Conversations with Bill Kristol

Guest: Jack Goldsmith, Professor of Law, Harvard University
Assistant Attorney General, Office of Legal Counsel (2003–2004)

Taped October 11, 2018

Table of Contents

I: Cybersecurity and Cyberwarfare (0:15 – 31:09)

KRISTOL: Hi, I'm Bill Kristol. Welcome to CONVERSATIONS. I'm joined today by Jack Goldsmith, professor of Law at Harvard Law School, but despite that, an extremely intelligent and sensible fellow. Served in the Bush administration in a senior position at the Justice Department – OLC, right? Office of Legal Counsel?

GOLDSMITH: The Office of Legal Counsel.

KRISTOL: The very prestigious, in-house lawyer for the administration, so to speak. And you've written widely on many topics, but today we're going to discuss cybersecurity, something you've written on, have been focused on, and are alarmed by, I think. Is that right?

GOLDSMITH: I would say that I'm pretty alarmed by it, yes.

KRISTOL: So let's talk about that. I mean, from the outside, there are occasional hacks, you read the stories – obviously, most famously, maybe Russia in 2016. But I don't know, can't we deal with these? Is this really a huge national security problem? Is this going to be a major part of our national security challenges over the next decade or two?

GOLDSMITH: I do think that it is a major national security problem. The government certainly sees it that way. It's always at the top of the list of threats and the threat reports that the government issues.

KRISTOL: I've been struck by that, talking to people not from that area who don't have an interest in promoting it, in a sense, just four-star generals who – you have senior positions and get briefed up on what could happen – and they think hard about it and they really are alarmed.

GOLDSMITH: And there are several things to be alarmed about. One thing that a lot of people are alarmed about are the so-called "cyber Pearl Harbor," where the computer networks attached, say, to the electrical grid or the like would be attacked; and that an adversary could bring the electrical system down, or part of it, or make the numbers on Wall Street lack integrity or the like. So there's that possibility, which we've heard warnings about but haven't seen yet.

But there's also just the death by a thousand cuts, smaller type of threats. The extraordinary extent of cybertheft of important American business secrets; the theft of military secrets; the disruption on digital networks that we saw, most prominently in the Russia hack; and all of these things are happening and have been happening, and we seem unable to check them.

KRISTOL: I was going to say, presumably when there are new technologies there are new opportunities for theft. [For example] credit cards online, people stole credit card numbers and now it's a problem, but everyone lives with it, and you use your credit card and every three years you get a phone call that…

GOLDSMITH: So, we've adjusted to that problem and presumably, the enormous financial benefits that credit card companies are reaping from online business outweigh the extra cost they have to pay for fraud. So parts of it are manageable.

The essential problem is that the offensive threat is greatly magnified because, essentially, all of our wealth and power in some sense is embedded in these digital networks. And almost all of them are connected to the internet, and that means that adversaries – you don't just go up to the Pentagon and break in the door to do serious harm. You can do it from the other side of the world.

So the number of adversaries are just multiplied enormously. And on top of that, it's just the nature of digital systems is they're very hard to defend – that the offensive actors, the people trying to do theft or disruption, they have an advantage that no one has been able to reverse yet.

KRISTOL: Yeah, so let's talk about that because that's a classic thing people study in national security, right? Offense seems to predominate for a while and then defense often catches up.

GOLDSMITH: Defense hasn't caught up yet. Some people say there's speculation that with the advent of artificial intelligence that maybe defensive systems will be able to discover the vulnerabilities, and be able to patch them and to ward off offensive attacks much more efficiently than we can now, but we're definitely not there yet.

And the essential problem is that these networks are very complicated. They're very complex and they operate – the way software interacts with hardware and with other pieces of software leads to openings for an adversary to be able to exploit. And the adversary, of course – this is an old principle of national security – the adversary only has to find one weakness, whereas the defender has to defend every weakness. And over time and with numbers, offense has been so far able to win.

There are lots of other problems. We haven't put in place the right incentives for individuals and companies to take the proper steps to defend their networks. There are a lot of things that we could do to improve cybersecurity that we haven't done because regulating in this area is hard and controversial.

But essentially, it's a situation where we have many, many more adversaries who sitting at a computer network can do enormous harm to us, either through theft or disruption, from the other side of the globe.

KRISTOL: So let's talk about the adversaries. I guess the kind of harm they can do is – it's not like conquer – well, maybe it is. Can they take over something? Or is it more just sowing chaos?

GOLDSMITH: It's not like a nuclear weapon where they can blow up a city. And it won't directly lead to a takeover or anything like that. And the worst case scenarios about electricity going off, or government communication systems being shut down, or the stock market crashing irretrievably or something like that, those remain far-fetched for a variety of reasons. That was a threat, but there are a lot of reasons, I think, to be somewhat less worried about that than lower-level threats that, because they're lower-level, are harder to defend against.

So the massive theft that our companies have suffered in intellectual property theft. The enormous disruption to our elections.

In a way, that's really the best example, is the Russia hack. When you strip it all away, all the Russians – the real effort was simply to do a phishing attack: a fake email sent to Podesta who clicked on it, and they got inside his emails and then released the information. That simple act of breaking into someone's emails and releasing the information, once it's released into our political system and our free-speech dominant system, it sowed chaos. And went to the core of our democratic government in a way that we're still living with. And it wasn't hard. It was very easy to do. And there just wasn't that capability before.

KRISTOL: Yeah, you could steal documents, I suppose. That's what spies did, right?

GOLDSMITH: And the United States famously – and this was a typical espionage technique to steal a document, and have it placed in a newspaper somewhere and publish it. But nothing on the scale of what we saw in terms of the impact.

KRISTOL: So why is it so hard to defend? I guess is it the structure of the way the internet's set up and the private actors? Or is it just the nature of the technology?

