Ministry of Communications
and Information
An Engaged and Connected Singapore

Transcript of Comments Made by Mrs Josephine Teo, Minister for Communications and Information and Minister-in-charge of Smart Nation and Cybersecurity, at Panel Session on "Cyber Strategy and Digital Governance – Protecting Sovereignty and Building Resilience" of The Sydney Dialogue (5 Apr 2023)

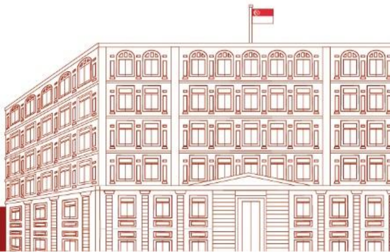
Q1) **Nele Leosk**, Ambassador-at-Large for Digital Affairs at Estonia's Ministry of Foreign Affairs: Hello everybody. Great to be here and looking forward to an amazing panel session that we are going to have. Welcome, Dirk Häger, Head of Operational Cyber Security, Federal Office for Information Security, Germany; Simon Milner, Vice President, Public Policy, APAC, Meta; Josephine Teo, Minister for Communications and Information & Minister-in-charge of Smart Nation and Cybersecurity, Singapore; and Nguyen The Trung, Managing Director, DTT Technology, Vietnam.

We will continue the discussions on **what is the role of technologies in our world and how it interplays with geopolitics.** You (Häger) take the approach of first seeing everything potentially that can go on, and then try to regulate it. I'm wondering whether this will be challenged by our colleagues, because it may be that you do not know everything that is going to happen. We had huge developments in AI very recently but when something else comes around the corner, we may not know what it is and handle the situations that we may not be able to predict.

Minister (chiming in): Technology is going to happen and develop at a very fast clip. And regulations are struggling to keep pace. But I'd like to come back to the point that you made in your opening remarks and to say that there is a **need for us to strike a balance.** On the one hand, we recognise the risks. But on the other hand, let's not forget the opportunities. So, **regulations have to be well calibrated in order not to impede opportunities**, from being made available to our citizens and companies. Yet at the same time, if there aren't enough guardrails put in place, then obviously, the risk of participating in the digital domain becomes so high that even if there are rewards, people may hold back. And that is the overall frame that we operate within – how to at the same time as promoting opportunities, also put in place measures, that gives people the assurance of trust and safety.

And here, I think there is a lot of scope for deeper thinking. **If we ask ourselves how you promote trust and safety, you can't run away from the fact that you must put in place good governance frameworks.** But to put in place good governance frameworks first requires us to unpack what governance needs. And if we were to break it down into essentially three components of good governance. It is the fact that the purpose is to prevent terrible things from happening. It is the fact that it tries to put limits on behaviours and conduct. And the third important element of good governance is that it has to be reasonably enforceable. If it's not enforceable, then it's just expression of hope.

So how do we bring good governance into play? There are things that we can do at the domestic level. For example, in Singapore, whether it's dealing with misinformation or disinformation, we have some laws and regulations that we introduced. We know by all means that they are not going to be enough, but they are a start.



In cybersecurity, you also can put in place good governance, and these we apply domestically. But the very nature of risks in the digital domain is that they are most often global in nature. The actors in the digital domain - whether they are global companies or malicious actors - they operate globally. **So, governance is not going to be nearly as effective as it needs to be unless there is cooperation at the international level.** It is in the domain of international governance that there is still a lot of room for us to work together. We could afford to pay more attention to good global governance in the areas that are of common interest. **For example, in cybersecurity, in AI and how machine learning is being deployed, and in data management - these are areas where good international governance is really needed.** And there is a lot of scope for development in these areas.

Q2) **Lesok**: There are very different approaches as countries have different approaches when it comes to regulation. In order to have a global, good order, we need good governance mechanisms. How do we not only make Meta responsible, and keeping their business space comfortable?

Minister: In any industry that has got global impact, the governance frameworks around them did not get developed overnight. They took many years. For example, an industry like aviation. Today, you and I do not worry too much about flying to each other's countries for conferences. But it wasn't always the case. Safety standards around global aviation involve many parties and took a long time to get right. This was also the case for the pharmaceutical industry when it came to ensuring safety of treatments and medications for patients.

In cyber and digital, I think we will have to go through this journey. The example I had in mind is a **Counter Ransomware Initiative that now involves 36 countries.** There are some elements of this Counter Ransomware Initiative that demonstrate the key pillars that contribute to effective international governance in the digital domain.

The first is the **importance of interoperability.** I think this idea was talked about across different sessions. But how does interoperability demonstrate itself through the Counter Ransomware Initiative? What happens when a ransomware attack has happened is that there is a need to stop the payment to the ransomware actor. And in today's context, because the ransomware actors work across different jurisdictions, they are actually taking advantage of the failure of interoperability to get away. So, the rules and regulations that would allow one jurisdiction to stop the payment to the ransomware actor doesn’t work across another jurisdiction. And regulatory interoperability is very important. So, the Counter Ransomware Initiative now says, “should we find a way in which notifications can be implemented in each of the member states that are participating in this initiative, so that we can all help each other to stop payment of ransom to these actors?”

