we’re going to find you some scholarships, and some federal dollars to do that.

And it may not even be a four-year program. But you’re going to get federal dollars, and then for however long you got scholarship money, you have to serve in the federal government for that length of time. So you’re not going to go work at the NSA or the CIA or at DoD. You’re going to go work in the Department of Interior. You’re going to go work in U.S. Census Bureau. You’re going to work in Department of Homeland Security. Other places where we need folks that have these talents. And then after you’ve served and you go work in the private sector, that private sector company is going to loan you back into the federal government for let’s call it ten days every other quarter. And so you achieve cross-pollination of ideas.

Steve Clemons: And what do I get out of that?

Rep. Will Hurd: You being…?

Steve Clemons: The national guardsman.

Rep. Will Hurd:
Well, the national guardsman is—you are exposed—the networks are so big in the government.

There’s no other place where you can get that kind of exposure. And so you get a skillset that is important when you go out—when you go to the private sector. And also, you’re getting school paid for, right? And so that’s the value. And then when you go and work in that company, the company is going to appreciate this, because they’re getting an insight into what’s happening in the federal government. The federal government is benefiting from having someone that has exposure in the private sector. And that’s where we’re going to start making sure that the private sector and the public sector are working a little bit closer together. And you know, we have the U.S. Digital Service.

Steve Clemons: Right.

Rep. Will Hurd: And these are for high speed, low drag folks, that are going to come work for the government for two years. Why not have a second section which manages this cyber national guard where if I’m a guardsman, let’s say I’m going to be employed in the USDS for four years, but really I’m getting loaned back for 20 days a year.

Steve Clemons: Is this proposal legislation yet?

Rep. Will Hurd: We are working on the text as we speak.
Steve Clemons: Who is your Democratic partner?

Rep. Will Hurd: We’re still—there’s plenty of folks that want to…

Steve Clemons: You could put a “wanted” sign out there.


Steve Clemons: You know, “Help wanted.”

Rep. Will Hurd: Yeah, we haven’t established that. But look, there are plenty of people that I work with a lot on the Democratic side when it comes to these types of issues. But we want to make sure we start getting some actual text down, so everybody knows exactly what we’re trying to achieve.

Steve Clemons: Will, you were a spy.

Rep. Will Hurd: I was. Spy master, technically.

Steve Clemons: You were a spy master.

[audience murmuring]

Steve Clemons:
Yeah. You were a spy. I mean, you were literally—I mean, I’m not even joking. You were genuinely a spy. And that’s maybe why George Little is here. Worked for the CIA...


[laughter]

Steve Clemons:
And yeah, worked for the CIA. You did covert—and anyway, I haven’t read David Ignatius’s new novel, A Quantum Spy. It just arrived there. But I did read over the weekend John le Carré’s book A Legacy of Spies. I don’t know—has anybody read le Carré’s latest book? Yeah.

0:09:00
I happened to love it. But how much digital stuff was in that book? Almost nothing. So it gave me a snapshot of what old spycraft was like. You know, it was drop boxes. It was—I mean, it took you back into George Smiley days that I thought, wow, that preceded the age and the ecosystem we’re in now. Ignatius is interesting in the stuff that he writes, in the novels, because he’s looking at financial intelligence and how you target people and drones and sensors and hacking cars. And I don’t know what quantum spy is, but you were a spy. And I just want to know, how good or bad are our intelligence capabilities? When you look at what’s happening in the world, what other governments are doing.

Person:
[0:09:42 inaudible - crosstalk], Congressman.
[laughter]

Rep. Will Hurd:
[laugh] Look, our intelligence capabilities are still the best in the world, right? But we can improve.

Steve Clemons: On what basis?

Rep. Will Hurd:
It’s because of the talented individuals. And let’s use 9/11 as an example. The day I drove my Toyota 4Runner from San Antonio, Texas, to Washington D.C. was the day of the USS Cole.

0:10:04
And that was the U.S. destroyer in the Gulf of Aden off the coast of Yemen that was bombed by Al-Qaeda. I was in the CIA when 9/11 happened. On September 12th, I was like the fourth or fifth employee in CTCSO—the Counterterrorism Center of Special Operations division which prosecuted the war in Afghanistan.
Steve Clemons: Mm!