GOLDSMITH: There are a whole list of reasons. I'll give you a few. The nature of the technology. The complexity of the systems means that it's very hard to find every potential malfunction or every potential way the system – that the software, and the hardware, the various pieces of software could interact with the software in-the-machine, the software on the communications networks and the like. Those create what are called *vulnerabilities*, and once there are vulnerabilities that means that all of these actors – which who knows how many there are – can potentially find a weakness and get in from the other side of the globe.

And there are steps you can take to prevent that. You can cut the network off, for example, from the internet. Or you can take steps to make it very, very, very hard for an adversary to get in; and some of our most sensitive systems, especially in the government and the private sector have these super-hardened defenses. But even there, the possibilities for mistake – putting a thumb drive into a machine that has malware on it that could make an attack possible. Technologically, putting up defenses is very, very hard.

Then there are market problems that keep us from defending the network. So a lot of the vulnerabilities in the networks could be taken care of with proper regulation, for example, to give users like you and me more of an incentive to have proper internet hygiene and cybersecurity hygiene on our own machines. We really don't have that incentive now, but if we had to pay for it in some sense or we were penalized for not being on the network for not having proper cybersecurity, that might bring a lot of the machines up to cybersecurity standards.

The companies that suffer these attacks, if they could somehow share the threat information, what they're seeing with other companies or with the government and coordinate that better, we could raise our defenses. That proves very hard to do because companies don't want to share their information when we worry about the government being involved in the private sector. There's a huge worry about any regulation that would raise our cybersecurity defenses might kill innovation, which is our strength.

And the West Coast lobbies for the big internet companies and the communications companies who don't want any government regulation are extremely powerful. Basically, we've known what some of the solutions are to make things better, not to make a perfect defense, but to have better defense, but we have not been able to implement them.

KRISTOL: Yeah, it does seem like it's different, and I've sort of made this point that, in the nuclear age or whatever, nuclear weapons were very powerful to say the least. We had problems in the '50s. Perhaps our nuclear retaliation wasn't set up in a way that would disincentivize the first strike properly and questions of whether we had survivability, but the government could change it. Herman Khan and [Albert] Wohlstetter or people could consult with the government and say, "Hey, we should have more nukes on submarines," or mobile or whatever.

And you could do that. I guess here one problem is that society's attacked as much or almost as much in a cyber way, but the government doesn't control the entities, right? Or even the ability to respond – well, we'll get to the ability to respond; I guess that would be the other question.

GOLDSMITH: Just to finish your thought, the government doesn't control the channels of attack. The analogy and the dis-analogy is exactly right. The nuclear problem, in retrospect, it was a huge problem because the destructive capability of those weapons was quite clear and coming up with the solution took an enormous amount of brainpower and study. But you're right that the government was basically able to implement it through arms treaties, and through building certain types of weapons, and through organizing the government in a certain way. Whether we solved the problem or not, we were able to deal with the problem fine for decades and decades.

This problem is just beyond measure more complex. There's no single government solution that the government could compose like that and impose like that. And the main reason is, as you suggested, is so much of this activity takes place in the private sector. Google's a private company. That was the channel through which Podesta's email was hacked.

And the networks themselves through which all the communications travel and through which all the malware and the bad acts happen, those are private communication channels that we normally think of – unlike air and land where the government has complete control of the borders – we don't think that the government should be able to be fully in those networks because of free-speech reasons, and privacy reasons and the like.

These are channels of private attack that are doing enormous damage to our country that the government really doesn't have full access to. So in that sense it's unlike other national security threats. And that's a huge difference.

KRISTOL: Yeah, I was thinking of other analogies: people fly private airlines into the U.S. and could bring in dangerous things, but there's Customs at the border.

GOLDSMITH: We don't have perfect defense at the border, obviously, but in theory the government is in there doing its best. And we don't have that in the cyber context.

KRISTOL: There's no equivalent of Customs –

GOLDSMITH: There's equivalent of Customs.

KRISTOL: – that you have to go through to access U.S. space.

GOLDSMITH: There are pipes at the border through which communications channel, but we don't allow the government to be in those.

KRISTOL: Now, is that a matter of constitutional law, or just our own predilection toward the private sector?

GOLDSMITH: It's both.

KRISTOL: The government could – could it not mandate? It does mandate in some areas, I know, certain basic standards of protecting data.

GOLDSMITH: The government could mandate more cybersecurity through a variety of means that forces the private sector to take this problem more seriously. It has not been able to do that because just about everyone thinks that – or certainly the companies think that – any effort to impose these will kill the efficacy of the systems, and the innovation and the technologies. Whether that's true or not, or whether there's a happier middle ground – The government is slowly but surely trying to raise standards, but it's very slow.

And the point is the government itself can't be at the border watching the communications come by inside the network. And so the question is can the government – we have a lot of government regulation of the private sector to enhance our national security and we've been moving in that directly slowly in the cyber context, but the government has been moving very, very slowly because we don't have a consensus on what the right steps are.

KRISTOL: Yeah, I was thinking of other areas. The government prevents certain foods from entering the country, if it's contaminated, bad drugs. There are a lot of private sector efforts in trading and manufacturing that the government doesn't control, but that it limits, regulates, and monitors.

GOLDSMITH: But the other problem is it's not like you can tell Verizon, "Please stop this phishing attack at the border." It's not easy to see when it's coming across. It's just an email. And it's an email with a payload that's probably encrypted. So even an injunction to Verizon and AT&T, "Please stop bad stuff at the border." It would be meaningless.

KRISTOL: And we've gotten so used to the convenience – when I'm abroad, email back home. You don't even think twice about it. The idea that you'd have to go through a bunch of steps or have a different security protocol, it would be very –

GOLDSMITH: Another central problem is that even two-factor authentication, which is a very simple, but consequential step at enhancing security, a lot of people go crazy over that because it takes an extra five seconds to get into a system. And so there's resistance even to mandating simple positive steps like that because the point of convenience is an important one. We're so addicted to the convenience of these technologies, and the convenience, in the short run, always wins out.

