Opening Address by Minister for Foreign Affairs Dr Vivian Balakrishnan at the 10th Asia-Pacific Programme for Senior National Security Officers on 11 April 2016, 9am at the Marina Mandarin

Ambassador Ong Keng Yong,
Executive Deputy Chairman, S. Rajaratnam School of International Studies,

Introduction

1. I would like to acknowledge the presence of Mr Benny Lim and Mr Peter Ho. These are Singaporeans who spend their lifetime studying national security and it is a humbling experience to stand before you and try to add some points which perhaps are worthy of your consideration.

2. To our guests from overseas, a warm welcome to Singapore. This is the tenth anniversary of APPSNO and as we also note, this is the tenth anniversary for CENS. Ambassador Keng Yong has already told you the topics which have been considered and which have, in fact, become more pointed and more prickly in recent times.

National Security Revisited

3. This year's theme is supposed to be *National Security Revisited*. In order to try to give you something which I hope will be relevant, since I will not pretend to be a domain expert, I thought I will focus my comments today on terrorism, cyber security and its nexus with emerging technologies, the Internet, cyberspace and new media. Since I am also the Minister-in-charge of the Smart Nation, that gives me a leg to stand on and hopefully to make some useful comments and provide some food for thought.

4. Let's start with terrorism. In my view, terrorism is fundamentally the use of violence in pursuit of a political objective. The point here is the word 'political'. In other words, it is a political exercise, and it uses religion and ideology merely as a vehicle, as a lever in order to divide society and incite hatred, with its ultimate objective of achieving political power or a political end, with violence as almost a design feature. So the point is that it is a political exercise. In itself, this is not a new tactic. This has been going on, we could argue, for millennia or at least centuries. But what has changed in the last twenty years is the way Internet technologies have developed and the way social media has also enabled and amplified both the reach and changed the modalities of terrorism. And there are several effects of New Media which I will highlight and which I believe are relevant to national security officials.

5. First, the fact that we now have global communications, not just at government level but at people-to-people level, at social levels. This prevalence of connectivity and awareness, and the fact that people can communicate seamlessly has not led to a utopian global happy village where everyone understands everyone, everyone is tolerant, everyone gets along, and everyone has developed a global consciousness or

sensitivity. On the contrary, the fact is that suddenly everyone is acutely aware that you are a minority.

6. You see, for most or for all of recorded human history, people have lived and died amongst others who looked like them, smelt like them, prayed to the same god, lived in the same way. And when tribes met people who spoke a different language, prayed to a different god, behaved slightly differently, the usual and traditional human response has been conflict, ostensibly to mark out territory and seize resources. But the point is that the tendency towards violence in response to differences is actually hardcoded. But because most people spent most of their lives interacting only with people who are like them, there was that sense of familiarity and sense of assurance.

7. But now that we live in a globalised age, everyone, even if you are a member of the majority community in your own home state, you are aware that you are a minority in the global stage. So it's what Amin Maalouf, a Lebanese writer based in France, has referred to as this 'minority complex' that suddenly everyone has developed. And with a minority complex comes all the insecurities, all the imagined hurts, and this desperate need to find that identity or define that identity, even to manufacture that identity sometimes. And very often, this search for identity also has a violent edge to it. So the point I am making is that we now live in a world where no matter how crazy you are, you can find someone crazier than you to affirm your views on the Internet. So it should not surprise us that in fact it has led to a sharpening of radicalism, a sharpening of exclusive identities, and a reaffirmation of the temptation to resort to violence, both physical violence or even political violence, as people search, emphasise and reaffirm identities, imagined or real. So that is the first point, that we actually live in a world in which radicalism is accentuated by the very technologies of the last two decades.

8. The second point is somewhat related and that we may be reaching the end of the age of the mass media and instead, entering the age of narrow-casting. Many people, especially young people, have stopped reading the newspapers or listening to radios. You ask your children how many of them watch the television news. Take it from me very few actually do. And then you ask them, 'Where do you get your news from?". And for many of them, the answer is on their social networks. And yet, if you examine everyone's Facebook newsfeed - and I am sure most of you have Facebook accounts - if I were to ask you to turn to your newsfeed on your Facebook account, every one of us has a unique newsfeed. Of course it depends on the algorithm that Facebook implements. But each one's newsfeed is unique because it supposedly filters and provides what they think you are interested in. In other words, we now live in a world of fragmented echo chambers – we hear what we want to hear, we ignore what we don't want to hear or inconvenient truths are not heard. And in fact from an academic point of view, this leads to a 'shallowing' of discourse, a world in which there is a dearth of deep thought and cogent discussion across diverse perspectives. You get a more monochromatic world and a narrowing of minds.

