

THE ASPEN INSTITUTE

ASPEN SECURITY FORUM 2017

NO ROOM FOR ERROR: ADVISING THE PRESIDENT ON HOMELAND
SECURITY AND COUNTERTERRORISM

Thursday, July 20, 2017

LIST OF PARTICIPANTS

THOMAS BOSSERT

Assistant to the President for Homeland Security and
Counterterrorism

DAVID SANGER

Chief Washington Correspondent, *The New York Times*

* * * * *

NO ROOM FOR ERROR: ADVISING THE PRESIDENT ON HOMELAND
SECURITY AND COUNTERTERRORISM

(9:00 a.m.)

MR. BOSSERT: (In progress) in a way that we haven't fundamentally nipped at the root.

Now, how do we do that? We're going to try some different tactics. That doesn't mean we're going to be right. We're going to try some new things. That doesn't mean that they're better. We'll find out with time. So I don't want to gloat until we have an objective analysis. But one of them is pretty clearly that this President would like to delegate a lot more of the responsibility to people a lot closer to the decision-making.

Now that comes with a lot of political risk, but it also comes with a satisfying response and a faster reward, if you will. So what we're going to try to do, what you'll see evidence of obviously with the fall of Mosul and other things in the offing on our Defeat ISIS campaign is a decentralized approach. That's not necessarily a better one, but it's going to work I think in this case, and it's shown some early progress. So that's our initial difference.

Some of the additional changes will have to be our ability to foreshadow the ISIS 2.0, something that some people were critical of the last administration not seeing; I'm not. I think that there was a predictable vacuum that we created, but it wasn't necessarily predictable that we'd have a team with black flags that would fill that vacuum in this capacity. So what we need to do now is decentralize the Defeat ISIS effort, but think more carefully about centralizing a strategic approach to the other 18 countries where we've got failures.

MR. SANGER: So Tom let's bore down for just a moment on that. One of the things that we have heard about the early decisions that were being made as you try

to push this decision-making down is that some of the standards that were used by the Obama administration may have changed. For example, the Obama administration had frequently talked about not launching a city attack, whether it was by unmanned aerial vehicle or Special Forces or whatever, unless there was a near certainty that there would be no civilian casualties. And we're hearing reports, although I have to confess I have not seen concrete numbers that back this up, that the civilian casualty numbers are actually increasing quite dramatically. So tell us what you're seeing and tell us has the standard changed? And if so, what is the new standard?

MR. BOSSERT: Okay. So first answer is little trite and that is we won't talk about our classified efforts and classified programs, and that puts me in a little bit of a disadvantage. But instead of talking about the programs -- and some of them have been written about too much in our papers and I long for the day that our intelligence programs are not in the newspapers anymore, David.

MR. SANGER: Tom, this may be one area where you and I just ought to talk about fishing, yeah, right.

(Laughter)

MR. BOSSERT: That said, appreciating what you do, I do think that there's a few underpinning goals that you've asked that I can address, right. There are standards of near certainty that people discuss but the idea here is for you to remember that we want to make sure we minimize casualties to the civilian population around any bad guy.

So we've had a lot of armed conflict standard for a very long time that speaks to proportionality and other things that are key to our value set, but the Obama administration codified that, which I think belonged and existed in our decision-making process for a very long

time beforehand. And part of that has to do with maintaining the consent of the governed.

So we don't want to conduct military operations in countries without the consent of the governed who still have some -- great deal of say in that country, and that's the newness of our terrorists challenge. We have countries who have otherwise reasonable governance structures and governed peaceable people who are plagued by a terrorist problem that they can't handle without our -- without our assistance and our use of force.

So if we start bombing criminal elements in some U.S. city and we accidentally hit a peaceable otherwise suburban neighborhood, we're going to run into problems with the peaceable voters there in the mayoral system. So by analogy we have to maintain that same degree of standard overseas. So maintaining that kind of support from the governed also comes with a responsibility to maintain the support of our partners. We've only done this by, with, and through others, something else that we've maintained. We changed a little bit of the knobs on by and with and through from the last team, but we're still doing it with partners, and we're not doing it with large troop deployments.

And so what we'll do here is maintain the ability to get that partner buy-in if we begin to use standards that are approaching that law of armed conflict standard, and we lose our partners as a result that would be a negative outcome.

So our standards are based on those bedrock principles, based on our values, and those classified programs that we write. We are examining them, we are rewriting them, we're primarily rewriting them to address who makes the decision, not what the standard is.

MR. SANGER: Okay, so I get that part, but I just want to circle back on the core question, which is this phrase of near certainty, is that gone from the

standards that are now being applied to this at this lower level?

MR. BOSSERT: So those are terms that are in programs that we don't discuss, but as we examine those programs and who makes those decisions, those are terms that are always right for a review.

MR. SANGER: Okay.

MR. BOSSERT: But you ask the trend analysis question. I don't know the trend analysis on increased casualties, but that's something that we have to keep an eye on because if we end up losing the support not only of the governed but of the good guys, then we become the -- we become the bad guys in this. And we lose our moral high ground. So the idea is to be a little bit more full throated and maybe I'll elaborate there.

Okay we haven't just decentralized the authority; we are moving in a direction where we are going after terrorist networks, not individuals by long and lengthy analysis. But we are beginning to go after groups by virtue of their inclusion. And if you have decided to join Al-Qaeda or some other group that we don't find acceptable, then you have decided to join the enemy and you are a legitimate target. That is a difference.

MR. SANGER: So does that mean that you're back to something we saw during the Bush administration where for a while we saw attacks that would take place on suspicious convoys that look like they were serving a group, for example, without knowledge of who the individuals were?

MR. BOSSERT: Well, I hope we have a little bit more than just the suspicion, but yeah I think the idea of attacking networks, by the way, is not only something that we use in terrorist -- counterterrorism efforts, but it's something we use in counterdrug, counternarcotic efforts, counter-human trafficking efforts. These are network-

based approaches that have worked in South America and they're going to work in the Middle East.

