MINISTER, PRIME MINISTER'S OFFICE, SECOND MINISTER FOR HOME AFFAIRS AND TRADE & INDUSTRY, MR S ISWARAN'S SPEECH AT THE OPENING CEREMONY OF INTERPOL WORLD 2015 ON 14 APRIL 2015

President of INTERPOL, Mrs Mireille Ballestrazzi

Secretary General of INTERPOL, Mr Jürgen Stock

Ministers

Distinguished guests

Ladies and gentlemen

Good morning,

I am delighted to join all of you this morning at the opening ceremony of INTERPOL World 2015.

INTERPOL World 2015 is a significant milestone; it is the first major conference driven by the INTERPOL Global Complex for Innovation in Singapore, which celebrated its official opening yesterday.

I am heartened to see the very strong support for the inaugural run of INTERPOL World. Amongst us are several Ministers from around the world, as well as representatives from industry, government agencies and academia. With over 200 exhibitors from across the globe, and approximately 4,000 participants, this will be a strong platform to foster an open dialogue between industry and the government on the pressing safety and security challenges that we face. In particular, the Strategic Partners Programme will bring together stakeholders from both the private and public domains to identify security challenges and design solutions.

INTERPOL is a leading crime-fighting institution that facilitates international collaboration in an increasingly complex safety and security domain. INTERPOL World is the manifestation of INTERPOL's vision and recognition that the key to securing our future against the threat of organized crime and terrorism, is continuous innovation and close partnerships.

New age of security challenges – changing landscape of crime

Criminals and terrorists are taking advantage of advancements in technology, globalization and rapid urbanization. This has ushered in a new wave of threats that can destabilize both global and local security.

Technology enabled crime - Cybercrime

The same technological advancements that have greatly improved our lives, have also aided the nefarious objectives of criminal groups; some of them have even established themselves as early adopters of technology. From surveillance and planning; communications and transportation; to concealment of crime and expansion of its reach – crime is being committed in new ways which defy traditional security countermeasures.

How serious is the threat? Cybercrime is one of the most predominant technology enabled crimes of today. Computers, smartphones and the Internet are pervasive in our businesses and daily lives, with the Internet penetration rate reaching more than 40 per cent globally. The 'Internet of Things' will continue to expand in myriad ways. We are already witnessing a move from connectivity to hyper-connectivity. Our homes, vehicles and even devices that sustain our health, are

networked. These smart systems will enhance the user experience and enhance resource optimization. However, the threat exposure has grown with the increased network usage. New cybercrime attack vectors and more points of entry are being introduced, allowing criminals to easily steal personal information for fraudulent activities, or worse, cripple entire systems simply by targeting one device.

We must therefore expect cyberattacks of greater scale and severity of impact, and plan on that basis to protect our countries and economies. The move to cloud computing aggregates immense data in computer servers around the world. This poses higher security risks, as hackers can now access massive amounts of data by hacking just one server. Mobile phones store a huge amount of personal information. Yet, mobile phone security and good hygiene is not widely practiced by mobile phone users. Our increasing dependence and reliance on technology also means that criminals and terrorists can easily manipulate the information we see on our screens to their advantage. This is evidenced by the availability of technology that enables cybercriminals to intercept wirelessly transmitted information. Even secure communication channels have been known to be intercepted by man-in-the-middle malware.

Clearly, cybercrime is a rapidly evolving and major threat from a law enforcement and security perspective, with criminals and terrorists constantly finding new ways to harness the cyber landscape for profit and propaganda. Our security mechanisms need to keep pace.

Globalization

With globalization, criminals are now able to operate in loose and fluid networks to avoid investigations and prosecution. The increasing global footprint of

crime shows that geographical boundaries are no longer constraints when it comes to the scale and impact of crime. For example, the geographic reach of counterfeiting has been aided by improved transportation networks, as well as new and cheaper technologies. The prevalence of counterfeit medicine poses a serious threat to global public health. The counterfeiting of anti-malarial medicine for instance has become a multi-billion dollar business, with sophisticated operators who evade detection by authorities. Even though malaria can be prevented and cured with good medicine, one third of all anti-malaria medicine is suspected to be counterfeit, resulting in needless suffering, and especially affecting the less privileged segments of society across countries.

