THE BROOKINGS INSTITUTION
CENTER FOR EAST ASIA POLICY STUDIES

ASIA TRANSNATIONAL THREATS FORUM: COUNTERTERRORISM IN ASIA

The Brookings Institution
Falk Auditorium
Tuesday, December 4, 2018
Washington, D.C.

[Transcript prepared from an audio recording]
* * * * *
ANDERSON COURT REPORTING
1800 Diagonal Road, Suite 600 Alexandria, VA 22314
Phone (703) 519-7180 Fax (703) 519-7190

PARTICIPANTS:

Welcome Remarks:

JUNG H. PAK
Senior Fellow and SK-Korea Foundation Chair in
Korea Studies, Center for East Asia Policy Studies, The Brookings Institution

Keynote Address:

YEONG GI MUN
Chief, National Counter-Terrorism Center
Office for Government Policy Coordination
Prime Minister's Secretariat, Republic of Korea

Counterterrorism in East Asia:

JOSHUA GELTZER, Moderator
Visiting Professor of Law, Georgetown University Law Center

AUDREY KURTH CRONIN
Professor, School of International Service, American University

MAYUKO HORI
Chief Officer, Counter Terrorism Unit,
International Safety and Security Cooperation Division
Ministry of Foreign Affairs of Japan

SAMM SACKS
Cybersecurity Policy and China Digital Economy Fellow, New America

Implications of Counterterrorism Policies:

JEFFREY FELTMAN, Moderator
Visiting Fellow, Foreign Policy, The Brookings Institution

ZACHARY ABUZA
Professor, National War College

JAMES BAKER
Visiting Fellow, Governance Studies, The Brookings Institution

JI-HYANG JANG
Senior Fellow, Asan Institute for Policy Studies

* * * * *

P R O C E E D I N G S

MS. PAK: Welcome to Brookings and thank you for being here. This is the event Counterterrorism in Asia. The Olympics last—earlier this year hosted by South Korea, and the next two Olympics will be in Tokyo and in Beijing, have really highlighted the issues of terrorism in East Asia. We thought this was a good opportunity to bring—to look at this issue in depth with regional and U.S. perspectives.

Today we have an all-star lineup of global and regional experts on counterterrorism and terrorism in East Asia as well as the implications for global governance. So, we'll address all of these issues in two panels today.

It is my pleasure that Mr. Mun Yeong Gi, who is the chief of the National Counterterrorism Center of the Republic of Korea has joined us and agreed to give our keynote speech today. He also serves as a secretary general of the National Counterterrorism Commission and has contributed to the establishment and development of the national guidance on counterterrorism activities.

Mr. Mun holds responsibility and authority for issuing the national terror alert as well as organizing the overall national CT activities and coordinating roles and functions of relevant agencies in South Korea.

As head of the counterterrorism headquarters for the Pyeongchang Olympic games, Mr. Mun has led the Security Control Room, International Intelligence Cooperation Office, immigration control teams on the ground, and secured the safe and successful Olympics in cooperation with the VIP Security Control Center as well as the management task force for North Korean participation.

Mr. Mun has served as the commander and staff of the special operations forces until he retired as a deputy commander of the Special Operations Command in South Korea.

Mr. Mun has served in the Iraq war and in East Timor and has carried out numerous joint operations, and he is currently working on his Ph.D. in his spare time at the Kyungnam Graduate School. So please welcome Mr. Mun Yeong Gi from South Korea. Thank you.

MR. MUN: Yes, good morning. Thank you for your generous interactions. I'm Yeong Gi Mun, the chief of National Counterterrorism Center of Republic of Korea.

First I wish to extend my deep appreciation to Dr. Jung and the other members of Brookings Institution. This is my great honor to deliver keynote address before the most renown experts.

Today I'd like to share with you the lessons learned from the counterterrorism activities during the Pyeongchang Olympic games. Let me briefly highlight the counterterrorism effort in Korea. Prior to 1980s, South Korea took reactive approaches when it comes down to each counterterrorism measures reacting to the terrorists from North Korea. Many of you remember the Blue House raid in 1968 and the Rangoon bombing in 1983, the primary example of this approach. The Korean government has been responding to these kind of North Korea's provocation with the Integrated Defense System. However, our counterterrorism effort has been substantially intensified in the 1980s since South Korea hosted two major international event, '86 Asian Games and '88 Seoul Olympics.

Since then the national counterterrorism guidance was established by the executive order. Accordingly, national counterterrorism effort has been expanded to be able to deal with the range of threat posed by international terrorists. After 9/11 and the Paris devastating terror attack in 2015, the government established the terror prevention law in March 2016. KNCCT was organized, and I became the first chief of the Center. These days new terrorist threats are looming on the horizon of South Korea.

For instance, we have over two million foreigners, increasing number of refugees, and multi-ethnic families raising new security concerns. Currently the Korean government is monitoring around 50 suspects identified as terrorism risks. With all of this experience and effort, the terrorism-related circumstances have been successfully controlled. Also, we have strict gun control and explosive policies compared to most of the other countries. Thus, South Korea is considered as one of the safest countries in the world, despite ongoing building tensions with North Korea.

Now, I'd like to talk to our preparation activity before the Olympic and the security activities during the

Olympics. North Korea carried out six nuclear tests in September 2017. The North also launch the ICBM Hwasang-12 three months before the Olympics. As a result, many countries and media raised serious concern about the safety in Korean Peninsula to just release that his security concern invited the old key actors related to the Olympics for security briefing. Hundreds of people, including national delegate, media, and government agent attended the two-day meetings in which we openly discussed potential security concern and countermeasures, and so all the participants were determined to be there and we learn that the active flow of information was crucial.

Next I'd like to share how we developed the counterterrorism plan for the Olympics. There are three different phase in part. The establishment of counterterrorism headquarters year-and-a-half prior to Olympics was first phase. In February 2017, one year before the game, the headquarters held pretest event in order to identify potential threat and risks. We developed basic security plan based on the results of those tests. We were able to recognize potential vulnerabilities.

In the second phase, the three months before the Olympics, we held the final drill. All agencies rehearsed the security plan to prepare for possible terrorist attacks. During the last phase, 50 days before the game started, we set up 18 Security Command Center for all venues and key facilities. We opened the old Social Security Control room and activated the on-site safety system.

During the opening ceremony rehearsal, we tested all counterterrorism measures and the necessary equipment, transportation for spectators, and the traffic-control system was searched. The counterterrorism headquarters carried out the three months major drills for better cooperation and teamwork among governmental agencies. After each drill, the headquarters revealed the results to improve the procedures. The Security Control Room was (inaudible) 24 hours to monitor security measures throughout the Olympics. It was also monitoring the security situation of the 18 Vanhoose and Etholate villages. It maintained the realtime communication with the subunit through daily update on counterterror activities and the other security matters.

One of most impressive counterterrorism aspect was the undercover armed forces operations. A Special

Counterterrorism Unit was stationed outside the Vanhoose to ensure all-time security. Undercover SWAT Team and QRFs operated the facility to immediately respond to the emergency situation. High tech security systems such as intelligent CCTVs and facial recognition devices also contributed to the public safety.

Our prevention activities started several years ago. Registration of terror-related suspects was one of the initial steps. In April 2017, the Ministry of Justice ratified the Advance Passenger Information system called API. This program was soon implemented 168 airport in 45 major countries. The API allow passenger data to be shared across the governmental department to prevent the potential terrorist suspect from attempting to enter the country. The government had updated their list of 36,000 suspect with the cooperation of foreign intelligence agencies. This updated list enabled us to successfully identify one suspect who enter the South Korea under different name. This was possible because of the close relationship with the foreign intelligence agencies.

We have expanded the number of Olympic international intelligence cooperation participating countries and agencies. The number 34 countries and 52 intelligence agencies. This was the largest international intel operation in our history. In particular, the CIA analytic tools and techniques to identify vulnerability at our facilities and FBI provided additional information on foreign terrorist suspect. Thankfully, we successfully identified fourteen terrorist suspect among 19,000 ID card applicants during the verification process.

There are lessons learned during the Olympics. First, we realized that we should have scheduled things earlier to provide sufficient time and research to educate and train our 15,000 volunteers. Extreme weather made the security checks longer than what we originally expected. There are also malfunctions of our equipment. We realized the importance of clear communication. A coherent policy implementation was a very challenging task. For example, if I categorize the tumbler as restricted items, the souvenir shop at the venue were selling them at the same time.

Lastly, I'd like to share few future challenges, not just restricted to the Olympics and international games,

but rather in a general sense. Tomorrow, a single terrorist can cause far more shocks and fear than 9/11, not good. And cyberspace became their playground and the artificial intelligence would be their toys. We might not be able to identify any indications. As you know, there are various indications during 9/11. Increasing number of terrorists are taking advantage of the ubiquity and anonymity of the cyberspace. This make it impossible for us to prevent all (inaudible).

Next the cultural differences along with the language barriers were another challenging aspect. Just like the same, I was in Kashmir and Istemal, Iraq and Afghanistan regions. Plus vertical and horizontal intelligence sharing are required in timely manner.

Next in conclusion, thanks to the international intelligence community, I'd like to call our Olympics as a 3 Zero games. There are no crimes and no absent athletes.

I'd like to thank every one of you for giving me your undivided attention and for your precious time. Thank you once again for having me here today. Thank you. If you have any question, please -- I'll do my best to answer them, and I want to speak through Korean interpreter. Thank you. Yes, please, yes, sir.

MR. TAYLOR: Terence Taylor from the International Council for Life Sciences here in Washington, D.C. Sir, you mentioned towards the --

MR. MUN: Just a minute, please. Yes. Go ahead, please.

MR. TAYLOR: You touched on some scientific and technical developments towards the end of your remarks in looking ahead. Probably one of the characteristics terrorists can exploit is surprise, both in the weapons and equipment and so on they might use and of course for the place and target of the attacks. A surprise is very much in the hands of a terrorist. I wonder what -- in looking ahead at these scientific and technical developments, what concerns you most amongst those developments. You touched on artificial intelligence and cyber, but other perhaps less commonly used techniques such as the use of chemicals at Kuala Lumpur, for example, two years ago against a current North Korean target. So what concerns you most in the scientific and technical development? Thank you.

MR. MUN: (Through interpreter) Well, thank you. Maybe you are from a military as well. In our military, we have a saying the Confucius has some advantages -- operatives have advantages, they can choose their own time, own place, and their means. However, the defense cannot choose any of these, of course, because we do not know when the attack will take place. As such whenever there is an operation that takes place in a regular war, intelligence becomes very important. You have to know what may happen and you assume or -- you give probabilities to certain activities that may take place and then that's where you commit the most of your resources. Otherwise you have to save your assets, right? Although terrorism is not the same as regular warfare, it's important that we have to focus our abilities and assets on our best intelligence. As to the future challenges, intelligence itself. Once we have indications, even if the intelligence itself is not 100 percent reliable, and once we have these indications, we act upon those. The way we act on it is more of a preventive nature. Once we have an indication, we commit our assets and then prevent what may be brewing, and that's our best defense. I hope that was enough.

MR. FELTMAN: Thank you very much for your remarks. My name is Jeff Feltman. I'm here at Brookings, but until recently I was the U.N. undersecretary-general for political affairs, and I had the honor to accompany Antonio Guterres, the secretary-general to the opening ceremony of the Pyeongchang Olympics. My first comment is simply to say congratulations. For those of us who were there, it really was very, very smooth; very, very organized. It's clear there was lots of security, but it was not disruptive to the ability to participate and enjoy the opening ceremony, so congratulations for all this work.

When I was at the U.N., two of the hats I wore were -- for five of the six years I was there were related to counterterrorism. I was the head of the Counterterrorism Implementation Task Force, which is a coordinating body inside the U.N. on counterterrorism issues and I was the executive director of the U.N. Counterterrorism Center, which was a capacity and technical assistance small unit inside the U.N. to try to help countries implement Security Council resolutions related to terrorism. One of the sort of frustrating aspects of all of this working in the U.N. context on counterterrorism was the difficulty in encouraging countries to share their information, to share their experiences, their lessons learned more broadly.

I was wondering given the experience you had with the Olympics, how are you sharing this more broadly

with other countries that would be hosting major international events?

MR. MUN: (Through interpreter) thank you for your question. To be honest Korea we have been able to come this far with the help of the international community and we are acutely aware of the help that we have received from outside, and this goes to the civilians as well as the government personnel. So I think we are trying very hard to be a responsible international member. We because have received many help from overseas before, we are trying to also reach out and to provide help to others whenever we can. As such outreach is an important part of our government activities. Earlier there was a mention of API, and this API cannot be a success without the help of each individual members. When it comes to terror -- possible terrorist list of suspects, we do not have all that many people on our list actually, but we do provide this list to other countries. Also for certain known terrorists, we try to arrest them and put them through the justice system. All these things, we do it in conjunction with the international community. Of course we have the special situation where we have to deal with the threats from North Korea, and North Korean provocations are -- we think of it as terrorism as well. So from the North Koreans, we have a constant fear of terrorist activities that may take place. Also we have people coming in from outside, overseas, who may harbor terroristic thoughts. As such, it's important for us to help out and also receive help from the international community. Thank you.

MR. MAXWELL: David Maxwell, Foundation for Defense of Democracies. Thank you for your presentation. What do you attribute your success to, is it deterring the terrorist attack or good intelligence and prevention? If deterrence is a factor in your success, what were the specific deterrence measures that you can share with us that you deemed as successful?

MR. MUN: (Through interpreter) Well, fundamentals are important. In the 60 years of our history, we have been in constant conflicts with North Korea. So, whenever our agencies, especially intelligence agencies, get involved, we have known how to coordinate with one another very well. We have been put through fire by North Korea for long, so we have better fundamentals through these well-trained people. As to the most recent activity that occurred, it's the power of intelligence. We have been able to gather many quality at the intelligence. Honestly without good intelligence, you can't carry out a good

anti-terroristic measures. Thank you. Hopefully that was good enough. Maybe just one more question, please.

QUESTIONER: Sue No from NCTC. Can you briefly talk about the major terrorism trends that you're witnessing in South Korea, and also can you describe what your priority concern when it comes to prospects of terrorism in your country?

MR. MUN: (Through interpreter) Yes. In Korea, other than what I have discussed, we are worried about homegrown terrorists. Also we have many houses which are nuclear sized, one-person household, and then also there are broken families that take -- are taking place quite a bit in Korea. People have difficulty differentiating between the cyber reality and actual reality. As these young people grow up in cyber spaces, will they really be able to distinguish between the reality and the cyber reality. They are very prone to being these -- new ideas -- new ideologies that may be exposed to them through these cyber spaces. So maybe it's not just limited to Korea, but it's something that may take place in the intelligence arena. It seems many countries have come to realize that they need to come together to have more effective counter-terroristic programs, so maybe -- it's very possible just a lone wolf would be more of a terrorist trend than a group. Thank you very much. Thank you for your attention.

(Recess)

MR. GELTZER: Great. Well, good morning everyone. My name is Josh Geltzer. I used to serve as a senior director for a counterterrorism and financial Security Council, and I'm really delighted to be included in today's fascinating conversation on terrorism and counterterrorism in Asia. Thank you for those tremendous remarks on the Olympics. As somebody who has spent a lot of time in government preparing for the security situation at the Rio Olympics, it is tremendously impressive all that you did to prepare and the results obviously show for it. So thank you for getting us off to a great start.

