Center for Strategic and International Studies

Global Security Forum 2015: Opening Session

Speaker:
John O. Brennan,
Director,
Central Intelligence Agency

Introduction:
John J. Hamre,
President and CEO,
CSIS

Conclusion:
William J. "Bill" Lynn III,
Chief Executive Officer,
Finmeccanica

Location: CSIS, Washington, D.C.

Time: 8:00 a.m. EST
Date: Monday, November 16, 2015

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

JOHN J. HAMRE: Good morning, everybody. Welcome. We're very pleased that you could join us today. We've got police activity down the street, so we've got a lot of people that are delayed. And unfortunately one of them is Bill Lynn, my dear friend Bill, who is our partner – Finmeccanica is our partner for these conferences – and Bill is stuck in traffic. And so he will – he will be here. If there's a chance for him to say a few words later, we'll do that, but we can't hold things up because the director is here.

Before we do public events, we've always – we've done this for two years since we moved in here. More meaningful now after the events in Paris over the weekend. If there's a problem that emerges, I'm going to ask you to follow me. I'm responsible for your safety, and I'm going to have to ask you to follow my directions. The emergency exits are right here in behind me, and we will go out – there's a stairs that goes down to the street. It's right behind this door, but each of the three will lead there. I'd ask you to follow me in – well, my instructions. I am going to spend my time taking care of Director Brennan, but I will also take care of you, too, so.

It's a real privilege to welcome John Brennan. I've had – I've had the privilege of working with John on and off for 20 years. He had – of course, he is the director of the Central Intelligence Agency. I don't know that anyone is better prepared or equipped for this job than John. John joined the agency 35 years ago. And so imagine having someone who is so deeply schooled in the foundation of this critical agency that is at front lines for us every day, and he has been leading these last two years. But this is – he spent five years in the White House before he got there, and so this is a very long time for anyone, and he is doing an exceptional job.

I feared, because of the events of the weekend, that we might not have him this morning. But I'm grateful, John, that you are able to come. I know that he hasn't slept much for the last three days, so we're delighted that he's here. And I want to say will you all please, with your applause, welcome John Brennan? Thank you. (Applause.)

JOHN O. BRENNAN: Thank you very much, John. Thank you for those kind words, as well as for the invitation to invite me to speak here this morning at CSIS and at the Global Security Forum. I had the pleasure of speaking at CSIS when – at is previous residence when I was serving at the White House as assistant to the president for homeland security and counterterrorism, and it's a privilege to come back and to share my thoughts with you this morning on some of the key global challenges that our country faces today.

I also want to take this opportunity to express publicly my deep appreciation to John Hamre, who has led CSIS for nearly 16 years and who is certainly one of the leading lights in the field of national security. After a distinguished government career, John has continued to make important contributions to our national security. And I think I speak for all of us in thanking him for adding such wisdom and value to the public conversation on global issues. Thank you, John, so much. (Applause.)

In many respects, CSIS shares the mission of our intelligence community: to help policymakers identify, understand and, hopefully, successfully address the myriad national

security issues that our nation faces in a dynamic and very dangerous world – a very dangerous world indeed.

My opening remarks this morning are different from those I reviewed and finalized in the early afternoon of last Friday. They are different because our sensibilities and our souls have been jarred once again by the horrific and wanton violence perpetrated upon the innocent in the streets, cafes, and concert halls of the beautiful city of Paris. Our hearts ache for the scores killed and injured in those savage attacks, and our thoughts are with them and their families.

Likewise, our condolences and our thoughts go out to those killed in the crash of the Russian airliner a little over two weeks ago in the Sinai, Egypt.

And while we await confirmation of culpability for those tragedies, they each bear the hallmarks of terrorism carried out by the so-called Islamic State of Iraq and Levant, or ISIL, an organization of murderous sociopaths that carries out its criminal and morally depraved actions under bogus religious pretense. With its roots in al-Qaida in Iraq, and empowered by a large influx of foreign adherents, ISIL over the past several years has swallowed up large swaths of territory in Iraq and Syria, brutally killing thousands upon thousands of men, women and children along the way. Not content to limiting its killing fields to Iraqi and Syrian lands, and to setting up local franchises in other countries of the Middle East, South Asia and Africa, ISIL has developed an external operations agenda that is now implementing – it is implementing with lethal effect.

I am sure we will talk more about ISIL in the question-and-answer session, but let me note that the grave threat posed by the phenomenon of ISIL makes it absolutely imperative that the international community urgently commit to achieve an even greater and unprecedented level of cooperation, collaboration, information-sharing, and joint action in intelligence, in law enforcement, in military operations, and in diplomatic channels. The ISIL threat demands it.

