THE BROOKINGS INSTITUTION
BROOKINGS CAFETERIA: Offensive cyber operations in US national security
Friday, April 26, 2019

PARTICIPANTS:

**Host:**

FRED DEWS
Managing Editor for New Digital Products
The Brookings Institution

**Guests:**

BILL FINAN
Director
The Brookings Institution Press

AMY ZEGART
Senior Fellow
Freeman Spogli Institute for International Studies
Davies Family Senior Fellow, Hoover Institution
Professor, by courtesy, of Political Science

HERB LIN
Senior Research Scholar
Center for International Security and Cooperation
Hank J. Holland Fellow in Cyber Policy and Security
Hoover Institution

MOLLY REYNOLDS
Senior Fellow, Governance Studies
The Brookings Institution

(MUSIC)

DEWS: Welcome to the Brookings Cafeteria, the podcast about ideas and the experts who have them. I'm Fred Dews.

Offensive cyber operations are increasingly important elements of U.S. National Security Policy, from the deployment of Stuxnet to disrupt Iranian centrifuges, to the possible use of cyber methods against North Korean ballistic missile launches, to the U.S. Defense Department's new cyber strategy; the role of offensive cyber capabilities as instruments of national power continues to grow.

Today's episode features a discussion with the Editors of a new volume from the Brookings Press on this important national security issue.

Herbert Lin and Amy Zegart are scholars at the Hoover Institution and Co-Directors of the Stanford Cyber Policy Program. *Byes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, is the title of their new work.

Also in today's show, Senior Fellow Molly Reynolds examines the congressional oversight of the Trump administration: From Subpoenas to Possible Impeachment.

You can follow the Brookings Podcast Network on Twitter @PolicyPodcasts to get information about and links to all of our shows, including our new podcasts, *The Current* which replaces our 5 on 45 Podcasts, plus *Dollar and Sense*, and our *Events Podcast*.

And now, here is Brookings' Institution Press Director, Bill Finan, with Herbert Lin and Amy Zegart, who called in to the Brookings Podcast Network Studio from California.

FINAN: Thank you, Fred. And hello, Amy and Herb.

LIN: Hi.

ZEGART: Hi.

FINAN: I want to begin by asking you a question about the book's dedication which is to the men and women of U.S. Cyber Command. But before I ask you to tell me what Cyber Command is. I want to step from that and ask: what is cyberspace? Since that is the realm this book is focused on.

LIN: Cyberspace is basically computers and the information that close on them, and you could also add network -- communications networks to them, so it's computers, communications networks and the information on them.

But then you have to ask things like, is your refrigerator -- which is going to be part of the Internet -- part of cyberspace, and I think most people would say, yes, even though it doesn't sound like it. It's basically everything in the world that's electronic that depends on information or information technology to process, and to manage.

So, your smartwatch is part of cyberspace, your car is a part of cyberspace, your electric generators are a part of cyberspace, and having a computer on your desk is a part of cyberspace, and your smartphone is a part of cyberspace, and the network on which it runs is a part of cyberspace. So, cyberspace is increasingly everywhere.

FINAN: And what is Cyber Command?

ZEGART: Well, U.S. Cyber Command is a part of the Department of Defense, depending on when you ask that question, you might get a little bit of a different bureaucratic answer, but it's formerly a component of U.S. Strategic Command which was in charge of all of our nuclear deterrence and assurance capabilities, space capabilities and cyber was folded into that.

Now of course Cyber Command has been elevated to its own command, so if you think about it, it's the part of the Pentagon that is really tasked with supporting all the regional Combatant Commanders with their cyber needs.

FINAN: And it seems -- I'm sorry, go ahead.

LIN: And I should also point out that Cyber Command and the National Security Agency are now together, now whether they should stay together in the future is a big policy question, but they are officially part of one organization at this point.

FINAN: So, the National Security Agency and Cyber Command are one entity?

LIN: That's correct.

ZEGART: That's right, and the leader is the same person dual-headed in both organizations.