I have joining me three folks who are exactly the people you would want to hear from on understanding the state of terrorism and the threats in Asia. So let me introduce the three of them and then pretty quickly turn things over to them. And we will look forward to getting questions from you all after their

presentations. First, Mayuko Hori just flew in yesterday.

MS. HORI: Yes.

MR. GELTZER: From Japan and we are delighted to have her here. She is Chief Officer of the Countering Terrorism Cooperation Unit and Deputy Director of the International Safety and Security Cooperation Division within the Foreign Policy Bureau at the Ministry of Foreign Affairs. She has been in that role since August of 2017. Before that has had a distinguished decade long career at the Ministry of Foreign Affairs previously serving as assistant director of the Economic Treaties Division in the International Bureau at the Ministry of Foreign Affairs and before that dealing with a whole host of regional issues involving China, Mongolia, Cambodia, Laos so she has both a tremendous regional perspective as well as a real portfolio right now that has focused on security threat. I know we will learn a lot from her presentation.

Second will be Audrey Kurth Cronin. Doesn't come from quite as far but we are still delighted to have you here. Audrey is on the faculty at American University School of International Service. Before that she was director of the Center for Security Policy Studies and director of the International Security Program at George Mason University and before that has taught at the National War College, has taught at Oxford and has been leading voice in thinking about terrorism and counter terrorism for a while. All of us who have worked in this field have benefited from her writing and her thinking over a number of years now, and she has a forthcoming book on emerging technologies and how violent nonstate actors use them which I know we will all benefit from. It's a key issue and it is great that she will be tackling that and sharing some of her wisdom on that intersection of issues here today.

And we have Samm Sacks joining us as well. Samm is newly cybersecurity policy and China Digital Economy Fellow at New America based in New America's New York offices. She leads New America's Digi China Data Governance Project. Before moving to New America, she was at CSIS where she was a senior fellow in the Technology Policy Program at CSIS as I mentioned. And before that has worked on related issues in the private sector including at the Eurasia group and at Booz Allen. So delighted to you have you joining as well. And I think as you can tell from the backgrounds of the folks you will be hearing from, there seem to be at least a couple of things to watch for in their remarks you are about to hear. One is the

role of technology, that is true in terrorism and counterterrorism generally these days but in particular I think it is going to play a dominant theme in some of our discussion today about the state of terrorist threats in Asia.

And another is the regional dynamics, right. Terrorism always happens somewhere and the geography of that, the context for that effects what the threat landscape looks like. It affects the policies that can be contemplated in response to those threats and setting the terrorist threat in the particular regional dynamics and foreign policy situation of Asia I think is going to be part of our challenge this morning. But that's more than enough from me so I am delighted to get to turn things over to Mayuko to start us off. Please.

MS. HORI: Good morning, everyone. Thank you for having me here today. The threat of terrorism has been spreading geographically. It is no longer a problem only the in the Middle East and Africa, it is also an urgent issue in Asia. I had talked to 2020 Tokyo Olympic and Paralympic Games, prevention of terrorist attacks is one of the most important issues in our country. Today using my official capacity, I'm going to talk about the Japanese government effort related to countering terrorism and violent extremism. Firstly, I will briefly review the global situation on terrorism, in particular focusing on Southeast Asia. Then I will touch up on the trend of terrorism. Finally, I will explain our policy such as how we respond to the situation and the trend.

First of all, let me talk about global situation. According to statistics although the number of terrorist attacks numbers worldwide has been declining since 2014, about 90 percent of all the terrorist attacks in this have been occurring in Middle East, North Africa, South Asia and sub-Saharan African region. Under this circumstance as a remarkable trend in 2017, the number of these has increased by nearly 30 percent over the previous year in Southeast Asia.

We just reviewed the situation of terrorism in Southeast Asia. Not only in the Middle East and North Africa, but also in Asia, the groups that identifies themselves as ISIL have been posing threats. Those ISIL affiliates have emerged across the Southeast Asian countries. It demonstrates that the threat coming from

the Middle East could directly impact this region. Last year, in the southern part of Philippines, several ISIL affiliate merged and occupied the city of Marawi for several months. It indicates that they have high capability of fighting. Also in Indonesia in this May, the three suicide bombings by all the family members including the children happened. We confirmed that that was a new form of terrorism which we have never seen. We recognize that the threat of terrorism in Southeast Asia is serious and it is vital to prevent the spread of a violent extremism in this region.

Now let me shift the focus to Japan. Although there have not been large scale terrorist attacks within Japan in the past year, there is a potential risk given that ISIL continues to call for terrorism in various parts of the world. The largest scale event including the Olympics in 2020 could be a target. Under this circumstance, we have been shown terrorism and its strongly required to our government more than ever. Focusing on countering the terrorism and the violent extremism in the Southeast Asian region, that is geographically close to Japan and deeply involved in many field is very important and urgent matter for Japan's security. So far I explained the global situation of terrorism. Then I move on to the next topic.

I would like to explain the trend of such terrorism and violent extremism. We are closely watching the point on the slide as a trend. The first one is FTF, (inaudible) will relocate to Asian countries which keep spreading violent thought. The second one, frustrated travelers. The case of Indonesian suicide bombing which I mentioned is included in these categories. The third one, spread of violent extremism. This is a dilute course of terrorism. The fourth one, IED. The point of is that it is easy for anyone to overthink the materials of IED and also easy to get the information how to produce it from the internet. The fifth one, soft target. We are the, where a large number of people gather. The sixth one, this issue is related to terrorist finance. And then last one, misuse of internet.

Among them, we needed to pay attention to the internet issue in particular. It has been skillfully used by terrorist groups as a tool to, for example, stimulate an inside terrorism for those who are dissatisfied with society. This could be of course a homegrown type of terrorism, or a lone type of terrorism. There are interesting research results. According to the one conducted in Indonesia, 85 percent of university students and high school students in Indonesia have access to the internet and it is used as a main source

for getting knowledge about religion. It shows the potential magnitude that will influence that the internet brings among the young generation.

Also recently, concerning IED, the remarkable incident occurred in Japan. In this summer, a case occurred in Nagoya City where a university student was arrested for producing high explosives at his home. The student reportedly said that I was interested in bomb. I recognize that it is used for terrorism. So according to Japanese scholar, this incident could indicate that there is foundation of terrorism in Japan. Furthermore, it also can be analyzed that there are certain type of groups, certain groups of young people with dissatisfaction with Japanese society and those feelings could emerge in a violent way.

So far I talked about the trend of terrorism. Based on this information, I move on to the next topic which is our policy. So what should we do to eliminate terrorism? We did say that there is no panacea for terrorism but Japanese government adopt a comprehensive approach in countering terrorism cooperation policy. That is first one, improvement of countering terrorism capacity. Second one, major to prevent and counter violent extremism. Third one, economic and social development assistance. We call this three-layer structure.

The first one is border control in other words. It is to stop the threat coming from outside. This category also include capacity building of criminal investigation, prosecution to a judge, terrorist globally. The second one include one only preventive measures but also de-radicalization of already radicalized people. The third category is a major to create foundation for social stability for people's better life.

So I would like to mention a little bit about what kind of projects are implemented more specifically. Three international organizations, the Japanese government forms and implements projects shown in the slide. Most of all, training for practitioners and workshop for our government officials to deepen their understanding and share knowhow. Also, grassroots activity to disseminate knowledge among civil societies are included.

As measured against violent extremism in March this year, sorry. A recent example -- one recent example

is improvement of countering the terrorism capacity is introduction of face recognition system to study them in Indonesia where the Asian games was felt in this August. Also by using this system, we held a workshop for practitioners in Asian countries to promote utilization of biological data.

As a measure against violent extremism, in March this year, we invited religious officials and government officials engaged in measure against violent extremism from the Middle East and the African region. We exchanged views on measure to prevent and to counterterrorism with these authorities.

Finally, also domestic security is beyond our ministry's capacity. But let's look at domestic measure against terrorism in Japan briefly. Towards 2020, a close minister of security system has set up to strengthen domestic security measure. The cabinet office announced counterterrorism measure for 2020 and beyond. Under this policy, seven pillars are set up as indicated in this slide. Under each pillar, relevant ministries and agencies have been working. My division is working under pillar seven, international cooperation mainly. Among them, the exchange of information which corresponds to pillar one is essential.

Also, public-private partnership are another important aspect. For example, just recently I took a bullet train in Japan and found that the security patrol on board was much more strengthen than before. I was a bit surprised. So this is private company's efforts toward our national agenda. But strengthening these measures could include critical issues such as transfer of information including personal data or surveillance of civilian life and so on. Therefore, while preserving these efforts, we have to consider carefully in order to avoid infringement of rights such as privacy and freedom of expression and form.

In conclusion, I had talked 2020. Prevention of terrorist attacks is one of the most important issues in our country. Certain Asian regions could be the threat in Japan due to geographically close relation and also deep involvement in many fields. Therefore, to stop the spread of violent extremism conducive to terrorism in Asia is a challenge. At the same time it is important for Japan's security too. Thank you very much for your attention. (Applause)

MR. GELTZER: Thank you very much. Terrific, thank you.

MS. CRONIN: Well, I would like to thank you all for being here. I feel very honored to be talking to you on terrorism and particularly technology. I do not claim to be an Asian expert. I do know a thing or two about terrorism and tactics of terrorism and the evolution of technology so that's what I'll talk about mainly. But I'll begin with some broad overview comments about observations with respect to where the region seems to be going, and how I think that fits into the broader history and patterns of terrorism as we have experienced them over the centuries. So the unintended consequences of Asia rise will compound old problems and will create new terrorism challenges. And in the absence I would argue of better cooperation in maximizing the opportunities and minimizing the risks of new technologies and emerging technologies, I believe that the region would face growing instability in the coming years.

So I'll address three brief points. The first is the implication of growing regional connectivity and the associated vulnerability that comes with that especially with respect to technology. And secondly, the underlying drivers of terrorism in Asia that are already currently in place and finally, the evolving technological means for lethal attacks by individuals and small groups going forward into the future. So a bit of past, present and future I hope.

So to begin with connectivity, this has been the story of the 21st century. Connectivity throughout Asia has been one of the biggest developments of our time. Yet connectivity opens up new vulnerabilities both virtually and in the real world. Connectivity has of course been a global phenomenon but in the 21st century it has been driven by the rise of China and other Asian countries.

For example, as part of its One Belt, One Road global initiative, China has spent some 62 billion dollars on development and transportation projects in Pakistan. One part of the Chinese Pakistan economic quarter, I'm sorry, that was million dollars. Anyway, one part of the Pakistan economic quarter, the CPEC goes through Baluchistan and toward a Chinese operated deep water port in Guador on the Arabia Sea.

Baluchistan is the home of two long existing insurgencies. The Separatist Baluchistan Liberation Army

and parts of the Afghan Taliban located in Quetta. And the Islamic State which has claimed credit for killing two Chinese citizens in Quetta in 2017 also has a presence there.

Violence against Chinese workers in Pakistan is increasing and escalating. Just last week the Baluchistan Liberation Army attacked the Chinese consulate in Karachi. The Pakistani government has created a dedicated CPEC force of 10,000 security personnel but it struggles to handle the treat. Meanwhile, the Uighur minority has long resisted Chinese sovereignty. Uighur militant groups such as the East Turkistan Islamic Movement have sought refuge in the Pakistan, Afghanistan border and have deep links with al-Qaida and the Taliban in both Afghanistan and Pakistan. But that separatist movement goes well beyond and before and has deep historical roots that predate any rise of al-Qaida or any of the Islamist groups.

Now one would think that high tech connectivity would automatically serve the interest of China, that the aggressive surveillance measures being taken to suppress the Uighurs would automatically give them the advantage here. But there is a long history of state repression when it comes to terrorist movements. To a certain degree it is true that china has gained an upper hand. In Xinjiang province there are video cameras, frequent ID check points and police stations every 100 meters. Chinese -- China also forces members of the Uighur ethnic minority within China to download and install a mobile app that sends details of their activities to a government server. And they're planning a similar kind of surveillance system to protect the CPEC quarter in Pakistan.

I would argue that this approach has three serious weaknesses well beyond those that infringe upon the human rights of those who are targeted. The first weakness is that the app that individuals must download has serious vulnerabilities that could easily be hacked by a third party. And secondly, especially in places where China lacks territorial control, individuals can move around and leave their devices behind. And third, China will pay very serious political costs if anything goes wrong because even in remote areas, connectivity now makes it very difficult to do anything without being observed. This will be the case even if elite Chinese counterterrorism forces are deployed abroad to respond to terrorist threats. That will cause local backlash and there will be serious political implications.

Secondly, moving from connectivity to serious drivers of future unrest. I believe that these drivers are in place in some parts of Asia. Asia's growing disparities and economic wealth may create new rationales for political violence against pre-existing ethnic, religious and tribal boundaries and even geographical divides as in urban-rural resentments.

Asia's 20th century record of having one of the lowest levels of inequality changed at the end of this century. There are rising disparities in income, wealth and opportunities throughout much of the region. While overall poverty rates in Southeast Asia have declined, the gap between rich and poor has increased sharply especially driven by disparities in education, healthcare and wages. So many have found wonderful new prosperity. Between 1990 and 2008 especially in India and China, 700 million people were lifted out of poverty and that's wonderful, good news. And there are notable exceptions in this trend toward in equality, as in Japan and South Korea. But in much of Asia, the rich have just gotten richer. Between 1990 and 2010, China, India, Indonesia and Malaysia have all expanded a deterioration of the genie coefficient measures of income inequality although Indonesia is trying to reverse that trend now.

Anyway, political violence, looking at this very broadly is not directly caused by economic inequality, but the incentives to engage in crime and corruption increase and the frustrations that accompany inequality of both income and opportunity expand the ability of militant groups to recruit. So whether directly or indirectly, inequality increases the potential for instability and these pressures are then coupled with the generally young demographic especially in Southeast Asian countries. For example over 60 percent of Indonesia 270 million people are under 40 years old and the median age among the biggest Southeast Asian countries and India ranges from 26 to 30. So Asian society's that in the past have avoided the kinds of sectarian schism that we see in Europe and the Middle East are now experiencing polarizing forces that divide religious, economic and racial groups with fresh unrest in places like Thailand, Malaysia and the Philippines. Historically, these are classic drivers of terrorism, both state repression and political violence.

And then finally, technology. The changes in technology will increase individual access to lethal means. There is good reason to believe that terrorist tactics that have been more or less conservative for the last

oh, at least six or seven decades which have relied on guns and bombs mainly, 88 percent of all terrorist attacks in the world have relied mainly on guns and explosives. Anyway, and including the new trend toward suicide attacks. There is good reason to believe that we are about to see a major technological change.

Asia's central role in emerging technologies from social media to crypto currencies, from CRSPR gene editing to artificial intelligence, drones, additive manufacturing or 3D-p rinting, Nano technology; these will all put unprecedented levels of dual use technology and capability into the hands of many more people including those who intend to commit terrorism, political violence and crime. This will happen even as the traditional forms of terrorism continue.

Philippines President Duterte's warning earlier this year that airports, ports, and other public places remain vulnerable to terrorist attacks is accurate. Protecting ports and entry points in places like Singapore for example will continue to be absolutely crucial. But old tactics will be joined by new technological means for which we have not yet developed effective countermeasures, nor the kind of cooperation that is necessary to minimize their effects.