At CIA, we work closely with foreign intelligence security services around the globe to advance our shared counterterrorism goals. Over the course of many years, we have forged broad and deep partnerships with our closest allies in Europe, such as Great Britain, France, and many, many others. These strategic relationships have been instrumental in helping to knit together a transnational architecture that allows counterterrorism officials and experts to work closely together across sovereign borders to disrupt terrorist plans and activities. And while many terrorist operations have been thwarted as a result of strong transnational teamwork, tragically, not all terrorist plans are uncovered in time.

These strategic counterterrorism relationships need to stretch far beyond the traditional transatlantic environment and alliances, which is why we are working closely with so many services in different parts of the world. For instance, we are working very closely with our Egyptian partners, who are working tirelessly to prevent ISIL terrorists from launching attacks that are aimed at derailing Egypt's political reform initiatives and economic development objectives. I reiterated our commitment to strengthening our counterterrorism partnership with Cairo in a call to my Egyptian counterpart just this past weekend. And while Washington and Moscow have significant policy differences on how best to bring the bloodshed in Syria to a

close, I have had several conversations with one of my Russian counterparts over the past several weeks about ways to strengthen U.S.-Russian counterterrorism cooperation, specifically on the ISIL threat.

These relationships are an essential adjunct to diplomacy and military operations. By working with our foreign partners, we enhance global security by helping them tackle challenges that threaten us all. And we benefit from a wider net of collection and from the insights of local services, all of which enhance the intelligence we provide to policymakers.

The fact is, good intelligence – timely, accurate and insightful – is the cornerstone of almost every aspect of national security policy today, from military action to diplomacy to international law enforcement. With good intelligence, our policymakers can better understand the risks, the challenges, as well as the opportunities attendant to key national security issues, which is ever more important given the unprecedentedly complex and overlapping array of major challenges to U.S. and global security that we face today.

The impression one might get from the daily headlines is that the world has become more unstable. And, indeed, the historical record supports that judgment.

In the past three years, there have been more outbreaks of instability than at any time since the collapse of the Soviet Union, matching the rate we saw during decolonization in the 1960s. This has not been a period of protests and government – this has not just been a period of protests and government change, but of violent insurgency, and in particular of breakdowns in many states' ability to govern.

Ongoing conflicts in Syria, Iraq, Ukraine, Yemen, and Libya, and parts of Africa are clear examples. The human toll is reflected in the U.N.'s recent announcement that the number of refugees and internally displaced persons in the world is the highest it has been since World War II. And of course, all of this localized strife gives rise to the persistent threat of international terrorism.

When CIA analysts look for deeper causes of this rising instability, they find nationalistic, sectarian and technological factors that are eroding the structure of the international system. They also see socioeconomic trends, the impact of climate change, and other elements that are cause for concern. And so let me touch upon a few of those this morning.

First, the ideas, institutions and states that have undergirded the post-Cold War system are under significant stress. It is easy to think of this as a phenomenon confined solely to the developing world, and that is certainly where we see states that have actually failed and borders that no longer carry any practical effect, such as the border between Syria and Iraq. But there is considerable stress on governments in even the world's most stable regions.

In Europe, for instance, the migration crisis, sluggish economic growth and a host of other factors have given rise to heightened nationalism, secession movements, and the increasing popularity of political parties on both the far right and far left. Even ideas that were the pillars of

the continent's postwar prosperity, such as economic integration and democracy itself, are being questioned in some quarters.

Across the globe, in both authoritarian and democratic societies, governments are finding it increasingly difficult to meet the demands, realistic or not, of their skeptical and restive populaces. The so-called Arab Spring revolutions were not fought for democracy per se as much as they were fought for relief from regimes that had failed to meet basic standards of governance and civil society. And as we have seen, when people become disillusioned with the powers that be, social media enable them to more quickly and easily form associations that defy the status quo. And in part, that is why the global landscape has been changing at a faster and much more disruptive pace.

How nations respond to these challenges, adapt to them, and evolve will be one of the great plotlines of the 21st century. When I meet with my foreign counterparts – both from friendly and from not-so-friendly governments – I sense a very real apprehension about instability and its various manifestations: terrorism, humanitarian crises, proliferation and so on. Interestingly, I hear these concerns even from officials representing governments whose policies are quite arguably contributing to the problem.