So we now have the Internet of Things coming where every device is going to have a chip in it and be connected to a network. And the conveniences that are going to come from that are enormous, but the vulnerabilities that comes from that we're not going to see right away. We're going to reap all the benefits of convenience, and wealth, and comfort that the systems give us, and we push the cybersecurity problems down the road. The Internet of Things, which connects everything, is an enormous cybersecurity problem that is really only a secondary concern right now. And that's the problem, we grab the convenience, we see the short-term benefit and we push the cybersecurity costs downstream.

KRISTOL: Could you explain the Internet of Things thing a little better for us?

GOLDSMITH: The Internet of Things is just – I just got a new air conditioning system that is connected through the internet to my phone, so I can adjust the air conditioning from my phone before I come home or whatever. I resisted, but my alarm company wanted to put in a new alarm that was connected to the internet and on my phone. And I try to resist these things whenever I can. All of our devices – the toasters, refrigerators, *clothes* – everything is going to be connected to the internet because data can be generated about that that is both good for the companies and, they would say, good for the consumers.

There are all sorts of benefits that come from these, but this is just enhancing enormously our digital dependency and that means that adversaries, to the extend we get dependent on this, can take it down

and manipulate it. Cars that are connected to the internet, many people worry can be hacked and cause mayhem for travel. Anything that's connected to the network is a subject of potential attack and disruption.

KRISTOL: How much of this in your view is a foreign adversary problem? How much of it is just random criminal gangs abroad? Or how much of it could also just be domestic terrorists and such?

GOLDSMITH: It's all of these things. The government used to worry most, I think still does worry most, about foreign governmental adversaries because some of the high-end cyber operations take a lot of computer power and a lot of intelligence that sometimes only governments have. And so the biggest adversaries everyone thinks are China, Russia and Iran. North Korea also is developing a really important cyber capability, which has allowed it to steal a lot of money and in a way circumvent sanctions with very little investment.

So most of the threat comes from governments which have lots of sophistication and power in the space. But, increasingly, there are these massive criminal groups that are sometimes connected to states – for example, in Russia – that do a lot of this. And we've seen examples where kids who are 17 sitting on the other side of the world can just on their computer cause disruption. The array of threat actors goes from the teenager in his bed to the Chinese government and everything in between.

KRISTOL: And I guess it is true – you read about these hacks, I do, at least. I'm one of these people who also doesn't – it's slightly annoying to use the two-factor. It's not really annoying, you just have to get used to it.

GOLDSMITH: It takes five, ten seconds.

KRISTOL: But then you think, "Well, I don't have anything really important. What do I care if someone reads my email setting up this conversation," and so forth. But, of course, that's not the right way to think about it, right? Because it's not just they're just penetrating your email, they're penetrating the whole company, or penetrating everyone with whom you're emailing, I suppose?

GOLDSMITH: Yes, that's right. That's the right way to think about it. If they can get into your email system, they could learn a lot about the people you're communicating with including a lot of private information, which you may have nothing to hide, but someone else might have something to hide. They could selectively release things that could be embarrassing. We could all have things in our emails, I'm sure, that if selectively released would be embarrassing to us.

If that person happens to be the head of the Democratic National Committee, you can sow huge confusion. The hack into Sony was –

KRISTOL: What about that? That was a big one. I guess I'm generally struck, and this is just confirming your point, and there's this big – Sony, very famous company, big hack, a lot of publicity for like two weeks. Did anyone do anything about it?

GOLDSMITH: Sony lost a lot of money and we don't know what, if any, sanctions the United States imposed on North Korea because we're basically out of bullets on that one. And they took, I can't remember how many billion dollar loss on it. Part of doing business now is dealing with these threats.

But we've become inured to them. If that had happened – Adversaries are doing things now that are hugely harmful that we really don't see. The Sony hack, you saw some released emails. That was the harm? They destroyed computers. They destroyed a lot of Sony's wealth, but we don't see the harm.

When they steal the plans to our fighter jets, we don't see that in the same way as if they had carted it out in a truck. All of these damaging things are happening, and they're on the front pages more and

more, but I think because we don't see them literally in physical space they don't set off the same alarms. If the things that were happening to us in cyber were happening in real space, we would be at war because we're really suffering huge losses. But we don't see them and therefore we're not as alarmed.

KRISTOL: And is it true that – You need some intellectual capital, I suppose, to be an effective cyber attacker – but it does level the playing field, in the sense that to actually build nuclear weapons or fighter bombers, you need a lot of actual money and actual engineering –

GOLDSMITH: I would go further. It doesn't just level the playing field, it gives significant advantage to our adversaries. Because you're absolutely right, to build nuclear weapons there are only a few counties in the world who can do that, who have the wealth, the intelligence and the resources to do that.

KRISTOL: And one can usually sometimes see it happening and the country can act to stop it, which is usually not the case here.

GOLDSMITH: Obviously there are secrets that are kept, and ascertaining intentions and actions, even with regard to real space weapons is a challenge and always has been, but nothing like this. The array of actors that can cause harm are enormous and, as you said, North Korea's a great example. Because this is a country that's barely connected to the internet, that does not have a lot of intellectual capital, does not have a lot of wealth, but in the last three or four years they've been able to develop a cyber exploitation capability that has enabled them to reap a lot of wealth. And to really – you've heard people in the government saying, this changes the nature of our relationship because the threat is not just they use nuclear weapons. They have other threats as well against us.

And here's an important part that we haven't discussed. The United States is, because it's so deeply digitally-dependent, maybe the most digitally-dependent country in the world, we have the most to lose from these losses.

So time and time again, especially under the Obama administration, you saw this. It's been a feature of this field. You have the Obama administration, when something bad happens – the Russia hack's a perfect example – they hesitated to respond. And the reason they hesitated to respond is because the technical term is they feared escalation. They feared that, "Well if we do something to respond to the Russians, what could they do back to us?" And because we have so many vulnerabilities in the digital space, the worry is that we'll lose an escalation.