Another level in which this Counter Ransomware Initiative is demonstrating how we can all be more effective together is the idea of **building resilience.** Because as a ransomware is happening, you must have a way to stop it and you must have a way to disrupt it. But not all of us are equally adept at stopping it. So, building capacity and each one of us learning how the other is disrupting ransomware is another good approach to international cooperation and achieving good governance internationally.

The third aspect is how we can build **norms of good behaviour**. Because the actors in our own jurisdiction respond to our own laws, regulations and policies, we have to be willing to share notes with each other what's working for our respective jurisdictions, and then not be shy about fostering higher norms as we go along. This is the kind of international cooperation that will lead to good governance around. I think the beauty of the approach of the Counter Ransomware Initiative is that regardless of your ideology or political beliefs, all of us want to get rid of ransomware.

Q2) **Lesok**: When it comes to data sharing, we talk so much about it but is it really happening and whose task is it to make it happen? For example, we should have 23 cross border data services in the European Union by 2023. I am very sceptical and don't think it will happen because we don't want to share data with each other despite having the frameworks actually in place. How do we make it happen?

Minister: I always like to think that the answer to "how" is "why". It goes back to us trying to understand why is there a need? And why is there an interest to share information and to share data?

You really can't run away from just the two fundamental needs. Data is a very valuable resource. The collection analysis, the harvesting of that data, can be tremendously useful to organisations for growth, reaching new markets and understanding your customers. It can also be very useful in terms of your organising your businesses and operations in a more efficient manner to cut down on waste and so on.

The incentive to try and get hold of the data and be able to make full use of it is there. I think the issue really is that because it is such a valuable resource, then there is also the issue of theft of that resource. There is also the issue that maybe that resource could be misused. And that's why you want to put in place appropriate guardrails. And again, we must ask ourselves, what do those guardrails look like? And I would suggest that there are also at least three elements to it.

One is that you need clear **accountability**. Whichever organisation is in the business of collecting, storing, and using that data, they need to know what their obligations are, and they need to be held to account. That's one very important feature when I think of any good data governance framework.

The second is that whatever rules that are put in place, you've got to make them **accessible**, and you've got to recognise the fact that not every company is big and well-resourced. There are many companies out there that actually are still struggling to cope with regulatory requirements. And we have to find ways of helping them to access these kinds of rules in a way that is suitable to their context.

At the same time, another way of thinking about accessibility is that if there is this strong interest and desire to get hold of data, are there ways in which you can build up secure ways of exchanging the data? We do some of this in Singapore. For example, in the logistics industry, we have a secure data exchange platform so that supply chain players and stakeholders can all be part of this network. We have the same setup for financial services. And in terms of making it possible for trading partners, people and businesses in the trading ecosystem to also exchange data securely, we built a platform called TradeTrust. These are some of the ways in which we can try and bring accessibility to light.

A third important component I think of data management is **partnerships**. We really have to recognise that again, this requires good international cooperation. It's easy in our respective jurisdiction to invent a set of rules around proper use and accountability requirements around data. But imagine businesses in today's context having to work across so many different jurisdictions. It is quite impossible to meet all of our requirements and still get the business going in an efficient manner. So here, again, I think is another call for international partners to work together to facilitate data management, as well as data flows.

Q3) **Lesok**: I would like to think deeper on something that Nguyen The Trung, Managing Director, DTT Technology, Vietnam mentioned that people and everybody likes to use technology. And I am actually wondering whether that is necessarily true. When we see definitely what is happening in Europe that people are getting more sceptical about digitalisation, because of everything that can go wrong, your identity can be stolen, data will be misused, your keys will be erased, and so forth.

I would say that this has become a burden and potentially an obstacle for governments to introduce new digital innovations. As diplomats and government officials, we are contributing to it and trying to build this awareness around all the risks. So we are saying, "be digital, the digital identity is a new thing for you". But if you go to digital, you will have all the bad things happening.

How do what we have to do as big players, such as companies, increasingly bigger players in this virtual space, but also governments? How do we get this innovation spirit out? And not be driven only by everything that can go wrong?

Minister: In Singapore, we certainly believe that honesty is the best policy. We have to be very frank with our citizens, where the opportunities are and also where the risks are. And the more aware they are of the risks, the more they can protect themselves. But at the same time, it also is a responsibility of government to bring together the relevant parties to introduce the right measures that will improve the real level of safety.

On a day-to-day basis, if my digital transactions make me vulnerable to losing lots of money, that's really not something I want to engage in. And it goes back to what we are prepared to do to introduce the right measures in order to govern the space. And in this domain, it's not the case that all governments around the world are already very experienced in doing this, and you can just adopt playbooks. We are all learning and the more we are able to learn from each other, I think, the more likely it is that we will make progress together.

+++++