In Europe, anxiety has risen in states along Russia's periphery after Moscow demonstrated its willingness to use military and paramilitary forces in Ukraine. And in the South China Sea, tensions persist as China unilaterally pursues its territorial claims, including actions that rival claimants perceive as violating their sovereignty.

At the same time, the principle of democratic governance is under siege. For the ninth consecutive year, Freedom House in 2014 reported more declines than gains in the quality of democracy worldwide. Worsening ethno-sectarian and socioeconomic strains are eroding democracy, as is the rise of a more sophisticated form of authoritarianism that forgoes brute force and heavy-handed propaganda in favor of media manipulation, ubiquitous surveillance, criminalization of dissent and controlled elections.

Second, the resumption of strong, sustained growth in the wake of the 2008 financial crash and eurozone crisis has been elusive for some of the world's largest economies. Even China's economy, with its seemingly endless potential for growth, is slowing.

In many developing societies, growing pessimism about the prospects for economic advancement is fueling instability. Regions with burgeoning youth populations, such as the Arab World, have been unable to achieve the growth needed to reduce high unemployment rates. Perceptions of growing inequality have resulted in more assertive street politics and populism. At the same time, slower growth has left these nations with fewer resources to devote to economic, humanitarian and peacekeeping assistance to address these challenges.

Mankind's relationship with the natural world is aggravating these problems and is a potential source of crisis itself. Last year was the warmest on record, and this year is on track to be even warmer. Extreme weather, along with public policies affecting food and water supplies, can worsen or create humanitarian crises. Of the most immediate concern, sharply reduced crop

yields in multiple places simultaneously could trigger a shock in food prices with devastating effect, especially in already-fragile regions such as Africa, the Middle East and South Asia. Compromised access to food and water greatly increases the prospect for famine and deadly epidemics.

And finally, the rapid advance of information technology has given rise to an entirely new and wide-open domain for human interaction and progress: the cyber realm. As an intelligence officer, much of my job involves dealing with the unintended consequences of the cyber revolution. For as much as it brings the world together, it also serves the purpose of those who wish us harm. Of greatest concern, the cyber realm gives small groups and even individuals the potential to inflict damage on a scale previously restricted to nation-states. And while states are largely rational actors subject to deterrence, the same does not apply to terrorists and criminals.

Both government and private networks are under constant attack. The Department of Homeland Security reports that more than 640,000 cyber-related incidents affected federal agencies in fiscal year 2014. The massive and prolonged hacking of employee records held by the Office of Personnel Management underscores the intensity of assaults on government IT systems. And I am personally all too familiar with the ease with which miscreant hackers can use social engineering techniques to perpetrate criminal intrusions into personal email accounts, and information technology and communication systems.

Unfortunately, there is every reason to expect cyber intrusions to increase in quantity, cunning and impact. For one thing, the economics of cyberattacks are skewed to favor the attacker. Exploits, or malicious software tools, are easily acquired. In fact, their prices are falling dramatically in some criminal markets – not because of declining demand, but because of an increasingly competitive marketplace. These exploits can be reused on multiple targets, and the likelihood of detection and punishment remains low in most instances.

And while the vast majority of cyberattacks target money, proprietary information and privacy itself, we need to realize that the range of potential targets is much, much greater. We simply cannot discount the very real possibility of attacks against vital infrastructure – utilities, transportation, and other essential underpinnings of modern civilization.

The world has changed dramatically since I first raised my hand and swore an oath of allegiance to the United States government as a 24-year-old, newly-minted CIA officer eager to make a difference in August of 1980. I remember vividly taking a seat at my first desk on the sixth floor of our Langley headquarters, putting my fingers not on the keyboard of a computer but on the keys of an electric typewriter, which was quite high-tech at the time. Thirty-five years later, our lives – as well as our fingers – are inextricably linked to the cyber realm, the new digital frontier where most human interactions, transactions and communications take place. And while that digital environment holds tremendous potential and opportunity for the further advancement of humanity, our increasing dependence on it brings obvious risks and challenges.

To deal with those risks and challenges, reactive strategies are insufficient. There has to be systemic learning informed by constant information sharing, so that one organization's

detection becomes another's prevention. In other words, countering cyber threats is very much a team effort.

And a crucial point to bear in mind is that about 85 percent of the World Wide Web's critical infrastructure is held by the private sector. This is a privately owned and operated environment in which the rules remain uncertain at best.

A number of federal efforts in recent years have promoted the sharing of cyber threat information between the private sector and government. DHS and FBI, for example, have programs to share cyber threat information with a broad community of industry stakeholders. We should be sharing a lot more information than we do as a nation, but programmatic, technical and legal challenges – as well as concerns about privacy and the role of government – have hampered progress.