FINAN: For a group that's been around for a decade, as it is this year, not much has been heard about it, and I'm glad to see this book out which offers a full chapter on, to actually explaining its history.

I also notice there's a table in the book that shows that Cyber Command's budget went from 120 million in 2010, to over 500 million in 2015. Why the huge increase in budget?

ZEGART: Well, if you think about the change in cyber threat landscape, that's changed and increased orders of magnitude more even than the budget I would argue. So, if you look at the Director of National Intelligence Threat Assessments, in 2010 cyber did not even rank in the top three threats in that annual threat assessment.

But 2012 it was ranked in the top three and it stayed there ever since. So, what you're seeing, the budget is reflecting the dramatic rise, and the importance and the magnitude of cyber threat.

FINAN: Your book is the first volume to look at the use of cyber weapons offensively. Can you give us some examples of what are offensive cyber weapons?

LIN: An example of a cyber weapon is the webpage that a bad guy hacks so that when you click on a link it automatically downloads malware into your machine that gives the bad guy remote access to your machine so that he can do anything on your computer that you can't, even though he's sitting 3,000 miles away. That's an example.

FINAN: Okay.

ZEGART: Perhaps the best known example in the press reported, would be the Stuxnet. So, reported to be a joint U.S.-Israeli enterprise to delay and degrade the nuclear capabilities in Iran.

FINAN: A problem for many people is that this metaphor of weapon is hard when Herb talks about a webpage, it's hard to think of that as a weapon, but I don't know if there's a new terminology that will now to enter into the discourse or not, as we go along.

LIN: People often talk about malware, that software that does bad things, that's only one kind of a cyber weapon, the enterprise that Amy just talked about, Stuxnet, wasn't a weapon, per se, it used a variety of different cyber weapons to accomplish a goal.

So in the terminology of the book, it was an operation, an offensive cyber operation aimed at the Iranian centrifuges that were enriching uranium, so we conducted an offensive cyber operation using a variety of cyber weapons to cripple the centrifuges.

ZEGART: But I think, Bill, you hit on a very important point, which is that the nomenclature is confusing, and it's not particularly helpful. So, if you talk to computer scientists they hate the term "cyber", right.

And we think about, and Herb has heard me say this many times, we've been in the cyber world for a while together. Imagine that I told you that we're really concerned about a new category of capabilities called vehicle-borne threats. And vehicle-borne threats are a series of threats that encompass everything from terrorist attacks using truck bombs to carjackers. Well, you would probably say that makes no sense, because it's a sort of cats and dogs assortment of various threats.

But that's exactly what we've done with cyber. So, when we talk about cyber threats, policymakers, pundits and academics alike, are referring at various times to everything from criminal types of activities, like stealing your credit card, to massive, organized, state-sponsored campaigns. Like Russia's election interference influence operation.

And so that makes it very difficult to have conversations and formulate policies in a systematic way because the terms are so broad.

FINAN: What I was going to ask, too, and you just brought in Russia. Give us a few other examples of cyber -- offensive cyber attacks, as you mentioned in the book, come from not only Russia,

but China and North Korea. I think that makes it a little bit more concrete.

LIN: The North Koreans brought Sony Pictures to its knees in a cyber attack on the Sony Corporation in 2014. They thrashed a variety of computers, before that they stole a bunch of confidential, I mean, sensitive information. They published a lot of it, all because Sony Pictures had the temerity to issue a movie -- a not very good movie -- about Kim Jong-un.

And this was regarded as an insult, and they demanded that they not release the movie, and Sony said, no. And so North Korea decided that it was going to exact a price from Sony; so, that's another example.

Still, another example is the Iranian attack on Saudi Aramco, which is the biggest oil company in the world, they thrashed about 30,000 Saudi Aramco computers, and crippled its business operations for quite a while, till they recovered. So that's another example of an attack.

The Russians are widely believed, in the United States, to have conducted a cyber attack against various components of the Ukraine electric grid, to shut down their power for X-number of hours, and so on, in what many people believed was a precursor to potential Russian attacks on other power grids, including those of the United States. So, those are some examples.