9. The third impact of new technologies is that today, even non-state actors have developed sophisticated and slick marketing techniques, and audio-visual materials that

they produce far exceed the ability of most governments, in terms of their ability to capture attention, to persuade, to mobilise or to incite. And it should not surprise us, therefore, if you look in the last twenty years, if you look at what Al-Qaeda, its affiliates and its successors, al-Nusra Front and more recently of course people talk about ISIS or Daesh, all of them have mastered New Media. They have been able to propagate their message, create echo chambers and accentuate radical thought, and they've been able to create global tribes with a certain world view, a certain identity in order to pursue certain political objectives. So it should not surprise us, therefore, when we see that these terrorist organisations have a world reach, because their media has a world reach. Nor should we be surprised by the unprecedented scale of their operations because it is related to their ability to communicate, persuade and mobilise on an international scale. Nor should we even be surprised by the fact that increasingly, what we are struggling with are Lone-Wolf attacks by so-called 'clean skins' - people with no record.

10. So think about it, since 2013, ISIS has conducted or inspired attacks in a wide-range of countries. You know about Iraq, Australia, Egypt, France and Saudi Arabia. We think about the November 2015 attacks in Paris, with 130 people killed and over 350 people injured, the January 2016 attack in Jakarta with eight people killed and 24 injured, and most recently the May 2016 attacks in Brussels, which left 32 dead and 300 injured.

11. You think about these attacks, not only in terms of their global reach, but even in terms of the people engaged in these attacks. You will see that very often, it's led by people, not first generation immigrants, but it's second or third. People who may have been born in these countries but somehow feel a greater affinity for a cause whose source is very far removed from the area of operations. So we see that ISIS, an organisation like that, has been able to attract new recruits who can identify with that message and this enables the establishment of regional chapters all around the world. And we haven't seen the end of this yet.

Lone Wolf Attacks

12. Lone wolf attacks - we have all seen an increase in this across the world. The attacks are apparently spontaneous and low-tech: using knifes, taking of hostages, creating bombs using commodity ingredients etc. And the trouble with dealing with this type of attack is that it's apparently just your regular ordinary citizens who are carrying out these attacks. They don't need conventional military training and in fact, they don't even need very sophisticated resources. These lone wolves would often have an even higher chance of success precisely because they operate without outside assistance, without the data trails that security agencies often depend on to identify persons of interest. In Singapore, we are not immune either. Just in April 2015, a 19-year-old self-radicalised Singaporean was detained under our Internal Security Act. He had planned to join ISIS in Syria, failing which, if he couldn't get to Syria, he decided he would instead conduct attacks locally, including targeting the President and the Prime Minister. Yes, we may have dealt with him, but the question is how many more people are in similar circumstances with a similar frame of mind.

Success of Online Radicalisation

13. So we've seen successful online self-radicalisation, and ISIS has been able to leverage on this technique across the world. It has got a very sophisticated social media ability that, I think many governments wish they had. Their use of social media platforms like Facebook, Twitter and Instagram is much more appealing, in its own perverse way, than that of probably most of us in this room. They've got their own English online magazine "Dabiq", which helps spread its propaganda.

14. Southeast Asia is a target. If you go on the Internet now, go to YouTube and search 'ISIS Bahasa', you will see videos produced by ISIS, with beautiful Arabic music, wonderful Arabian landscapes, English subtitles and the speaker or the narrator reciting in Bahasa. Think about that: where else in the world would a slick video with Arabic music, English subtitles and delivered in Bahasa have appeal. It's directed at us and our people. And so we should not be surprised that more than 1,000 Southeast Asians are fighting in Iraq and Syria. And there is even an ISIS unit for Bahasa-speaking fighters, called *Katibah Nusantara*.

Ability to Attract Women

15. Another interesting related development to this wonderful propaganda machine has been the fact that they've been able to attract women to this cause. And this is somewhat different from the past where they're just trying to get fighters and trying to get people who are engaged in violence for its own sake.

16. An unprecedented number of women have travelled to Iraq and Syria to join ISIS. An estimated 600 women from the West have joined ISIS by the end of 2015. A key role of the women is as wives, mothers and homemakers, by helping set up families with young male foreign fighters, and there is actually a method to this. Because it anchors these foreign fighters to the organisation and it makes it harder for them to leave.

17. Some female ISIS members are active in social media and they have been very successful in recruiting new female members and spreading the ideology online. An example of such a female member is Aqsa Mahmood. She left Scotland in 2013. She was active and successful in encouraging other women to migrate to the caliphate, and even creating a suitcase checklist for would-be female recruits. She was instrumental in engaging and convincing at least three British school girls to travel to Syria in February 2015. So today, when we sometimes read reports of women suicide bombers, it should not surprise us because the technology, the message and the modalities has now crossed even the gender barrier.

Cyber Security

18. Now, besides terrorism, another emerging area of concern for all of us is cybersecurity. Governments and individuals have been aware that our computer

systems are at threat. If anyone doesn't believe it, they are not aware of the reality. But the scale of the threat has increased exponentially.

19. Today's cyberattacks range from state-sponsored espionage to commercial espionage. And we have seen attacks against critical infrastructure threatening national-level interests. Both governments and corporations have come under attack.

20. "Anonymous", the worldwide Internet vigilante group, has targeted several government websites around the world. In 2014, Sony Pictures was the target of a massive data hack.

21. Cyberattacks on critical infrastructure in telecommunications, transportations and power plants have potentially serious consequences for our population. One example was the attack on the Ukrainian power grid which resulted in a massive power outage in December 2015. This was apparently the first major instance of a successful attack against an energy critical infrastructure. Let me ask you, do you believe that is the only critical national infrastructure that has been penetrated? This may be the first of its kind cyber-warfare attack that affects civilians. It will not be the last.