Congress over the past few years has tried, so far without success, to pass laws addressing the need for comprehensive cyber policy, especially on information sharing. The fact is, 20th century laws cannot effectively deal with 21st century threats. Within the past few weeks, the Senate passed the Cybersecurity Information Sharing Act, which is roughly similar to two bills passed in the House. And we may see a conference bill by early next year, which would be a very important step forward.

And as our country deals with this issue, and specifically the security and privacy concerns that revolve around information sharing, it is important to note that security and privacy are certainly not mutually exclusive. The benefits of improved information sharing can be achieved in a manner that protects privacy and civil liberties. My hope is that America – ideally, along with our allies and partners – can eventually adopt a comprehensive legal and operational approach to this threat without being forced to it by a catastrophic cyberattack, in the same way that 9/11 forced our country to integrate its national security assets in a more rational and effective way against terrorism.

Shortly after I returned to the agency some two-and-a-half years ago, I started to consider what we could do to ensure that CIA is well-prepared for both the opportunities and the challenges of the future, and the digital world stood out as an area that required special and immediate attention. When I asked a group of our senior officers last fall to ponder the agency's future and come back with a strategic plan, they agreed that we had to do a much better job of embracing and leveraging the digital revolution. Consequently, one of the pillars of our modernization program that we launched this past March was the addition of a fifth directorate as part of the biggest change to CIA's structure in five decades: the Directorate of Digital Innovation.

This new directorate is at the center of the agency's effort to hasten the adoption of digital solutions into every aspect of our work. It is responsible for accelerating the integration of our digital and cyber capabilities across all our mission areas – espionage, all-source analysis, open-source intelligence and covert action. Multiple elements of the agency in the past have responded to the challenges of the digital era. But if we are to excel in the wired world, we must place our activities and operations in the digital domain at the very center of all of our endeavors.

Our new digital directorate was launched last month, and we expect it to contribute enormously to every facet of our global mission. Alongside our partners across the intelligence community, we at CIA will be more capable and effective in safeguarding our country from the full range of threats we face beyond and within our borders.

And let me conclude by saying what I have always – what I always say to each new class of agency officers to whom I administer the oath of office every month at our headquarters in Langley. I have the absolutely best job in the world, bar none, because each day I work with some of the most dedicated, talented, courageous and patriotic individuals this country has to offer. And in light of the nature and scope of the national security challenges I just highlighted, the need for the contributions of these individuals at CIA has never been greater.

Thank you, and I look forward to taking your questions. (Applause.)

MR. HAMRE: John, thank you very much. I think we all can see why we're so grateful that you're serving at such a crucial time. You're a wonderful leader.

Let me just say we're going to take some questions. I'm going to moderate this a bit. No lectures. I'm going to cut you off – if I get a lecture, you're going to get a humiliating response from me. So nobody came here to listen to you with your thoughts; they want to hear his.

Josh, we're going to start with you.

Q: Good morning. My name is Josh Rogin. I'm a reporter with Bloomberg View.

Director Brennan, thank you for your time today and thank you for your service.

The Paris attacks, the blame, of course, lies primarily at the feet of the terrorists. But I think I give voice to the question a lot of us have in this room and around the country when I ask: How was this allowed to happen? We're talking about an attack that involved dozens of people communicating from multiple countries, planning for perhaps weeks or months, and yet the world's leading intelligence agencies didn't even catch a whiff of it as far as we're to understand. Is that right? What went wrong? And what needs to be done now to make sure this never happens again? Thank you.

MR. BRENNAN: Well, first of all, as I mentioned in my remarks, many of these terrorist operations are uncovered and thwarted before they're able to be carried out. And when I think about what happened in Paris, clearly there was a(n) effort that underway for quite some time, that was fairly sophisticated because of the nature of the attacks in terms of their simultaneous nature.

We work very, very closely with our French partners. I have an exceptionally strong relationship with the heads of the external and internal services. A lot of our partners right now in Europe are facing a lot of challenges in terms of the numbers of individuals who have traveled

to Syria and Iraq and back again, and so their ability to monitor and surveil these individuals is under strain.

Now, I know the French are going to be looking at what might have slipped through the cracks. But I can tell you that it's not a surprise that this attack was carried out from the standpoint of we did have strategic warning. We knew that these plans or plotting by ISIL was underway, looking at Europe in particular as the venue for carrying out these attacks. But I must say that there has been a significant increase in the operational security of a number of these operatives and terrorist networks as they have gone to school on what it is that they need to do in order to keep their activities concealed from the authorities.