ZEGART: I would add one other category of examples, which is offensive cyber operations that really have as their primary purpose, espionage. So, the attack on the Office of Personnel Management, which is largely believed to have been perpetrated by the Chinese Government to steal the classification records of more than 22 million Americans, would be a classic of that.

If we take a step back, I think about cyber attacks really designed to target three things. One is information, so espionage, compromising the integrity, availability, confidentiality of information. Two, is beliefs, so we see with the Russian election interference and attack to hack our minds.

And the third is physical effects, or things that go boom. Right? So it could be things that go boom, or it could be just SCADA systems, industrial control systems that operate dams, it could be turning computers at Saudi Aramco into bricks. Attacks that have physical effects which easier, I think, to understand when there are kinetic or physical impacts of a cyber attack.

LIN: Of those three, the book only addresses the first and the last. There's nothing in the book on hacking our minds, although that is a very important part of the problem.

FINAN: That's for another volume, another realm.

ZEGART: That's the next book, Herb.

LIN: (Crosstalk).

FINAN: It seems to me from reading the introduction, also the other chapters, that the focus for

the United States has been predominantly on cyber defense, and this was a new realm to talk about cyber offense, and focus on it. Is that correct? And if it is, also, what are examples of cyber defense?

LIN: Well, okay, so it's new in the sense that there's a lot more written about cyber defense and cyber offense for a number of years, even the idea that the United States Government might be interested in offensive operations against other nations in cyberspace was classified.

Not the technology, not the methodology of it, not the doctrine behind it, just the idea that United States wanted to do it was classified. Michael Hayden is quite articulate about this point, and he's a Former Director of NSA. He says that his staff prevented him from using the term offensive cyber operations, just the term, on more than one occasion.

Cyber defense is basically what you do to protect your system against the bad guys. So, whatever we're doing to try to prevent our systems from being hacked by the bad guys more or less counts to cyber defense, and that has been essentially unclassified for many, many years. And so there's a lot more about that topic than there is on the offensive side.

FINAN: The book's main focus is on articulating, devising a strategy for offensive cyber operations, and I thought it would be helpful if you could explain the difference between tactical and strategic for listeners first.

ZEGART: So, when we think about strategic versus tactical cyber operations, strategic really has two components to it. One is more of a long-term view, not what's going to happen tomorrow, but what could happen over the horizon.

The second component to strategic is magnitude, what is going to have a major impact on the target on a geopolitical situation. Tactical, by contrast, is really about the nuts and bolts of, what are we going today. So in the typical military example would be a tactical decision, it would be: how do we take out that bridge over that hill, tomorrow morning?

Whereas a strategic question would be: what do we think about the capabilities of this particular actor, and how they may change over the next 6 to 12 months?

FINAN: What struck me is the use of -- I don't think it was necessarily intended use of nuclear weapon strategy, but that seems to hover over all of this. How to think about cyber offensive strategy in terms of nuclear weapons strategy, because you use terms like deterrence, credibility, proportionality, and some of the more interesting conversations in the book, and the chapters were exactly questions of, how do you deter. So, how do you deter a cyber weapon attack?

LIN: Well let me first address your comment about nuclear strategy, and so on.

FINAN: Mm-hmm.

LIN: Yes. We do talk about deterrence, but of course deterrence is a concept that goes, way, way back, it's much older than nuclear weapons are. So, it's an intellectual question as to how you might deter an adversary using nuclear weapons or cyber weapons against you.

So what we really find in all of this, is that many of the same questions arise with nuclear and with cyber. The same questions, but the answers are completely different. So, yes, we are inspired, many authors are inspired by thinking about nuclear deterrence, but that doesn't mean that the answers, the conclusions they came to about nuclear applied to cyber.

So, just to give you one example, there is no experience at all with a nuclear war other than World War II, the last two bombs on Nagasaki and Hiroshima. Fortunately, there's no experience of fighting a nuclear war. There's also no experience fighting a cyber war on any kind of a large scale.