MR. SANGER: Let me take you briefly to detention policy. So President Obama famously said he was going to close Gitmo. He got through eight years and had no place to go move it to. He did reduce the population a lot. And tell us now, as you've had a chance to go review this, what's going to look different in the detention policy from the Obama years.

MR. BOSSERT: Well, I don't have a new detention policy to announce, but I'll tell you in my own personal advice to the President, I think at this point we're in a position where I think we've got a very small universe, 41 or so, detainees in that facility. We were at the height of 600 or 700, as this group knows, at some point. So both Presidents, Bush and Obama, diminished that population quite a bit. But here we are today, and I'm a little bit worked up about this. Here we are today with three viable options for taking an enemy combatant off the field: we can kill him, we can catch him and release him after a few weeks maximum, or we can outsource our responsibility and send them to a third party.

And if you're worried about humane treatment of enemy combatants, then you should be worried about outsourcing their treatment and care to third parties that we can't completely govern control. And as a result of our deficient policy and our inability. And maybe I'll even lean forward a little bit more. There's a concern within the military justice system on the Military Commission approach that there not be any undue command influence. Well, I'm not in their command structure and I certainly wouldn't want to impose any undue command influence, but it's been a little bit too long for KSM to sit there in pretrial hearings.

I can't understand why he's got a 25-person legal defense team 15 years later without even a hearing. It just doesn't strike me as sensible. So for me that seems like do command influence not undo. I would hope

that we can figure a way to get that Commission process to work. I would love it if we could undo the wrongheaded Supreme Court decision the Boumediene case that extended habeas rights to enemy combatants taken off of foreign land, but I don't think we will. And so we either had to come up with an Article 3 approach that works, or with a military commission process that works more quickly and fairly, or we're going to be stuck outsourcing this responsibility and having people sit down there for the rest of their lives without any resolution.

So for now it's open for those that have been already detained. If we can come up with a better process, it can be not so much open for business but we can reopen any facility that we want to house enemy combatants that are legitimately taken out of conflict.

MR. SANGER: Which takes me to my next question. Early in the administration, probably week two or three, you may recall there were a flurry of draft executive orders that magically made it into the New York Times, Washington Post and other places. One of them referred to reopening black sites, and then when a further iteration of that showed up that phraseology, that whole concept was gone. What is your -- do you believe at this point that with Gitmo and sites that are under the control of the United States, you can handle whatever you have coming?

MR. BOSSERT: No. I would prefer us to have an ability to house enemy combatants in a way that we control without having to outsource that responsibility. I mean I'm completely clear in my view, but that requires a whole lot of staff work and a whole lot of incumbent responsibility on my part and the cabinet's part to give the President that absolute --

MR. SANGER: But the idea of encouraging allies and partners to reopening detention sites is not part of your plan?

MR. BOSSERT: Yeah, that's right. I mean, look, we'll have to keep options open, right, until we come up

with that perfect solution, or at least an acceptable one. But I want to make sure I fight back on this black site conversation and there's a lot of nomenclature, there's a lot of baggage associated with this. There wasn't any water boarding ever at Gitmo.

I go to these events and the Attorney General, and I actually ask this question both, how many people think there was waterboarding and how many people were waterboarded at Gitmo, and people usually say, "I don't know, five or six or 100." None, so that treatment has been associated through movies and the cultural zeitgeist with that facility. But that facility is not one in which we ever engaged in those enhanced interrogation techniques. So the facility, the techniques, the detention practices, they're all separate, and I think it's within our best interest to separate those and black sites are just encumbered with that.

MR. SANGER: One last one on terror-related issues. This administration has made Iran a priority in declaring that it's engaged in terror-related activity. On Monday, the -- I'm sorry on Tuesday, just before coming out here, the Iranian Foreign Minister, Javad Zarif, who had negotiated the JCPOA, the nuclear deal, saw a number of us in New York and made two arguments: the first is that he believes at this point the administration's determined effort to try to convince American allies and partners, including President Trump's comments at the G-20, were in violation of the JCPOA, which says that Iran must be able to enjoy the full benefits of reintegration in the Western economies and that the United States and its partners will do nothing to try to impair that. And he basically charged that you're trying to reimpose nuclear sanctions by renaming them as terrorism related or something else.

The second argument he made was that given American activities in Syria and elsewhere, we were in a bad position to be lecturing the Iranians about how they should operate in their own neighborhood. So I just

wanted to see if you wanted to talk about that for a little while.

MR. BOSSERT: So let's see, there's two questions there.

MR. SANGER: Yeah.

MR. BOSSERT: The first is the Iranians accuse us of bad activity.

MR. SANGER: The Iranian accuse you of violating the terms of the JCPOA.

MR. BOSSERT: Okay. So let me let me answer it this way. The JCPOA has consumed a lot of oxygen in this debate for good reason. Our President has been very clear that he believes it's a bad deal. I believe they have every reason to comply with the letter of a bad deal. It's a bad deal. So, of course, it's in favor of them. It's in their interest to comply with something that doesn't impose pain on them in a way that we would have preferred to impose pain on them had we been in office. So for them to then come back and accuse us of bad action and bad activity is a kind of a probably a name-calling exercise, David, and I'll address it in a little bit of a different way.

MR. SANGER: You may view it as a bad deal and whether it was good or bad or as the President said to me in an interview last year when he was a candidate, he could have negotiated a much better one. The problem you're not dealing with Iran right now is a race toward nuclear weapons and if all of the complications you have, you don't have the additional complication right now --

MR. BOSSERT: Well, I hope you're right. You seem self-confident, but I'm not.

MR. SANGER: Do you have any evidence that they are in fact pursuing nuclear weapons at this point?

MR. BOSSERT: I have every hope that they're not and no reason to believe that the deal did or did not change their aspirations. And so what I'd like to do is point out that they are not only bad actors, but they are bad actors outside the four corners of this arrangement. So we're talking about the arrangement and their compliance with the spirit of it, whether they did or didn't pay their rent on time and whether they mitigated that later by paying it late, right, whether they had heavy water or didn't.