And then we're paralyzed; we're deterred from responding. And you saw that excuse – David Sanger's book went through this in some detail. Time and time again, when in the face of the Sony hack, the Russia operation, Iranian attacks on U.S. banks, Jim Clapper, who's the head of the DNI, I'm paraphrasing, but he basically said, "I thought this time we were going to finally respond and go back against the Iranians. But we didn't because the Commerce Secretary said, 'I worry if you respond that they're going to do something worse to our banks.'"

Our deep digital sophistication and dependency is a weakness. The combination of more threat actors and our relative inability to respond is a huge problem.

KRISTOL: And the fact that offense is easier than defense, I guess.

GOLDSMITH: Yes. Now, I should add, it's both easier to do in the sense of the investment, and resources and the ability to escape detection and the ability to do it from afar means that the adversary has a larger advantage. I should add that the new National Security Agency Director, General Nakasone, said throughout the spring during his confirmation hearings and public speeches, and then we've heard this more in the last few months in the Trump administration, that the administration had decided to get much more aggressive in using our offensive cyber operations to try to respond or to try to take down in advance these operations.

Again, based on what the newspaper said, this is what the Obama administration hesitated to do. So there seems to be a realization in the last year that we have to take more aggressive steps, and there seems to be a realization, or at least a hope, that we can worry less about retaliation.

KRISTOL: And do you think that's plausible though? That you could have this kind of – what would that be? Not quite mutually assured destruction. I want to talk about that, too. A) It seems to me the way the nuclear thing got solved partly was kind of a mutually assured destruction. That seems a little trickier and more complicated in this area.

GOLDSMITH: But I think it's working to some degree. We'll talk about that.

KRISTOL: Okay. That, and then the second point would be what you just discussed also. Could you preempt, I guess, maybe that's the right analogy?

GOLDSMITH: That's what the thinking is. The thinking is less that we should retaliate in response than that we should just take away the capabilities upfront. And that we should be much more aggressive in using our extraordinary intelligence apparatus, extraordinary intelligence capabilities, plus our extraordinary offensive capabilities in cyber which we tend to hesitate to use, at least according to the government and everything else you read.

There's been a change in thinking, it seems, in that we're going to be using these tools much more aggressively, especially to try to preempt the attacks – i.e., to stop them before they happen. But Nakasone said – this is in spring of 2018, and no one really pays attention – we're the punching bag of the world right now in cyber because we don't do anything in response.

KRISTOL: Could we, in your view?

GOLDSMITH: We could be doing a lot more. It's dangerous. We certainly could be doing a lot more.

KRISTOL: Leaving aside escalation, but just a practical matter. Are we ahead of others?

GOLDSMITH: I'm not in a position to say first-hand, but by all accounts, yes, we are. There's a difference between having these tools and being able to use them, though. And we have a highly legalistic culture.

KRISTOL: We can't just decide one day we're going to disable a quarter of China's something –

GOLDSMITH: There's also the very tricky problem of how you think about retaliation. But yes, by all accounts we have the most sophisticated and powerful weapons.

KRISTOL: And the government – those are government [weapons] –?

GOLDSMITH: I'm talking about in the government. President Obama, he bragged about this at a press conference. He goes, "We have the most powerful weapons in the world." At the same press conference when he was basically saying we can't use these weapons because we're worried about retaliation.

So, it seems, from reports coming out of the NSA and the government, from various reports actually, that the government decided to start using these weapons more. So maybe we're at a turning point. We'll see if it leads to fewer attacks or to more escalation, maybe both.

KRISTOL: Yeah, that's a little worrisome. And are we set up well, in your view – this is something you've though about in a lot of different areas of governance – are we set up adequately in the government to coordinate to do this?

GOLDSMITH: On this question I'm not sure. I don't think that we are. Even within the National Security Agency, there's something called Cyber Command, which was created about eight or nine years ago, which now is a full-blown Combat and Command akin to Southern Command or any other unified Command.

But Cyber Command is dual-hatted with the Director of the National Security Agency, so the Director of the National Security Agency is both in charge of the electronic spy network and in charge of our offensive cyber capabilities. And there's a close relationship between those two things. That's why some people think they need to have the same person in charge because, to use these weapons offensively, you have to be able to break into the systems, and there's always a tradeoff because to get into the systems, the spy side of the house wants to get in there and not be seen, not be known, so they can collect information and do their spying business. And the offensive side of the house wants to take advantage of that penetration and do stuff that might show them getting caught.

So there's a coordination problem even within Cyber Command and National Security Agency. Right now it has one person at the top, and there's a debate about how that should be organized. So there's that point that we have, whether it's a good idea or a bad idea to have the spies working next to the offensive operators, or whether they should be separated and have two different people. And there are tradeoffs.

See, even in that space we haven't figured it out. Government-wide, we're not well-coordinated. We saw this with the Russia hack: We had very competent people atop the Homeland security, the FBI, the National Security Agency, and it wasn't clear some of the times who was supposed to be taking which leads. There has been a "cyber czar" in the White House who has been an important role, but fairly ineffectual.

The short answer to your question is I don't think that we've figured out how to organize ourselves for cyber offense or for cyber defense.

KRISTOL: The Russia hack – leaving aside, in a way, the politics of it, or did the Trump campaign know about it – that is a pretty interesting public policy case study, and I'm sure people have studied it. Is the lesson from that a worrisome lesson?

GOLDSMITH: The lesson is we're in a lot of trouble.

KRISTOL: They paid whatever price they paid with some sanctions, but basically, it's not clear what we could even do to counteract it, I suppose. Right? What, are we going to hack their elections?