In the wake of the ISIS caliphate, returning foreign fighters did not prove to be as serious a problem as we feared. Instead we have seen self-radicalized individuals or small groups who are already in place and whose attacks are especially hard to predict or prevent in advance as Director Mun has explained to us. ISIS and other violent jihadists have shifted their attention to fully exploiting social media applications like Telegram, to promote radicalization within places like Indonesia, Philippines, Malaysia, Bangladesh and other Asian countries. So going forward, militant individuals and groups will have access to disruptive technologies that can create bigger threats and command greater attention especially by hitting high profile targets. I'm not arguing that these technologies are all bad. There are wonderful elements and wonderful aspects but we have to be prepared for the risks as well. Anyway, these high-profile targets include the cesium laden drone that landed on the roof of the Japanese prime minister's office in 2015 and the 2016 plot by Indonesian terrorists to fire rockets at Singapore's Post Marina Bay Casino.

More importantly, technology is already changing how and why people get involved in violence to begin with. It is not just a matter of studying an individual technology at a time. It is a matter of looking how the motivations and the involvement in violence are changing.

Here are anyway three unprecedented technological changes that will affect the future evolution of political violence in Asia, I believe. The first is mass interactivity. The robotic replication of messages sent by automated fake accounts, live streaming of attacks and high-quality first-person film making that makes anyone a high-quality televisions producer. You don't have to carry out terrorist attacks to have political effects. For example, by using social media to polarize domestic populations as happened with Facebook's role with respect to the Rohingya in Myanmar. Secondly, individuals can combine clusters of technologies and create something new. These technologies, many of which are developed as platforms to enhance the individual ability to engage in innovation, that's unprecedented. It used to be that you had to have a certain level of expertise in order to build some of the things that we are now enabled to do. In many cases for excellent reasons, but in some cases for nefarious purposes on the platforms that we have. UAV's or drones or remotely piloted vehicles, 3D-printed or additive manufacturing and nascent autonomy, all offered extended reach to a broader range of actors. Individuals, small groups, terrorists. I don't think that we can only look at the category of terrorists anymore. Crime, these things are very much melded together. For example, China is the largest producer of popular hobbyist drones, the DJI Phantom. It's a lot of fun. I love to play with mine. They are a lot of fun to play with but with smartphone advances, increased autonomy, more secure digital links, better cameras and the ability to carry much heavier payloads, they are becoming much easier to weaponize. And that will surprise us as you move forward into the future.

Finally, our vulnerabilities are greater than ever, especially in advanced countries like Japan, Korea, China, Australia or Singapore. Our new electronic appliances and computerized devices are part of the internet of things which is the interconnection of millions of computing devices, most of them equipped with sensors that directly receive and transmit data without human involvement. Things like kitchen appliances, thermostats, door locks, voice activated assistance or hospital heart monitors are all vulnerable to hacking. You can't even buy products anymore without that kind of connectivity because

the data that is being collected about you is often the most valuable thing of all. It's not even the cost of the appliance. But this also provides an avenue of attack by individuals and small groups including criminals and terrorist groups and perhaps individuals. The attacks will be very difficult to counter in the future not least because commercial companies have neither the means, nor the commercial incentives to make their applications secure.

So to wrap up, I think that Asia is poised for rapid change in political instability unfortunately, not just because of long standing drivers of political violence like inequality, not just because of potential radicalization and domestic polarization especially in South and Southeast Asia, but also because of the attraction of new technologies and more advanced countries. Asia leads the world in many emerging technologies. The only way to ensure future stability is to maximize their benefits and minimize their risks to have a conscious effort to do so. But at this point, the region, as is the case with most of the rest of the world, lacks the institutional frameworks and the commercial incentives to build appropriate legal and regulatory regimes and guidelines to do so. (Applause)

MS. SACKS: Thank you very much to Brookings for having me. It is also an honor to be on a panel of all women talking about technology and national security so appreciate that. I'm -- my expertise focuses on Chinese technology and cyber policy. I'm not a counterterrorism expert, so I will talk about counterterrorism from the legs of internet and policing technology. And, you know, today we have talked a lot about the use of technology to enhance the tactics and the reach of terrorists so in my remarks I'm going to flip that a bit on its head and talk about the use of technology by governments and counterterrorism experts focusing on China.

First, I would like to talk about the legal tools and that the Chinese government is developing to enhance its reach in counterterrorism. Then I'm going to talk about Xinjiang and what is happening there with technology and third, I'll talk about the export of digital technologies to policing and counterterrorism experts around the world emanating from China.

So, China is in the process of rapidly building out a legal system which gives the government greater

control and visibility into the internet and to the digital space with implications for surveillance. The most important piece of this evolving legal regime is China's counterterrorism law. There are dozens of different laws and regulations together so I'm going to just focus on three. The counterterrorism law and some other regulations primarily used by the Ministry of Public Security in China.

The counterterrorism law introduced broad discretionary tools that the government could use in assisting with national security investigations. There is no official definition of terrorism but when we look at Chinese law, a lot of the time these sort of catch all phrases related to supporting national security investigations are taken as a sort of signaling that can be used for domestic stability operations with terrorism as an obvious focal point.

So the counterterrorism law gave Telecom and internet service providers, it required that they provide technical support and assistance to the government as well as tools for content monitoring to focus on eliminating extremist content online and also requires logs of user activity and information. One development that was interesting in this law is it removed a very controversial provision which would have required telecoms and ISP's to install back doors. It also removed a provision requiring data to be localized on Chinese servers and we could have a whole discussion about data localization and what that means from a law enforcement perspective.

But this has been used, there is a -- data location in China is something that is actually cropped up in other laws and regulations even though it was removed from the counterterrorism law with the idea that data stored locally can be more accessible for law enforcement officials. So these are, this is one foundational text. The Ministry of Public Security has since issued a number of other measures, most notably the internist security supervision and inspection regulation which again allowed broad discretionary tools for the government to go in and conduct random onsite investigations as well as to draw information stored on users.

Last week a new data security guideline was just released in draft form. I worked with a number of linguists and we actually published a translation of this, it is available on the New America website with a

brief introduction. But this yet again another tool that can be used for accessing user logs and onsite inspections. So, these are from a kind of legal perspective, some of tools that the government has been using.

I want to talk second about Xinjiang because you can't have a conversation about counterterrorism in China without looking at developments that are occurring there and this was mentioned in some of the earlier comments. You know, there have been some very disturbing developments specifically about the use of technology for enabling mass surveillance, incarceration and re-education of the Uighur Muslim population in Xinjiang. Chinese authorities claimed that this is an effort to address violent separatism and really just extremism.

But technology has been a focal point with the idea that developments in Xinjiang have been a petri dish for some of the new technologies that are being rolled out in counterterrorism efforts. And just to give you a sense of what these are, a few of them were highlighted earlier. You also have QR codes on the front of residents households which can be used to scan and quickly sort of in scannable bits access information about what people, peoples families networks, what they are accessing online, voice data collection, facial recognition to create databases, intelligent cameras, ubiquitous scanning, GPS tracking, I mean, the list goes on.

Now there is a lot of -- I think that there is a lot of concern and rightfully so about the use of these technologies in Xinjiang. I want to pose two questions because I think that we are in a moment right now where there are growing concern about China but it's important to be accurate in sort of the way that we are discussing these issues.

The first question is to what extent are developments in Xinjiang going to expand nationally? I think that there is an assumption that this is already happening and it actually is not and so we need to be looking for specific evidence of these sort of Xinjiang case study becoming used on a national scale in China. The second are the limitations of what these technologies are actually capable of doing. There is a perception that in China data is easily shared in standard, usable formats across the country, across companies,

within the government and this is simply not true from a technical and an organizational standpoint. There are a lot of data silos that exist that actually make that much more difficult than I think some would assume.

To give you just an interesting case study of how this was playing out, the Chinese ride-sharing company DiDi had some issues earlier this year where two passengers were murdered while they were using the DiDi platform. Shortly afterwards the police requested that DiDi turn over all of its data both on the drivers, the passengers, the routes, the vehicles and DiDi actually resisted turning over that data. They made that request three times and it was only on the third time that they turned it over. And I think people would automatically assume isn't that data already in the hands of the police? Well, it's not and we saw how that played out.

So what DiDi did in response is they actually showed up at the local police station with boxes of hard copy data that was in nonstandard format and was completely unusable. So they're now undergoing a rectification process on this front, but I think it is important to highlight that data sharing in China is not as seamless as some would think.

Even Tencent, one of the large Chinese internet platforms which runs the social media app Wii Chat notoriously does not share data even across business segments within their own company, right. So this is something that the government is going to have to address and as we -- if for those who think that the Xinjiang use of technology is an experiment that is going to rapidly expand across the country there are some important limitations to that.

However, even in the absence in the most sophisticated advanced capabilities on some of these surveillance technologies, often-times it is the perception of surveillance itself that forms an important deterrent and there has been some important work that is reporting done on this. Paul Moser specifically of *The New York Times* has documented the fact that even though people don't know exactly what is going on, you've seen a, you know, reduction in jay walking just because of the threat that their name could appear on a big billboard.

So lastly, I want to talk about the topic of export of Chinese police and surveillance technology to other countries. There is a report came out recently from Freedom House talking about the rise of digital authoritarianism and there have been some important cases of this. You have in Venezuela for instance the Venezuelan government worked with the Chinese telecomm company ZTE to develop a digital ID system which can be used for tracking from mobile payments to social applications.

Hikvision which is one of the major facial recognition technology companies in China actually has a significant global market share. It occupies 11 percent of the global market share for technologies from cameras, drones, household robots and this is a company that is very likely involved in the mass surveillance activities underway in Xinjiang which raises important question about, you know, to what extent are foreign investors benefiting from some of these surveillance technologies in use in places like Xinjiang. This is a company that had 34 percent return on equity at one point, right. So we need to look at I think there are some efforts underway that might potentially sanction this company and others that are involved.

But it raises important questions about the diffusion of digital technologies and what happens when they get in the hands of governments around the world that are using them in ways which raises important questions from a privacy, from a civil liberty perspective. I think that there is a certainly an attractive model that is presented because you have an options to -- you can see how in the case of China, technology has been used for a -- as a force of economic prosperity and connectivity in ways that have certainly benefitted apart from some of the troubling aspects that we discussed. But at the same time, there is -- you can -- the Chinese government has modeled how you can have proliferation of digital technology in a way where you also have very strong tools of government mentoring and control of that technology. So I think that has been a main driver of some of the proliferation of it. But with that I'll close and look forward to incorporating the China case study into the broader discussion. (Applause)

MR. GELTZER: Terrific. Well, thanks to all three of you for really thought-provoking remarks which I think give us all a lot to digest and hopefully a lot to ask some questions about. So I'll use the moderator's prerogative to ask a couple, largely to give you all time, I hope, to think of questions for the panelists.

But let me start with where Samm left us because I was struck by how I took a, something of a deep breath, a sigh of relief when you talked about some of the information not flowing from the private sector to the Chinese government which struck me as a strange reaction on my part. Because especially since 9/11 a lot of us in government have worked very hard to try to get information to flow from the private sector to the government and vice versa especially for law enforcement and national security purposes. And we have talked about breaking down barriers and setting up fusion cells and encouraging a sharing of things that might keep us all safe. And yet in the context of obviously a different government, I took a deep breath. So that sounds actually like something of a relief that the ride sharing info isn't necessarily going to the government the way I would have thought it did in a place like China.

And so I guess I would like any of the three of you who are interested to reflect a little bit on what it means on the one hand for good counterterrorism in particular to require information sharing, private sector to government, within the government, government to private sector. We heard that even in the preparation for the Olympics, information sharing was critical. And in the other hand, reaching a point where there is so much information that at times the idea of it flowing freely makes at least some of us a little bit nervous. Any of the three of you want to kind of tackle that and reflect on where the balance might be or what it means in the current environment technologically to grapple with that tension?

MS. SACKS: I'll just expand briefly on the China case.

MR. GELTZER: Please, yes.

MS. SACKS: And I was recently in China at a data security summit at Ali Baba.

MR. GELTZER: Oh interesting.

MS. SACKS: Where a lot of these discussions were taking place among the Chinese tech companies and some of the Chinese scholars that are writing the data standards in China right now. And, you know, I witnessed an interesting exchange on this topic. You know, I think that some would be surprised that there is actually debate on this in China as well and the case of Apple has come up a lot in Chinese conversations. And so I heard sort of Chinese tech companies discussing well, who do you agree with in that situation? Do you agree with Apple or the U.S. government? And it's a source of conversation so I'll just throw that out there to say that these debates are not just happening here. I think they are happening

globally as well.

MR. GELTZER: And this was Apple's post-San Bernardino show down with the government over the iPhone.

MS. SACKS: Exactly

MR. GELTZER: Interesting.

MS. SACKS: So another area of work that I have done a lot of research into is sort of the emergence of data governance in China and there are a number of new rules and standards that are coming on the books in China around how data is collected and stored and shared both with companies and with the government. My view of this is that there are sort of two tracks when we think of data protection in China and the government has very broad tools as I mentioned to conduct surveillance and national security investigations. But companies are now facing greater restrictions on what they can do with user data. So there is sort of two tracks to how these rules are being applied which is a different approach.

MS. CRONIN: I would like to admit that I am not talking about the most cutting-edge technologies. So the states are well head of any individuals or groups in their use of technology. I think it is going to be some, depending on, I mean, we can talk about specific examples, but I think it is going to be a few years, five years, perhaps a little longer before you see some of these means that I described, 3D printing, especially that's a long term, but, you know, quad copters, the various types of technology is CRSPR that people have access to in various degrees of primitiveness or advanced capability.

This is -- I'm looking forward. The states are always going to be stronger with respect to how they use technologies. I think we are very wise to be looking at how China uses technology and how they share information. I would only say that the counterterrorism model that has been evolving where we work very hard to increase counterterrorism intelligence, information sharing, I think that is going to be replaced gradually by an actual concern about how people use means.

So you -- if you have got great intelligence, you can gather that intelligence about targets that you have some clue about in advance. Whereas if you are talking about individuals or criminals or terrorists, or

groups, not even necessarily terrorist groups, but groups who have access to technologies that they can use in unpredictable ways, that's -- no matter how much information sharing you have, if it's someone who is self-radicalized or engaging in activities that harm other people, it is -- the most information sharing and counterterrorism and intelligence is not going to solve that problem. So I guess what I'm arguing is that we need to have a little bit more of a return to the focus upon means not just information.

MR. GELTZER: Yes. So let me pick up on that. I will ask one more question and then we will open things up to the audience. If and it picks up on what you were saying, Audrey, about the technology channeling what is ultimately a radicalization on the part of an individual. Mayuko, you had a slide there that talked about CVE, PVE, countering or preventing violent extremism and I'm, want to ask the group a question I get asked and don't have a good answer too. So maybe I will walk away from this with a better one. Which is sometimes I get asked of course you need to have countering, preventing violent extremism as part of a CT strategy. You can't give up on the idea of trying somehow, bracket how, to stop that radicalization at the individual, before the individual makes use of technologies, before technologies can try to identify someone before they turn violent. Something and yet the question I get asked is are we really any good at is as governments? Or do we really have -- if not best practices, at least decent practices that at a country wide level get at the possibility of vulnerable individuals going down a path towards violent extremism.