Now what I'm trying to indicate here is the Iranian pattern of behavior is more troubling than just the four corners of this document. They've continued to take hostages and they need to release or return Bob Levinson. Now they've continued to take hostages as a tool and tactic. They've continued to mistreat people in their region with regional aggression, right.

They've continued to be a state sponsor of terrorism. They're unsettling conditions in Yemen and the Saudi Arabian southern border region. This is behavior that's outside the four corners. It's within my scope and my lane of responsibilities. They're state sponsor of terrorism. There are things that concern me, and so I'd like us to pursue Iranian sanctions and start building a bigger case and a broader case for our concerns with Iranian behavior and get -- I don't want to get away from it. It's fair reporting, but expand a little bit the conversation.

MR. SANGER: And what kind of sanctions do you have in mind?

MR. BOSSERT: Well, right now we're making a case for additional financial sanctions, but I think that those sanctions can be pretty much as broad and consistent with their bad behavior as we can do within our legal system, and once again go after their ability to export oil. In the end what we learned during the run-up to the accord was that the only thing that really gets their attention right is their oil capability.

MR. SANGER: Do you envision the Trump administration seeking sanctions that would restrict their ability to export oil?

MR. BOSSERT: Yeah. I don't want to issue the threat. I'll let the President decide that for himself.

MR. SANGER: Okay. Syria, well, we touched on very briefly in the course of the Iran conversation. So the Washington Post, The Times, others all reporting today that the President made a decision number of weeks ago to wind down the program to help support the rebels in Syria in part because it wasn't being very successful and in part because the rationale for it had somewhat eroded. You've no longer made the removal of Assad a priority, and because of the negotiations you have underway with Russia on deconfliction zones, you no longer are trying to get the Syrians to come to the negotiating table the way Secretary Kerry attempted for the past year and -- last year and a half of the administration. So to the degree that you can talk about that decision-making and the goals, tell us where we stand there.

MR. BOSSERT: I smile because it's your second classified program you'll ask me about.

MR. SANGER: Probably not the last.

MR. BOSSERT: And the second time I'll say, I long for the day that we stop reporting those. And believe that we could have done it with that and made the same case. That said without addressing that program or its existence or whether we have a program to even discuss, David, I'd like to say that you focus the problem a little bit better than we talked about. And that is the notion of whether we prioritize Assad's removal or not, right. And I think there's probably even some question as to whether the last year of the Obama administration had seen agreement among seniors. Maybe if your reporting is to be believed, there was some disagreement at that point

and at that time between the Secretary of State and the President as we concluded that administration.

MR. SANGER: More than a little.

MR. BOSSERT: And so I'd say it's pretty fair for us to take a relook at that and what clearly this President has done is attained some ceasefire that's durable through some cooperation with the Russians, despite all the domestic political brouhaha. I think he's shown some courageous leadership there. I think he's demonstrated the desire at least to have safe havens so that we don't have a refugee and a migration problem that plagues Europe and eventually the United States in a way that we can't maintain security control of. And I think that at some point there's a large humanitarian effort there that needs to be recognized.

And so we'll see if the safe haven holds, we'll see if the ceasefire holds, but I don't think it's important for us to say Assad must go first, but I think it's absolutely imperative for me to correct the record and suggest that the United States still would like to see Assad go at some point. And I think we've made that clear to our partners and to the Russians and to the regime itself that that would be our desired outcome, but we need a political outcome in Syria.

We don't need a militarily imposed outcome with no political strategy to fill in that void when we're gone. And we need to figure out how we're going to rebuild Syria after that. And I think it's pretty clear to the world that Assad still in control is not going to be the best future case outcome for a peaceable, politically resolved Syria. And so whether it comes first or second or soon thereafter, it would be a nice outcome.

MR. SANGER: Do you believe that to rebuild Syria, you must or should keep Syria within its current boundaries? Do you believe that ultimately Syria is going to end up getting broken up?

MR. BOSSERT: I certainly hope not, but I'll defer directly on that. So we have a Secretary of State who's now managing what you know to be one of the most difficult issues between the Turks and the Iranians and the Jordanians and the Israelis all in that area of the neighborhood of the Middle East. I don't think that there's a border conversation that would be productive right now, but we certainly have partners that are pursuing what we need them to pursue to Defeat ISIS first; and to maintain some stability and control and safe zones second; and to maintain a ceasefire in the South third.

Now you asked about Iran. I'd certainly hope that they don't continue their regional aspirations and pursue their aggressive activities through this so-called land bridge or crescent that would be a further destabilizing effort that we can't tolerate.

MR. SANGER: Let's turn to some cyber-issues, that's the other big part of -- another big part of your portfolio. So let me start with the most basic question. Director Coats who we saw in the audience here, Director Pompeo who we'll hear from this afternoon, have all said to Congress and others that after reviewing the intelligence, they are persuaded that there was a comprehensive program by the Russians to try to go affect the outcome of last year's election. The revelations on that started just about -- just a little over a year ago when we learned about the DNC hack through the CrowdStrike revelations.

So first, you've now had a chance to review all of this. Do you believe there was a comprehensive Russian program? And do you believe the Russians are going to come back here and elsewhere in the world to try to influence future elections?

MR. BOSSERT: Yeah. So there's a pretty clear and easy answer to this and that's yes.

(Laughter)

MR. SANGER: Like I said, you're short, direct, okay.

MR. BOSSERT: So, okay, now let's talk about what's really relevant here. The misunderstandings that surround that yes. What we have is a foreign nation state engaging in a behavior on an inherently unsafe medium, the Internet, to try to collect, steal, and then release embarrassing information, among other things, from the DNC. That we saw that ranged from a risotto recipe to some internal memos of some important -- at a political committee.

Now we all then have to debate whether you were -- any one of you persuaded by any of that rhetoric in those releases and those unacceptable efforts and behaviors by a foreign nation state when you came to the polling place. But it's always a worthwhile practice for me to remind everyone, especially because there are viewers that aren't as edified as this group that are watching elsewhere, that there was no evidence. And so those same people that gave you that commentary to lead into that question and to include Mr. Brennan who's here have also -- a Mr. Clapper who will be here -- said that there was no evidence of hacking into the ballot boxes.

