



## **Transcript**

**Director of National Intelligence James Clapper**

**Intelligence and National Security Summit**

**Washington Convention Center, Washington, D.C.**

**September 7, 2016**

Speakers: James Clapper, Director of National Intelligence

Letitia Long, Chairman, Intelligence and National Security Alliance (moderator)

*This transcript has been edited minimally for brevity and clarity.*

[\*]

CLAPPER: When I was president of SASA, the predecessor to INSA in the 1990s, I tried to promote a combined symposium with AFCEA, but I could never pull it off. This event now marks the third year in a row for this joint summit. So I want to congratulate everyone who is involved in both organizations, AFCEA and INSA, in putting these things on, and now they're becoming a custom.

So it proves that over time, things do change. But I think we can safely say it's an idea whose time has really come and that you've made it stick.

This has also been, for me, a very useful forum to convey messages and roll out IC-wide initiatives. At the first AFCEA-INSA summit two years ago, I rolled out the 2014 National Intelligence Strategy, which included our principles of professional ethics for the intelligence community. And last year, I rolled out the principles of intelligence transparency, our IC transparency working group which is now a permanent council, and a number of community-wide transparency initiatives.

So this year, I realize about the only thing we'll be rolling out the door in the next four months is me. (LAUGHTER) So I thought this morning, I'd talk about what seems to be on everyone's mind, which is the forthcoming transition of our presidential administration and IC leadership.

In about two months, 62 days to be exact, we'll know who the next president will be, hopefully. And many of the faces and names at the top of the national security structure will probably accordingly change.

Now, any presidential transition is a very vulnerable time for the country. During President Obama's inauguration in 2009, I had a unique opportunity to see this, experience this first-hand.

Just like for the State of the Union speeches, during inaugurations when everyone who's anyone is on the D.C. Mall, the administration picks a designated survivor, a Cabinet official or Cabinet-level official to stay in an undisclosed location away from Washington, D.C., so that in case something terrible happens, that person could assume the duties of the president.

Now, during the 2009 inauguration, that person was Bob Gates, not me. As secretary of Defense, Bob was, I think, the only holdover Cabinet official from President Bush's administration. And at the time, I was the under secretary of defense for intelligence. So I got

to be the acting SECDEF for Bob while he was playing designated survivor. So I spent the inauguration in a cave at Fort Ritchie, Maryland.

The experience definitely drove home the vulnerability that we experience during a transition, and particularly the exact moment when the baton is passed from one president to the next. This upcoming transition will happen at a particularly, I think, difficult time as we're facing the most complex and diverse array of global threats that I've seen in my 53 years or so in the intel business.

So we are living in what I've come to call a world of unpredictable instability in which two-thirds of the nations around the world are at some risk of instability in the next few years. Let me illustrate with some perspectives just on Africa.

Africa is enormous; over 11 million square miles with more than 1.1 billion people. And just between the years 2010 and 2015, 52 presidential elections were held on the continent, contributing to the constant political change. More than 1,130 armed conflict events occurred, resulting in conservatively over 50,000 fatalities.

And there are two key factors driving the scope and complexity of unrest which span political, economic, security, cultural and ethnic sectors, and resulting clashes between varying factions, massive humanitarian crises and perpetual regional instability. And so that led to some interventions from the U.S. and other nation states, as well as multinational organizations.

So Africa is just one region of the world where such turmoil is present. Nearly everywhere, the IC can point out the potential for failures or collapses. We certainly can't anticipate the specifics, the when, where and how for our policymakers. This unpredictable instability has been a constant for certainly this administration and will be, I think, for the next one too no matter who our president is.

In the coming decades, an underlying meta-driver of unpredictable instability will be, I believe, climate change. Major population centers will compete for ever-diminishing food and water resources and governments will have an increasingly difficult time controlling their territories.

And so because of all of these factors, after ISIL's gone, we can expect some other terrorist entity to arise and a cycle of extremism which will continue to control us for the

foreseeable future. And by the way, our more traditional adversaries like Russia and China and Iran and North Korea will continue to challenge us.