Rep. Will Hurd:
If you were to ask me then, would it be 16 years before another major attack on the homeland, I’d have said, “You’re crazy. Something’s going to happen.” Right? And the fact that we haven’t had an attack like that in 16 years is a testament to the men and women in the intelligence services, our diplomatic corps, that are working every single day, doing really hard things. When you’re in the CIA, and you get tasked with, “Hey, you’ve got to stop this,” you don’t say, “Hey boss, we don’t have enough—our budget’s not big enough” or, “We don’t have enough people.” You go do the job. Right? And that’s that can-do attitude that persists. So our intelligence services have to be right every single time.

0:11:03
Bad guys have to be right once. But where we can improve, especially in the digital world—our banks have a better idea of where Russian malware is going to come and attack them next, OK? Because they deal with this, millions of attacks, per month.

Steve Clemons: And do you—I just want to—do you think Russia is a serious threat to the United States?

Rep. Will Hurd:
One hundred percent it is. One hundred percent it is. They are our adversary, not our ally. And so, let’s take what these assumptions our banks have, turn those into collection priorities, task our core collectors—people that did the job that I used to do—and go collect that information, and then get it back in the hands of our friends in the private sector, so that they can defend against that next-level attack. So we shouldn’t have any hubris within the federal government, within our collectors, saying, “We know everything.”

0:12:01
I speak at as many high schools as I can, and I always tell the kids, “I know what I know. I know what I don’t know. But what I don’t know I don’t know is the largest of those three categories.” And in the NSA, in the CIA, in DoD, we have to accept that there’s a lot out there that we don’t know, and we should be leveraging the talent out in the private sector to help us fill those gaps. And so, turning private sector assumptions into collection requirements is not hard. Tasking core collectors—it’s fairly easy. But getting that information back in the hands—that is the difficult—that is a difficult problem. And that’s what some programs are trying to do, and that’s something that I’m interested in working on as well.

Steve Clemons:
You have been pretty critical of the Obama administration for having essentially created siloes that made it hard for this kind of information and awareness to be communicated, particularly overseas, with export control issues. I’d love to just get a chance to understand whether any of that has been fixed in this new administration.

0:13:00
Rep. Will Hurd:
So, has some of that been fixed? No. And I would say Tony Scott, who is a former...

Steve Clemons: Maybe you can explain to the audience better than I can what your objection was.

Rep. Will Hurd:
There was a number of issues. But first and foremost, I still believe, and just my criticism of the previous administration was not a partisan thing, because I do believe one of the last few issues in Washington D.C. that is truly bipartisan is cybersecurity. And so, we have to—a big issue was this thing called Wassenaar. This was other countries saying that anything that can be used in a cyber world that a bad guy can use should be considered under export controls. And so that meant that if Accenture was doing a technical vulnerability assessment of an entity in Italy, and the things they learned they emailed to their office back here in Washington D.C., they would have violated an export control, right? That’s crazy.
0:14:12
Now I would say this process worked, because this was a multilateral forum overseas, and the State Department came back and said, “This is what we’re going to implement.” Commerce was the implementing agency. They sent out a summary of what’s going to happen. The entire security community reacted. Congress—we did hearings on this, and Commerce said, “Hey, we need to pump the brakes on this, and go back to Wassenaar and renegotiate.” So we’re still currently in that renegotiation to fix that. But I think this was an actual example where the entire process worked to make sure that the input from the private sector was used to fix some official position. And this is where I think a lot of these international issues need to be faced.

Steve Clemons: Hmm.

0:15:03
Now I also have a problem with many of our European allies, that look at—they try to use the specter of Snowden, saying that the U.S. doesn’t appreciate privacy, when that’s a fallacy. Because Germany, who is also one of the biggest countries criticizing the United States, the government owns like a third of the telecommunications infrastructure. The B&D, their local service can do things against German citizens in Germany that the NSA and the FBI would never have dreamed about doing. So there’s a disconnect there with many of our allies.

Steve Clemons: One of the questions we were just talking about is—we read a lot about what the Chinese are doing the penetrate systems—OPM, various companies, corporate espionage. What the Russians are doing in hacking. And I’m just interested—is the United States doing any of this?

0:16:00

[laughter]

Rep. Will Hurd: No, look. So the…

Steve Clemons: I mean, I know we did Stuxnet, but Stuxnet seems so small and trivial now when we look at the scale of what other state players are doing in the cyber space. So we know about Stuxnet. We know that Israel and the United States engaged in this. We don’t know a lot else. And I guess—I know you know the secrets, and I just want to know whether we should feel confident or we should feel like we’re pathetic.