Urbanization

Finally, we have also seen the growing trend of urbanization changing the operating landscape for many law enforcement agencies. In 2014, the UN reported that 53 per cent of the world's population lived in urban areas. This is expected to increase to 66 per cent by 2050. Cities are also growing in size with the rise of mega cities. At this point in time, there are over three dozen cities around the world with a population of more than 10 million residents.

Urban areas present an operationally challenging landscape for the enforcement authorities, as they are characterized by high population and critical infrastructure density; increased diversity and disparity; and rapid social and cultural changes. These changes present new safety and security challenges, such as a lower police-to-citizen ratio and crowd control problems.

Policing driven by innovation

How should law enforcement agencies respond to these mounting threats in this new age of security challenges? Criminals and law enforcement agencies are locked in a competitive cycle of co-evolvement, where we fight for technological competitive advantage. There is thus an urgent need for law enforcement agencies to leverage latest technologies and adopt innovation as a key enabler of policing work. Innovation in policing methods and tools is the key to ensuring that law enforcement agencies stay ahead of criminals and ultimately triumph.

Forging collaboration networks

Faced with such a complex, interlinked and evolving security scenario, our law enforcement agencies cannot work alone. It is crucial for stakeholders to forge strong networks of collaboration, to pool and leverage each other's' resources, develop deep expertise and create innovative policing solutions. This is not an option or a good to have; it is an imperative.

G-G collaboration

Collaboration is required at different levels. Given the increasingly transnational nature of crime, international cooperation at the Government to Government level is essential. This will help ensure swift identification, mitigation and investigation of threats. It can be achieved through bilateral as well as multilateral frameworks. And, there is much to be done on this front.

G-B collaboration

Just as the impact of crime is not confined to the public sector, similarly, the responsibility for confronting such threats is not the sole preserve of government agencies. We need to explore and drive closer cooperation between government and business, to develop mutually beneficial partnerships. Opportunities for collaboration are plentiful, from information sharing, research and development, capacity building and training, to the setting of standards and policies. For example, the private sector remains at the frontier of innovation. Law enforcement agencies can help to shape R&D efforts of the industry by providing data and problem statements, or creating testbed opportunities, which allow industry players to develop technological capabilities that are more operationally relevant.

Industry players are also able to contribute information, for example regarding cyberattacks and their impact, which can be tapped for joint analytics and horizon scanning, to aid law enforcement to accurately appreciate and forecast crime trends. Such collaboration demands new mindsets and approaches underpinned by mutual trust and respect. We must embrace such change to take B-G collaboration to a new level to effectively tackle these new threats.

Singapore's position on innovation and PPP

Singapore strongly supports the need for continuous innovation, and recognizes the value of a multi-stakeholder approach to drive innovation. A prime manifestation of this multi-stakeholder approach is our Smart Nation Programme.

The Smart Nation Programme is a Whole-of-Government initiative established under the Prime Minister's Office, which aims to bring citizens,

government and industry players together, to identify issues and co-develop solutions, aimed at transforming the way of life in Singapore through technology and innovation. The concept is simple. The Government lays the foundation by building the infrastructure and framework for industry stakeholders to contribute, turning Singapore into a laboratory to harness technology.

Aligned with the big picture of building a smart nation, Singapore embarked on the Safe City Testbed. The testbed is an innovation platform for government agencies to collaborate with industry partners, to create breakthrough technologies and solutions for urban management and security. By leveraging latest technologies in data and video analytics, simulation and modelling, we have developed urban management solutions that help government agencies improve operations and reduce resource requirements. For instance, the testbed developed a crowd simulation model for indoor environments using our rapid transit system stations. Real-time crowd counting techniques developed can be applied to emergency, evacuation and rescue scenarios, and to predict crowd behaviour and movement in a crisis or at a major event. Such innovations will have a significant impact on the conduct of our operations and bring real value.

To conclude, innovation is fostered through networks of collaboration and active exchanges among stakeholders. I am confident that this milestone programme and exhibition will challenge and inspire all of you, to generate fresh insights and new perspectives on solutions for the challenges of today and the future.

On this note, I wish you all a fruitful and productive INTERPOL World 2015 Expo and Congress. Thank you.