So we don't have an election that was tampered with at the ballot box. What we have is a foreign nation state getting caught and, among others, acting badly on the Internet and attacking what I'll call the dotcom, and I'm not trivializing this, but there's the dot-gov, if you will, and that's the spy-versus-spy game that we always talk about and then there's the dot-com. And it violates our sensibilities when a spy attacks a company, so when dot-gov goes after the dot-com. And we have a responsibility, at this point, to address a few things, and I think Secretary Kelly has probably spoken pretty eloquently about his need to develop a public and private partnership to share information in that regard. The government has a big responsibility, but I think we have an even bigger one to increase our defenses and do it more quickly.

MR. SANGER: So, Tom, you and I have spent a lot of time talking about cyber-deterrence.

MR. BOSSERT: Let me come back to --

MR. SANGER: Sure.

MR. BOSSERT: -- but if you pivot to deterrence, it's important to know that increased defenses is one half of deterrence and the other half is what I suspect you're about to ask me about.

MR. SANGER: Well, we'll get to increased offense in just a minute.

MR. BOSSERT: Okay.

MR. SANGER: But on the deterrent side here, given the magnitude of the Russian effort and all that we've heard about it, do you believe when we look back at this incident five years, 10 years from now, we will determine that the Russians paid a big enough price for what they did in order to bring about some level of deterrence from their future activity?

MR. BOSSERT: So right now there's no bad cyber-actor. Other nation states have acted poorly, the last administration rightly called out the Chinese. The Iranians, the North Koreans, the Russians, there are a number. And they tend to not be countries that are like-minded with our worldview. And they are right now not paying enough. They're not paying anything. It's a very cheap exercise for them and a very high reward, and so no.

Now, if you're asking me whether in every individual's mind that they're going to get a commensurate punishment and comeuppance, that's going to be hard to answer. There's probably 340 million opinions on that in this country. But right now I would say that there's not one single price that one single bad actor on the Internet is paying that's high enough, both punitive or

preventative. And we have an incumbent responsibility to either change that equation or to announce this a dead technology that we can no longer rely upon. I am not ready to do that. I'm ready to put some policy changes in place that are going to increase the cost to the bad actor and then unify the likeminded so that we can throw the people that are not on that page out of the Internet if necessary.

MR. SANGER: So to put that in the context of had that new policy been in effect when the Russians were coming after the State Department, unclassified emails -- the White House on classified emails, the JCS, and then the activity during the election. In your mind, understanding that your cyber-deterrence report is not due until August, if I remember, what kind of activity -- what kind of responses do you think would have been appropriate for the United States to enact across the range of those -- of those activities the three attacks I mentioned and then the election?

MR. BOSSERT: Well, let's review what we did. So the last administration punished them, sanctioned them, issued a national security emergency in order to allow those authorities to predate and presage those actions. This President, Trump, continued that national emergency and continued those sanctions. Both Presidents --

MR. SANGER: By the sanctions, you're talking about --

MR. BOSSERT: On the Russians.

MR. SANGER: On the Russians of which the only ones I really saw were --

MR. BOSSERT: You weren't satisfied, I understand.

MR. SANGER: -- evicting 35 Russian, the perfect 19th century solution to a 21st century problem, and

closing two facilities that you were likely to have to get back at some point.

MR. BOSSERT: I take it you're not satisfied yet.

MR. SANGER: I would -- I would simply suggest that it wasn't fulsome.

MR. BOSSERT: So as we review this I'll keep going --

MR. SANGER: Okay.

MR. BOSSERT: -- because in addition to what we did and what the last administration did and what we continue to do, we sat down in a very sober and pretty fast fashion, unfortunately, as I moved into that (inaudible) that you described in the basement. I decided that we had to put in place something that was actually doable as opposed to -- as opposed to those tools that are 20th century that you've articulated. If you only have a 20th century tool, you're going to use it. Well, we used it. It wasn't adequate in your mind. It wasn't adequate in my mind. What we need to do living in the largest cyber-glasshouse in the world is to figure out how to increase our defenses and put in place a rational strategy before we go out and do things that are going to make us and our private and critical infrastructure owners more vulnerable.

So we'll satisfy you but we just won't satisfy you in enough time I think. Give me until August, at the very least, and I'll start to articulate some of the cyber policy. But, if you will, maybe have another question, give me an opportunity and I'll see if I can start the foreshadow for this group what a cyber-strategy might look like under this administration.

MR. SANGER: Well, let's say that you're seeing continued activity from the Russians, the North Koreans, the Iranians of the kind you've seen.

MR. BOSSERT: Yeah.

MR. SANGER: If you had a Sony case today --

MR. BOSSERT: Yeah.

MR. SANGER: -- A destructive hack --

MR. BOSSERT: Right.

MR. SANGER: -- on a commercial activity, if you saw an attempt to get inside voter registration systems, even if it didn't, as you said, affect the vote count --

MR. BOSSERT: Right.

MR. SANGER: -- what would you advise that we respond?

MR. BOSSERT: Okay. So the first thing you need to do is make sure that we don't have the David Sanger rule, and that is to be the one guy that decides what it is -- I'm joking -- what it is or is not --

(Laughter)

-- what is or is not an acceptable behavior on the Internet, right. I mean so by that I mean we need to have some agreed-upon norms and standards and expectations. By the way, something President Trump then told, in my recap of what we've done, President Putin pretty directly in their meeting. A lot has been said about their meeting and what he said and agreed to, but the first --

MR. SANGER: You're talking about the first meeting?

MR. BOSSERT: Not the dinner conversation.

MR. SANGER: Yes, right.