So I would be curious for any of you who want to jump in on it as to where are we? We are at least in the states almost 20 years after 9/11. Where are we in terms of actually trying to prevent human beings from traveling down a path of radicalization and extremism? Is it -- are we any good at it? Its -- I never know what to say so I'm hoping I walk away from here with a better answer to give when I'm asked it. Do you want to start, Audrey, or do you want to start, Mayuko?

MS. HORI: It's not a direct answer to you but there is social stability is the most important things and social stability which makes people feel happy. That's a point. Then there is feeling of isolation or dissatisfaction towards society. That feeling is existing Japan then that could emerge in a violent way sometimes and may cause terrorist attacks in sometimes but point is, it's quite difficult to find them.

MR. GELTZER: Yes.

MS. HORI: So then also we don't have enough experience about those things so in that sense we need to learn from the foreign country.

MR. GELTZER: Do you want to chime in, Audrey?

MS. CRONIN: Well, I think that de-radicalization, countering violent extremism has had some good effects. I think that it was the right idea. But it's very difficult to apply in a kind of a generalized way in every part of the world and in fact it is not for any individual to argue how people should deal with individuals within their own societies and the ideas that they have.

So the problem with the CVE framework that I see, despite its excellent intentions, is that it's extraordinarily difficult to apply unless you have locals that have bought into the ideas and if you can avoid causing communities to feel as if they are alienated and made into the other. So the problem with getting out ahead and talking about prevention is that you're identifying people that you think might potentially become terrorists and when to do that you automatically give them a sense of alienation.

So I think that's the weakness of that framework but as I say, we have had some success with de-radicalization in some parts of the world. The bigger picture though is that areas of instability have overtaken some of the successes that we have had. I mean, if you look at the Middle East, the fact of the Syrian civil war and all the hundreds of thousands of people that have been brutally killed there, how can that offset arguments that we need to counter violent extremism among those whose relatives may have been involved as victims? So we also have to look at the kind of big picture of what is happening politically in the world.

MR. GELTZER: Those are two answers that are both better than the ones that I usually give. Let me pick up just on this idea of alienating communities and go back to Samm on Xinjiang because it seems an opportunity to say a little bit more about that. The idea of taking prevention to what looks like sort of an, in my view, an extreme approach by the Chinese government. What is that doing to dynamics there? How does that play out over the long run to have run something of a prevention on steroids approach? What do you think?

MS. SACKS: Yes, I mean, I think that it is frankly pretty horrific what is happening there. I mean, it's mass incarceration in the name of de-radicalization and re-education and there is no other way around it.
MR. GELTZER: All right. Let me open things up and if, I think if you put your hand up a microphone will be swiftly brought to you so I invite your questions. Please. Great.

QUESTIONER: Thank you. I'm Yuko from George Washington University. I would love to ask about the prevention. In China there is a social network sorry, social credit point system. Does -- how do you evaluate this system? Is it effective to prevent the terrorism? Thank you.

MS. SACKS: I thought at some point today the social credit system was going to come up. It seems every week there is a new article in the media talking about a dystopian panopticon future under the social credit system. So for those of you who aren't familiar with it, in 2014, the Chinese government issued a planning document outlining this vision for a social credit system in which citizens would be -- its sort of looking at if you violate a court order or you speak loudly on a train or a number of sort of various of actions or transactions would lead to some kind of benefit or punishment and would be tracked.

At to date there, as I mentioned before there are a lot of technological limitations that I think are not well accounted for and the social credit system is another example of this. To date the way that it is being used is law enforcement data so as I said if you are in violation of a court order or a traffic violation, you may not be able to buy a train ticket or some kind of other benefit that would accrue.

The next level of this is algorithmic governance in which your social media, relationships, your communications, online content gives you a sort of translates into what kind of discounts you can get, when you shop and restaurants or can you get a mortgage and send your children to school? We are still not at the level where that kind of broader algorithmic governance is fully being implemented.

In reality there are dozens and dozens of mini local versions of the social credit system which are being piloted around the country. There is not one centralized place where that data is being sent, shared and then applied because it's just a massive undertaking and there are bureaucratic organizational reasons for

that. So, it's still in very early stages. I think that the document as envisioned in 2014 is much more aspirational. The Chinese government is great at coming up with national plans and aspirations. They're less effective sometimes in actually implementing them. But certainly, it is something that is going to be an important area to watch in this case.

MS. CRONIN: This is not my specialty, but I have to say that even just the idea of a social credit system, whether it is working effectively across the bureaucracies and whether the data is shared or not, just the idea of it horrifies me.

MS. SACKS: So and I'm just going to play devil's advocate here and I'm not in any way defending it but just, I want to give a sort of Chinese perspective on this just to play devil's advocate here. So when we think about a Chinese system that had -- think about Equifax in the U.S., credit scoring. Chinese financial system had nothing like that. You had rampant sort of food safety scandals where infants are dying because they're getting products that are tainted with chemicals.

You have no way of evaluating credit as more people are sort of purchasing online in the digital economy. No way to, you know, scams are rampant where you have sot of fraudulent activities. There was a big scandal where a patient died in a hospital that had just been promoting all these sort of medications and treatments. So in the idea behind it originally was let's find a way of having some kind of accountability. You know, with Equifax in the U.S. for a while they were, you don't necessarily opt into that.

I spoke with a Chinese tech company that said look, if you look at Confucius for years has talked about their three things that a government needs. Food, an army and trust or credit. And he said Confucius says that credit or trust is the most fundamental to governance. So I'm just again, not defending it but just to sort of throw out that the system was created to solve a sort of practical problem as China, you know, modernized and built up a, you know, a broader connectivity system as we talked about.

MS. CRONIN: Okay. Well, just to give the devil's advocate answer to that.

MS. SACKS: Yes.

MS. CRONIN: I am --

MR. GELTZER: Now we have two devils sitting on the stage.

MS. CRONIN: Well, no I'll actually give my answer to that. All right.

MS. SACKS: Yes.

MS. CRONIN: I don't think that any kind of parallel with Equifax holds because Equifax is one sector. And Equifax is about a relatively limited amount of your financial behavior and let's face it, if you really want to, you can just pay in cash, right. It's about whether you are going to be able to have the trust in order to get a loan. This is a very narrow example.

Any parallels with a system that tracks your behavior, your personal behavior across a broad range of different areas of your life is horrifying. And I don't buy that perspective. I would like to say though that the United States in order to find the way forward, I really think we need to lead. I mean, we are sort of reacting to how people are using data in various and how authorization governments are manipulating our new technological means and yet we don't seem to be facing the fact that if we don't reduce the risks and build a framework that takes advantage of the opportunities in a way that is not strictly driven at least in my personal opinion, you know, mainly driven by profit, we are going to look very hypocritical and we are going to find ourselves in a pincher movement between, you know, governments that basically have a very chaotic approach or are not very well developed in terms of technology and those that over use technology in the ways that a social credit system to me in the abusive ways I think that that is.

MR. GELTZER: It was a great exchange and it encapsulates what I was grabbling with in my own head after these presentations which is this push we have had here to fuse, fuse intel and yet when we see fusing of things that sometimes may get overstated because we don't exactly understand the gaps in a place like China that they are trying to fill, we go well don't fuse that. Don't fuse it at that scale. And that seems like a healthy debate to have it but it's somewhat contrary to a lot of us in counterterrorism who say all source intel, fused as much as possible brought to Bayer, as may interactions with the government not just when you're at the airport but when you want access to a lab. When you want some -- so it's a -- I think your exchange is encapsulating what is so hard about dealing with the data that governments now have at their disposal. Let's see who else. Yes, please.

QUESTIONER: Terence Taylor, International Council of Life Sciences. Thanks very much for your insights, immensely valuable. I wonder if you could add a little bit. I remember Ms. Hori referring to organized crime and how that may be exploited and promoted. Two dimensions there, one is through handling of financing and taking advantage of technological developments in that area, and also, these are people who don't share the objectives of extremism, they're simply making money out of this and this presents I think a particular challenge. I would like to hear comments on that.

And secondly, why is a long history of it is state sponsored terrorism. The use of non-state actors and state actors for that matter particularly which will perhaps advance and accelerate and I would like to hear your view on this, the use of the new technologies or the novel technologies. When one can say well it is very hard for a group or an individual in a garage somewhere to use more advanced technology but there is another dimension, both the organized crime element and the state sponsorship. Thank you.

MR. GELTZER: So I think the question and make sure that I get this right, looks to situate the conversation on terrorist actors within the context of organized crime and then within the context of state sponsorship of terrorism as well. And I wonder if you will be willing to talk -- your presentation mentioned that this is in some way is an inseparable universe of threat actors and if you would be willing to saw a few words on how you see that relationship from the terrorist actors themselves to that broader grouping of organized crime, state sponsorship and then maybe if others have thoughts as well?

MS. HORI: In our policy, we don't separate those state sponsorship terrorism or we have organized terrorism. So that's the things which I know.

MR. GELTZER: You treat them as a whole.

MS. HORI: Yes.

MR. GELTZER: As a whole, a single problem set. Yes. Audrey, did you want to chime in as well on --

MS. CRONIN: Yes.

MR. GELTZER: -- how these pieces relate and?

MS. CRONIN: I think that the melding between organized crime, trafficking and other kinds of profit seeking uses of new technologies is less and less distinguishable from terrorism unfortunately. I mean,

you can determine whether a group has a political agenda but sometimes you can't necessarily -- it's very difficult sometimes to determine what the motivation of an individual is especially if that individual engages in a suicide attack.

So we have depended very heavily upon motivation in order to divide different kinds of frameworks with respect to the use of violence and I think it is becoming increasingly difficult to do that. So I agree with you that the interlinkages with organized crime are much deeper and more sustainable now than they have been in the last 20 years and groups are benefiting from organized crime and they are also feeding into organized crime. It is difficult to separate them and in some ways I think organized crime with respect to human trafficking and many of the other things that are going on in Asia as well as in other parts of the world are more serious than the terrorist attacks that occur because there are many, many, hundreds of thousands of people who are trafficked and who are abused and in other ways damaged by organized crime.

As far as state sponsorship, I think this is another thing that was overshadowed after the end of the Cold War because you no longer had those motivations to try to use proxies in order to fight Cold War battles and is now coming back in a very big way. State sponsors are more able to use cyber means to reach individuals and to provide individuals those capabilities beyond whatever they used to have in the 20th century. So I think you are absolutely right.

MR. GELTZER: Great. Please.

QUESTIONER: So it's my understanding that Japan actively participates in international discussions when it comes to CVE programs and I was wondering if you could talked a little bit about Japans plans to implement their domestic CVE program within Japan.

MR. GELTZER: I'll repeat the question just to make sure folks can hear it. The question was about Japan -- excuse me, Japan's participation in international discussion about CVE, countering violent extremism, PVE, preventing violent extremism and the question was about Japans plans to implement domestically

that sort of countering violent extras work.

MS. HORI: Well, the, our ministry, I mean, the Minister of Foreign Affairs works for the foreign policy aspects so they are countering terrorism policy. So actually the domestic security is under the national policy agencies matter but we already cooperate together. So well, well, let me see. Yes, national policy agency. Yes. Well, for example, information sharing. We Ministry of Foreign Affairs has also intelligence units and they have their counterpart and they do information sharing. But also National Policy Agency also do the information share with their counterpart but their purpose is to share the info in order to promote the domestic security that's the difference what we are doing and the national policy agency is focusing. Through that activities we are implementing counterterrorism policy within Japan.

MR. GELTZER: That sounds, if I'm understanding her, that sounds roughly similar to what we had created over the past few years in the U.S. government where within the office of the counter terrorism coordinator at state, there was a new deputy to the coordinator who focused on the international conversation, I believe still focuses on the international conversation about CVE, while at the same time there was for us housed at the Department of Homeland Security a task force focused on domestic implementation of CVE and part of the challenge was how to get that link robust so that the conversations that the external facing person at the state was having reflected what we were actually doing domestically and brought back lessons learned and that the domestic task force was benefitting from the international conversation. Is that about roughly analogous to how your system works?

MS. HORI: Yes.

MR. GELTZER: Yes.

MS. HORI: Yes. When we attend the international conference like GCTF proposing, some meeting or some other relevant organization, when the relevant organization hold a meeting, we ask National Policy Agency to come together, to attend the meeting. Then they get the information, the know how, then they will get back to their office then take it their policy, domestic policy thoughts or activities. We try to yes, cooperate in any case between the counterterrorism measures internationally and domestically.

MR. GELTZER: Okay. Thank you. There was a question over here on the corner and then we will go over

from that.

QUESTIONER: Thank you. My question has to do back to the Chinese companies having this conversation about government versus industry sharing of data and I'm curious just to dig into that a little bit more what -- were there any acknowledgements of the difference between persistent digital surveillance through these platforms versus an after the fact digital forensic study à la San Bernardino and Apple and how those are two very uniquely different things and maybe even through the lens of the Uighurs in Xinjiang province.

MS. SACKS: Absolutely. So in the case I mentioned, DiDi the Chinese ride-sharing company, there is a regulation in China that requires ride-sharing companies to provide real time access to their data so essentially hooking up their platform vehicle, passenger, GPS routing, all of that data in real time to a government national and local level ministry. So it turned out that DiDi had been completely in violation of that and just frankly wasn't doing it.

And so what happened after the murder of the passengers, is this started a huge controversy and there were Chinese scholars writing in and saying if DiDi were to comply, that would actually be a violation of China's cyber security law which I think many in the room would be surprised to hear, has a broad consent requirement which requires consent before collection of use and use of data.

Now then there is open questions about how exactly that's implemented and this can be easily manipulated because in the cybersecurity law you have consent requirements but at the same time, you have these broad tools that the government can use to go in and under that same law conduct on-site inspections, require more real named personal information of users. It's a contraction in the law itself. So, this has actually being hotly debated.

I think now DiDi is obviously going to have to comply with that, right. But there are different rules. Some do require real time access, others are more after the fact to support as national security investigation.

In the case of Xinjiang specifically, I think that this is an area where they are experimenting more with this real time data access in ways that are going to be very, very concerning.

MR. GELTZER: Samm, can I ask a follow up question to that which there may be no answer to but after San Bernardino, Apple made very clear publicly why it was taking the stance it was taking. In fact, before it ever filed its what ultimately is statement of position in court, it actually put out a statement from Tim Cook to the Apple user base but of course to the world at least setting out its public position as to why it was resisting the government demands.

Do we know as DiDi said, why not be in compliance here. Is it ideological? Is it because they want foreign investment? Is it because there is, they feel that the pinchers of two different laws in a sense that within China? Do we have any sense?

MS. SACKS: Well, DiDi didn't in particular -- didn't specifically but I can answer it in a broader context of --

MR. GELTZER: Great, yes.

MS. SACKS: -- of what is driving data protection in China and I think it is very different. That's why I don't call it data privacy. I call it data protection and I think there is an important decision between -- I think there is a microphone over there that's loud.

MR. GELTZER: I think that may need to, the ear piece may still be on.

MS. SACKS: Turn that ear piece off. I think there is an important distinction to be made between data security and data privacy. In China, the concerns are not about the government having access to the data. The concerns are about criminals and, you know, fraudulent misappropriation of data which is actually a main issue. There is a black market where data is sold and bought on these extensive data broker chains and that's a real concern and I think that is what is driving a lot of this. But then there is a sort of feeling of safety that if the government gas your data, that's a responsible guardian of it.