And of course, technology will continue to be disruptive. Just think about the fact that Uber is the biggest taxi company in the world and they don't own any cars. Airbnb is the biggest hotel company and they don't own any properties.

It is difficult to predict how technology will affect national security. Tech areas like artificial intelligence, healthcare and agricultural, self-driving cars and 3-D printing have the potential to revolutionize our lives for the better or they could present vulnerabilities that are very hard to predict.

So with all this as a back drop, I think it makes a lot of people nervous that with an election cycle that's been sportier than we're used to, we'll drop a new president with new national security leaders into this situation - in 135 days, but who's counting?

I know a lot of people of been feeling uncertainty about what will happen with this presidential transition. Been a lot of catastrophizing, if I can use that term, in the 24-hour news cycle, and of course, on social media. So I'm here with a message. It'll be OK.

About two weeks ago, I participated in a meeting at the White House led by the White House Chief of Staff Dennis McDonough in which was the first formal meeting between the current administration and the two transition teams. And I was struck by how sober and professional and courteous and civil the conversation was.

When you pass on an inkling to whomever succeeds this administration some insight into the magnitude, complexity and the gravity of what it is to lead the U.S. government. Our nation has a great legacy of orderly transition and power, going back to George Washington retiring in 1797, when he turned the presidency over to John Adams. I remember it well.

(LAUGHTER)

Because of our mission and our professionalism, today's IC I think represents a pillar of stability during such a transition. In contrast to the rapid technology advances and the unpredictable instability of the world and any uncertainty surrounding an election and transition to the next administration, one constant in national security is the people of the intelligence community.

Over the past few years, our nation has held a very public conversation about our work and how we should conduct it as an intelligence community. I believe a lot of what has been lost in the public debate about how we conduct intelligence is why we even do it in the first place. Why does any nation state conduct intelligence?

I spent a little time and thought on that question, and I think we conduct intelligence, maybe at its most basic level, to reduce uncertainty for our decision-makers. And that could be the president in the Oval Office or it can be a war fighter, if I can stretch the metaphor, in an oval-shaped foxhole.

We can't eliminate uncertainty for any decision-maker, whether in the Oval Office or the foxhole, but we can provide insight and analysis to help their understanding and to make uncertainty at least manageable so that our national security decision-makers can make educated decisions with an understanding of the risk involved, so that we, our friends and allies, can operate on a shared understanding of the facts of the situation.

That's why we're already briefing the candidates to help reduce uncertainty for our next president, whoever it is, so that he or she will step into the Oval Office with as good an understanding of our complex and uncertain world as we can help provide.

And I've thought a lot about our work through sort of a historical lens, and maybe that's because I've lived through a lot of history. Although despite what I said before, I really wasn't there when Washington turned the presidency over to Adams. (LAUGHTER)

I was deployed at the time, so I missed the ceremony.

(LAUGHTER)

Only kidding.

So today, considering the press of public interest in what the IC is doing during this presidential transition, which is unlike anything we've seen before, I want to shed a little light on what we're doing.

First off, to dispel a myth; we're not giving President Obama's PDB, or any PDB product, to the candidates. In fact, the tradition of giving candidates classified briefings predates the existence of the PDB.

In 1952, President Truman offered the first candidate briefings to General Eisenhower and Governor Stevenson, and the newly-formed CIA conducted these briefings. Truman felt an obligation to do that because of his experience and how woefully uninformed he felt on his first day in office as president when he succeeded President Roosevelt.

In fact, he hadn't known of the existence of the Manhattan Project until 12 days after he was sworn in as president, and he had been Roosevelt's vice president. So he wanted his successor to be a little better prepared based on the nomination to be president, not on any clearance the candidate held or had held.

That precedent has carried over for every election since then – since 1952. The CIA handled those briefings until 2008, when the Office of Director of National Intelligence assumed the responsibility.

As a point of trivia, there have only been three elections in which briefings were offered to candidates from both major parties: 1952, 2008, and now this year, 2016. Those are the only years in which one of the candidates wasn't already receiving intelligence briefings as the incumbent president or vice president.