MR. BOSSERT: The point here is it's unacceptable, right. And the point is that that point's been made clear and reiterated now by two very different Presidents. And that's a little bit lost, but we can't then say this is something acceptable or not acceptable after we see it. And if I will, I'll be a little critical of last team, but remember my caveat when I came in here, this is not a criticism based on malice. This is just an observation based on the perch that I sit in now. We had an opportunity to do something a little bit more strategic in the past and given the time constraints and the tyranny of that time, we ended up with an ad hoc approach, each time using the sensibilities of the President at the time to drive our actions.

What I'd rather do in the future is figure out what together we consider acceptable behavior on the Internet, an unacceptable behavior, articulate that to the world so they know it, gain agreement inside our government that we're not going to -- we're not going to violate that rule. The golden rule has to apply here or we lose credibility, and then move forward with punishing it when we find evidence of its abuse. That's a big step and I want to stop by saying that that's a multilateral international obligation. We've had a lot of multilateral successes. There's a group of government experts at the UN that did a lot of work on that, and they came up with norms and rules. We need to agree upon them. We need to codify that in some way that we all find acceptable as a nation, and then we have the terra firma that we need to go forward and say you have violated that rule and it's time for you to be punished.

MR. SANGER: You have a unit at the State Department that was trying to negotiate that out. We hear it is either going to be reorganized or eliminated. It's not entirely clear and may not be clear until the full State Department reorganization is out there.

MR. BOSSERT: Yeah.

MR. SANGER: What's your ideal about what that would look like? Is that activity still centered in the State Department? Do you have a smaller, bigger, different kind of cyber unit within that?

MR. BOSSERT: So I'll work back. What I'd like to see is a vision, and then I'll come back to the tactical detail, what I'd like to see us pursue now is not a multilateral approach to deterrence. Once those rules are in place, I think history has taught us that that multilateral approach to action is a -- is a fool's errand. If we have a UN Security Council vote on what we're going to do to punish a bad cyber-actor, it will likely be inevitably be held up with a vote and objection on whether you had enough proof, whether you've shown your evidence, and revealed your classified programs, all the other things that we've seen in the past as nonstarters in cyber attribution.

What I'd like to start doing is pursuing with Secretary of State Tillerson's support and help and with others, Director Coats, I'd like to start seeing us pursuing a bilateral approach to punishment. And so I'd like to see us and another like-minded country get together on a particular case, agree that the evidence is sufficient, that the standard has been met, that the bad action and bad activity violated the standard I mentioned earlier of norms, and that we're going to pursue some action on it. And here's where we're playing jazz music, and by that I mean we're improvising. There is no playbook for what is proportionate in cyber and there is no playbook for satisfying the David Sanger rule. And so what we're going to have to do is find a way to experiment and see if it was in fact proportional, if it was in fact retractable enough to be suitable, and whether the rest of the international community of likeminded find it to have been pleasing.

MR. SANGER: And that penalty may not necessarily be in the cyber realm.

MR. BOSSERT: I hope it wouldn't be. In fact there's no evidence to suggest that that offensive cyber is a deterrent. Nobody's sitting around saying, "Well, they might hack us, so let's not hack them." I've not seen anyone say that from an individual hacker to a nation-state in my last 17 years looking at this problem. Instead, though, I'd like maybe some secondary sanctions. We could play with that. That's not just blocking somebody's bank account, but that's blocking their ability to do business in other banks in other countries that do dollar-denominated transactions. Those are pretty draconian and we wouldn't want to do that without at least a partner with us.

Anyway that's an idea time now. I'm now a little bit out over my skis. We haven't figured out yet what we want to do in terms of punishment, but I'd like to move forward in a bilateral way, keeping the United States in a position of being able to enter into those agreements first with preconditions. And there's a lot of -- there's a lot of 20th century support for how we've done this before with SOFA agreements. There is some predicate for me to believe that this would work, and ultimately remember we will end up, hopefully, with a multilateral group of like-minded people that have all come together with us in a willing bilateral fashion. And so you've seen me, I flew to Israel and made this arrangement with the Israelis.

We announced our first bilateral cyber-arrangement between the United States and Israel, and this administration will probably announce others. And one of the things I'd like to do is use that opportunity to negotiate with them some other things that are bedrock principles. We can talk about them with your future questions, but once those bedrock principles are met, we can then punish together. And then lastly we're going to have to, most important, figure out if there's a metric for success, whether it actually deters the bad action, and that's something you'll report on and then I'll stop calling it the David Sanger rule.

MR. SANGER: Okay. One of the other cyber-activities that we've seen in the past few months has been the spread of attacks like the WannaCry attack. And we saw first in Britain. I was just in Ukraine a week ago and they got hit a few weeks ago with another variant that really made it impossible to do even basic credit-card transactions and so forth.

MR. BOSSERT: Yeah.

MR. SANGER: One of the concerns you read about this is that some of the vulnerabilities that these are based on appear to have leaked out from, let me find a delicate way to say this, U.S. taxpayer supported activity that somehow leaked out of American systems, government leak number three. The U.S. government has never acknowledged these and I understand why you wouldn't. But you've got to be concerned about the perception around the world that the United States has exploited some vulnerabilities and then out of carelessness, bad luck, insider threats, Russian activity, who know whatever it is that these have gotten out into the wild and been used against us. So tell me how you're approaching this problem.

MR. BOSSERT: Yeah. So a couple things, this is -- this is an argument that I want to completely and completely and directly reject, okay. So let me start with the premise of my argument. You wrote an article recently drawing an analogy to a stolen missile where you suggested that if the United States were to develop a vulnerability and then to lose it through theft or loss, some insiders theft in some cases that we've seen reported Snowden-type material, that we would then be in some way responsible for having lost a missile.

MR. SANGER: If we lost a missile, that was used elsewhere based on our technology that there would be hell to pay for that.

MR. BOSSERT: That's -- to put a fine point on your question that's what you're asking.

MR. SANGER: Yes.

MR. BOSSERT: I want to make sure I not only reject that analogy but caution against the use of poorly or misapplied analogies because they lead to misunderstandings. And I'll stop there.

MR. SANGER: I'll take that you didn't like that one, yeah.

(Laughter)

So take the analogy on, tell us why it's wrong.