MR. GELTZER: Interesting.

MS. SACKS: And so I think that is an important framework in if we think about in relation to the Apple

case or even in relation to GDPR.

MR. GELTZER: Very interesting. Definitely different from Tim Cook's view of government.

MS. SACKS: Yes.

MR. GELTZER: Yes. Interesting. Okay. There was another question. Yes there.

QUESTIONER: I'm Hannah Handle from OST Policy. I have a question basically based on the issue of kind of localization within these countries. When we look at India for example there is a big breakdown oftentimes between communication with local prosecutors and police. You will see kind of almost no effective communication happening there.

In Korea the rotation of prosecutors of very year from different offices to ostensibly minimize the potential for corruption, oftentimes results in issues of criminal cases not really being able to be maintained because the new prosecutors have no idea what is going on and once they learn, they move. But we need that local input for effective implementation of policies that are large and important such as CT and CVE so how do we expect effectively implementation of national and regional strategies for CT and CVE when the segmentation within each state can actually hinder those efforts?

MR. GELTZER: Do folks have thoughts on that about the -- it may even be two questions. One is a sort of local federal divide or at least lack of optimal cooperation on these issues and the other is that at some level people who get this specialized expertise move and you're then in the positon of dealing with folks new to some of these issues. I'm tempted to ask Jim from all the FBI experience what it is like to deal with people who also move around jobs pretty quickly but we will spare him until the next panel. But do folks have thoughts on that?

MS. CRONIN: Well, this is one of the challenges of CVE because it's not as if you have perfect communication among the actors that you really want to communicate well so I think you've beautifully described the problem. I'm not sure what the answer is. It's another way of explaining why CVE is extraordinarily difficult to carry out. I will say that some of our governmental dysfunctions that are sort of leftovers of things that have happened decades ago and are meant to protect rights but nonetheless

prevent effective communication, those are exactly the kind of frameworks I'm talking about needing to be fixed if democracies are going to be healthy as we move forward into this age of the 21st century new technologies.

MR. GELTZER: Great. Other questions? Please. There is one along the aisle here and then we will go across the aisle.

QUESTIONER: I had just a clarifying question specifically for Dr. Cronin. Talking about the use of more advanced technologies in counterterrorism over time and understanding logically that this is in the future and that it's going to take time for them to get these technologies, but I was wondering if you could kind of talk about how right now there is kind of a trend to use more crude methods? So like Islamic State promoting --

MS. CRONIN: Yes.

QUESTIONER: -- less technology. So could you talk about that dichotomy of the potential use in the future maybe that wouldn't be Islamic State affiliates or just the difference between the trend to very minimal technologies versus using more technologies in the future. And additionally could you talk about the dichotomy between the rural, more unequal terrorism extremists and how they would use it whereas like a lot of the technologies would probably be in like more urban, more wealthy hands. Thank you.

MS. CRONIN: Okay. So the answer is both and. I mean, these are not dichotomies to me. These are different potential avenues that groups go down and they tend to be opportunistic. So the Islamic State was telling people to use cars to kill people because that's what they were capable of telling people to do. And most of the people that they were reaching out to had very little training or very little inclination and time, mostly time, to learn to be able to carry out a more sophisticated IED attack.

So what I'm saying is that groups at different phases as they go along, the Islamic State very much in a defensive period was reaching out to self-radicalized individuals and using the easiest thing that they could get their hands on because that was the most expedient way to immediately carry out violence. It wasn't that that's what they would have preferred, it's that that's how they wanted to have violence quickly so as to how a sense of strength for the Islamic State at that time.

Now when we are talking about technologies, I mean, I have kind of been very general, I haven't been getting into the details as much because sometimes I hesitate in forums like this to give a, you know, sort of give my bizarre and twisted ideas for how nefarious actors can use these technologies because that is not necessarily something I want to share with the broader group of people who might be using them. But --

MR. GELTZER: Not in the book.

MS. CRONIN: Well --

MR. GELTZER: Hinted at in the book. You have to read the book to find out if they are in the book.

MS. CRONIN: Okay. Let me just give you one example. If you have a quad copter and you're able to carry a very heavy camera and you're able to use that quad copter to go up and over and see whether there is a forest fire in California, that is a fabulous use of that technology. But that camera can weigh enough that it can also be a small explosive. So using a quad copter to deliver, you know, a small high explosive is very easy and it's been done.

And it was done by Islamic State not because they thought they could beat their opponents, this was not a matter of them actually thinking that they could have an effect that would cause them to succeed on the battlefield, it's a matter of a demonstration because they were trying to reach a broader audience and show that they still had strength.

In Australia, they're using GoPro cameras to go down within mines rather than having to send people down there. This is a fabulous thing because it is very dangerous work. You can send a robot or a drone depending on what you are trying to do down underneath into very difficult places below the earth. That same kind of technology could very easily be used to go into a sewer and loaded with an explosive, a high explosive and, you know, you can just spin that scenario out for your own selves.

So, you know, we can talk about lots of specific technologies, some of them we're way ahead in terms of thinking about the implications, you know, the additive manufacturing people who have access to 3D printing, they may be able to make a simple drone but most of the time they don't have the equipment or the materials or the advanced types of machines that you would need to do any kind of serious weaponry

but that is now. That's something that I would say you have to go out a few decades. It depends on the specific technology but the key thing that has changed is that you can use these technologies together in clusters and create something new.

MR. GELTZER: We have time maybe for one more question. I think there was one on this side of the aisle. Yes, please.

QUESTIONER: Thanks. My name is Ray Ramos, I'm on the Deputy Director for Special Operations on the Joint Staff. In terms of Southeast Asia where we commonly see ISIS, you know, Indonesia, the Philippines, they don't have the, you know, AI capability, computing power that we see with like China. So my question is while China may have some reservations about doing sort of that CT work inside their own country, do we see them doing that in other places in Asia or not as hesitant to, you know, gather data and influence the counterterrorism in Southeast Asia and some of these other countries that don't have the ability to do so just in terms of spreading their influence in Asia or at large if that makes senses?

MR. GELTZER: That's interesting. Maybe I'll even broaden it and just sort of China's role in counterterrorism regionally, outside China through technology and otherwise. Do people have a sense of where that stands, what the trajectory looks like? Maybe we will pass on that one.

MS. SACKS: On the tech and again, I apologize, I'm not a CT expert so I can really only comment on the technology piece. I think there is certainly an effort to work with other governments in the region to use the sort of policing and surveillance technologies that China has used domestically in other markets and we have seen, you know, numerous examples of that.

MS. CRONIN: Yes, and that's essentially what I was talking about with the cooperation with Pakistan and the CT, PCTU's, the same kind of surveillance technologies that have been used within China. I mean, it is much harder because if you don't have control over a piece of territory and you don't have a population that is advanced enough to use those technologies, you're somewhat, you're quite limited.

And we also have to remember that the political effects of the technologies are important. It's not like we can only be technological determinists. In different situations in different parts of the world are going to differ but I think we need to pay attention to that dimension.

MS. SACKS: There is also another dimension which is the Chinese government's use of trade relationships to win support for their own counterterrorism efforts in Xinjiang. I mean, as an example I think that there have been other Muslim countries which have been hesitant to comment on the Chinese government's behavior in Xinjiang because of close relationships with Beijing. And so to that extent that they use One Belt One Road and other mechanisms in the region to use trade and economic relationships that could offset resistance to some of those activities I think we see that too.

MR. GELTZER: Terrific. Well, next up will be a panel on the implications of counterterrorism in Asia but for now, please join me in thanking these three terrific panelists. (Applause) Thank you all very much.

(Recess)

MR. FELTMAN: Well, that was a fascinating discussion, and now we get to move into the question of the implications of counterterrorism. I'm Jeff Feltman. I'm a Visiting Fellow here at the Brookings Institution, and it's an honor to be on the stage with such distinguished panelists. There was a lot of discussion in the last session about preventing violent extremism, countering violent extremism. And Jeff, maybe you're the author of this, but when I was at the U.N., a few years ago, the Obama administration put a lot of pressure on then Secretary General, Ban Ki-moon, to come up with a report to member states about best practices, about preventing violent extremism. It was extraordinarily difficult to pull this off, partially because of the substance. As you heard from the earlier panel, what works, what are best practices in reality on preventing violent extremism it's a very hard question to deal with, but it was also extraordinarily difficult because of the politics inside the United Nations.

And we were part of the—we were the Secretariat, we were putting together this report, but the member states were watching us with incredible scrutiny for a couple reasons. One, is they saw the preventing violent extremism report by the Secretary General as basically being an invitation for the U.N. or other member states to interfere in the domestic policies of individual member states.

If we're saying you shouldn't disenfranchise entire segments of your population for fear that you could radicalize them that means we were passing judgment on what states were doing. So that was hard. But the other part, the other reason why it was so difficult was because there were some states that were really concerned that we started to question the implications of their counterterrorism policies, where their counterterrorism policies that actually created terrorists. And so I'm very interested to hear this panel talk about the implications of counterterrorism policy because it had a real practical impact on the work we were doing at the United Nations to fulfill a U.S. request to develop the report on preventing violent extremism.

The three panelists here bring a lot of experience from different perspectives, crossing from academic and research to government experience, and looking at different regions of the world in how they interact on counterterrorism. James Baker, at the far end, is a Visiting Fellow in Governance Studies here at Brookings. He's also had a very distinguished career in Government including four years at the General Counsel for the FBI. And he's worked on a number of national security matters that are of relevance to our discussions today, including the Foreign Intelligence Surveillance Act, and he also headed the Former Office of Intelligence, Policy and Review, which was part of the Department of Justice -- became part of the Department of Justice's National Security Division.

Dr. Jang, Ji-Hyang Jang, who just traveled here from South Korea for this policy is a Senior Fellow and Director of the Middle East and North Africa Center at the Asan Institute for Policy Studies. And if you look at the Asan Institute's website, as I did in preparation, and you look at the areas that this nonpartisan think tank in Seoul covers, it reminded me of Brookings, all the different source of areas that you cover at Asan. But Dr. Jang has worked in particular in researching the Middle East. You know, the political economy, the political Islam, in the Middle East and in North Africa, how this relates to democratization, to terrorism -- to the state building. And she's the author of a number of books and articles on this issue about the Middle East and North African.

And then immediately to my right is Professor Zachary Abuza, who's a Professor at the National War College in Washington, and he has focused on South Asian politics and security issues, including

questions that have come in the earlier discussions on governance and insurgencies, human rights and maritime security. He too, is a well-published author with five books, and a number of other studies on this issue. So I'm, again, honored to be here to moderate this panel. And as with the previous sessions, each of them will speak for 10 to 12 minutes, then we'll open up for questions. So, thank you very much.

MR. BAKER: Thanks everyone. It's great to be here. I appreciate the opportunity to talk about CT. I've been asked to focus on the issues related to civil liberties, privacy, and human rights. And so, some folks might find it ironic that the Former General Counsel of the FBI is giving a talk about that particular topic, but actually I spent a significant amount of my career worrying about those kinds of issues. And indeed, I've said before, that I actually think of myself in a significant way as a privacy lawyer, because that's been part of my responsibilities.

So, I'm most definitely not an Asia expert, so don't expect that from me, but what I think I'll be bringing that I think is transferable, you know, in a variety of different contexts, is some of the ideas, I guess concepts that I've learned dealing with these issues in the United States before and after 9/11, and some of the ways that we've approached it, and at least reflections about how I think about it.

And I'll also come at it from the perspective of, you know, in my career of having done both—having conducted and been responsible for assisting the conduct of counterterrorism operations, helping the operators achieve their objectives, and then also being responsible for conducting oversight of those activities through a variety of different means. And so, I'll try to merge those together and give you some reflections, perhaps some lessons learned, and with a focus on trying to synthesize some of the things that I've learned. So, I know in the audience it seems as though we have a range of different types of experiences so, you know, some people have been doing this for a long, long time, and are very well versed in how to deal with counterterrorism operations, and perhaps people who are less so.

So, if I can start out with this metaphor that I'd like to use to give folks a sense -- folks who have not actually been involved in counterterrorism operations before, to give them a sense of what it's like, and then that I think will help us think about -- help at least me -- helps me think about how to conduct

oversight of those activities to make sure that privacy, civil liberties, human rights are being respected. So, if I could just start off for a minute and talk about, and I think this kind of merges some of the things that we talk about before in the first panel, so, let me talk about counterterrorism and soccer for a moment, okay, or football for those of you who refer to it as football. So, counterterrorism and soccer: so a lot of people have used the metaphor that the objective of counterterrorism officials is like the goalie on a soccer team, and they have to stop every single shot at the goal and make sure that no shot scores, because if even one -- if the opponents take 100 shots and the goalie stops 99 of them, the one shot that gets through is a disaster for the counterterrorism officials.

So, that is true, but it is way, way worse than that, if you're conducting counterterrorism operations, way worse than that, because here's at least how I experience and think of it. Okay, so you're the team on -- your team is on the field trying to defend against the bad guys, and there are several problems. Number one is the bad guys -- one of two scenarios, they could be invisible, the other team that you're playing against in the soccer arena may be invisible, you can't see them on the field, which means it's extremely difficult to detect them, and you may not even know -- they might not even be there. It could be that you're defending against an opposing team that's actually not even on the field, you just don't know. You are -- it is extremely uncertain as to whether they're out there, and if they are, where they are. You have really no idea, and that's kind of what it feels like. That's sort of one part of it.

The other part of it is also that they could be wearing the uniforms of your team, because they're embedded -- for example, if you're trying to deal with counterterrorism domestically, they're embedded with your folks. They look like your folks; it's not easy to distinguish who is the good guy and who is the bad guy because they're wearing the same uniform. So this is rather problematic if you're trying to figure out who to deal with. It's worse than that though. So, you guys, if you're the counterterrorism folks, you're trying to deal with this, and you're wearing the uniforms and you've got your structure, and people have positions on the field that they have to play, and you've all agreed on that, and sometimes people try to encroach in different people's positions, and you get in disagreements with that.

And then it all happens, the bureaucratic infighting happens most definitely. But you are trying to follow

a set of rules that are established in a variety of different ways, and in theory are consistent with the laws of soccer. I think in soccer you don't have rules, you have laws. And they call them the laws of soccer.

So, you're trying to adhere to the laws of soccer. This other team, which may or may not be there, which may or may not be wearing your uniforms, really does not have to follow any rules. So, these nice little lines that you've got on the field, and the way that you set up plays, and you can't touch the ball with your hands, and that type of stuff, they don't care about that. They don't care about that. They're not following any rules whatsoever. In fact, to go back to the first analogy of, you know, just kicking the ball into the goal, they don't even have to stay within the lines on the field, and they can achieve their objective by going around behind the goal, lifting up the net and shoving the ball underneath from the back, right.

That's, they've achieved their goal, they've totally violated whatever rules, whatever conceptualization you had of how this is supposed to be done, and they've achieved their objective. They don't really care how they did it, but they've done it.

So, it's pretty bad. But it's even worse, because if you layer in technology, and the changes that are constantly coming at us in terms of technology, both from the perspective just the world is changing, and different -- and people, regular people, innocent people, society is using technology in a variety of different ways, the bad guys are using technology in lots of different ways. They're being very creative because they're trying to do a better job of avoiding detection by you, so that makes it harder.