No one knows what an all out cyber war between major adversaries like Russia and the United States, or something, we don't know how that would go. So, there's a lack of empirical knowledge about any of that -- and that's a good thing, we are not calling for cyber war, right, to get the knowledge, but that's an important similarity.

Your question is about how you deter, that is a big question and nobody knows how to deter it very well. There is a chapter in the book that talks about the U.S. approach to dealing with adversary cyber attacks now, because it analyzed what the United States has recently, in the last year or so, adopted a new strategy for engaging with adversaries in cyber space, and it is overtly and explicitly more forward-leaning and more in your face than the previous strategy, which was one that was explicitly described as a policy of restraint.

Now, what's really clear is that this policy of restraint in the past hasn't worked because people have been still coming after us in cyberspace a lot, and in fact the consequences have grown.

So, the United States has decided to try something else, which is, the restraint doesn't work, well, let's try less restraint. That strategy calls for what they call persistent engagement, forward defending and defending forward, and increasing resilience, and the increasing resilience part is something that we've been doing for a while, but the defending forward and persistent engagement are real important changes.

But defend forward means engage the adversary as far away from U.S. networks as possible, that means as close to the adversary as possible. That means either in their networks or in intermediate networks which may belong to what we call gray space, and stuff that may belong to other third parties.

And then there is a question of persistent engagement, which means constantly mixing up with them all the time which, in their words, will force them to shift more resources from offense to defense,

and therefore bother us less.

Whether this process is going to actually have the desired effect of persuading them to not engage with us, well, we'll see. At least one chapter in the book raises that question in a big way.

ZEGART: Let me just add, I think this question of: what's deterrence good for anyway, is a critical question, and if we could just take a step back and it's worth thinking about: what's the difference between just plain old defense, and deterrence, whether it's cyberspace or physical space?

And with defense the idea is that, if you have strong defenses, you're going to defeat the adversary in battle. But with deterrence the point is that that you're going to convince the adversary not to fight in the first place. They're close cousins, but they're not the same, and that's a really important distinction. I do think, I mean, Herb and I may disagree on this, but I think we've become a little too deterrence crazy.

I think deterrence in the public discourse has become shorthand for, how do we get the bad guys not do what we hope they won't do without using too many resources to do that? And this is particularly true in cyberspace, the tendency tends to be, deterrence is the answer, now what's the question.

So, the implicit assumption is that we can deter anybody. We hope we can deter everybody from doing everything, and that clearly isn't true, it hasn't worked as Herb has pointed out in the past. Cyber Command's new vision suggests that the past strategy hasn't worked particularly well.

And so it's worse actually parsing a little bit more carefully, what types of cyber activities we think are most deterrable, and what types of cyber activities are not?

Now, I don't think anyone has a very clear answer to that, it's a really hard question, but even if we look at the latest Nuclear Posture Review, it makes appoint of saying that the United States Government reserves the right to use nuclear forces, or nuclear retaliation, even in the case of a nonnuclear strategic attack.

Fill in the blank here. What's in between the lines, it's including a cyber attack on the United States. Do we really think the United States Government would launch a nuclear retaliatory strike after a cyber attack of however consequential damage might be on the United States? Lots of debate about that, is that really a robust deterrent strategy? Probably not.

FINAN: I'm glad you brought that up because one of the more fascinating parts of book, for me at least, was the chapter to discuss the use of kinetic force to retaliate as a deterrent aspect. The idea that if someone uses cyber weapons to take out a dam in the United States, we might reply with a missile, hopefully, not a tactical nuclear weapon, to take out a dam in that country. It seems like that's a

step much farther real that most of us have ever thought of.

LIN: Well, stated U.S. policy has always been that we reserve the right to respond to the provocation in a manner and place at a time determined by us. So, we are never committed to doing cyber against cyber, responding in cyberspace to a cyber attack.