MR. BOSSERT: I want to, because what I'd like to do instead is say three-level setting things: first, it would be an abdication for us, the United States, or any nation to stop developing exploits -- and I see some others here that are probably nodding their head on this -- that would allow us the means to develop intelligence to protect our country and our interests, okay. That's a sacrosanct premise that I will stop with.

Secondly, the weaponeering and the analogies are very, very different. A missile is a missile it's a missile no matter how you use it and who uses it. A cyber-vulnerability is not. There are a whole lot of players involved in taking some piece of code -- and by the way, let me stop there and take a step back and digress. Now the United States or any other government or hacker for that matter doesn't develop the vulnerability, right. The software has the vulnerability; we find it. Now you've got that vulnerability identified in an exploitable way. The hacker develops an exploit. That's a hammer. It can be used in a lot of different ways, but if it's stolen and then turned into something that's used as a weapon or a tool because someone adds to it a delivery method, a long stick, a spike, and a nuclear weapon on the end of it that hammer looks a lot different at the end. So the exploit can be used for good and for bad, and if the exploit is lost and used by a bad actor,

it doesn't look like a missile anymore. And so there's a lot of problems with that weaponeering analogy and I give you the second one.

MR. SANGER: So the liability is all on the hands of the person who's using it, using the vulnerability, and not necessarily -- there's no liability in your mind on somebody who may have discovered a vulnerability, not reported it, and then lost track of it.

MR. BOSSERT: So the culpability right --

MR. SANGER: Yeah.

MR. BOSSERT: -- is the question. But you've also now got the software manufacturer that had a vulnerability. Now you've got the software manufacturer that developed and pushed a patch, which in this case they did. And now you've got the user of the software that does or does not, and in this case a lot did not, implement that patch. And then you've got third-party providers that for various reasons do or do not use those patches or update those software tools. So you've got 15 different players often involved in this. And the weaponeering is a little bit different, too, right.

Now you'll have a Major that knows how to use a rocket because it's going to go and make a bug splatter and he's going to point it at a target within his area of operations and he's going to follow the LOAC rules that we talked about, and it's going to make a certain explosion and kill the target. Terrorist tools are the same way, right, but cyber-tools are different. Cyber tools are exploited in ways that can be profoundly misused. And what you saw from WannaCry was a want in the deployment not a targeted one, and that ended up affecting in a way that the hacker couldn't control the entire world, right.

We're lucky that that patch was out. I'm grateful to Microsoft that they not only made that patch free, but they pushed it out on their old unsupportable XP software platforms. That's something they had never done

before, and they did that in a way that ended up saving lives, because that hack spread around through hospitals and other things that could have caused the loss of life and the hacker didn't have the ability to stop and say, "Wait a minute, this has gotten out of control. This has now affected China, Russia, Great Britain, and things that we're not going to collect ransom from. "

So if you want to say they took a missile and turned it into a geothermal global nuclear weapons program, I think maybe your analogy will start getting a little closer, but you'd still have to insert 15 different weapons manufacturers, tool crafters and parties that are involved in defending and creating offensive capability. So it's a little bit of a misnomer, but it's a big-time attempt to try to accuse any company or any government of wrongdoing. I think that's -- I think that's a wrong thing to do.

I would add a third point here now that I've digressed. The third point here is if we were to give this up, it would be a tantamount to -- it would be tantamount to intentional disarmament, right. And this unilateral disarmament argument has been made. I want to reinforce it. There is no other government in the world that does what we do. We find vulnerabilities, talk about whether they have any real serious national security implication for us, and talk about whether those implications might be offset by the cause or the harm if they were misused. And then we decide to give away upwards of 90% of what we discover to the good guys so they can patch against the use of those vulnerabilities against the bad guys. We are the only country in the world that does that. The 10% roughly that we keep, we keep for the use of our own national security and protection. And for us to now give up those other 10% because of a misunderstanding of the tool I think would be foolish.

MR. SANGER: One more in the in the cyber realm that I just was wanted to make sure that we covered. You have now inherited a plan from Congress to separate out

Cyber Command from the NSA. It's mandated in the NDAA but without the timing, we hear this moment may be coming. First, how soon is it going to be? And secondly, what are the risks you think of doing this? Can Cyber Command live on its own at this point? Does it have the capability? Could we end up replicating the capabilities we have in the NSA, which would be expensive?

MR. BOSSERT: So I'll deflect by saying I forgot one part of my last answer. And that is that a missile is used once and blows up. A cyber-tool is used and is reused and is reused and is reused and it exists in the Internet forever. Cyber Command and NSA have two very different functions and purposes. They're often misunderstood, but for right now the NDAA requires a whole lot of conditions-based outcomes. So if we don't meet those conditions, we can't make that decision to separate.

So Secretary Mattis will ultimately decide whether he wants to elevate Cyber Command to a four-star combatant command and make that recommendation to the President. And then if he decides that he would like to separate those two, which is a resource question as much as it is a dual-headed management question for him, he's going to have to meet some internal operating capacity requirements that are condition set in law, and that would take some time. So I would defer to Secretary Mattis. I'll certainly be involved in helping the President think through his recommendation, but I think that his recommendation on elevation and potential separation would probably come this summer.

MR. SANGER: So relatively soon. There was one, of course, on President Obama's desk that he did not act on last summer.

MR. BOSSERT: Right.

MR. SANGER: And so you think we're pretty close to having the conditions ready it sounds like.

MR. BOSSERT: I think that the decision could be made now. The conditions, if the decision were two separate, wouldn't be met for some period of time. And I wouldn't want to --

MR. SANGER: That could be a year or more you think.

MR. BOSSERT: Whatever it takes, I wouldn't want to put them on a deadline that they couldn't meet.

MR. SANGER: Let's go to one other area before we go to some questions. Bio-defense, an area where you want to go make some changes. Tell us a little bit about it.

MR. BOSSERT: We left cyber too soon.

MR. SANGER: Okay.