GOLDSMITH: There are many lessons that you might learn. There are many lessons. One lesson is that our concept of critical infrastructure needs to be broadened to include almost everything. No one imagined that it was going to have this impact on our democracy that we're still living with, literally. It's really a wake-up call that every potential actor, someone connected to public policy has got to be very careful in their cybersecurity.

KRISTOL: So there's the email hack, but there's also the –

GOLDSMITH: Use of the social networks.

KRISTOL: Yeah.

GOLDSMITH: That's a huge topic and it's debated about the extent to which the Russians – there's no doubt that Russian influences were using social media to try to influence things. Foreign propaganda in elections goes way back, and we've practiced it for a very long time, the United States has. But this seems different because the power of it gets multiplied. It's still a debatable question about the actual

impact that the manipulation of social media had, but the combination of foreign influences in these very robust social-media networks and our First Amendment, which permits robust speech.

And the other problems, independent of foreign adversaries, that the internet is creating, especially Twitter and Facebook with extreme speech, mob speech, the splintering of people's inputs, news inputs and the like. There's a lot of bad things that are happening to our democracy, I think, just as a result of the combination of our free-speech commitments and these social-media networks *even before* you have foreign adversaries.

It was Russian then, but now everyone is seeing that it works with very little penalty. We can expect in every election for our adversaries – Why wouldn't they? It's a relatively inexpensive way to cause us harm– to use these and other tools to try to disrupt our democracy. The problem is a serious one even before we get to foreign adversaries, but they just exacerbate it.

II: Countering the Threats (31:09 – 57:30)

KRISTOL: And in terms of dealing with it – I guess I come back to this question of the private sector entities. I think that does seem to be just conceptually – if we called the White House to discuss this, and you've thought plenty more about it than I have, but how to get people to – I suppose there have been analogous things in defense? Obviously, there were defense industries where the government had to make sure that companies did certain things and did them in certain ways. They mostly did it by paying them, basically, to do it, I suppose.

GOLDSMITH: We still have something like that with the defense contractors, something not quite as tied to the state, but effectively, they are.

KRISTOL: Right. And so a civilian aircraft manufacturer, part of it becomes quasi-governmental in the way it operates. But of course you can't do that, presumably, with Google and Facebook, to say nothing of every financial institution, every –

GOLDSMITH: There's the First Amendment and the First Amendment forbids the government from regulating speech. So there's a lot of discussion about this in legal circles, whether we need to rethink the First Amendment in light of the problems that we've seen in recent years.

But the first problem is what should they be doing? What should Facebook and Twitter be doing? It's very, very, very hard to know: do we want these very powerful, private networks regulating speech in effect? Now, they do regulate speech. They have their terms of services. Do we want them going beyond what the First Amendment would do? Do we want them disallowing speech that the First Amendment would otherwise allow if the government was regulating it?

KRISTOL: That's a slightly separate issue. And, I mean, I'm personally fairly –

GOLDSMITH: I don't think it is a separate, if I'm understanding of your question, because you want to have the government do something, but the question is: *do what?*

KRISTOL: I'm thinking in the more limited way. I think that's the bigger problem. I don't know, the trap door.

GOLDSMITH: Oh, I see. Cybersecurity issues.

KRISTOL: One could imagine analogously to other things. I'm don't know I'm just making this up, but the government probably has some way of tracking every airplane and if there's an emergency like a 9/11, telling them to stand down and so forth.

My impression is that, if you think about it, we do have not the analogous power, or at least the companies have resisted it, online. So if there's a sudden attack, we can't go to the Facebook or to Google and say, "We need to see what's happening in this part of – ". I don't know. I'm making this up.

GOLDSMITH: Let me answer that in two ways. The answer to the question in part is yes. When these companies have a serious high-level attack, when Google was attacked by the Chinese about a decade ago into their most secret parts of their system, they immediately went to the National Security Agency. And when these high-level attacks happen, and sometimes in real space, the government can do things to assist and does work with these companies.

That by itself is dangerous. The companies don't want – it's not good for their business model to have the U.S. government involved too much, so they tend to stay on the sly. There are things that can happen. There is coordination between the government and companies for very high-level stuff. No one thinks it's adequate, but there are systems in place.

But just think there are many, many, many forms of attack. What could the government have ordered once Podesta's emails are released? Once it's out there – this is an important point. In Russia they can control the media. In China, they can control the promulgation of harmful information once it's out. We can't. And our system is such that we don't think that's a good thing.

And so, once that bad thing happens the government can't put it back in the box. In fact, Obama was disabled. If you remember he said over and over, "I was afraid to take more aggressive steps against the Russians or to make a bigger deal out of this because I was afraid it would look political in the mists of a campaign." So the government is disabled for political and First Amendment reasons for a lot of these attacks from fully responding to them.

And that, if I can just finish the point, is if you think about that, that gives our adversaries a huge asymmetric advantage, because that's one tool we really can't use against them. We really can't do a phishing attack on Putin. Maybe we've tried. Some people think that the Panama Papers, which showed a lot of cronyism with the Russian oligarchs among other things – Putin and others charged that was a CIA operation. Maybe that was the equivalent – I'm not saying it is because I don't know – but maybe that was equivalent of the DNC hack in terms of trying to steal information and embarrass a foreign leader. But the impact in Russia was much smaller than the impact in the United States because they have a completely different communications infrastructure.

KRISTOL: And I suppose, one gets a little queasy, maybe one shouldn't though, at the thought of just endless back and forth of us disrupting them and them disrupting us, and one does have a vague sense that we have more to lose from this ultimately.

GOLDSMITH: This is why we have hesitated in the face of – there are many explanations for why the United States has, at least in public and seemingly in private also, hesitated in the face of all these attacks and intrusions. But the main one is that anything very aggressive we fear we have more to lose than to gain. That's a terrible situation to be in, because if our adversaries know that, they're just going to keep up these low-to-medium-level disruptions. And we if don't do anything about it, they'll just keep it up.