And as I mentioned, there are a lot of technological capabilities that are available right now that make it exceptionally difficult, both technically as well as legally, for intelligence and security services to have the insight they need to uncover it. And I do think this is a time for particularly Europe, as well as here in the United States, for us to take a look and see whether or not there have been some inadvertent or intentional gaps that have been created in the ability of intelligence and security services to protect the people that they are asked to serve. And in the past several years because of a number of unauthorized disclosures and a lot of handwringing over the government's role in the effort to try to uncover these terrorists, there have been some policy and legal and other actions that are taken that make our ability collectively internationally to find these terrorists much more challenging. And I do hope that this is going to be a wake-up call, particularly in areas of Europe where I think there has been a misrepresentation of what the intelligence security services are doing by some quarters that are designed to undercut those capabilities.

MR. HAMRE: Mitzi?

Q: Thank you. I'm Mitzi Wertheim with the Naval Postgraduate School.

You used a very important phrase called systemic learning. I'm stuck by the inhibition of asking questions that exist. I've been with the Defense Department for almost 40 years. And Apple has a really interesting technique. Everyone who goes to Apple is told: If you don't know, ask. We all learn together. And I urge that to you and every leader in government because the volume –

MR. HAMRE: Question, Mitzi. Question.

Q: How would you do that? (Laughter.)

MR. BRENNAN: Well, I very intentionally used the term systematic learning. The world is changing before our eyes. As I mentioned, in the last 35 years, since I've been involved in national security, the technological revolution has totally, totally transformed not just the intelligence work, but our daily lives. And so the people who are growing up today, they're growing up with technology in their hands. But that technology has tremendous, tremendous implications. As I said, it can be done for good or it can be done for harm, in terms of the use of that technology.

And I do think, you're right, as a – as a society, as a government, we need to make sure that we're not making faulty assumptions because of what the past has told us. We need to make sure that we understand. And this is why we created this Directorate of Digital Innovation. I want to make sure that we and CIA understand all of the implications of that digital environment. What does it mean if I want to have my officers operate clandestinely and covertly overseas, when everywhere we go these days we pick up digital dust – whether we go to a Starbucks and pay with our credit card, rent a car, go to a bank, an ATM, whatever. We create a forensic history. People who are joining the agency today have forensic history already.

And so I want to make sure that we're able to operate the way we always have in terms of our ability to collect intelligence that is necessary for this national security in this new digital world. So systemic means, to me, across all the various realms that we operate within, and particularly in that cyber realm.

MR. HAMRE: Margaret Warner.

Q: Good morning, Mr. Director. Margaret Warner from the PBS "NewsHour."

If you look at just who was involved in this attack, it really looks like the exact same connection between Brussels and France – you know, whether it's ease of travel, unmonitored, whether it's where they get their weapons and how they go back and forth. And I'm just wondering after those Charlie Hebdo attacks, what kind of changes did they make in that relationship? And in retrospect, what more could they have done?

MR. BRENNAN: Well, I will defer to my French partners to talk about the types of things that they are doing and that they did since the Charlie Hebdo attack. But as you point out, the plot that was uncovered and disrupted in Belgium earlier this year has all the similar types of hallmarks that the attack against Paris had in terms of individuals that were directed to carry out these attacks. We know that there are smuggling networks inside in Europe, not just in terms of human traffickers.

But the stocks that were overrun in the 1990s in Eastern Europe as far as all of the AKs and other things, I think there is an active black market that a lot of these criminal elements will be able to take advantage of. So when I look at the interaction between the various countries in Europe and the ease with which, because of Schengen and other things, you can travel across borders, it makes those borders quite porous in many respects, which means that the challenge for the French as well as other security intelligence services becomes that much more daunting.

And I do think part of the issue is that there is an overwhelming number now of cases that they need to pursue. I was just reading in the press this morning that Prime Minister Cameron announced that there's going to be an additional 1,900 British intelligence and security officers that will go to MI5, MI6, and GCHQ because of the need to make sure you have the experts to be able to deal with these issues, and so that we're not limited in terms of who we can look at more closely or who we can follow. So I think a number of European countries are probably going to

take note of what happened in Paris and see what they can do to boost not just their capabilities, but their resources.

Q: (Off mic) – is the U.S. going to do the same – the same?