22. In Singapore, we acknowledge the threats but we also recognise the benefits that technology and innovation bring to us. And so in Singapore, we have embarked on the vision of creating a Smart Nation.

23. This initiative is fundamentally not about technology, but really about people. And we want to apply technology in order to do three things. First, to enhance the quality of lives of ordinary citizens and to improve the services of government to these people. Second, to create opportunities because what is most urgent now, on the political agenda, is the creation of good jobs, especially for the middle class. Because technology is such a revolutionary force that probably 30-40% of jobs are at risk, and if we can't transform our economies to equip our people with the right skills and empower our businesses to take advantage of this new revolution, we will run into a political and economic problem. And the third objective of the Smart Nation programme is social cohesion.

24. I have already explained to you that nearly having worldwide communications systems does not create a global happy village and even at the local level, it can lead to a more fragmented and less cohesive society that we could otherwise have. So, we want to both take advantage of new opportunities and arm our people but also remain cognizant of the risks and the dangers posed by the same technologies.

25. And that is why last year, we also created the Cyber Security Agency to strengthen our capabilities and resilience, and we have also set up a cyber forensics laboratory in order to investigate and respond promptly to cyberattacks, especially those targeted against critical infrastructure.

26. We don't believe that we should just be fearful and paralysed, but we think we can take active steps to both pursue opportunities and minimise risks.

What We Need To Do

27. So, let me share a few ideas on what I think should be appropriate response by governments and by national security agencies. First, I believe that it is crucial for all of us, at the state level and at agency level, to urgently upgrade our infocommunications infrastructure. In the face of very sophisticated global terrorist networks, it is not tenable for any state or for national security agencies to be behind the curve. There is no excuse for that.

28. So, for example, broadband connectivity, mobile connectivity, for security agencies, it should be the best in class and each of you, in your own state, should go back to your government and demand that national security agencies have the best network infrastructure. There's no reason for you to be second or third. Sensors - location sensors, data sensors, temperature sensors, videos, are now so cheap that cost should not be a limiting factor.

29. In fact, it is not physical infrastructure but it is the explosion of data that will be available and your ability to analyse it smartly and in real time. That should be the real challenge for national security agencies and our security agencies should be always on, always connected and always watching. Now, at this point, I know I am now treading into politically sensitive territory when I say "always watching". So let me come back to that point later.

30. The second recommendation I would leave with you is that international collaboration, and even inter-operability, is absolutely critical. No single country, and certainly not Singapore because we are so small and so open, can deal with or overcome these global threats on our own. We need to share information and we need to share intelligence between countries if we are to thwart these attacks or to deter would-be attacks. This includes the identification of radicalised individuals who are making their way to join terror groups based on travel records. I know we have all moved towards biometric passports but we really do need to have a far greater level of integration in our ability to identify people, to track movements across boundaries because this is an international threat and none of us can depend purely on our immigration officers, working in isolation at the airport or the harbour.

31. We also meet another difficult challenge – it is how we identify individuals who have been self-radicalised online. Because these are individuals who by definition are "clean skins" and who would not otherwise be on the radar of security agencies.

32. We need platforms that bring the international community together to network and participate in meaningful discussions, and that is why today's meeting is so important. Conferences like APPSNO add value by bringing security practitioners like you from Chile to China, New Zealand to Norway, to get together to exchange views

and plans, where relevant. So I believe we need to be bold and we need to push the envelope.

33. Third, and most controversially we actually all need to embark on deep policy reviews on very difficult topics. Topics like the right to privacy, the encryption of communications and the freedom of expression.

34. You see, the problem is in the initial euphoric days of the establishment of the Internet. There were many people who dreamt of a completely free and unregulated space, with absolute freedom to say anything, the ability to transact secretly across borders, and to mobilise people for any cause without interference or being watched by security agencies. This was a dream of some of the early pioneers of the Internet.

35. But I believe there is a false dichotomy between the real world and the cyber world. I believe we actually only have one world – a technology-enabled world and what goes on in cyberspace has real impact on the real world, and the sooner we get to grips with these difficult policy issues the better, because we need to get the balance right. Balance between, say freedom of expression, rights to privacy, and the ability of national security agencies to investigate, pursue deeds, deter threats and aggression, and for appropriate political responses. So we need to have the balance right, we need to get the politics right and we need to get the operational responses right. So I thought I'll just leave these three points for your consideration and conclude by saying we actually live in a more unsettled world.

36. Technology has amplified and has not reduced the threat of radicalism, extremism. It has, in fact, led to the phenomenon of a global threat and it behoves us, it behoves all of you as national security practitioners, to get to grips with this new technology, insist on being best in class, work effectively together and get the politicians and the people to have a serious discussion about getting the balance right, getting politics right in order to ultimately secure the safety and security of our societies.

Concluding Remarks

37. So I hope I have provided enough food for thought. I wish you all a most pleasant and useful discussions in the day or two ahead. Thank you all very much.