MR. BOSSERT: But I'll let you --

MR. SANGER: Well, we'll come back -- we will come back. You have things you want to say on cyber, probably on 702 and the like.

MR. BOSSERT: I do, I do.

MR. SANGER: 702 is up for renewal. Are you going to get a clean renewal of it? Do you have something else in mind?

MR. BOSSERT: Let me do this for time so you can go to bio-defense. I kind of view cyber and 702 and some of you might have seen a US-UK data sharing agreement that we're pursuing as an administration decision as part of a theme of lawful access to information, which I think it's all related. So this theme of lawful access to information is how I think of the problem and how I'd like the President to think of it. If you don't have lawful access to information, you can't really talk about cyber-security.

In 702 there is absolutely no question, I've put this out publicly, and this is our administration's position that we need that tool and that those that misunderstand or intentionally conflate it with Title I FISA and things that are in the news and domestic intrigue is a damaging thing and it's an unfortunate thing depending on whether it's intentional.

702 is the part of FISA that allows us the authority to collect intelligence on a foreign person in a foreign land, period. It's not the part of the authority that allows us to collect intelligence on a foreign person in the United States, or on a U.S. person anywhere. This is a foreign person on foreign land and it yields intelligence that saves lives, period, end of story. It's unassailable. We have two generations of administration officials that have all said this unanimously.

So Congress rightly set a sunset clause when they put this new authority in place. It was a 10-year sunset clause. We thought that was a good opportunity for us to assess whether it worked. It's worked. We've had a court. We've had a PCLOB, this civil liberties oversight process, and we have had no abuses. Now we've had internal problems that those mechanisms have identified and corrected, but the FISC court has come out every time at every juncture, even the last ruling, and reauthorized and reissued what we need to do the certification process to continue the program. And even Charlie Savage on your team came out and wrote a very fair piece on that the last time the FISC court came out and said some critical things. So even the New York Times --

MR. SANGER: You're pretty generous to the family of New York Times articles --

MR. BOSSERT: Even the New York Times,

MR. SANGER: Yes.

MR. BOSSERT: The local New York rag got it absolutely right that we need 702 reauthorized and that the oversight functions that are there protect American people.

MR. SANGER: You'll go tell your boss you're impressed with our reporting.

MR. BOSSERT: I showed him that Savage article and he was appreciative, and I was appreciative of him doing it. So on that, though, here's a little future thinking for your cocktail party tonight when you talk to me. Why do we need a 702 authority in 10 years' time? Why do we need that again? Why is it that a terrorist in a foreign land has any U.S. legal protection?

Well, they don't. They don't need U.S. legal protection, but it just so happens that we make some really great tools, and so they like to use Gmail and they like to use Twitter, and they like to use Apple devices, because we have American innovation. In some cases that data never traverses in American pipe, but nevertheless we have an authority in place that says we need to gain permission from a U.S. court to pursue information from a foreign bad guy on a foreign land talking to another foreign bad guy.

Eventually we'll have a different view of the Internet and we won't make it so parochial and so sovereignty based, but for right now we do. And for right now we need that reauthorized and for right now I assure you that it's not being abused. And the one part of it that we couldn't control that we weren't abusing intentionally but we couldn't have the internal controls to look you in the eye and say a 100% couldn't be abused or misused we turned off. It's this theory of upstream collection. We turned it off and I commend Admiral Rogers for recognizing that he just didn't have the backend capability to keep those databases separate when we turn it off.

MR. SANGER: Will you just go one more bit and explain to people what that upstream collection is?

MR. BOSSERT: Yeah. So it's what we call --

MR. SANGER: A complex concept, yeah.

MR. BOSSERT: It's what we call upstream VAS and I'll make it really simple. If you have an email between David and Tom, and Tom's the target and I'm a foreign bad guy on a foreign land, we can -- we can look at that under the authority if you meet those preconditions. If Jane is doing research on Tom on the Internet, that might be an upstream VAS activity and that collection might end up being picked up. Well, now Jane might be a U.S. citizen or she might have collected on a Tom that was we have to make sure we sort that out.

Some of that upstream VAS collection activity ended up yielding results that we couldn't segregate. And so from a technical perspective, we turned that off. They don't do it because we can't make sure 100%, Clark wouldn't be able to as an AG, look at that and say a 100% you'll never have a violation despite your best intentions. I believe we'll get to a point where we can turn that back on and the technical back-end capacity will be there, but for today this is to and from collection of foreign bad guys doing foreign things in a foreign land. They're bad and they meet the definition that the court oversees, and I think we need that authority.

And I think there will be approval by the smartest and the most thoughtful bipartisan approval on the Hill. And I think there'll be a few that have some understandable privacy concerns and they won't believe my assertion that we maintain controls. And then I think there'll probably be a few that intentionally conflate it with all the other domestic intrigue. But my hope is that we get it done but my foreshadowing to you is that at some point in the future we're going to have to relook at why we do it that way and why the pipes and where the data traverses matters to our legal system.

MR. SANGER: Let's run quickly to bio because we're running out of time and I do want to get to a few questions from the audience. You have in mind a new bio initiative. Tell us about it.

MR. BOSSERT: Yeah. Maybe this is news. And for the (inaudible) involved you'll appreciate this, and this is something I should say has captured me since I was motivated into this field on 9/11. You'll recall the anthrax attacks that scared us soon thereafter. We have not had, as a country, a comprehensive bio-defense strategy ever. We've had a lot of efforts, we've had a lot of good Presidential directives under President Bush and Obama, and we've had a lot of fits and starts in our investments.

We've had some medical countermeasures and some debates on how to distribute them. But at this point, we need to look clear-eyed at the fact that we might have a devastating pandemic influenza or an intentional anthrax attack, or just to add to your concerns if you weren't watching in the newspapers, there was a Canadian scientist that recently developed synthetic horse pox. That's not going to kill any of us, but that suggests that somebody might in the future now possess the capability to produce synthetic smallpox without the live virus.