So just to be clear, one team produces and delivers the PDB, as we always do, and a completely separate team produces and coordinates the cross-agency effort to brief the candidates. And in fact, in our effort to try to make sure that there's no political influence on the briefings, the candidate briefing team does not coordinate with the White House and only career intelligence officers give the briefings, not political appointees like me.

Similar to prior elections, we set ground rules months before the briefings started, which the White House concurred with, on June 22nd. And the IC has essentially been operating independently since then.

We have a list of topics that we offer to each candidate. They can ask for briefings on any or all of them. They can also ask for briefings on new topics. If we give briefs on new topics, we'll make sure both candidates have a chance to get those same briefs. Otherwise we don't tell either campaign or the public what happens in those briefings: not what topics each candidate shows interest in or gets briefed on, not how either candidate reacts and not what questions get asked.

And we take that confidentiality so seriously that I am still sworn to secrecy about what happened when I briefed General Eisenhower and Governor Stevenson. (LAUGHTER)

Another geezer joke there, I just thought I'd...

(LAUGHTER)

But I'll make a serious point. People all around the world, not just opposing parties, want to know what the candidates are thinking. That's why we've seen attempted cyber intrusions against parties and candidates going back more than one election cycle.

We've certainly seen it this year with the network intrusion against the Democratic National Party. The president said last week, and I quote, "Experts have attributed this to the Russians." So I won't get out ahead of the president on this, particularly while the FBI is still conducting an investigation, but I can reiterate his other point. The Russians hack our systems all the time, not just government, but also corporate and personal systems. And so do the Chinese and others, including non-state actors.

The point is, cyber will continue to be a huge problem for the next presidential administration, as it has been a challenge for this one.

But back to the IC's role in this orderly transition. On the day after the election, the briefing process I described changes. The new president-elect will receive his or her first PDB briefing, and it will be essentially identical to that which President Obama receives.

Later this month, I'll send over proposed ground rules to the White House about how we'll make all that happen. And later, my office will also provide support to prepare the next DNI and next generation of IC leaders.

This whole process is built on the precedent set by Harry Truman back in 1952. And I'm really glad, as a citizen, that he made that generous decision to better prepare his successor. I talked about the uncertainty of our world and the diversity of threats we face. I believe, I know, it's crucial for our next president to step into office on January 20th as informed and prepared as possible to face that uncertain world.

President Johnson once said, "The president's hardest task is not to do what is right, but to know what is right." And having worked closely with and for our current president, I can absolutely attest, that statement by President Johnson still holds true. Knowing what is right is the president's hardest task. The IC can't make that decision for him. We wouldn't want to.

When it comes to national security, it's our job to give him the intelligence he needs to decide what's right.

So our work means a great deal to the person we call, "Intelligence Customer Number One." I believe that in this time of change, when we don't know today who our next intel customer number one will be, what our national priorities will be or what challenges we'll face next, I'm confident that our unique accesses and insight will continue to help our national leaders manage this inevitable uncertainty, for a long time to come.

So let me wrap up with a story from about 54 years ago, in 1962, about a year before I actually started in the intel profession. I was an Air Force ROTC cadet at Otis Air Force Base in Massachusetts, when I briefly met President Kennedy. He'd flown into the base, to Otis, en route to a family vacation at their residence -- the family residence in Hyannis Port. And so they "fell out" all the ROTC cadets to greet him when he got off the plane.

And somehow, I ended up in the front row of the rope line when he got off Air Force One. There were maybe a dozen of us right up against the rope and the President came through and shook our hands. And each of my fellow cadets gave the President his name - that's what we were instructed to do - and told him which aircraft they wanted to fly in the Air Force. And when he got to me, I gave him my name and he asked me what I wanted to do when I joined the Air Force. And I told him I wanted to be an intelligence officer.

He paused, looked at me a bit askance, he said "Good, we need more like you," and then continued down the rope line. I'm sure President Kennedy never gave that little exchange another thought. I, on the other hand, never forgot it.

That's the impact our work has at the highest levels of government, something I learned as a 19-year-old -- 20-year-old ROTC cadet. And at the time, I certainly never would have dreamed in my wildest imagination that I'd close my intelligence career in a job in which I'd have the privilege of briefing the President.