Now, as a practical matter, if you would look around, with one exception, which I'll get to in a minute, we have never responded outside of cyberspace to a cyber attack. The one exception to that is that we have issued law enforcement indictments of people, and we've arrested people, or we try to arrest people, we put them on most-wanted lists, and stuff like that.

So, we certainly have done that. We haven't successfully arrested anybody from any of the major states that have come after us as a result of their state-sponsored activity. I think that's true. I'm not entirely sure. But I think that's true.

ZEGART: I would add, I think we've imposed sanctions.

LIN: Well then (inaudible) -- explicitly for cyber, for cyberattacks?

ZEGART: Sanctions against Russia, you could argue, there's certainly a component.

LIN: Or for the election, if you want -- okay. Yeah. Fine, I'm willing to along with that, if you use the information operation as an example of offensive side, but sure. Yeah. Sanctions and arrests, closing down embassies, that kind of thing, so we have done stuff, but we certainly haven't retaliated in any forceful kind of way.

And as you probably know there is lots of pressure to do so. As I think Lindsey Graham said, we have been throwing pebbles at them in return, and we ought to be throwing bigger rocks at them. That's the theory anyway.

FINAN: You devote a section of the book to the private sector's role in cyberspace, you know, that the private sector plays an unusually important role in this area. Why is the private sector an important player in this realm? And what are the ways that it plays a role?

ZEGART: Well, I think the private sector is an important player for several reasons. First, the private sector is the pretty big segment of the American economy, so we should be a little more care careful about. I think there are different parts of the private sector that play different roles.

FINAN: Okay.

ZEGART: So, the first way in which the private sector plays an outsized role in cyber is that 85 percent of our critical infrastructure in the United States is owned and operated by private sector entities. The government can't go it alone in cyberspace in a way that it could in other domains. So, that's fundamentally different.

I think the second way that the private sector plays an important role, and the chapters in the book get into this, is that there's a lot of cyber activity done by contractors in cyberspace, and so as an offensive cyber operations actor and supporter, you have a number of different private sector companies.

So, if we think about what's in the public domain, third party actors like FireEye, or before them Mandiant, you have third-party actors actually publicizing cyber attacks and attributing responsibility for cyber attacks, not governmental actors, third-party private sector actors. So, that's sort of the second way.

And then the third way the private sector plays an outsized role in cyberspace is they really are, in some ways, the front line. So you think about companies like Facebook, Google, Twitter, social media firms, they're not just platforms, though I'm sure their executives and their Boards of Directors would like to hide behind the fact of their platforms. They are battlegrounds, and the battlegrounds on which much of nefarious cyber activity is now taking place.

And so the rules by which they determine what content is allowed or not allowed, what they choose to go after, or not go after, how they choose to take down terrorist content or the rest, they're acting in many ways as governments would act, but they don't have the same kind of national responsibilities.

LIN: Let me build on two things that Amy said. The first point was that the private sector owns lots of cyberspace, and the third was what she just said. Both of those facts underscore the idea that the United States has to mount the Whole-of-Society response, not the Whole-of- Government response.

The point is that government is only one part of society. And this is probably the first time, where you talk about major defense issues outside of a world war, like World War II, where all of society really has to be mobilized to deal with the threat.

And of course most people, for understandable reasons, do not think of themselves as being at war with anybody else. So, getting this whole-of-society response to what people like Amy and me think as a serious threat is pretty hard.

FINAN: Which countries pose the greatest threat to the United States in the coming years?

ZEGART: Well, there are sort of four big ones in the cyber landscape that pose significant threats to the United States, and they're not going to be surprising to anybody who is listening. It's Russia, China, Iran and North Korea.

Now what's interesting about those four, is that they're also four states that pose serious and

rising challenges with respect to nuclear proliferation, right, Russia, China, Iran, North Korea.

They are four states that at various times have been very aggressive at territorial aggression, so Russian, Ukraine, China and the South China Sea, Iran, and fomenting terrorists activity across the Middle East, and of course North Korea.

And they are four countries also that, in various ways, are really challenging the international order. So, you have this convergence of four major destabilizing trends, cyber, nuclear, territorial aggression, and erosion of the international order all in the same four states.