MR. BRENNAN: I think the U.S. has significantly increased our resources, certainly since 9/11. But every day we are constantly evolving. To me, it's a continuous improvement process and with systematic learning. So we are working very closely with our French partners now to understand exactly some of the mechanisms and techniques that these operatives used. But as I said, their operational security really is quite strong.

Q: Yes, indeed. Thank you so much for your comments today.

Given the very large number of European Union citizens who have, as I said, traveled to the conflict region and been involved with ISIS activities, and the impossibility of sealing Europe's borders against these vast tidal waves of people flows, should we regard this type of attack as a one-off event, or do we have to contemplate the terrible possibility that this could indeed be a new normal?

MR. BRENNAN: I certainly would not consider it a one-off event. It is clear to me that ISIL has an external agenda, that they are determined to carry out these types of attacks. This is not something that was done in a matter of days. This was something that was deliberately and carefully planned over the course, I think, of several months, in terms of making sure that they had the operatives, the weapons, the explosives, the suicide belts. And so I would anticipate that this is not the only operation that ISIL has in the pipeline. And security intelligence services right now in Europe and other places are working feverishly to see what else they can do in terms of uncovering it.

So I do believe that this is something that we're going to have to deal with for quite some time. The challenge inside of Syria and Iraq right now in dealing with ISIL is something that is going to, I think, take quite a bit of time yet to be able to destroy ISIL. But it's not going to content itself with violence inside of the Syria and Iraqi borders. It's going to be looking abroad. We see what happened recently in Lebanon as well, in terms of attack in southern Beirut which, again, bears all the hallmarks of ISIL. So it's not just Europe. I think we here in the United States also have to be obviously quite vigilant.

Q: Ron Taylor with the George Washington University Center of Cyber and Homeland Security.

My question is, given that the concert hall, the restaurant were in the private sector domain, many private sector organizations over the recent years have increased their awareness that they have a security role. So you see more chief security officers, more vice presidents of security. So you foresee kind of a moving – a movement toward more cooperation with the private sector and, in particular, those security components within the private sector that could play a role in this kind of fight?

MR. BRENNAN: Well, certainly by definition in the cyber realm there has to be that partnership. As I mentioned, 85 percent of the World Wide Web is owned and operated by the private sector. And so what we need to do as a country, not just as our country but other countries, we need to find that type of relationship with the private sector that is built on mutual confidence and trust and understanding in terms of what the respective roles and responsibilities are.

I think we still have a ways to go in that area. There is reluctance on the part of many within the private sector to share information about what some of the internal operations and maybe penetrations of their systems because of concerns that it could affect their stock prices, or whatever. I think we need to find the mechanisms where there's going to be confidence on both sides that information can be shared without having the untoward implications that I think some fear.

But also on just the physical security side, as was pointed out, it was outside of a soccer stadium. There is very close cooperation here in the United States between law enforcement, intelligence security officials, homeland security with major sports franchises, teams, organizations, making sure that those venues are strong in terms of their precautions they take. The Homeland Security Department has done a very good job of reaching out to state and locals, and making sure that then the extension to the private sector.

This is not something that the government itself can handle. I think it shows that, you know, the United States is a big country. Europe is a big continent. And there are not enough resources to be able to anoint everybody to be a government intelligence security or law enforcement officer. And there needs to be responsibilities on the part of individual actors in the private sector, as well as individual citizens. I think this is unfortunately a feature of our time.

Q: Good morning, sir. Kylie Morris from Britain's Channel 4 News.

Can I ask, there's been a lot of discussion about whether or not the U.S. has underestimated the threat from the Islamic State, perhaps focusing rather on issues of containment in the Middle East, in Iraq, in Syria, and even on the threat posed by lone wolves, but not looking at the capacity of the organization to stage the kinds of attacks that we've in Paris and Beirut?

MR. BRENNAN: I don't think we are underestimating at all the capabilities of ISIL. Its growth over the last several years in particular – but as you know, that it had its roots in al-Qaida in Iraq. It was, you know, pretty much decimated when U.S. forces were there in Iraq. It had maybe 700-or-so adherents left. And then it grew quite a bit in the last several years, when it split then from al-Qaida in Syria, and set up its own organization.

There is a real effort on the part of the United States and coalition countries to contain its spread inside of Iraq and Syria. And I think there has been a containment of that momentum. We saw it was rolling along in Iraq and other areas. It trades some territory in Syria now and again, but it has not had that type of momentum inside of those two countries. Which is why I

think they are looking abroad now to have these spectacular attacks, because what they want to do is to future their narrative about the caliphate which is growing and is successful.