That's one of many reasons why there's been this apparent shift in the government towards both *talking* about being more aggressive offensively, and hopefully about being more aggressive offensively.

KRISTOL: But if you have a lot of adversaries are you even sure who is behind some of these attacks?

GOLDSMITH: We have enormous intelligence capabilities and we've gotten much better at attribution, but not always. And it takes time sometimes to figure out exactly who did it and working for which government. It's hard.

KRISTOL: Coming back to the defensive side, because if the, sort of threat of counteroffensive isn't always so great, then we'll also need to think more about the equivalent of civil defense as opposed to retaliation. Practically, is that very, very hard, even if you have perfect cooperation?

GOLDSMITH: So I think that no one that I know thinks that we can defend all of our networks in any robust way. A lot of people think the answer is what's called "resilience," that we just have to learn to take these blows. And in some sense that's what we've been doing.

You could say – so my view, until the Russia hack, was that maybe all these intellectual property thefts, and low-level disruptions, and denial of service attack, which brings a computer down for a day or something, that maybe all of that is just a cost of doing business. And that that's just the cost we pay that we have to get used to and accept for the enormous benefits along every dimension that digital networks bring to us. And at the 40,000-foot level, that's the way I thought about the cybersecurity problem at least as a possibly: that this is just something we have to get used to, and we have to accept this and just have to learn to get good at dealing with it.

The Russia hack changed that, because that went to the core of our – it showed a vulnerability that goes to the core of our governance systems and elections. Once you see that elections are vulnerable – and it really doesn't seem like that's an acceptable cost of doing business, because we if we can't have confidence in our elections, we can't have confidence in our government and the country is in serious trouble.

So resilience, I think, and getting better at dealing with these blows and anticipating that you're going to lose information, you're going to have your emails hacked, and adjusting your behavior accordingly to raising defenses a little bit, there are steps we can take to manage the problem. But there are certain elements of it I think that aren't manageable. *Elections*. If we can't fix that problem, I think we're in a lot of trouble. And I'm not optimistic.

KRISTOL: Right. I guess thinking about it, the cost of doing business argument is a little like shoplifting. Every store –

GOLDSMITH: Yeah or the credit card example.

KRISTOL: Yeah. They just write off one percent. It's going to happen. But of course, the difference is shoplifting doesn't systemically destroy or corrupt or make problematic everything else that's left in the store. You're just losing one percent of your merchandise. And even in the credit card example, it's individual. The credit card pays off a few bad charges.

GOLDSMITH: Fair enough.

KRISTOL: So this is worse. This is why this is different, I guess, because they can penetrate – It would be as if the shoplifter doesn't take a few things from the store, but releases something into the store that destroys all the merchandise.

GOLDSMITH: But we haven't seen a lot of complete destruction. That's the interesting thing. The Sony hack, they actually burned a lot of computers and a lot of data. We haven't seen a lot of what are called "cyberattacks," where you actually degrade or destroy the information. Almost all of the damaging stuff, like the Russia hack, like China's theft of IP, is just theft and release, or not release.

And the point about doing business is, even if we take into account the enormous loss we've had of military intelligence and the enormous IP losses we've had, we've benefitted enormously, our economy and our country.

By the way, we haven't talked about that we have extraordinary offensive capabilities where we can use these tools to learn a lot about what our adversaries are doing, and we reap enormous benefits from that as well.

So I don't want to deny that we're getting enormous benefits out of this, and the cost benefit calculus, frankly, it's hard to assess because we don't fully see the benefits if we don't full see the cost taken in the aggregate.

But when it gets to our electoral system, I just think that's a different type of problem. That's something that can't be weighed in a cost-benefit calculus. There's not a compensating benefit that we're getting there that's calculable.

KRISTOL: And one can toughen and one can harden the voting systems, but that's different, you're saying, from the public discourse. You can't harden the release of emails?

GOLDSMITH: You can't really have defenses against doxxing, as that's called. Hardening the voting systems itself is extremely hard if they're connected to the internet. Even if you can do that, you can through these mechanisms introduce uncertainty.

KRISTOL: Bad information, "polls open till midnight," until they're not–

GOLDSMITH: Bad information and how can you disprove that information? You can do that or you can introduce credible reasons to think that maybe this election box wasn't secured. And when that threat combines with a culture now that, independent of this, where we don't take truth seriously, we don't know what truth is, where the nation is divided about what it sees in a way it's never been before. The potential for disruption in enormous.

KRISTOL: One thing I take away from this conversation as I guess we come near the end is it's very interesting, and something I haven't thought nearly enough about, is we're talking routinely about adversaries, and their threats and counter-offenses, and maybe we need to signal that we're willing to do more. It is striking to me that when we're discussing an area of technology that I think most people over 20, 30 years have thought of as "globalization" and "international harmony" in a certain way, not in a simple-minded way, but it is true that, in fact, it's amazing how international the internet is.

GOLDSMITH: That's true. Remember how hard it used to be to call someone in Europe in order to communicate with someone abroad?

KRISTOL: And buy things and read things, and that's sort of a large part of it. And yet, here we are having a conversation which is very much, in traditional terms of nation states and adversaries. I suppose some of the question is how much we have to go back to thinking in that way, but how hard it is to think in that way about – you know, airplane production – and this is a little true of science and nuclear weapons, I suppose, once the genie's out of the bottle, you can't keep it in one nation state then.

GOLDSMITH: Right. Nuclear capabilities, right.

KRISTOL: Pakistan can export stuff, and scientists can go across borders. Still, at the end of the day, the nuclear plant is either in American or in Iran, and the fighter bombers either are ours or the Russians', and I guess that's really what makes this so much more difficult.

GOLDSMITH: It makes it much more difficult, and you're right.

KRISTOL: Is Google in America? I'm not being facetious. It's literal. Literally.

