MINDEF
SINGAPORE
SPEECH
Visit http://www.mindef.gov.sg for more news and information about MINDEF and the SAF

# Keynote Address by Permanent Secretary (Defence Development), Mr Ng Chee Khern, at the International Naval Engineering Conference (INEC) 2017

17 May 2017

Chief of Navy Rear-Admiral Lai Chung Han,
Distinguished Guests,
Ladies and Gentlemen,
Good Morning,

## Introduction

Welcome to the International Naval Engineering Conference 2017 or INEC in short. Since the inception of INEC in 2013, I am heartened to see that this conference has seen a significant increase in participation. It continues to be a platform for leading defence establishments and navies to strengthen relations and partnerships, to seed new ideas and innovations, and to broaden networks for collaboration.

At INEC 2015, I shared about the approaches that Singapore had untaken to adapt and transform in an uncertain security environment. And I mentioned that we could be at the cusp of a potential Revolution in Military Affairs. The last one started in the 70s and 80s, and had its main thrust in precision warfare. I believe that we are in a current revolution that has to do with advances in cyber capabilities, space and robotics. If brought to maturity, these technologies could bring about disruptive effects and profoundly change the nature of warfare.

**Advances Continue Unabated**

Since I last spoke, advances in technologies have continued unabated, and there have even been instances where technologies themselves are being disrupted by new advances. Take unmanned technologies for example. At the onset, unmanned operations were limited by line-of-sight, requiring human controllers to be in close proximity. They were essentially remotely piloted aircraft rather than true unmanned aircraft. However, with key advancements in artificial intelligence (AI) and robotics yielding superior sense-and-avoid capabilities, true autonomous aircraft is now possible. This ability will be a game changer in high payoff areas such as instant drone deliveries, or in the military context, in Intelligence, Surveillance and Reconnaissance (ISR) operations.

Indeed, our society and security landscape will continue to be influenced by wider technological trends. One of such trends that have gained significance is called the 4th Industrial Revolution, or 4th IR in short. This is a term coined by Professor Klaus Schwab, Founder and Executive Chairman of the World Economic Forum. It is characterised by a fusion of technologies that is blurring the lines between the physical, digital and biological spaces, and sees advances in data science, AI, quantum and cognitive computing, robotics.

The 4th IR is a disruptive force. As defence planners, many of us consider geography as an immutable challenge -- something that cannot be changed and will last forever. But even that is set to change as cyber and information capabilities transcend physical geography. Cyber and information travel at the speed of light. A single cyber-attack can simultaneously impact systems across every physical battlespace across land, sea, air, and even space. You just have to watch what has happened with WannaCry in the last few days. This is a paradigm shift. Previously, when we fight with physical systems, we have to protect ourselves mainly from potential adversaries that are closing in on us. In the cyber world, potential adversaries can come from anywhere. It is no longer about guarding against who is in your vicinity, but who is acting in the vast and wide cyberspace.

The 4th IR is disruptive in other ways too. In the past, military capabilities have always been more kinetic in nature and thus their immediate technical or tactical use and effects of systems were bounded by the laws of physics. We know exactly how aircraft, ships and combat systems would perform and react, and we can always rely on Operational Research to size up what we need for our force structure. However, in cyber operations, we do not know how the adversary's system will behave or react, as his course of action is much concealed and no longer as deterministic. Human psychology and behaviour will come into play a lot more. Doing force structure in such a context would henceforth be extremely complex and difficult as it is not as amenable to simple modelling and simulation.

The key to 4th IR technologies such as cyber and AI lies mainly in recognising the shift in battle dominance from one that is hardware-based to one that is likely to be software-driven. Being software-centric, the potential application and effects of these capabilities are dependent on the quality of coding and sophistication of techniques and algorithms applied. This adds to the complexity. While we could be deterministic about the performance characteristics of an adversary's physical weapon system, the 'performance specifications' for cyber or information systems are far less quantifiable. We had previously already seen this in the Electronic Warfare (EW) domain. It was always hard to know how a battle or a war would be won or lost when EW plays a significant part. But arguably, it will be even harder to determine who is good or more capable in cyber or information warfare until the battle unfolds. With cyber warfare thrown into warfare more generally, the collapse of one side or the other can potentially be even swifter than in a fight where only hardware dominates. What all these mean is that the face of warfare has changed drastically to become even more non-linear and unpredictable.

**Robust Designs, Flexible Capabilities**

The 4th IR will indeed bring about new paradigms. And changes will continue unabated because the way in which 4th IR technologies would evolve is likely to be very fluid and unpredictable intrinsically. What implications does this have for us? One thing is clear, and that is to exploit these 4th IR capabilities, we will need to alter and change our traditional approaches to technology development.

The theme for INEC this year, "Robust Designs, Flexible Capabilities", therefore, reflects the importance of seeking new and novel approaches to fully exploit the opportunities that disruptive technologies will offer. To drive robust designs, defence planners will first need to have new sets of competencies and processes to develop a fuller understanding of these technologies. At the same time, we need to be bold and agile in testing ideas, so as to quickly narrow down the right ones that will meet our needs.

#1: Develop Mastery of 4th IR Technologies

The key to cyber, information and AI lies mainly in the techniques. These software-centric capabilities are conceived, designed and evolved by programmers. Just how sophisticated and advanced these techniques are will ultimately depend on human ingenuity and intelligence. Hence, building up a body of expertise in this area will be crucial. The Defence Science and Technology Agency (DSTA) has hence set up a Digital Hub, where we would bring together and harness digital technologies such as data analytics, artificial intelligence, and the Internet of Things, and to build long term capabilities in these areas.