And there's simply no way you could have told me in 1962 that I'd spend six-plus years briefing our nation's first African-American President. That's something my parents would have been astounded by, my father certainly, and my mother would have been very proud of.

I look back over my half century in the intel business and can see the evolution of our IC. We are better, much, much better now than we were 53 years ago when I first took my oath of office as a young second lieutenant. We're better, more capable than we were 15 years ago, on



September 11th, 2001. And I believe we're better, or like to think we are more integrated than we were six years ago when Vice President Biden swore me in as the DNI. Although I'm going to leave it for somebody else to grade my term paper.

The reason we keep evolving and keep getting better is because of the people, the people in this room, the people in the IC and their instinct to serve. The nation continues to be a bedrock constant, just as it was when I started. Yes, the world changes, the threats evolve, the technology mushrooms, but our people, our IC will be a steady constant of vigilance and stability as it will be through this transition.

I couldn't be prouder to serve in this great community. And that's something that you'll keep hearing from me for another 135 days - but who's counting? So thanks very much.

(APPLAUSE)

LONG: Terrific job, Jim, as always.

uyAnd when we were backstage, I mentioned to Jim that I always learned something new whenever he talks. When he heard the comment about getting continuing education credits for this session, he said, "Well, I'd better say something." So, what I learned actually was a new word that I've never heard before, and that's catastrophizing.

CLAPPER: Yeah.

LONG: Yeah. Now, I am heartened that you said everything will be OK. And everything will be OK. You ended with talking about the people. So let's start with that.

So, 54 years later, if you were starting in the intelligence community today, what would you tell yourself now? Or what would you tell someone who is starting in the intelligence community today?

CLAPPER: Well, what I would tell -- I don't know what I'd tell myself. But I would tell, you know, people that are contemplating, particularly young people, contemplating coming to the intelligence community that it's a noble profession, I think. You are helping to discharge a sacred public trust. There's always a new challenge everyday. And just work hard and think about one assignment ahead of the one you're in.

LONG: OK. Good advice. I think you gave that to me about 20 some years ago.

What's on the top of your list to tell the next DNI?

CLAPPER: Well, it depends on who it is, I guess. I think probably, at least initially, do no harm. I think it's always a good idea to kind of survey and assess how things are operating today and then give some thought to whatever changes that the next DNI may want to make, which are inevitable.

Hopefully, he or she will build on the legacy of what we leave, just as we built on the legacy of the first three DNIs. So I would -- also, of course, the DNI will be governed by, guided by whatever direction he or she gets from the next President. So that will clearly determine change. Also have to remember that the Congress certainly gets a vote in any change, no matter how inconsequential one may contemplate for the intelligence community.

LONG: So, speaking about the next President, let's assume you have the opportunity to meet with the incoming President, not far fetched. I would hope, in fact, that would happen. What will you tell the next president are the qualities that she or he should look for in the next DNI?

CLAPPER: Well, I hope above all, it is somebody who is willing to tell truth to power, to be objective and to tell it straight. I think that's kind of a rockbed principle, a holy writ, almost, of what the intelligence community is all about.

LONG: OK. Let's shift gears a little bit. You talked a bit about technology. And technology has mushroomed, to use your word. From a technology standpoint and integration standpoint across the intelligence community, what's your 60-second elevator speech on IC ITE (the Intelligence Community IT Enterprise)?

CLAPPER: Well, it's designed to take us to the next level of both integration, sharing and security. Probably less than 60 seconds.

LONG: Are we past the tipping point? Do you see it as an enduring initiative into the next administration?

CLAPPER: I think so. And the reason I say that, is because we have, had buy in, certainly from the leadership, you always get the, you know, passive aggressive resistance from some people, which is inevitable with any change. It's just human nature. But I believe it's one of the

reasons Stephanie and I stuck around as long as we have, is, hopefully instantiate IC ITE so it will be too difficult to turn off.

I think the major reason, though, is not because it's something we've been driving as much as people are really starting to see the virtues of what is entailed with IC ITE . It's actually not about an IT upgrade. It's more about fundamentally changing the way we conduct our business. I think people are starting to see the virtue of that, and that's -- people voting with their feet, so to speak, is what is really going to instantiate it for the future.