LIN: I would add a fifth one, which is not quite at the same level, because they're not nation states, but the fact that you have a variety of hacking services for hire, none -- at least officially -- organizations that basically provide cyber attack services of various kinds for hire.

So, now you can be the smallest nation in the world, if you want to conduct a cyber attack against somebody, you give them some money and they'll conduct the cyber attack for you upon payment of the appropriate amount.

It used to be that, if you were a nation state you had to have the indigenous capability to do something bad in cybersecurity. Now you can just go out and buy it.

ZEGART: I think that's a really important point. One of the big changes, what's new about this era compared to earlier eras with threats to the United States in particular, is the diffusion of technology, that you don't have to have the material resources of a major power in order to inflict outsized damage, whether it's destruction or disruption.

And so, particularly, the spread of the technology, like artificial intelligence, and other technologies is leveling the bad buy playing field to the disadvantage of the United States.

FINAN: So it has this immense multiplier effect that (crosstalk) does have to worry about --

LIN: That's right.

ZEGART: Yeah.

FINAN: -- that the usual resources that that nation had to have in the past, land and military manpower, et cetera.

LIN: Right now, all you need is a stolen credit card to do it.

FINAN: (Laughter) Are we prepared? Is the United States prepared?

LIN: No.

ZEGART: (Laughter) How much do you want to depress people, who are (crosstalk)?

LIN: I mean, look, over the past 30 years since I've been working in this business, we have gotten better in cybersecurity, there's just no question about that. So, our defense is against the

cybersecurity threat of 2010 are pretty good. But of course it's now 2019, and the bad guy has gotten better also, and perhaps has gotten better than faster than we've gotten better at having good defenses.

So, that gap is increasing and, you know, we are getting more and more into the situation. We want information technology everywhere, and Amy often talks about being the most connected, and therefore the most powerful, we are also the most vulnerable because of that connection.

Right now my home does not have an Internet-enabled refrigerator. In five years I won't be able to buy a refrigerator that doesn't have Internet capability. You know, you can now buy a pair of Nikes with Bluetooth connectivity that will do self-tightening.

Why do I want my shoes on the Internet? I mean, the sort of stuff is just happening over and over and over and over again, and it gives us better functionality. Well, maybe, maybe not. But, you know, at some point you may have to ask yourself, are you getting enough out of that to be worth getting the vulnerability that you'll get on it. And I think we don't have any good answer to that.

ZEGART: And again, I think if we think about the physical domain, which most of us are more comfortable understanding, if you think about what's happening with the Nike shoes or Herb's refrigerator that he's going to have to buy, is that the attack surface for cyber bad guys is growing exponentially.

Are we prepared? Well, prepared is a relative concept. Are we prepared compared to the threats that we're facing? So Herb says we're better than we were in 2010, but the velocity of the change in cyber landscape is eclipsing our ability to keep up.

FINAN: And with that, I'm going to thank you both, Amy and Herb -- (laughter) -- for this tour of cyberspace, and our attempts to put a positive face on it, however negative it might be.

ZEGART: Thanks so much for having us on.

LIN: Thanks.

DEWS: You can find the new book, *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, edited by Herbert Lin and Amy Zegart, on the Brookings website, or wherever you like to find books.

And now, here's Senior Fellow, Molly Reynolds, with a look at, *What's Happening in Congress*.

REYNOLDS: I'm Molly Reynolds, a Senior Fellow in Governance Studies at The Brookings Institution.

Members of Congress are finishing up their annual spring recess. But much of their attention of late, like the public's, has been on the report written by Special Counsel, Robert Mueller, summarizing

the results of his investigation into Russian interference in the 2016 Election, and possible obstruction of justice by President Trump.

Now much of the report, redactions excepted, is public, Congress must decide how to proceed. The modern Congress must live with the choice the Framers made to make impeachment a process to be undertaken at the discretion of political actors.