Rep. Will Hurd: So the United States still has, when you look at capabilities, and you compare this against other AP…advanced persistent threats—that’s the term of the baddest of the bad…

Steve Clemons: Hmm.

Rep. Will Hurd:
…we’re in that top tier. Period, end of story. Are we using the capabilities that we have enough is I think the better question, and my answer would be no. And let’s take Eastern Ukraine as the example. The Russians are using the latest and greatest tactics techniques and procedures in electronic warfare in Eastern Ukraine. Are we utilizing the latest and greatest in counter-electronic warfare in Eastern Ukraine to stop—to protect our ally, Ukraine, and to counter the Russian aggression? The answer is no.

0:17:16
And so who is the equivalent of the Navy Seals when it comes to electronic warfare? And if somebody knows the answer, I’m still trying to figure that out.

Steve Clemons: Cool. You can see him right after.


[laughter]

Steve Clemons: Quantum computing.

Steve Clemons:
You have regularly said that we're not doing enough in this space, that it's a blind spot. We need to devote more resources to quantum computing. I want to know why, and I want to know who's blocking you.

Rep. Will Hurd:
So Vladimir Putin a couple weeks ago said that whoever masters AI is going to be…

Steve Clemons: Run the world.

Rep. Will Hurd: Run the world. He's wrong. It's whoever masters quantum computing is going to be the sole hegemon.

0:18:04
And quantum computing is important because it completely negates how we do encryption right now. And so that means the digital tools and tactics we've been using to protect information for 50 years is going to be negated. And that means if you have—let's say the Russians or the Chinese has sucked in all this data that's encrypted. You can't read it right now. Whoever gets quantum computing is going to be able to break that and read that information. So whoever gets there first is going to have a significant leg up.

Steve Clemons: So who's your opponent politically on this?

Rep. Will Hurd:
Well, there's nobody politically against doing more when it comes to quantum computing. Making sure we have the federal funds for basic research that supports this and making sure that we're working with industry.

0:19:04
There's folks in Silicon Valley that are working on this. Folks here in Washington D.C. that are working on it. Many of our allies—the Canadians in the Waterloo region are very involved in looking at quantum computing. But we have to make sure we're focused on this. And it's hard for—look, I still think that to me—and I have a higher than average, better understanding of this—to me, quantum computing is still a philosophical exercise, right?

Steve Clemons: Right.

Rep. Will Hurd:
Because a bit can be a one, a zero, both, neither, or all four all at the same time? Like that's still—that's a concept that's really hard. Thanks for the couple of engineers that giggled. [laughter]

Rep. Will Hurd:
It's a tough concept, because it's so different than what we've always known—a bit can be a one or a zero. It's on or off. Right?

Steve Clemons: In the aggregate, on a scale of one to ten, ten being very literate, what is the digital literacy of your colleagues? The cyber literacy of your colleagues? [laughter]

0:20:00
Rep. Will Hurd: Four?

Steve Clemons: Yeah. That's…

Rep. Will Hurd: But let me say this. Let me say this, though. They understand the threat. They understand that this is a problem and something needs to be done. And so the recognition that there is a problem is nine. What we do about it and how we solve it—that's a lot lower. And being able to evaluate many of the different issues is difficult. Because look, there's still some basic questions that we haven't answered. What is a digital act of war, and what's an appropriate response? Different parts of the federal government has opinions, but there's not something that we have agreed to. And so if you can't—I believe there should be some red lines saying, “If x is done, y is going to be the response.”
Steve Clemons: So before I go to the audience, last question, since you mentioned act of war. Do you share Bob Corker’s concerns that the president’s lack of temperament or his behavior is tilting us towards World War III?

Rep. Will Hurd: No. Look, it’s real simple. Encryption is good for our national security. It’s good for our economy. We should be strengthening encryption, not weakening it. And it’s technically impossible to have strong encryption with any kind of back door in it. And so, this is a conversation that we’re going to be involved in forever. Look, I don’t know what crypto war we’re in right now. Is it five? Is it six?

Steve Clemons: So before I go to the audience, last question, since you mentioned act of war. Do you share Bob Corker’s concerns that the president’s lack of temperament or his behavior is tilting us towards World War III?

Rep. Will Hurd: I think the national security team that we have is one in the first rate. The fact that—what I find funny is…

Steve Clemons: But the team is different than the president.

Rep. Will Hurd: Well, but the president is the person that selected the team, right?