And I think one of the most important things for us to do is to be able to take away any type of momentum or success, both in the area as well as beyond. But as I said, there have been a number of successes that have prevented ISIL from moving people, moving material and other things to carry out attacks. But unfortunately, this attack several days ago in Paris just shows what devastating impact it can have, because their agenda is to kill, pure and simple.

As I referred to them as murderous sociopaths. They have this sort of nihilistic sort of approach that they're just trying to kill as many people – you know, young children, whatever. It doesn't matter to them. It's a warped – it's a twisted mentality. And that's why we have to do everything we can as urgently as we can, in my view, to contain the growth inside of the Middle East, but also beyond.

Q: Peter Armpree (ph), analyst and former diplomat.

You burn a Jordanian pilot, you get Jordanian airplanes over the Islamic State. You attack Paris, you get airplanes in the sky over Al-Raqqa. As one who may occasionally be privy to the internal dialogue of the caliphate, can you shed any light on the logic of pissing off yet another country and getting bombers over your territory? And secondly, is there any chance that they will start playing games in Israel, which is guaranteed to deliver plenty of bombers over their territory?

MR. BRENNAN: I don't understand your first part – the first part of your question. But I think it is incumbent certainly on those governments that have particularly been affected by the scourge of ISIL's terrorism to be able to respond and try to prevent follow-on attacks. And there have been efforts on the part of coalition partners as well as the United States to make sure you go to the source of the terrorism because we know that in Syria, in Raqqa, that's the area where ISIL really has the base for its external operations activities. And so what we need to be able to do is to address ISIL's external agenda not just as it is able to put operatives in other countries, but also at the source of it.

And Israel is in a very challenging and dangerous neighborhood. It is something that, you know, we are looking at very closely in terms of what is the impact on ISIL not just on Syria, Iraq, Jordan, but also Lebanon, Israel and those areas. So again, this is something that we're going to have to deal with in the coming months and years, I fear. So what we need to do is not to assume that anybody or any country is immune from ISIL's touch.

Q: Good morning. Hamid Lalu (ph), Operational Culture Center at MCU (sp), analyst.

ISIL has probably been infiltrated by many intel services from all over the world since it's an overt organization, versus al-Qaida that is covert. And since these inter-entities don't necessarily work together given their classification, do you think it's time to review the way this intel work together? And secondly, you use the term sociopath. Do you think that will take

away actually their rational mode of operations, because they seem to know what they are doing and they are quite efficient in their work? Are Baathists behind this?

MR. BRENNAN: As far as intelligence agencies around the world working together, this is challenging because there are multiple agencies and organizations in individual countries, each with their own authorities, each operating under certain types of legal parameters. And then what you need to be able to do is to be able to interoperate as effectively as possible. I always use the term about the importance of systems engineering.

We here in the United States, we have many federal departments and agencies, as well as state and local, city organizations – police departments and others. Trying to create that architecture where you can move information and data at the speed of light, taking into account the different types of limitations, requirements, responsibilities, and authorities is really quite a challenge. I think we've done a great job here in the United States over the last 10 or 15 years. I think we still have a ways to go.

But creating – extending that architecture then internationally, when you have so many different organizations around the world, we are still working through that. And I do believe that it is something that we're going to make further progress on. Technology is there. But making sure that we're able to handle information while at the same time respecting privacy rights, civil liberties, I think this is one of the challenges in terms of how do you balance all of that.

And as far as sociopaths, sociopaths can carry out any number of acts of violence. It doesn't mean that they are rational. It means that they are just opposed to civil society, law and order, and resist the recognized authorities and system of governance that we have. So again, I think that the ISIL adherents are misguided. Unfortunately, the narrative that comes out of ISIL in Syria and Iraq, they're making great use of YouTube and various social media as a way to attract people under the false banner of religion. And that's what it is. It's a false banner.

Q: Sergei Kastei (ph), Financial (University of ?) Moscow, Russia.

May I ask two quick questions?

MR. HAMRE: One question.

Q: OK. My question is, how do you feel about prospect of cooperation with Russia from your talks with international colleagues? Thanks. Especially in light of sanctions, which are still in place?

MR. BRENNAN: My conversations with my Russian counterpart, which has taken place a number of times over the last year and, as I said, including over the last several weeks after Russian military forces found their way into Syria. And these talks focus on what it is that we can do together to try to prevent the flow of individuals into and out of that theater of operations. There are over 2,000, maybe 3,000, Russian nationals that have come down from the Caucuses, from Chechnya, Dagestan, and other areas, into the Syria-Iraq area. There are a number of individuals, Shishani, who are senior officials within ISIL.