LONG: So recognizing this as an unclassified forum, is there anything you can share from an operational standpoint where IC ITE has had a substantive impact on an outcome to a problem?

CLAPPER: Well, while I'm getting a specific example, I'll just say, what we're seeing that -- one of the benefits of it is discovery. Whereby an analyst, who even if he or she doesn't have access to a particular data, the design of IC ITE is intended such that I will facilitate at least discovery that there is other data available.

And we've seen examples of that working already, and notably -- I'll just highlight in the counterproliferation business. That's probably all I can -- far as I want to go on specifics, but that, to me, is one of the great virtues of iSIGHT (ph).

LONG: OK. Continuing with technology, we are very dependent upon technology for our tradecraft to do our business. Do you see, as more and more technology comes in, you mentioned artificial intelligence -- do you see a point where there will be, or has there already been a decrease in human intelligence collection?

CLAPPER: Well, no. I don't think we'll ever see a lessening of the need for human intelligence collection. At least not in the foreseeable future, any future I can see. We're always going to need that. And of course, artificial intelligence itself is controversial. There are big thinkers in this country who are very concerned about its governance, its oversight, and its regulation, something that is not properly overseen can get out of hand.

So it's another tool for us, and we will have to adjust both in terms of others who employ artificial intelligence as well as are using it ourselves in our work.

LONG: OK. We're getting a lot of good questions from the audience. Thank you. Please keep the questions coming. Send your questions to [questions@intelsummit.org](mailto:questions@intelsummit.org).

So, another question from the audience. You talked about the uncertainty of the world and diversity of threats. A lot has been said over the last three, four, five years that terrorism really dominates the resources and the efforts of the intelligence community. Do we have the balance right? Are we covering down on everything that we should be? Particularly, the current and the more strategic.

CLAPPER: Yes. Well that's -- that's a very good question, and it's one that I've -- we collectively, the I.C. leadership has agonized over it. Because we do spend a great deal -- we expend a great deal of resources, both money and manpower, certainly as a proportion of National Intelligence Program on C.T. And that concerns me, in fact, we skew a lot of our resource towards the top targets.

You know, the four countries I mentioned and the challenges posed by C.T. and cyber and now counter intelligence. So those are huge claimants, as we allocate resources, both money and manpower, in the National Intelligence Program.

And you always worry about, is the balance right? Have we continued to sustain what is expected of us, which is global coverage. And I do worry about the relative proportion and the skewing towards the top targets. Because it's the non- targets that have a habit of biting you. And so this is a topic that we will certainly discuss, tee up for the transition team for the next administration.

LONG: OK. There was a related question. Let me just give you the kudos that was a part of it. Good job on the global trends, and I know that there are a lot of folks who are looking forward to the 2030, which will be released in the next couple of months.

CLAPPER: Yes. Pretty soon. One of the great merits, virtues of -- a couple of global trends, of course, the first of which, it's unclassified, and almost as important as the output, the written product, is the process that we use to compile it. And it's a lot of dialogue, a lot of outreach with not the usual suspects, and we reach out to academics, foreign countries, we engage a lot of people that we wouldn't normally do in a classified context. That's one of the great strengths of this publication.

LONG: So there was a question actually related to that, which I think would be a nice follow on. How are we positioned to deal with impacts of such changes as climate and technology? And I know that that's one that's really looked at in the global trends.

CLAPPER: Well, I alluded to that briefly in my remarks, and I do think climate change is going to be an underpinning for a lot of national security issues. The effect on climate, which drives so many things -- availability of basics like water and food, and other resources, which are increasingly going to become matters of conflict, and already are, between and among countries. And so this is going to give rise to national security insight that we'll need to understand this and hopefully help anticipate it.

So I think climate change over time is going to have a (inaudible) effect on our national security picture.

LONG: I think many would agree.

All right. Let's shift gears a little bit. You spoke at the Space Symposium about a revolutionary intelligence space architecture that included automatic queuing, fast processing of imagery and persistence. And of course, that was something I talked a lot about when I was director of NGA.