And you're drowning in data, and you're trying to figure out how to access this data that you've got available to you, because you know if you don't use it in the right way, you're going to be blamed. And in addition, you're going to be blamed if something like that happens.

And in addition, the cyber security environment is terrible, and there are all kinds of problems and threats, and you can't keep your data or your system secure. So, back to the soccer field, if you add on the reality of technology, it's as though the soccer field itself, with all these problems I described, is now moving and undulating in unpredictable ways, and you're trying to predict, you're trying to play the game,

you're trying to play a defensive game to try to deal with these adversaries that may or may not be there, and may be wearing your uniforms.

So that's, at least in my mind, what it's like. I used to coach soccer so this resonates significantly with me. So, if that is how it is, then how do you as -- in an effort to protect privacy, civil liberties and human rights, how do you go about assisting the team on the field that's trying to deal with this reality.

And yet at the same time, make sure that they're conducting those activities pursuant to the rule of law, and that's what I think in terms of protecting civil liberties, privacy and human rights, it's all about protecting -- it's a about conducting intelligence activities under the rule of law. And I reason I focus on intelligence activities is because the main -- it seems to me the main driver of effective counter-intelligence operations is -- I'm sorry -- counterterrorism operations, the main driver or counterterrorism operations is to have effective intelligence.

To be an organization, this is what we aspire to at the FBI to protect the American people, this is our mission, protect the American people and uphold the Constitution, right. Do those things simultaneously, protect people, provide security and yet have freedom and privacy, and all the other rights that are enshrined in the Constitution and the laws of the United States, and to try to do those things simultaneously.

And to do that, we strove to be intelligence driven, so how do you collect this intelligence in this environment, how do you think about that? So to me I think, it's very important to think about, with respect to counterterrorism, and to have -- and to drive operations by having a clear sense of the goals that you're trying to achieve, and then having clear authorities that you have in order to be able to achieve those goals, and clear limitations on them. Limitations on what you're able to do.

To me, that is what intelligence under the law is about. To me that is what the rule of law is about. People throw around the term the rule of law quite frequently, and there's a lot of definitions, but I tend to think about it in terms of having clear, the need for society and including counterterrorism operations --

counterterrorism agencies, to have clear understandable rules that apply to everyone, and produce just outcomes.

To me, that's how I think about the rule of law. And when you're trying to conduct operations, and when you're trying to conduct oversight, it's critical to have clear rules, and it's critical to have clear limitations on what it is that you can do. And I think one of the problems that we have had over the years in the United States is, that what we think is clear, turns out not to be so clear. What we think are clear laws tend to not be so clear, there are disagreements about what the laws were actually intended to cover, and the disagreements about what they mean, there's disagreements about how to apply them in new context, there's disagreements about how to apply them to new technologies. And so this is -- anyway that's it -- clarity, the operators and the oversight folks need clarity, and that is not actually easy to obtain.

I'll just move quickly here. Intelligence officials need to collect intelligence through a variety of different ways in order to protect society. So there will be electronic surveillance, there will be confidential human sources, there will be undercover operations, you know, there will be captures and detention of people, there will be successes, and there will be failures, and there will be leaks with respect to all this.

So I think on the one hand we have to recognize that all of these things are going to happen. On the other hand, I think at least in liberal democracies, we have to recognize that, as someone said earlier about Confucius, that one of the central parts about governance is maintaining the trust of the people over the long-term. And so that's hard to do, and right now, I think post-Snowden, I think that's been a significant issue that says hindered, and made it more complicated, hindered the ability of governmental entities to conduct effective counterterrorism operations, dealing with this crazy technology environment that we're in.

But let me just go very narrow for a second, and then I'll wrap up. So, in terms of conducting effective counterterrorism oversight to make sure that we're protecting privacy, civil liberties and human rights, I think you need four things at least. And these are four key things; you need more than this, but at least a few things.

Number one is, you need to have effective management of counterterrorism agencies, it starts with the people who are in charge of these agencies, they are the first line of defense in making sure that the laws are adhered to, whatever those laws may be, and hopefully they're clear. And they're the ones that set the goals for the agencies, as they are set for them by the laws, the Constitution, other outside organizations.

You need to effectively manage, you need to have accountability within organizations, you need to have transparency within organizations so that leaders can understand what the heck is going on at the field level. If you don't have that, if the managers are not running the organizations effectively, you're basically doomed.

You do need clear laws, and I'll mention that a little bit, and I won't go into it too much, and you need to have them across all the different elements of the intelligence cycle, establishing requirements for intelligence, collection analysis and production and dissemination of information. You need to have clear rules with respect to all of that, that are sensible, that allow for operators to actually get their jobs done, and that are continuously improved over time because this is not a static environment that we're dealing with.

The third thing is, you need the right people in these jobs. The people actually matter, these are governments of people, they're not, yeah, are not ruled by AI yet, but so you have to have the right people in the jobs, or the right values, the right abilities, the right skills, and you have to have the right culture in these organizations. The culture of counterterrorism organization is critically important, especially the culture with respect to protecting civil rights privacy, et cetera.

And the fourth thing is that you do need outside oversight, you must have that, and it must be effective, and it must be conducted by people who actually know how these things are done. If you don't have that, and if people are so detached and removed from how actual counterterrorism operations are done, they're not going to know what questions to ask, they're not going to know where to look, they're not going to know what rock to turn over to understand that. If you don't have that, if you don't have meaningful,

robust oversight, then it is extremely difficult for organizations to -- for us to protect privacy, civil liberties and human rights. It has to be transparent, it has to be meaningful, it has to be efficient, and it has to be sustained.

So you need both the internal controls, external controls, clear rules. Those I think are what the essence of being able to both, simultaneously, deal with the soccer scenario that I laid out, and yet making sure that the team is doing what you want them to do. So, with that, I'll pause. And turn it back over to everybody else. (Applause)

MR. FELTMAN: To Dr. Jang?

MS. JANG: Hi. I'm Ji-Hyang Jang from the Asan Institute for Policy Studies. And first of all I'd like to express my dear gratitude toward Dr. Jung Pak, and the Brookings Institution for giving me this really exciting opportunity to talk about, you know, Korea and terrorism.

So, actually my topic is about implications of Korea's CVE policy, for like the Korean Peninsula, and Northeast Asia, and probably for the international community. But before I go to the main topic, let me briefly present about -- I don't know -- the relationship between Korea and terrorism or, you know, closer relevance between CVE, countering violent extremism in Korea.

Because in Korea we don't have many returning Jihadists, and we don't have to worry about, you know, valid evidence collected from Syria and Iraq to prosecute, you know, the Jihadists. And we don't have to worry about, you know, reintegration, rehabilitation for the returning Jihadists.

But we do have crucial issue related to the countering violent extremism in three different ways. Okay, first, the Koreans got – and is getting terrorist attacks not inside Korea but outside. Somehow we have a very small, tiny Muslim community inside Korea. We have 150,000 Muslims, and initially we have a really small number of foreigners like two million foreigners that account only for 4 percent out of entire population of 50 million.

Maybe because our immigration policy is more like assimilation, rather than, you know, multicultural, and like a tolerance-driven one. So, we have very homogeneity character inside Korea. But because of North Korea, which kind of land locked to South Korea, we should go out, so we went out through the expert-orientated economic policy, so many Koreans travel all over the world so intensively, and many Koreans do our own business outside Korea, and many Korean students are studying abroad, indeed.

So, we have many Samsung, Hyundai, LG, Kia, and the companies all over the world, and especially in the Middle East. And that's why so many Korean civilians, especially business people fell victim to the Islamic extremist terrorism. So we do have crucial relevance with the extremist -- violent extremism. And secondly, many of us might know that these days the ISIS people are not really, really just like -- I mean, they're different from al-Qaida.

Al-Qaida, are dying to win; before the ISIS, they just die for nothing. I mean, they're just dying without any particular reason, so we know that the root cause of recent youth radicalization is not really related to Islamic ideas, per se. You know, let me take example of ISIS, ISIS is a multinational, multilingual, multiethnic terrorist group. All the grassroots people, I mean members of the ISIS came from over 90 different countries, and they don't know how to read Quran, and they have no idea what Islam is, per se.

And maybe that's why we defeated the central leadership of ISIS so easily. Meaning that, you know, the ISIS grassroots members, they became the member through Internet, by self-selecting and, you know, bottom-up recruitment mechanism. So, they don't really don't care about central leadership, they don't respect the hierarchy, and they don't really listen to the order system inside ISIS. I mean, one of their main culture, if there's any, is internal egalitarianism. They just go out, operate, you know, terrorist attacks, very sporadic way, and then after they finish operating the attack, they might or might not report to the central leadership that they did.

So, given that, you know the current violent extremism it's not really related to religion or Islam. Many of us in Korea are worrying that, you know, like young Koreans who call their home country as inescapable hell dynasty, due to the -- due to, you know, the crazy intensive extremism, and extreme competition, and

high suicide rates, and entrenched inequality might turn out to be violent extremism through Internet. So, it's not really, you know, visible yet, but we are also really ready -- I mean preparing for playing soccer with the invisible team player.

And the third point is that Korea just wants to be a global actor who is responsible, so we decide to join the Anti-ISIS Global Coalition back in 2014, back then the member was like 64, and now we have 79 members of Anti-ISIS Global Coalition. And in 2014, the ISIS listed Korea as one of the Crusader, you know, target. So, we really have, you know, crucial relevance between ISIS or violent extremism.

And let me move on to the main point, if I may. Okay, I have two points to cover, the first one is Korea's cooperation with the international community to combat terrorism, and the second point is about, you know, how local authorities can enhance the effort of national, regional and international policy to CVE.

I guess the answer to the first question is nicely related to the third point that I just talked about. Korea wants to be a responsible, global leader, or player. Okay, we wanted to do that because we wanted to show—I don't know—to the international community that we do respect the international norms and principles, and we are ready to really uphold, you know, the Liberal International Order, and there is a little bit competition going on with Israel as well with Japan, which is a very healthy one, not really crazy, extreme one. So, we have a little competition. We facilitate our activity more in the global coalition and international community.

And the third one, which is most important, we really wanted to uphold our international, you know, norms and principles, and wanted to really, you know, stick to the Liberal International Order because otherwise, you know, we will encounter setback when we're dealing with North Korea and the Korean Peninsula issue, because we know that we really need to have the international support and legitimacy when we're dealing with, you know, the Korean Peninsula issue.

So, it's not really is about, you know, investment or something, but we are trying so hard to stick to the International Liberal Order because we're dealing with North Korea. And as for this, you know, Korea's

cooperation with the international community, there are kind of ongoing dispute regarding the issue, two of them.

The first one: how can we help the Syrian people without helping Bashar al-Assad Regime? You know, Korea's international cooperation role is limited between humanitarian assistance -- humanitarian assistant provider, we are not really fighting on the battlefield. And we are worrying about that issue because, again, it's a little bit related to the Korean Peninsula issue.

We are keenly observing the rise of the Iranian hegemony right after the defeat of ISIS, and then the victory of the al-Assad regime after, not really after, but in the end of the Syrian Civil War. Okay, the regional power configuration in the Middle East after ISIS, you know, after the combat against the ISIS, is led by Iran and Russia, and supported by Turkey and China.

And especially we are -- really witness that there is, you know, the presence of Iranian hardliners, the IRGC, the Revolutionary Guard, in Sanaa and Baghdad and Beirut, and Gaza Strip, not to mention Damascus, we are worrying because those, you know, pro-Iranian hardliner forces in Yemen, Lebanon, Iraq, Syria, in Gaza Strip, are just good customer for the illegal, you know, weapon selling of the North Korean regime.

So, given that critical, you know, analysis, or observation, again, how can we help the Syrian people without helping Bashar al-Assad, which is just such a good friend of, you know, Iranian hardliners? But then we know that we need to serve our role as a humanitarian assistance provider for the humanitarian disaster in Syria. So one of the alternatives could be the demining project for the Northeastern Syria where, still, the U.S. Army is locating and occupying. So, we are thinking about that particular project to help Syrian people.

And the second issue, the second kind of ongoing dispute regarding our role as a humanitarian assistance provider is that, again, it's really, this one is also related to the Korea's position and Korea's national interests as well. Under Trump administration, many, you know, kind of U.S. allies are observing that, you

know, these days, allies often are treated as, you know, free rider, or abandoned, or kind of treated as disposable one, and we saw that evidence when we looked at the Peshmerga by the KRG, Kurdish Regional Government, we are specifically interested in the fate of the KRG because during the Iraq War we stationed in KRG.

So, I know that KRG did a little mistake because the U.S. and other, you know, allies highly discouraged them to have independence, referendum election last year, but they did. And then they got -- kind of abandoned it despite all the contributions they made in the war against ISIS. So, okay; the alliance is quite important when, especially we talked about, you know, some countries cooperating within the international community. So, that kind of evidence or case is like discussed during the think tank community in South Korea.

And my last point, which is not really long, it's about how local authorities can, you know, reinforce the international and national efforts. Okay before even Mr. Kim Jong-yang, a Korean, was elected as the Chief of Interpol, I heard several times from my Interpol colleagues that Korea is very good at, you know, sharing information and sharing data, so far we deported 60-something -- 60-some foreigners who had connection with the extremist groups, and then we arrested about six who had strong ties with Al-Nusra Front, and we found out that seven foreigners who left Korea and then later joined the ISIS.

And those, you know, achievements were possible, thanks to the information sharing between Interpol and Korean authorities. So, I mean, maybe you got bored, but I wanted to, again, emphasize that the information sharing between local authorities and international community, and the international authorities are really crucial. So, that's the thing, but surprisingly or not surprisingly, I heard that the main problem between, you know, the cooperation is the cooperation problems, it mostly come from the internal administrational, you know, dispute or rivalry inside the country.

So, when I had conversation with my colleagues from European countries, and the United States, or from the Middle East, they're always complaining about, you know, the interagency or inter-administrational dispute, the friction rivalry. And Korea is not an exceptional case, and in Korea we have five different

agencies, dealing with the same issue, CVE.

We have Ministries of Foreign Affairs, and National Defense, and also NIS, National Intelligence Service, and National Policy Agency, and Director Mun's Counterterrorism Center -- Counterterrorism Center under PM's Office. And not surprising they're fighting, and that's not new. And I even witnessed that even inside foreign ministries; I mean, I often work with foreign ministry people so I see more of the mistake from them.

Even inside the Foreign Ministry, there's no really coherent, you know, policy toward CVE. For instance, like the foreign ministry, you really wanted to, you know, secure the citizens abroad. So they say they try not to provoke terrorists. So, why don't we kind of hide our active, you know, global coalition cooperation effort, because, you know, don't mess with the terrorists. So, that could be the problem as well.

So let me wrap up. Okay. We're fighting a very difficult combat. It is difficult because, you know, democracy is such a feasible target for those violent extremists, because we have open systems, we really do not put, you know, QR code on everybody's household gate. And we have obligation to protect our citizens' security, and also privacy, so it's quite, quite, quite challenging. But my presentation's summary could be that, okay, the fight against ISIS is done, and then Bashar al-Assad became a winner, not surprising Iran and Russia became the winner, and China and Turkey are helping them. And Koreans are really worrying because we know that there's strong connection between those bad guys in the Middle East, and some in North Korea. Thank you. (Applause)

MR. FELTMAN: Thank you, Dr. Jang.