Steve Clemons: Right.

Rep. Will Hurd: And so the fact that we’re in direct negotiations with the North Koreans is a 12th or 13th story—it’s crazy. If this would have happened nine years ago or ten years ago, people would have been like, “Oh my god, I can’t believe we’re having direct conversations with the North Koreans. Why is it not within the six-party talks framework?” So as long as there’s dialogue between us and the North Koreans, I don’t think you’re going to have World War III. And one of the things I learned when I was in the CIA—be tough with tough guys, and nice with nice guys. And so we have to be tough with the North Koreans.

Steve Clemons: Thank you. Let me open up the floor. Yes, right here. Good morning.

Person: Good morning. I believe it was two nights ago that Rod Rosenstein tried to rebrand encryption back doors as “responsible encryption.” I’m wondering if that new—that the rebranding has swayed your opinion any.

Steve Clemons: Yeah. How do you feel about the moniker “responsible encryption”? 

Rep. Will Hurd: But this is an issue that is going to be going on for a long time. And for me, and many of our colleagues, you can protect our digital infrastructure, chase bad guys, and protect our civil liberties, all at the same time. It’s hard, but we can do it. And our civil liberties are not burdens. They’re the things that make our country great. So yeah, you can call it whatever you want, but make sure you have strong encryption. Period, end of story.
Steve Clemons: Yes, right up here in front. He’s going to hold the mic for you.

Teiko McCollough [sp]:
Hi my name is Teiko McCollough [sp]. I was wondering if you could give your thoughts on cryptocurrency such as bitcoin and the regulation of things like that.

Rep. Will Hurd: Well, look, I don’t have—I haven’t—I look more at blockchain that I do cryptocurrency, right? And so I think blockchain…

Steve Clemons: Are they different?

Rep. Will Hurd: They are different.

0:24:00
Blockchain was ultimately the technology that allowed the kind of cryptocurrency to happen. But…

Steve Clemons:
But don’t you need bitcoin or something like that to create the backbone to reward the…?

Rep. Will Hurd:
Well, no. So you’re not rewarding. So a blockchain is just a distributed ledger, right?

Steve Clemons: Right, yeah.

Rep. Will Hurd:
That you can see any kind of changes. And not one person holds it. And so, you can use it in customs, right? Merck’s and IBM and DHS is working on a way on how you can use a blockchain to move products across the world. Walmart is using it to make sure they know where their cantaloupes have been, so if there’s a listeria or some other issue, they can look immediately—“This was in this facility. Anything that went through this, let’s find it.”

0:25:00
And so I’ve been focusing on blockchain as a tool that the federal government can be using in order to streamline processes. When it comes—I don’t think we’re going to get to a point where cryptocurrencies is the currency of the world. But I’m not knowledgeable enough about the nuance. All I do know is folks that have cryptocurrency, they’ve been targets of a lot of interesting attacks. One of the things I never learned is make sure you call your cell phone, and make sure that you can’t port your number to another cell phone. Because hackers have been taking advantage of two-factor authentication in order to steal bitcoin and things like that. So it has introduced a different type of attack on individuals that have this. But yeah, I think a lot of folks are still talking about this.

Steve Clemons: I just want to say The Atlantic loves having conversations with you.

0:26:01
We cover so much territory. We’ve run out of—we’re going to end right now, but one of the things that we didn’t get to, but I hope we can next time, is the distinction between dumb walls and smart walls.

Rep. Will Hurd: [laugh]

Steve Clemons: And how the kind of technology, sensors, whatnot, creates the kind of conditions you want. Because I know you’re not supportive of dumb walls, right?

Rep. Will Hurd: Yes. I like the…

Steve Clemons: Is that a—I mean, yes or no?

Rep. Will Hurd: I’m—yes, that is—I concur with the good gentleman from The Atlantic.

Steve Clemons: [laugh]
Rep. Will Hurd:
Look, building a 30-foot-high concrete structure from sea to shining sea is the most expensive and least effective way to do border security. And the reason we haven't been able to get operational control of our border in 2017 is we haven't looked at all 2,000 miles of our southern border at the same time. And the only way we do that is with technology. It’s a fraction of the cost. We can do implementation. And all the data we get, we can beam it to the men and women that are keeping us safe. So, always good to see you.

Steve Clemons:
Ladies and gentlemen, Congressman Will Hurd of Texas. Thank you so much.
[0:27:00]
[End of recording]