GOLDSMITH: This is a large question that a lot of people are debating. It's an American company, but in many respects, it sees itself as a global company. And one of the problems that the Googles and the Facebooks and the Twitters have had is when Snowden revealed the close connections between the American companies and the government, that harms their business abroad, and that's why they've become resistant forces against the government on this stuff.

KRISTOL: So there's partly a cultural problem or a cultural fad about these companies.

GOLDSMITH: Partly.

KRISTOL: But it's also just a literal fact, the internet isn't *physically* here. And therefore, "we can get tough," but unless we're cutting off relations with every person who's in Russia or in Belarus –

GOLDSMITH: You can't do it. And the point you made earlier, yes, we've gotten used to these devices. They're part of our lives. And they're extensions of us in some sense and they're massively convenient and life-enhancing in so many ways. And it doesn't seem like a national security threat when you're using it, but the government, I can assure you, sees this general problem as one of the most serious, if not the most serious national security problems. And getting the country in that mindset to deal with it and figuring out what the right answers are is very, very hard to do.

KRISTOL: That seems to be the key: at least get the country focused and thinking. You think the government is internally serious about this?

GOLDSMITH: They're internally panicked, I would say is the word, yes.

KRISTOL: Wow, that's interesting.

GOLDSMITH: Oh, yeah. Speak to anyone who deals with this stuff daily and they would tell you we've got a real problem; we don't know what to do with it.

KRISTOL: When you get to the level of Congress then it more sort of a, "Let's have a hearing with Zuckerberg…"

GOLDSMITH: I would say most of them are not serious about it.

So a lot of people said ten years ago – we've known about the cybersecurity problems. The people who are really in the know about cybersecurity problems have been making, the points we've been making now have been obvious for 20 years. And there's been this big question about how do we make these invisible threats real enough so that the American people can see how important they are so that they can get behind politicians to take aggressive steps.

Until about seven or eight years ago, this was something the experts knew about, but it wasn't on the front page of the papers. In the last seven or eight or nine years, hardly a week goes by when there's not a front page story about some large cybersecurity incident, culminating in the Russia threat. And a lot of people thought *that's what we need*, kind of an equivalent of a 9/11 to make the country be serious about the nature of threat and take the difficult steps it's going to take to address it.

And, unfortunately, that has not happened. The problem is apparent on the front page of the paper. There's nothing more serious that has happened in a long time than the Russia hack in the 2016 election in terms of national security. And yet, the country is fundamentally divided about that event, and all of the alarming things that have happened have not translated into political action.

So I don't know what event it will take for us to get serious enough to deal with this, but despite all the terrible losses in the last several years, we still are not there yet.

KRISTOL: I guess it's partly "getting serious" and partly, if you take the 9/11 analogy, which is obviously an interesting one because it happened. We did a whole bunch of things, obviously, harder to get in, and do airport searches, and some of them worked better and some of them didn't work so well. A lot of intelligence stuff. I was thinking about: what is the analogy to that? What is the analogy to TSA, whatever one thinks of TSA? It's a little hard to know, we're not going to stop people from emailing back and forth in Yemen. Are we going to monitor it? That would be a question that does get into First Amendment, NSA-type issues.

GOLDSMITH: And it's hard to do. You basically can't get it without a court warrant.

KRISTOL: That is striking. The political reaction against what I thought was minimal intervention given the ratio of risk versus intrusion.

GOLDSMITH: You're talking about with the Bush program?

KRISTOL: Or just the NSA metadata stuff, which struck me as actually –

GOLDSMITH: But you saw the reaction of the country to that.

KRISTOL: Yeah, or at least some politicians to that.

GOLDSMITH: The country was divided on that, I think. But the point is that, yes. I agree with what you just said, but we've seen evidence now in the public. We have and we haven't. We've seen headlines about these things happening. We know there's losses. We kind of watched the Russia operation happen in real time. We've seen the Sony hack and attacks on banks. All these things we've seen now, we've seen is just a smidgen of what could happen, but it's real now, and yet we haven't become alarmed as a nation.

And some people think it will take the electricity going down for two months on the East Coast to get people's attention. But if and when that happens, the steps that really need to be taken are enormous.

KRISTOL: Let's maybe finish by talking about that. If, God forbid, let's assume the country wakes up hopefully without a huge incident and huge cost decides, okay, maybe someone runs for president, *I'm going to deal with the twenty-first century's threats the way our predecessors dealt with the twentieth century threats and we're going to be serious about it*. If it takes a hundred billion dollars, if it takes a rewriting of large parts of our legal code, that's what has to happen, just the way with Truman we wrote national security policy and spent tens of billions of dollars. What would that even look like?

GOLDSMITH: That's a large question. I'll tell you a few things, but let me say that there's no consensus on that. When I look down the road and imagine worse-case scenarios in terms of bad things to happen to us, and if the fear, and anxiety and concern about national security looks enough, the kind of things that we'll see much more of, much more government involvement in the network directly – where working hand-in-hand in real time, either looking at the communications as they pass through or working hand-in-hand with the private sector to actually be in real space with government computer systems assisting, and as artificial intelligence develops, to try to find threatening attack factors.

Now that is something that is unimaginable now. If we get upset about metadata analysis, we're not going to have the government looking at actual communications. So we'd have to get pretty bad before that happens, but that's an obvious step.

KRISTOL: I suppose the analogy would be, we do have a government agency that monitors air space, and if someone flies in who's not an American Airlines, United Airlines or Lufthansa, that alarm goes off somewhere and someone says, "What's that plane doing?"

GOLDSMITH: That's the analogy. The disanalogy is, the airplane isn't speech. And it's not private.

KRISTOL: And there are not a trillion of them.

GOLDSMITH: And there are not a trillion of them. Exactly. That cuts in the other direction. One thing is much more government involvement.

Second thing is, I expect, and it's hard to know which way this will go, I expect much more regulation. Just much more top-down insistence on standards and cooperation about cybersecurity threats and about knowledge and vulnerabilities and knowledge about attack vectors so the whole country is kind of sharing in a robust way private- and public-sector attack information.