MR. ABUZA: Thank you very much for having me here. It's been a real pleasure to be invited. My general disclaimer, that I am here in my own capacity, I do not represent the Department of Defense or the U.S. National War College. I study Southeast Asian militant groups, and so I do thank you very much for giving me this opportunity to talk more comparatively about what works in terms of counterterrorism.

Terrorism in Southeast Asia is a persistent, but it's a very manageable threat. And I don't want to blow it out of proportion. And the other thing that we need to always think about is the fact that terrorism and terrorist groups are in constant flux, and there are five things I would like to quickly put out there, that we need to always be thinking about. How the threat of terrorism in Southeast Asia has metastasized since its al-Qaida origins, with Jamas Lamya into pro-Islamic State groupings. We also have to think about the implications of the loss of the Caliphate in Iraq and Syria, and how that is going to impact Southeast Asia as the Islamic State morphs into this global insurgency model. What does that mean for Southeast Asia?

There was a recent a declaration of an East Asian Wilayat a province of the Caliphate. We are still waiting to see how that manifests in Southeast Asia, but it has some implications to be sure. We also don't really know how the loss of the top four Southeast Asian leaders in Iraq and Syria is going to manifest in the region. They have been replaced by the B Team, they have less following, less importance in terms of controlling networks, social networks, financial networks.

And then finally, we're always trying to determine what do we mean by foreign fighters in Southeast Asia? Are we talking about the North African suicide bomber in Basilan very recently in the Philippines? Or are we simply talking about Malaysians and Indonesians making their way into Mindanao.

I want to focus my comments on two countries. I could talk much more broadly on Southeast Asia, but I want to stay focused on Indonesia and Philippines, kind of bookends on what works and what doesn't always work there.

Indonesia has had actually superlative counterterrorism since the Bali bombing in 2002. I can really not think of any country that has done a better job in countering terrorism, mitigating the threat, while at the same time defending the rule of law and democracy, and this is in a very fragile new democracy. Don't forget the Suharto fell in 1998 and had a very messy transition to democracy. Four or five Presidents in four or five years, it was a lot of turmoil. Indonesia has arrested around 800 people since 2002, and put almost all of them on trial, so this has really helped build up the rule of law and build up the judiciary in the country.

Now the attack that Ms. Hori mentioned earlier this morning, in Surabaya last May, the suicide bombings, this was an unprecedented attack. It included the first female suicide bomber in Southeast Asia, not to mention there are children, down to seven years old. It was a horrific attack. It was the catalyst for many new policies, some counterterrorism bill had stalled in the Indonesian Parliament, for many reasons. And then kind of after the attack it was railroaded through.

Now, the CT law, the new one, has some positive aspects, it criminalizes joining terrorists groups overseas. So, until that point, you could be in Indonesia and you could go and join ISIS in Syria, and that was not a crime. So, all of a sudden that is a crime. They lengthened jail terms for prison sentences. This might not seem like a big deal, but if you think about the Bali bombing, that 202 people were killed in back in 2002, other than the three top guys who were executed, every other person that was arrested in conjunction with that terrorist attack is free right now. So, prison sentences in Indonesia have been very short and so we're going to see longer sentences. Many more tools for financial investigations, and this is very important. Governments in Southeast Asia were very slow to understand the importance of financial intelligence units in countering terrorism. Indonesia finally has really started to appreciate the use of those tools. We've also seen that the Court has banned the Umbrella Organization for Islamic State in Indonesia. Now, I can argue that that's counterproductive, but it does authorities new tools.

And we've also seen Indonesia really get far more resources for their Elite Counter-Terrorism Police that was established in 2002. And this was so important because the Indonesian National Police, until 1999 was actually part of the Military, and it was very martial, it was very corrupt, and so the United States, with the help of Australia and Japan, put together this independent policing unit. Very, very high levels of *esprit de corps*, professionalism, and they were very well paid, they did a fantastic job. But there are also controversial provisions to the new law. The ability to strip citizenship, I have fundamental problems with this as both a human right, but do we really want these itinerant Jihadists roaming around.

I'm concerned about the increased use in preventative detention, and I'm very concerned, especially for the sake of democratization, that the new law gives the Indonesian Military a formal counterterrorism rule. And it's necessary in certain places, I understand that, but I also see it as part of a larger process of

the Indonesian Military trying to claw back many of the political powers, and the economic powers that they've lost since 1998. And I think it certainly plays into the Jihadist's narrative that the state is oppressive and anti-Islamic.

Now, the new powers, and with those new powers, since Surabaya you've had the arrest of almost 200 people. Now that might sound good, except it reinforces the salience of prison reform, and I can think of no country that needs prison reform more than Indonesia. First of all, prisons remain very permissive environments in Indonesia. The top two Islamic State Leaders are in prison in Indonesia, and they still get their sermons out, they still recruit, and they still are able to orchestrate attacks from behind bars. Twice in 2018 IS convicts took over prisons in the country. Now, the first time might be forgivable, the second time, we've got a more -- a larger problem here.

Indonesian CVE programs are actually quite good, they're very different than Malaysia's, or Singapore's, which I'd be happy to discuss in Q&A, but Indonesia also has very limited resources for these types of programs, and on top of those short prison sentences so far, they had very little in the way of post-release monitoring authorities, there's no system of parole, the police are simply spread too thin to deal with these things.

Now, another thing that we've seen in Indonesia of late is a willingness to take on big technology. Indonesia is not a small country, and people are very actively involved in social media. Telegram was the big player in terms of being the forum of choice for Jihadists. In July 2017, the government threatened to shut Telegram down until they shut down certain channels. And Telegram actually complied and shut down 55 channels. Indonesia forced Telegram to open an office in the country, this is what Ms. Sacks was talking about before, in terms of data localization. Now, all of a sudden when Telegram does not comply, they have legal skin in the teeth. You have executives that can be hauled to jail.

So, there are different tools that can do -- there are still limits to what we can expect in going after the big tech and social media, simply because there are too many technical work arounds, mirroring encryption, et cetera. I have other concerns about Indonesia. There are around 600 Indonesians in Iraq and Syria,

many of whom are women and children. They brought entire families. So, what does it mean, when we start to get those reintegrated back into Indonesia? They really haven't thought this through very well.

They've had other problems. The group, not everyone in JI, the al-Qaida affiliate, joined Islamic State. JI social networks are very robust in the country, as the government we would say, they're left of boom. They're not engaging in violence, and the government has given them enormous space, but their social networks, their Mosques, Madrassas, kinship ties are still very strong. They're lying low right now, because they're just letting the IS groups take the body blows. The government policies on Shi'a sects and other, what are called deviant sects, is not helping the matters, Indonesia used to be a very tolerant and pluralist place, it's much less so right now. Now, I'd like to end Indonesia on hopeful points. First of all, I give inordinate credit to the Indonesians for the social resiliency they have in terms of dealing with terrorism. Islam and Indonesia traditionally has been very syncretic, it's built upon a very rich Hindu culture, while Salafism is growing in the country, and it is growing, there is still a lot of pushback.

You know, just yesterday the Saudi Ambassador really put his foot in it, when the called the Nahdlatul Ulama, which is the largest Muslim organization in the world, a deviant organization. That is going to cause a huge pushback. That same Ambassador, just today, was shown embracing one of the Bali bombers, Abu Jibril, one of the founders of JI, and causing a huger uproar.

The other thing though is some of the creativity in countering violent extremism, and I'd like to point attention to two schools that have gone up. The Indonesian Government has allowed schools for terrorist children. And in fact one of these schools was founded by a terrorist suspect from behind bars. He went to the Head of the counterterrorism authorities and said, listen, we've got a problem, I'm in jail, no one is taking care of my kids, they're going to resort right back into IS or JI social networks. We've got to get them out of these Mosques and Madrassas.

And they set up a school where all these children from terrorists, including one of the survivors of the Surabaya bombing, a young little girl, are now being educated at the expense of the state. Now, I really would love to see any discussion of that getting through the FBI's legal office. There's no way in hell we

would ever encounter something like that. But it's very creative in saying: we've got to get out of these social networks.

Let me move on to the Philippines, because the Philippines is very important, not just for the sake of security, the Philippines which is the treaty ally of the United States, but more broadly, because what happens in the Philippines does not stay in the Philippines. The Philippines has much broader regional security implications. We found that when terrorists need a place to lie low, or train, or prepare other attacks in the region, they do so from the Philippines simply because there is so much, maybe not ungoverned space, but very poorly governed space.

There is an alphabet soup of different groups in the Southern Philippines, secessionists, terrorists, but this very confusing pattern, and I've spent 25 years studying these groups, and it still confuses me sometimes. It's very easy, for different organizations, to come in and graft on, to manipulate them and use them for their own purposes.

We saw in 2017 a five month siege of the City of Marawi taken over by Islamic State Militants, or pro-Islamic state militants. And this really just underscores the ongoing weaknesses and capacity of the Philippines security forces.

The other important thing to note about the siege of Marawi was it was the first time that I can really think of that you had two different militant groups there that worked together. Luckily, even though we have this alphabet soup of different groups, they tend to be very divided by ideology, or ego more likely.

And so, they've just been -- we've never had to confront our real fears that these groups would start to act as one. And luckily, they've been so divided that they've been a manageable threat. Let me also mention the fact that the Philippines, because of the ungoverned space, really matters as IS morphs into this global insurgency. You cannot be a province of the caliphate unless you actually have territory. And, you know, you can have IS cells in Malaysia or across Indonesia, but nowhere in the region, other than the Philippines, can these groups actually, physically control space.

And that in itself will be a draw. We have seen these groups -- the Islamic State, for years, going back to 2014, tell militants, if you can't make it to the Islamic State Caliphate in Iraq and Syria, make your way to Mindanao, and they've been doing this. And so Mindanao will continue to be a draw. And I think that one of the reasons why it's so important, it's not that these foreigners can come in and necessarily have more expertise, bomb-making expertise. The most important thing that these foreigners bring in is some credibility, sometimes financial ties, but most importantly, they are able to bridge some of those parochial divides we see that divide Filipino groups.

The last thing we need to talk about in terms of countering terrorism is to think about maritime domain. We might not think about this in other parts of the world, but in Southeast Asia the maritime domain is absolutely critical. The TRI, a nation border region between the Philippines, Malaysia and Singapore, is really critical. We're seeing that's how foreign fighters get into Mindanao, it's how militants get in and out, but on top of that we've also seen a spate of maritime ship-jackings, and kidnappings which helps fund terrorists' operations. And because this -- the organizers from Northeast Asia, let me kind of conclude on this tie in to that, from March 2016 to the end of the year, we saw a spate of maritime kidnappings. Most of it was of Indonesian and Malaysian fishermen, tugboats bringing coal from Indonesia up into the Southern Philippines. But all of a sudden the ship-jackers started to get a little bit better, and a little bit cockier. And they took over a South Korean cargo vessel, kidnapping their Captain.

They went after large ocean-going Vietnamese ships, and they also tried to board a Japanese ship, luckily the Japan crew was able to take evasive actions, and repel this. But this is going to have implications for regional security. It's often said that piracy is combated on land. I would make the case that in Southeast Asia terrorism, in many ways, is combated at sea. We really need much in the way of better policing in the maritime domain from those three countries, unfortunately the Philippines, Indonesia, Malaysia all have very limited maritime capacity. Outsiders, the Americans, Australians, would love to help, the Singaporeans are itching to get in, but right now, unfortunately, we are not able to sufficiently bridge some of the sovereignty issues, and challenges there. So, let me leave it at that. Thank you very much for having me. (Applause)

MR. FELTMAN: We have about a-half-an-hour. Panelists, you'll need to put your microphones back on. We have about half-an-hour left in this panel. I want to thank the panelists for their very good insights. And since the time is short, I'll just confine myself to one question to you, Jim.

Jim, you gave a good list of elements needed to be able to protect privacy, you know, in respect to human rights, et cetera, while doing counterterrorism, and one the things that you said, was that you need clear laws. And of course there needs to be a clear understanding of what those laws are. But given the technology, and given often the paralysis that we see in this town, on Capitol Hill, how hard is it to get the clear laws in a timely fashion, for counterterrorism work?

MR. BAKER: Obviously very hard. I mean, I think that's one of the significant problems that we have, and something that government leaders need to grapple with. I think government leaders and the Legislative Branch, the Executive Branch, and the Judicial Branch, across the board, all struggle with understanding what the technology is, what it means -- and what it is, that's hard enough to understand.

MR. FELTMAN: Yes.

MR. BAKER: And then what implications it has for how adversaries are using it, and then how we deal with it, what data is being generated, and then how best to control that. So I think, quite frankly, organizations like Brookings, and other organizations need to help show the way forward, come up with creative ideas to -- well, to help them understand what's going on come up with creative ideas to do it.

But the process, the laws, as other people have observed, you know, in the United States the laws that protect our privacy are a complex patchwork of rules, that really don't address these issues adequately, and I think quite frankly now, the Europeans are way out ahead of the United States in terms of thinking about privacy.

There are efforts ongoing in the U.S. to try to change that. California has a new statute, there's work to try to come up with a federal statute, but it's a lot of work but it needs to be done, but it's not something as

you allude to, it's not something you could just do it and then forget about, you're going to have to keep up with it, because technology is just moving so quickly.

MR. FELTMAN: Thank you. We have one question here from our Chair.

MS. PAK: Thanks so much. I really like James', you know, the analogy to the soccer game, and that was in the U.S. context, right, but how do we expand that to the international context, where you know --

MR. BAKER: I think it applies to everybody.

MS. PAK: So not everybody explained whether -- even though the people on your team are not playing by the same type of rules, you know, worries about sovereignty, what liberal democracy is, what kind of governance methods you use. So how does that work, when at multiple levels you have conflict? Dr. Jang talked about the silos and, you know, the bureaucratic in-fighting. Jeff, in his comments, in his introductory comments talked about the problems that the U.N. saw in trying to get everybody -- in herding cats, and to deal with the individual's country's concerns about independence.

And so I was wondering if the speakers, you know, from the Southeast Asian perspective, from the South Korean perspective: who should lead, and how do you make sure that everybody is playing by the same type of rules?

MS. JANG: I think Mr. Baker's, like the analogy of the soccer game to the CVE is really perfect. Okay, for instance, when we are talking about the players, so we really do not include, you know, the non-members of the 79 Anti-ISIS Global Coalition, we do not have Chinese player, Russian player, and others, who really don't want to respect the international norms and principles and liberal order, and not to mention Iran, Syria.

But we do have 74 countries and 5 international organizations, and when we limit the members or players to the 79, the Anti-ISIS Global Coalition, then his analogy applies perfectly.

MR. ABUZA: I would say it's not just silos. But the silos are real and competition over scarce resources reinforced those silos, but it also makes international cooperation, and there has to be international cooperation because it's a transnational threat. Those silos make international cooperation harder, and we're going from country to country with their different political, social, legal cultures, can often make it very hard to find appropriate organizations as counterparts with similar legal authorities. Right?

So, Malaysia and Singapore can cooperate quite well because they have the tradition of the British system of the Special Branch, which has intelligence functions but not policing, that all of a sudden it gets different in other countries. In the Philippines where the military really has the primary responsibility, how can the police of other countries correspond? And so, we have those problems on top of it, and we just don't have a single, really good way for all these different security forces to share information. We certainly know that they're unwilling to share information.