How important is autonomy to developing this approach? And how well is the community progressing?

CLAPPER: Well -- autonomy?

LONG: So the automated tipping and queuing...

CLAPPER: Oh, yeah. Untouched by human hands.

LONG: Are we there? Untouched by human hands. Are we there? Should we ever be there?

CLAPPER: Well, we're getting there.

LONG: And would you...

CLAPPER: There's some great work going on right now under the auspice of the NRO on tipping and queuing. And when we reach the point where we have persistence in both SIGINT and GEOINT domains, I think to me, it's almost a no-brainer to do as much of this on an automatic tipping and queuing basis as possible and to get, as much as possible, humans out of it.

I mean, the classic pattern, particularly in the intelligence business is, I want my picture tomorrow. If I don't get it because of weather, you know, try it again. One of the real (inaudible) the discourse up to here's my problem. Now you (inaudible) intelligence community, particularly with an architecture that the question describes, will be a lot more responsive, a lot more agile and a lot more comprehensive than what we can do today.

LONG: It's bringing those customers along. So I think that's part of that challenge with the cultural mindset of I want a pretty picture.

CLAPPER: Yeah, that's right.

LONG: So -- so this administration has been focused on space resilience and ensuring that we have robust overhead capabilities. Do you think that focus and vision will transition into the next administration? And why?

CLAPPER: Well, I hope so. It would be -- in the face of the evidence, the face of what the -- both the Russians and the Chinese have embarked on a very aggressive, impressive space capabilities and counter-space capabilities that if we're going to continue to operate in the -- in that domain, which I think we must, the investments that we've begun and laid out over, you know, the future will need to be sustained. And it's hard for me to imagine that any administration wouldn't see the merit of sustaining it.

LONG: I think many in this room would certainly agree, particularly with our increased need.

One of our tracks today is about acquisition services, acquisition management, acquisition reform. How do you think we're doing in the intelligence community if you had to give us a score on a scorecard? And you know, are there specific rules, regulations, policies that hamper our ability to procure the services and things that we need?

CLAPPER: Well, I think first of all, we're doing pretty well in the IC. We have something on the order of 27 major systems acquisition programs across the IC, 17 of them in a row. And for the most part, they're in the green, meaning they're meeting (inaudible) performance and schedule goals. There are certain exceptions to that, but by and large, that's been my experience in the six years that I've had this -- this job.

The Congress requires very rigorous oversight by both ODNI as well as DOD on these programs. So they get a lot of governance, and by and large, I think we do pretty well, unless there's going to be some revolution in the federal acquisition regulations or the laws that govern this activity. You know, it's hard to see how we could streamline it much more than we already are.

I think we do pretty well and I think one of the things I'm particularly proud of in this regard is the fact the we've sustained our percentage of about five percent in the national intelligence program for research and technology. Even with the pressure of, you know, what you always have on the now and urgent as opposed to investing in the important in the future.

I think we've done a reasonably good job of that, given all the pressures and (inaudible) of program management these days.

LONG: So what do you think the state of the public-private partnership is?

CLAPPER: It is pretty good, it could always be better. We've certainly had our stresses over the last few years and that -- you know, that's -- again we've had our issues with the private sector and hopefully we will get over that, get past that.

Obviously, a key issue here is encryption, ubiquitous encryption and the impact that has on both law enforcement and national security. And I'm hopeful that some dialogue will take place that we can -- as we always seem to eventually -- find a balance.

LONG: I'm actually surprised that I don't have a question here on encryption. So, perhaps they're saving that for Admiral Rogers or Director Comey. OK.

CLAPPER: Good.

(LAUGHTER)

LONG: But let me give you one that's equally as thorny, if you will. How would you respond to the criticism of some that the intelligence community is sometimes guilty of over-classification? So, say a little bit about our classification system.

CLAPPER: We're guilty.

(LAUGHTER)

Well, we are.

LONG: And what are you doing to work on that?