#2: Instil a Multi-disciplinary Approach

As data, cyber and AI would be embedded in everything, in all hardware and weapons systems, whoever is able to make software work better with hardware will hold the dominating ground. This calls for a tight integration of software techniques with operational acumen of the battle ground to truly yield effective weapons systems. A multi-disciplinary approach would be needed. The blend of domains necessitates the need for different expertise -- not only engineers and scientists but programmers and data analysts to create the desired weapons effect. Behavioural psychologists and biological scientists may also be required to understand the human psyche and responses.

And in driving robust designs, the prescriptive approach of having the warfighters define the requirements and having the technical community to follow up on its implementation may no longer be so suitable. As we are far less familiar with the potential applications and effects of 4th IR technologies, the onus is for the operational and technical communities to develop capabilities in concert. So the 4th IR brings about another new paradigm. The operational and technology communities will need to be more receptive to having more "technical-push" and not just rely on pure "operational-push". It will test the strength and will of our existing operations-technology integration. Here, I must commend the Republic of Singapore Navy (RSN) for being very forthcoming in this and being very progressive. We have worked closely with the RSN as a live testbed for the defence technology community to experiment with 4th IR technologies in actual field operations. Such initiatives are a good reflection and way to cultivate operations-technology integration that we need for the future.

### #3: Be Open to "Experimentation"

We must also embrace the right mindset and culture to be able to seize the opportunities. A setting for agile development should be instilled. For example, we will need to accept failures as a necessary condition for success. It is important to create a "fail-fast, learn-fast" environment for the defence community to learn from past failures, and quickly build on them to shake out the right solutions sets.

In Singapore, the RSN's Littoral Mission Vessel (LMV) programme is one example of how test-beds were employed to work out new operating concepts. Locally established, the System of Systems Integration Laboratory (SOSIL) pioneered the use of cognitive task analysis, and modelling and simulation to test out new concepts in bridge operations -- integrating automation with work flow arrangements in order to figure out the optimal level of crew manning.

The Defence Science Organisation (DSO) National Laboratories has also recently launched a complex to drive "experimental laboratories", which include dedicated facilities to experiment artificial intelligence and robotics. The robotics lab facilitates prototyping, integration, simulation and testing of robotics systems prior to field tests. These experimental laboratories are made up of small groups of scientists and engineers from different domain expertise to collaborate and form ideas to shape the next generation SAF. Equipped with the right tools and infrastructure, having such small group set-ups are ideal as they build on the nimbleness required to facilitate quick exchange of ideas and co-development of solutions.

### #4: Leverage Expertise Beyond

Lastly, we need to look beyond the "siloes" of the defence eco-system to leverage what is already out there. Today, cutting edge technologies and expertise that have great potential for militaries reside in the commercial sector. For example, the foray into AI, robotics, data science and cognitive computing are driven at a fervent pace by companies such as Google, Amazon and Tesla. We will need to build new relationships to keep a good pulse of these technologies. Our rigorous but often slow and lengthy capability development processes may however discourage some of these non-defence companies from co-developing defence solutions with us. To energise this, we could explore unique partnership models similar to how Singapore has, for example, been working with Nutonomy, a driverless car company, by offering itself as a test-bed. The partnership looks to pilot self-driving vehicles in a big way as it views real-world testing as an important catalyst to create a viable alternative to individual car ownership. Similarly, militaries or the defence industries could think about offering useful test-beds for such companies to bring in their technologies for trial.

At the same time, we should also be looking out for local small-medium enterprises, or SMEs, as given their nimble size and entrepreneurial mindset, they could also be developing 'the next big thing'. But to start significant business with them may be challenging. For one, they may be less willing to establish contracts with us as they may not have the requisite financial standing to deal with bigger players. DSTA attempts to address these concerns through the formulation of an SME Engagement Framework. Through such an initiative, we are paving the way for these companies to participate in our labs in DSTA and DSO. Here we could quickly latch on to their ready expertise to co-develop solutions, particularly in non-sensitive areas.

**Conclusion**

To conclude, I have highlighted the potential impact and effects of the 4th IR technologies on the future security landscape. I have also shared that we need to seek new and novel approaches to fully exploit these opportunities.

This conference offers an excellent opportunity for us to share perspectives and have leading edge discussions on these difficult issues. Compared to previous years, INEC 2017 has seen a significant increase in technical papers and presentations to share research findings that are scoped towards emerging technologies such as data analytics for sense making, artificial intelligence for performance analysis and optimisation, cyber security to protect information and data, and integrated hybrid systems for manned-unmanned robotics. I hope that this conference will continue to seed technological innovations.

Next year, Singapore will be looking to host the inaugural Defence Technology Summit. It will be a platform for thought leaders from governments, industries, academia, and think-tanks from around the world to discuss the implications and opportunities of technological

advancements for defence and security. I hope that INEC 2017 will enable us to gain new insights on the potential implications of these disruptive technologies in the domain of the sea, and therefore help us seed further discussions during next year's Defence Technology Summit. I am confident that the exchange of global perspectives, operational experiences and technology developments will spur thought-provoking insights and drive technological frontiers to the next level. I wish each and every one a meaningful conference this year.
Thank you.

**News Release:**

- MINDEF Officials Officiate at 5th IMSC and 3rd INEC (MINDEF_20170516002.pdf)

National Archives of Singapore