Again, these are scary things, and I want to acknowledge I'm not advocating these. I'm just telling you if it gets really bad, this is where it'll go.

The third thing is, and I think we'll inevitably see, and again, not clear how far to go or what direction, we're going to see changing conceptions of the First Amendment. I think that we will – I'm not sure this is a good idea, but we will have government regulation of some sort. We already have it indirectly where the government is threatening social media companies*, you better get your house in order or we're going to do something*.

A lot of the things that the social media companies have been doing in terms of clamping down on speech – which I'm not a fan of by the way, but I understand why they're doing it – the question is, will that be able to be government-mandated in a fine-grained way? And will conceptions of the First Amendment change in that and other respects? Will we have a Fairness Doctrine return for social-media companies? And will the Supreme Court allow that?

The third dimension is: how will the First Amendment play out when these threats proliferate and the government tries to take more aggressive steps? I don't know which way it will go, but I'm confident that we're going to be thinking about that issue.

KRISTOL: I guess we could treat different countries differently, or maybe we technically, it's even harder to do – I'm just trying to think again just of analogies. We do have differential standards for Visas from Britain or from Yemen, and we think that helps us, presumably, make it so we can deter, or make it harder for some people who might come here with ill intent to get here from Yemen; we're less worried if they're coming from Britain.

So, analogously, one might have totally free flow of email and everything else, information back and forth, to some countries, and much tougher to others. Does that even work with the internet?

GOLDSMITH: It does work and let me tell you where it works. That's called the Great Wall of China and that's the problem. That's exactly what the Chinese have effectively done. They've put up this massive filter at the border. It's not perfect, but it's pretty darn good. They keep out the 98% of – and again, they're worried about malware, but they're also worried about speech. But what you just described, if we could do it for malware and other harmful propaganda, is effectively the Great Wall of China and that's what gives people pause. The *Great Firewall of China* is what it's called, and that's what gives people pause.

And it's just extremely difficult in a fine-grained way to know what to pick out and block. It's much easier if you're China and you just shut down the *New York Times*. But how do you find the encrypted piece of malware coming from a computer in Spain by a Russian agent to Podesta's email account?

KRISTOL: We don't want the government stopping us from reading Chinese press or anyone.

GOLDSMITH: Whether speech or whatever it is, we just worry about the government being involved in it. It's a scary thing. So the question is will the threat become scary enough to justify that?

KRISTOL: And then practically, can you even do it?

GOLDSMITH: How do you do it? I'm not deeply knowledgeable about artificial intelligence and how artificial intelligence will affect this issue. There are a lot of smart people, security analysts, who think that this may be the savior – that with machine learning, that machines can get powerful and smart enough to find all the bad stuff. And that seems hopeful to me and it's not obvious why AI on the offensive side wouldn't be just as powerful, if not more so.

But there are lot of people that think that they may be the silver-bullet solution, may be implemented by the private sector, that allows malware to be detected and patterns of malicious behavior to be detected in ways that humans beings can't do it. Technology might provide a solution for this, but so far technology's been creating the problem, not solving it.

KRISTOL: And we like the technology and the technology companies have a lot of clout, and I think that combination, don't you think, makes it very hard to even start the debate you need to have.

GOLDSMITH: It does, but I have to say I'm a little surprised about how the Google, and Facebook and Twitters of the world were on their heels after the Russia election [thing]. That's the first time – it's not clear what's going to become of this, but they seem a little less sure on Capitol Hill than they used to be in terms of their power. So maybe that's a sign of things to come. But, again, I'm really not sure what the right thing to do here is. The government regulating these companies on speech, it's just not obviously a good solution at all.

KRISTOL: But it may be part of what has to happen is we at least escape from a kind of utopianism, that it's all – There was the dystopianism of Orwell: these modern technologies are just going to make dictatorship easier and put freedom at risk everywhere. Then there was the opposite reaction post-'89, I would say, of modern technology is liberating and helped bring down the Soviet empire.

GOLDSMITH: Right. I think we're seeing in a lot of context that Orwell was ultimately probably right.

KRISTOL: We need to come back to taking Orwell seriously.

GOLDSMITH: Very seriously, yes. Look at the Arab Spring. Everyone thought that Twitter and Facebook were going to bring democracy to the Arab world. At first it seemed like that, but now five, six, seven years later, those countries have learned to use those technologies as tools of authoritarian control. China's way ahead of the game on that.

KRISTOL: China's combining very fast economic growth and great sophistication – more than us, in some ways, in terms of their routine use of technology in business.

GOLDSMITH: In some dimensions, payment systems they're ahead of us. Artificial intelligence, they're with us.

KRISTOL: But they are ahead of us in tracking free speech and dissidents.

GOLDSMITH: And China has done something that was an assumption of American foreign policy that couldn't happen. When Bill Clinton went to China in the 1990s and said, "Trying to control speech is like nailing Jell-O to the wall. You can't do it." And then Hilary Clinton gave a speech in 2010 saying, "You can't have economic growth with speech censorship." It just turns out not to be true. The Chinese have an extraordinarily open and robust commercial internet and, really, tons of speech as well, but they've

become very adept at controlling the types of speech that they see threatening with an extraordinary system of control that's getting more sophisticated all the time.

So they're showing that you can have commercial growth and some of the benefits of modernity that comes with a robust internet while at the same time controlling speech. That's a very ominous development.

KRISTOL: And at the same time posing threats to our –

GOLDSMITH: And then using these technologies against us. I wish I had something happy to say, but I don't.

KRISTOL: That's a good, cheerful note to end on. It's a good salutary warning, I think, and something that hopefully will, hopefully this conversation will stimulate some real, fresh thinking in the public, and on the hill and everywhere.

Jack Goldsmith, thank you so much for a great conversation. I learned a lot.

And thank you for joining us on CONVERSATIONS.

[END]