CLAPPER: Well, I put out a charge to the agency heads. This memo I put out involves four areas of pursuit that I hope they'll undertake. And we're starting to get those back in. I've got an excellent response from CIA yesterday on what we can do to be more transparent, not to over-classify. There's proposals going around, one of which is why don't we just not bother with confidential. That would somewhat simplify the system.

We have embarked on extensive declassification of historical documents. I participated with John Brennan last September at the University of Texas and again last month at Yorba Linda for the Johnson Library and the Nixon Library on the rollout of the declassified presidential daily briefs.

And we're doing a lot more of this than we ever have in the past in terms of declassifying as much as we can. But there's more work to be done here. And at some point, there will need to be, I believe, a fairly fundamental change in the classification system, not just in the I.C. but across the government.

The basic structure is of course born out of a hard copy paper era and the rules we have today really aren't compatible with the technology and the way we conduct our business. So at some point, I think they'll be -- have to be a fundamental change. In the meantime, I'm kind of working, you know, what I can within the confines of the current system.

LONG: So I guess that'll be one of the things on your -- your list of items for the next DNI and the next administration?

CLAPPER: Yeah. I'll wish them luck, too.

(LAUGHTER)

LONG: Recognizing we have a cyber track in our breakout sessions and -- and yes, we'll have Admiral Rogers here tomorrow. Can you talk a little bit about what the community is doing in the cyber arena? And do we have enough in place to really know and track cyber threat vectors, the actors, intentions? Always a hard thing to do.



CLAPPER: Well, it is, and of course, do we have enough? Well, the stock answer is always no. You know, I never met a collection capability I didn't like, you know? It's (inaudible) Rogers sort of thing.

So yes, we could always use more. I think we have a very healthy and have sustained a pretty healthy investment in the National Intelligence Program on intelligence support to cyber, which cuts across all the I.C. components.

I think our -- so I think we're doing reasonably well in, you know, assessing the threat. I think where more work needs to be done of course is in sharing with the private sector and in more ubiquitous, more pervasive sharing of threat data with both private sector companies and private individuals.

And that's kind of a work in progress.

LONG: Speaking of threat, do you see ISIS as an enduring threat?

CLAPPER: Well, ISIS will eventually be suppressed. But I think for some time to come, that we'll have more extremist organizations which will be spawned and which we will have to contend with. And we're going to be in, I think, a perpetual state of suppression for some time to come.

LONG: All right. Let's shift gears a little bit as we are closing, here. What are three things you will tell your successor as far as priorities for the intelligence community?

CLAPPER: Well, I think frame it around what's outlined in the IRTPA, the Intelligence Reform and Terrorism Prevention Act, which kind of lays out in broad terms what the DNI's supposed to do.

As the primary and certainly not the exclusive, but the primary adviser to the president on intelligence, counterintelligence, and security matters, manage the National Intelligence Program and there's a whole set of thoughts I will share with the next DNI on that on its management. And of course, then to try to lead the enterprise.

And so I would probably have under those three broad categories, it is how I'll probably frame the discussion with the next DNI.

LONG: So 54 years, is there anything that still surprises you?

CLAPPER: Not really.

(LAUGHTER)

I mean, there's -- sometimes people surprise me, that's all -- it makes it interesting, I guess. I really can't think of things that, you know, that surprise me necessarily, maybe distress me, concern me, that sort of thing. But no.

LONG: OK. Stumped the DNI.

What aren't you going to finish that you really wanted to as you came into the job six years ago?

CLAPPER: What was the question again?

LONG: What's being left undone?

CLAPPER: Oh. Well, I mean, lots of things are undone because these jobs are -- you know, you're a temporary steward of public trust. You build on the legacy of what you inherited and you'll pass on things to the next -- whoever takes over for me.

And all these things are journeys. It's not like gee, I'm all done with that by close of business Friday. And so there are any number of things that will continue to, I think, draw the attention of the DNI that will need to be worked.

You know, the mantra for me has been which I thought -- I think was the original intent of the 9/11 Commission and the IRTPA was integration. Hopefully, it'll get to the point where maybe we won't have to talk about it very much; it'll just be the default for the community.