So it's a very real concern to the Russians. And what we need to do is be able to help Russia prevent the flow of terrorists inside of their territory that are maybe destined to try to carry out some terrorist attacks. So we've been exchanging information. I think it needs to be enhanced. But I am determined to continue to work with my Russian counterparts because of the importance that I think we each can bring to this issue in terms of our insights, our information, our data, and sharing it.

We worked very closely with the Russians in the Sochi Olympics, and I think they very greatly valued the support we provided, the information we provided. I want to continue to do that, again, irrespective of disagreements of policy over Syria. I am determined to work with other countries' services the best I can to be able to prevent successful terrorist attacks.

MR. HAMRE: Stefan.

Q: Thank you. Stefan Kornelius, Süddeutsche Zeitung from Munich.

What's your recommendation on the borders and Schengen? Would you now say let's implement stricter external border controls and even close down the Schengen system for a while?

MR. BRENNAN: One of the things that I think we have to keep in mind is that what we don't want to do is to have these terrorists succeed in taking away the freedoms and liberties that we pride ourselves on, whether it be here in the United States or in Europe. And I know that there is a rush by some to say that borders should be closed, we should isolate ourselves. That is inconsistent with what I think our societies have been founded on over the last several hundreds of years.

And so what we need to do, though, is be mindful of the risks associated with the individuals that are flowing and to make sure we're taking the appropriate steps to vet and to understand exactly who they might be. But I don't think what we want to do is to just hermetically seal our borders because, again, that is not something that is sustainable from a social, cultural, trade, economic, political standpoint. Again, I just think that we have to take into account what has happened recently and how ISIL can try to take advantage of some of these flows, and what can we do to be able to optimize our confidence that we're able to filter our those individuals that are trying to do us harm.

Q: Zach Biggs with Jane's.

Given that these attacks seem to happen sporadically, should the public accept that this sort of coordinated attack is inevitable to some degree – that it can't be entirely prevented, despite the fact that a number of attacks are prevented every year?

MR. BRENNAN: I would never say that attacks are inevitable. We work tirelessly 24/7, around the clock, around the globe in order to prevent attacks from taking place. And our goal is to prevent every single one of them from taking place. So I don't have a sense of inevitability.

If there is a sense of inevitability, then I think that was – that would almost undermine the commitment of individuals who are working on this.

But I do think it's inevitable that ISIL and other terrorist groups are going to continue to try and to attempt to carry out these attacks. That is an inevitability for at least as far as the eye can see. But to me, it's not inevitable that they're going to succeed.

MR. HAMRE: I have to get the director out of here. I promised that he would be able to leave here by five-to, and I want you to – don't you feel reassured to have a man of this character and intellect who's leading us right now? Would you please just thank him with your applause? (Applause.)

I'm now going to turn over to Bill Lynn, my partner from Finmeccanica. He's going to say a few words for your further guidance here, and I'm going to take the secretary out.

WILLIAM J. "BILL" LYNN III: Thanks very much, John. Was terrific to hear Director Brennan, and I think it a great way to start this conference.

This is the sixth year that Finmeccanica and DRS Technologies has sponsored this conference. As you see by the audience going all the way back to the windows, it gets bigger every year. I think that's a tribute to CSIS.

The panels that you're going to see this afternoon reflect the deep bench of talent that CSIS has and their ability to attract outside experts. You'll see an incredible variety of topics covering the full gamut of global security challenges, and ending with an interview that – or a moderated discussion that John Hamre's going to lead with Henry Kissinger.

This is – I just want to close and thank everybody, just recognize John Hamre's leadership here. He's been at CSIS now I think at little bit more than 15 years. He had a tremendous career in government, starting at CBO, going through the Senate, and then into the most senior positions of the Department of Defense. And he still chairs the Defense Policy Board at DOD, contributing his leadership there. But his real mark, I think, has been to build this institution physically in this wonderful facility that he raised the money and designed, as well and more importantly the intellectual leadership that he demonstrates in this community. And he's able to cross partisan and political boundaries in an – in an era when that's become increasingly difficult. So I want to recognize John Hamre and CSIS for their leadership. (Applause.)

The forum will reconvene at 9:30, in about 35 minutes. They need to reset the building and the rooms for the panels. Look in your agenda here and pick. There will be, I think, three panels starting at 9:30 and then a second set later in the morning. So at this point, you can fight your way through to the coffee. (Laughter.) Thank you. (Applause.)

(END)