The Constitution does not create any sort automatic process for charging impeachment, nor does it describe exactly what constitutes a high crime or misdemeanor. Well, the historical record suggests that conduct need not be criminal to be impeachable, the actual determination of whether certain set of actions is grounds for impeachment is left to elected representatives. And because decision about impeachment are made by elected representatives, the process by which those determinations are made is inherently and unavoidably a political process.

An impeachment is not only political because it involves decisions made by elected representatives with the preferences and goals they're trying to see realized, it is also political because it involves the series of collective choices made by Members of Congress.

An individual member can force at least a procedural vote on a simple resolution providing for impeachment of an Executive Branch Office using what's called a question of privilege. Indeed we saw Democratic Members forced the House to take such votes twice during the first two years of the Trump administration.

Beyond that, however, the Clinton impeachment involved two separate votes by the Full House, one sending the report from Independent Counsel, Ken Starr, to the Judiciary Committee, and one authorizing the Committee to undertake an impeachment inquiry before the Committee began its actual impeachment proceedings.

The Full House Chamber subsequently voted on four separate articles on impeachment, followed by deliberation and vote on conviction in the Senate. Because impeachment involves these collective decisions, it also, unavoidably, involves the same kind of coalition building and management challenges that are plain, ordinary congressional decision-making.

As Speaker Pelosi, and other House Democratic leaders plot a course forward they will have to navigate pressures from various factions within the Caucus with some members pushing for more aggressive action, and other cautioning restraint.

Given the realities of the current political landscape, and the general reluctance we have seen on the part of congressional Republicans to take a strong, public stance against President Trump, it seems relatively unlikely that many, if any, Republicans will align themselves with pro-investigation or

impeachment forces.

Thus, this particular process is likely to be partisan, but just because it is a political process does not mean that this is a given.

As Democrats move forward, it is increasingly clear that they will face a hostile White House, largely uninterested in cooperating with a request for information in testimony. Not just on the result of the Mueller investigation, but more broadly.

This week alone, the White House has indicated that it will fight subpoenas to Former White House Counsel, Don McGahn, issued in connection to the Mueller probe, and to a former official in the White House Office of presidential personnel, who allegedly overruled the recommendations of career officials regarding security finances.

In addition, the President's personal attorneys are fighting a so-called friendly subpoena issued to an accounting firm by the House Oversight and Government Reform Committee to follow up at issues raised by Trump's former Attorney, Michael Cohen, in testimony before the panel.

Subpoenas are an important tool in Congress' Oversight toolbox, but they aren't a speedy one. If the target of the subpoena refuses to comply the litigation necessary of forced compliance can be very slow moving.

Indeed, historically, the influence of Congress' subpoena power has resulted from the Legislator's ability to threaten subpoenas in order to compel negotiations between a reluctant witness and the Committee.

The Trump administration, however, may be seeking to drag out the oversight process as long as possible, with the hopes of potentially riding out the clock until the 2020 Elections.

In addition, the White House may see political value in simply putting up a fight.

House Democrats then are likely to find themselves in an informational confrontation against the White House on a number of fronts, even if they don't ultimately choose to pursue formal impeachment proceedings.

And conflict with the other end of Pennsylvania Avenue, will be much of what's happening in Congress.

DEWS: The Brookings Cafeteria Podcast is the product of an amazing team of colleagues, starting with Audio Engineer, Gastón Reboredo, and Producer Chris McKenna. Bill Finan, Director of The Brookings Institution Press, does many of our book interviews. And Lisette Baylor and Eric Abalahin provide design and web support; and finally, my thanks to Camilo Ramirez and Emily Horne for their guidance and support.

The Brookings Cafeteria is brought to you by the Brookings Podcast Network, which also produces Dollar and Sense, the Current and our Events Podcasts.

Email your questions and comments to me at BCP@Brookings.edu. If you have a question for a scholar, include an audio file and I'll play it and the answer on the air. Follow us on Twitter @PolicyPodcasts. You can listen to The Brookings Cafeteria in all the usual places.

Visit us online at Brookings.edu. Until next time, I'm Fred Dews.