But these things are, as you know, are perpetual. And you, you know, sort of gauge I think most people, I -- at least I will, it's a little better than when I started. And I'd like to think it is and hopefully my successor will build on that.

LONG: So you just said the integration word again and one of the questions here is, is the structure of the intelligence community optimum?

CLAPPER: Well, that's a hardy perennial, you know? We Americans have a great proclivity for if we had some ill, some problem - let's reorganize. That'll make it better. Well, the older I've gotten, the less enamored I am of reorganizations.

LONG: We've noticed there have kind of been major shakeups lately.

CLAPPER: I think you're better served to make whatever organizational structure you have, which is always going to be imperfect. New wiring diagrams make people on the top floor happy. But too often, I've seen that people fail to recognize the second and third-order effects, the unintended consequences that you always have to adjust to.

Two of our agencies, CIA and NSA, are going through the throes of pretty substantial reorganizations. And in both cases, my advice to the groups that were studying these reorganizations or contemplating them was that I just recounted my experience. I've done three agency-level reorganizations in my time. I did one at NGA, which worked pretty well, mainly because I was there for almost five years to see it through. And then I did two in the early '90s when I served as director of DIA. The second one was intended to undo the bad effects of the first one.

(LAUGHTER)

LONG: So what's been your biggest career mistake? And what did you learn from it? Speaking of an actual question.

CLAPPER: We don't have enough time for that.

(LAUGHTER)

Next question.

LONG: Next question.

CLAPPER: Too many to enumerate.

LONG: OK. You've talked about intelligence. You've talked about integration. What about information sharing? How are we doing? What's the impact of the program management for information sharing environment? How are we doing with the NT-50s? I mean, just can you talk about information sharing writ large?

CLAPPER: Well, it has many dimensions. Let me start with the one you didn't mention, which is the foreign -- sharing with our foreign partners.

LONG: And our foreign partners, of course.

CLAPPER: I think today it is unprecedented, the degree to which we are sharing with foreign partners, particularly on CT. Now, there's an obvious reason for that. It has a way of -- the perception of the threat, particularly the terrorist threat, has a galvanizing impact on countries. And it does promote more sharing.

I've said before publicly, I think, at some point we're -- I'll probably have both feet in assisted living when it happens, but we'll do away with the NOFORN business with the commonwealth countries, and just perhaps extend dual citizenship privileges and obligations when we're in each other's intelligence footprint.

Because my experience has been, or observation has been that we have just gradually chipped away and chipped away and chipped away at that. And we're doing more and more integrated operations, particularly with the commonwealth, which is a good thing.

I think your question probably goes more specific to domestic. It so happens that today I'm meeting with a so-called non-Title 50 organization. Those are organizations in the government, agencies and departments, that are not formally part of the I.C., but do have intelligence, counter-intelligence and security-related equities. And so we meet regularly with them. We try to be as inclusive as we possibly can.

Similarly, and this is where PM-ISE (Program Manager for the Information Sharing Environment) has come into play, is in fostering greater sharing at the state, local, tribal and private sector level. And we've done a lot there. The instrumentalities I use for that, to help promote that nationally, are the system -- the network of domestic DNI reps that we have, which are 12 of the FBI special agents in charge, or in those cases where it's an assistant director in charge because of the size of the office.

And so we've done a lot there. It's better than it was 15 years ago, but I think there is clearly more to do in that realm.

LONG: What will you do on the first day after you leave this position?

CLAPPER: Sleep.

(LAUGHTER)

LONG: I think Sue -- I think Mrs. Clapper might have some other ideas.

CLAPPER: No, I don't. I'm going to start going to the gym: "two-a-days" at the gym: plan to lose about 15 pounds, and sleep. That's about all I've got in mind right now.

LONG: Well, Jim, thank you very much for your service. I will tell you almost every question in here actually had that at the bottom. After the question, it was thank you for your service.

CLAPPER: Well, thank you.

LONG: We are so fortunate to have you leading our community; for you to have agreed to stay on through this entire administration. And we look forward to your advice to your successor, and we look forward to inviting you back in any capacity. So thank you very much.

A big round of applause.

CLAPPER: Thank you.

(APPLAUSE)

END