We've come a long way since 2002, but still a long way to come. So the silos, it's a real problem. I'm concerned in Indonesia that the silos are actually getting taller and more of them.

MR. FELTMAN: Please?

QUESTIONER: Ned Megoo from *The Straits Time*s. I think I should address this to Zachary. From the earlier panel, Audrey Cronin had mentioned that terrorism is increasingly indivisible from organized crime, and I wonder if you share that assessment and if you could, possibly sort of parse it a bit for us. Thank you.

MR. ABUZA: Well no terrorist group I can think of right now in Southeast Asia has state sponsorship, and so obviously money comes in and all groups engage in some degree of criminality to support their operations. So, there is, you know, at what point is it crime if it's there to support the terrorist operation. And I think when we think about some of kidnapping in the Sulu Sea, how much of that is done by freelance fishermen who then sell hostages up the chain of command. And let me give you very clear example of this. They treat Filipinos very differently than they treat Malaysian and Indonesian captives

versus Western captives.

And we can see it in the price people pay for the ransoms, right? $10,000 for a Filipino, it's $100,000 for Malaysian and the Indonesian fishermen, and then, boy, once you get some Canadians or Europeans, you know, we are talking millions.

So, we do have that. I would also go back and look. We had some of this debate, and tying it into what Ms. Sacks was really talking about with the Uyghurs, they were pressing against the Uighurs in China. We've seen a steady stream of Uighurs going out of -- via Southeast Asia, Thailand, which you know very well, into Malaysia, and then onward to Turkey where they've been given more or less sanctuary.

And we had the Chinese put a lot of pressure on the Thais, and as you remember, the Thais forced these people, many Uighurs back. The women and children they got up, but they returned the men, and the images of this were very harrowing, you know, the black hoods and two policemen per captive on the plane. And these people were more or less never to be seen again back in Xinjiang.

There was a terrorist attack in Downtown Bangkok which was woefully mismanaged by Thai authorities, and a lot of it was pressure from Beijing. And the Thais like to say that it was a revenge attack because we crack down on human trafficking so effectively. That made no sense. You know, why would you launch a major terrorist attack in a country whose -- you know, the linchpin of the economy is tourism, to protest crackdowns in those networks. So, I don't think it's completely indistinguishable, sometimes I see governments really try to make the link when it doesn't exist.

MR. FELTMAN: Let me ask. Let me follow up on that if I may, Zachary. As opposed to Uighurs actually leaving and going elsewhere, do you see examples in Asia of the plight of the Uighurs, the Chinese policy towards Uighurs inspiring others? Or the Rohingya expulsion; or the extremist Buddhist attacks in Kandy, Sri Lanka, in March. Do you see these sorts of policies inspiring radicalization, extremism and terrorism?

MR. ABUZA: Let me start with the Uyghurs. I am agog that the Chinese treatment of the Uighurs has not come back to haunt them in any way in Southeast Asia. It really hasn't, and I don't know if that's because China is simply, the reality is there, the largest trading partner of every country in Southeast Asia, and they just have that much leverage, and the promises of BRI and AIIB funding, you know, forces the governments to crack down.

Indonesia arrested a number of Uighurs, a small number, but a number of Uighurs out in pro-Islamic State grouping, simply because it was easier for them to get there than make their way into Syria, where there's much more attention.

China sent their first -- you know the first case I can think of where they sent senior intelligence officials to sit in the courtroom during these proceedings and really tried to strong arm the Indonesian Government to render them back to the country.

Indonesian Government said they would and yet there's been enough public pressure on them, but they haven't so far. Now the Rohingya is a much bigger issue, and I think this is going to be something to watch down the roads. Ayman al-Zawahiri issued a statement after that pledging revenge on the Myanmar Government, and that was followed by a mishmash of different responses, competing responses from the Islamic State, but so far, and I chalk it up to nothing more than prejudice, no one has really come to do anything in the name of the Rohingya.

We've seen a steady stream of Southeast Asian militants try to get into Bangladesh in solidarity with them, the Malaysians have arrested a number of people en route, the Singaporeans are obviously keeping very close tabs on this, they have a lot of migrant workers from Bangladesh, and have been cracking down on some of the funding flows, the remittances back there.

But so far we haven't seen it. A number of years ago, not that long ago, there was a Rohingya organization that tried to blow up the Myanmar Embassy in Jakarta, I imagine that Myanmar assets around the world, assets and interests, will be targeted in the future. So far we haven't seen it, but it's coming.

MR. FELTMAN: Thank you. Yes?

QUESTIONER: Hi. I also had a question for Zachary. You mentioned that there will be implications of ISIS declaring its East Asia Branch an official province, so I was wondering if you could expound a little on what those implications might be, and kind of how that will play out with the networks in Southeast Asia's connections back to Syria.

MR. ABUZA: A very good question. Let me start with this. You had all these different groups and cells across Southeast Asia declare *bai'at* to the Islamic State starting in 2014. The Islamic State didn't recognize any of them until early 2016, it really took a long time, and I can't tell you why, if it's just racism, or if it was just -- the Islamic state was growing so quickly, and they were so busy -- builds in their caliphate they didn't even need Southeast Asians. 2016, they recognized them, but they didn't declare the caliphate until this past year. So, again, is that part of the fact that, ah, if we've lost the caliphate we've lost 99 percent of our territory, and we've got to think about a global insurgency model. That could be part of the implications.

I've been reading -- I don't want to talk trash and be a petty academic -- (laughter) -- There were some people that see the declaration of the caliphate as much more centralized and dangerous than I think it is. I think it's still very aspirational. I am just not convinced that the declaration of this caliphate is all of a sudden going to unite all these different cells and groups across Southeast Asia into one centrally-organized force. I just don't see it.

It's never happened before. If history is a guide, it's not going to happen now. It could pave the way for more funding coming in, but again, the top IS militants who've been in Syria, you know, for four-plus years, they've been killed, and it's really a B-Team. I imagine it matters in terms of propaganda and the narrative, but in some ways, the declaration of this province, show me the results. You know, in terms of real attacks and the ability to challenge states, I don't see it. And if anything it makes me thing that the IS is weaker than maybe I thought it was.

MR. FELTMAN: Hmm! Others, please? And then afterwards, just behind.

MR. TAYLOR: Terry Taylor. Thanks for your excellent insights. Every speaker both in this panel and previously has stressed the importance of international cooperation. I wonder if we could explore the character of the most effective form of international cooperation. Having worked with the U.N., having been involved in the counterterrorism implementation taskforce myself, 38 entities trying to work together. It seems, and we've heard mention of Japan's direct assistance, bilateral assistance, Korea's direct bilateral assistance, it seems to me as someone who has worked in this area internationally for some years, that that is the most effective. It's bilateral assistance. Or even sub-regional assistance.

Is there a better way we can handle the international cooperation? Obviously we have to work at the global level or work downwards, and especially things like the Financial Action Taskforce, for example, can be very effective. So, either it's bilateral or maybe sub-regional groups, plus specialist groups, that make the most effective contribution. Am I right? Or is there more we can do at the global or broader regional level? Thank you.

MR. FELTMAN: Dr. Jang?

MS. JANG: So this is a comment, right, what there a question?

MR. FELTMAN: Yeah. What can we do more effectively at the international, regional, global level in these areas?

MS. JANG: I think we are in a good shape.

MR. FELTMAN: I'm a Moderator, I'm a Moderator so it's -- I probably shouldn't jump in here, but following up on your comment, if I may. One thing that frustrated me when I was in the counterterrorism positions in the U.N., as part of my Under Secretary General position was, there's all this flurry of activity to pass Security Council resolutions on various aspects of counterterrorism, whether it's API, or other

issues, there's no follow up.

There's no follow up, there's no -- that the countries that are sponsoring these in the Security Council get all excited to get support for whatever the particular initiative is, and then they move on to something else. Where there should be the type of pressure on countries to comply with these Security Council resolutions that are usually passed under Chapter 7, they're obligatory.

And when you do a survey of how have these counterterrorism conventions -- resolutions were implemented, there's enormous gaps in countries, and yet there's no reputational risk to the country of not complying.

MR. BAKER: If I could just interject. I mean, I think -- I don't if it's a direct answer to your question, but I think that what actually happens is that the entities within governments that have the greatest incentives, because they have the greatest risks and the greatest responsibility to make sure that there is cooperation, are the agencies with sort of the boots on the ground, so to speak, both domestically and foreign.

So, for example, intelligence and law enforcement entities have extremely robust relationships with each other that have developed over time, that are sustained over time, because they have the need and the incentive to sustain those. And those are not visible to most people.

Those are not visible -- there's not a big show about them, there's not big pronouncements about them, there are not big international conferences, or whatever, they are sustained, existing relationship -- sustained relationships that have existed for a long period of time that are effective.

Now, there are significant, I think, over recent time, the technology piece that we've talked about, I think that raises a significant issue for them as data is located in one location or another, and the local laws prevent or make it more difficult for foreign entities, for example, to get data from the United States has been a particular issue over time, and a sort of a thorn in the side of the relationships, I would say.

But I think, focusing more on those, making sure that those are robustly supported over time I think is going to be -- that's what's actually happening, I think, regardless -- that's sort of what the undercurrent, regardless of what's happening at the wave tops.

MR. FELTMAN: Professor Abuza?

MR. ABUZA: I think regional leadership matters in many ways more than kind of the global top tier leadership. In Southeast Asia, if Indonesia is not willing to take the lead on something it really doesn't happen. And right now they're in a very reticent political mood.

You know, there was very little counterterrorism cooperation before Bali. After Bali, Indonesia took the lead, and they could. That's one thing to think about. But going back to bilateral cooperation, you know, sometimes that can be very counterproductive. You know, look at what the Americans have done in the Philippines. You know, it creates at some point, moral hazard. Does the Philippines Military, you know, even with their increased $4.4-billion budget, 85 percent of that goes to personnel costs. They have challenges of trying to modernize to deal with China even if Duterte is not going to stand up to China is perhaps it's their claim.

What incentive do they have to finish off the Abu Sayyaf? They have $15 million a year in U.S. counterterrorism assistance, after Marawi the Singaporeans started pouring money in, the Australians are pouring money in, the EU is pouring money in. And sometimes we create these moral hazards, you know, we are too quick with the checkbook. I really don't think we do a very good job at holding countries accountable and having benchmarks.

MR. FELTMAN: Yes, Dr. Jang?

MS. JANG: The reason I was a little cynical about the -- for the international cooperation to combat terrorism is because, again, these days those ISIS guys are not really a visible, you know, target or enemy.

The ISIS is different from al-Qaida, and therefore they're different from, you know, Mujahideen or the Muslim Brotherhood, meaning that, like we need to look at the weakest link of domestic power structure, so domestic issues.

Like, for instance, in the United States you don't have many, you know, returning Jihadists, but rather you have homegrown, like extremists who have guns. And we Koreans do not have such issues, but we are going to—we will be going to have those homegrown violent extremist issues sometime soon. We are sure of that. So, okay, the fight against violent extremism these days is different from the fight against al-Qaida.

The ISIS problem is more related to each individual country's domestic structure, so I agree with you saying that, you know, like with the U.S. bilateral financial assistance might be counterproductive. Again, the problem should be solved inside out.

MR. FELTMAN: I think we have time for one more question. Please?

QUESTIONER: Sir, you mentioned the Indonesia CT Laws recently changing; there may be room in there for more military involvement by Indonesia and domestic counterterrorism. So, I'll pose that question specific to Indonesia, but also *writ large*, you know, for Mr. Baker as well, in terms of judicial end states and the military involved in counterterrorism in Southeast Asia, what are your thoughts?

MR. ABUZA: In Indonesia in certain cases, it is appropriate. For example, one of the first groups that kind of morphed from JI into Islamic State was based in Central Sulawesi, and this place is very important to the narrative, the Mujahideen in Tunisia, Timor.

The police weren't going to go in. I'm mean, it's just dense, dense jungle, it's like, hell no, we're not going in. That's an appropriate role for the Military, but when you see it as part of an overall paradigm where the Ministry of National Defense is talking about Bela Negara, and trying to get the Military back into things like food security, and politics, and trying to rest back political authorities. I'm concerned, I really

worry about blow back and overreach and, you know, just competition with the police. You know, they see a lot of money in counterterrorism, and want in.

It adds to the legal issues. You know, at what point: can they arrest people? Do they have to have -- the Indonesian National Police embedded with them? They haven't thought these things through yet, and I just -- I really worry.

The Indonesian Military does not have a great human rights record, not that the police does, but it's better and improving. And I really think if we don't have these commitments to rule of law, and the Philippines has had a Military first strategy, and it's been a disaster. I mean, the Philippines just -- in 2018 is just as bad as it was, in many ways, in 2001.

You know, and we are committed, and I say this as a DoD employee, I am the turd in the punch bowl when it comes to this; you know, that we keep on supporting the AFP, regardless of their human rights abuses, regardless of whether they're willing to use artillery as a counterterrorism tactic, shelling, which is why Marawi looked like Mosul. You know, this is not smart, and at the same time, there's very little accountability of the Military, very little oversight which is so important.

MR. FELTMAN: Jim?

MR. BAKER: Yes, sir, just a few comments. So, as someone who is a huge supporter of the U.S. Military, I will also say that if the Military has to come in and deal with a counterterrorism issue, then it represents a failure of the civilian agencies.

So to me, I think the civilian agencies need to get their act together and avoid forcing upon the military, that's kind of how I think of it, the responsibility to come in and deal with the situation. So, that's sort of number one, civilian agencies should be the first line of defense, and I include both, you know, law enforcement, intelligence agencies, and those relationships that I was mentioning earlier, with the local authorities to make sure that we're providing whatever information, assistance, training, resources so that

the local authorities can deal with it. That's sort of one thing.

Number two is, I think in terms of bringing in the military, obviously it has to be lawful, and so it has to be lawful under domestic law and under international law, if the country can sense to it, then probably deals with the international aspect of that, but what is the authority that the United States has to put our folks at risk in these areas. I mean, there has to be -- this seems to me a clear authorization from Congress to be able to do that, so it's just -- I believe that. Related to that, I mean, having a clear -- everybody knows this, you know this in the military much better than I do, you have to have a clear mission. Like, what is the mission? What is the objective? What are the measurables? What are the milestones that you're going to try to achieve in this kind of environment before we go getting involved in that? And I think that's something that we, unfortunately, don't often -- we don't do it uniformly, and if we're going to put Forces in, we need to have clear objectives.

And the third thing, I guess is, if the U.S. Forces are going to be involved, it seems to me that's more -- in this kind of environment -- perhaps a role for U.S. Special Forces to assist the training, the development of the local forces, and let them deal with the problem. Provide them the expertise so that they can -- the expertise, intelligence training to be able to deal with the problem on their own, and as opposed to making this some type of U.S. Military lead in any way. At least that I've heard about. And I don't pretend to be an expert in Southeast Asia, but some of the things that I worry about.

MR. FELTMAN: Thank you. I'd like to invite you all to join me in thanking our panelists, Jim Baker, Ji-Hyang Jang, and Zachary Abuza, for a very interesting exchange. Thank you very, very much. (Applause)

SPEAKER: Thanks to all of you, to the Panelists and the Moderators.

* * * * *