And that scares me to death, and it's high time that we have a bio-defense strategy to address it and this administration is going to create one. And we're going to do a comprehensive one right out of the White House, and we'll publish it as soon as we can, and we'll try to tie together all the various NDAA requirements that touch on all the various different departments because we felt that was disjointed. I'm going to lead this as a coordinating matter for the President, but we then brought on a guy named Admiral Tim Ziemer, and for those of you that don't know him, he's the right guy.

He's our Senior Director and he should be all the evidence you need that this administration takes

seriously not only bio defense but the Global Health Security Agenda that President Obama promoted, and if I can, that is set to sunset in 2018, the Global Health Security Agenda. The United States has at this point put a \$1 billion into that effort and I'd like to make sure you understand that this President supports it moving forward. Even as our budget requests go up and down and people write criticisms of us, we are still the leading contributor to that effort. And diseases travel without visas, so let's not have a conversation about our, you know, visa immigration issue on this. This is a problem that you can't fix by shutting down our borders or controlling our entry.

Those controlling entry problems are different. This is a -- this is a problem that is global and the weakest country among us with the least preventative care problems or least preventative care capabilities are going to be the patient zero outbreak source. And they're going to end up killing and infecting the world, and so we need to put money into places that don't have the money to do it themselves to prevent loss of life here. So that's it. We will continue our full-throated support of the Global Health Security Agenda. We will hope to promote the other 10 countries and more continuing it once it sunsets in 2018 and extending it. And then lastly, we will put together a comprehensive bio-defense strategy for this country, and that's something I think the Hill knows, but I don't think the rest of the public knows. So you're the first to hear.

MR. SANGER: Great. So we have time for just a few questions. We'll start with Kim right here. There's a mic coming to you, Kim.

MS. DOZIER: Hi, Kim Dozier with The Daily Beast and CNN. You described-- is this on?

MR. SANGER: Now it is.

MS. DOZIER: Kim Dozier with The Daily Beast and CNN. You've described the ISIS strategy that you're

creating as being related to what came before it. The Obama plan had nine lines of effort. You so far have only described things like increasing the authority of people closer to the fight. Do you really need a new strategy? And when you roll it out, is it going to look a lot like the last one?

MR. BOSSERT: Okay. So two questions there. For those that didn't hear it, the question was what are the differences between the last administration to Defeat ISIS strategy and ours. And so I talked a lot about the differences between their strategy on counterterrorism in a global way. I think 2011 is the last time we published our National Counterterrorism Strategy and that's something that we will update and that's something that'll be a broader look towards the future in which we've taken the physical control, physical space away from the Caliphate, so to speak, away from ISIS. So what we're looking to do here is not only predict the 2.0 but predict what we need to do over the long term to address the problem as it manifests from Germany to Libya to the Sahel and in West Africa.

The Defeat ISIS campaign is an ongoing military campaign. We've not put out anything on our effort there, comparatively or otherwise, and President Trump has been pretty clear about his lack of desire to forecast his punches on that. And so I think that we'll just let our outcome speak. I will say one thing, a big thank you to the 68 members of the Defeat ISIS coalition because a lot of them have ponied up more money, more troops, and more support in their last meeting and in this administration, and that's a really big deal for some of those countries, and so we couldn't do it without them. And I think it's maybe all the evidence I could suggest here in this forum that we have a good plan and the changes that we did make, whether they were big or small, satisfied those partners, every one of them.

MR. SANGER: The lady in the blue jacket right there.

MS. BRIGGS: Hi. Rachel Briggs with Hostage U.S. Thank you firstly for mentioning Bob Levinson who's been held now for 10 years in Iran. I appreciate that. Could you comment on whether there have been any changes under this administrator to the hostage policy and whether you anticipate any changes or structural changes coming up in the near future?

MR. BOSSERT: Thank you for asking that question. Absolutely not. PPD-30, for those of you don't know, is a good document. It came out of a lot of family contribution. So no government official deserves any credit for that. The families of the hostages through frustration and experience led to the development of that Presidential policy. President Obama deserves some credit for signing it, and what came out of it and the key findings and the strategy that was published thereafter is all in place. We recognize every word of it and we've continued.

So I've picked up the responsibility that Lisa Monaco left for me. I've met with all the hostage families on a regular basis. It's a serious part of my job, and we're going to keep the structural improvements in place from the Hostage Recovery Fusion Cell. That's an interagency operator body focused all the time, 100% of their time, on their recovery and return of hostages, dead or alive, but then also the interagency body at the White House that meets on, at this point, weekly basis, at very least biweekly basis to talk about that at a policy level. So no changes, in fact probably a redoubled effort, and we haven't had a policy meeting of any significance where we haven't talked about the implications to hostages since I've been there.

MR. SANGER: One last question. Bart in the back there.

MR. GELLMAN: Hi. Bart Gellman from Century Foundation and Washington Post. On 702 and the idea that it collects strictly on foreigners overseas, end of story, both PCLOB, which you mentioned, and the President's

review board talked about the large amount of incidental collection and called for significant changes there. If you can't target Americans under 702, which you can't and you don't, but you pick up a lot of U.S. communications incidentally. Why should there not be a change that says you need a higher threshold to look at that, disseminate it, and use it?

MR. SANGER: I'm hearing we have very little time, so a quick answer.

MR. BOSSERT: I'm getting a time hooked, Bart. So here's the short answer. That's a fancy new term to develop some mistrust or distrust of that capability and authority and how we use it, but if you've ever seen an old movie, we've had Article 3 warrants issued against bad guys since the inception of our country. And if you decide to make a phone call to somebody that's being wiretapped just to ask them to help take your trash out, you have been incidentally collected upon. There is no difference there. The authorities know the difference between collecting on the bad guy and the mob that they're listening to, and the old lady next door who happened to call him and ask him to take their trash out for 200 years. And so there's no difference. There's an Article 3 comparison here, and that's the short answer. But there's some legitimacy to your question and so I get it to you after we're done.

MR. SANGER: Well, thank you, Tom, for this. We've covered a lot of territory. Really appreciate.

(Applause)

MR. BOSSERT: Thank you.

* * * * *