SINGAPORE DEFENCE TECHNOLOGY SUMMIT

26-28 June 2019

PROLIFERATION OF **TECHNOLOGY**
AND ITS IMPLICATIONS ON
DEFENCE, SECURITY AND SOCIETY


KEYNOTE ADDRESS
Mr Teo Chee Hean
Senior Minister and Coordinating Minister for National Security
Singapore

CONTENTS

KEYNOTE ADDRESS BY MR TEO CHEE HEAN

SENIOR MINISTER AND COORDINATING MINISTER FOR NATIONAL SECURITY, SINGAPORE

EXCERPTS

Questions Arising from Technology Proliferation

"Today, our societies are all grappling with the rapid advance of technology. We all want to be ahead of the game, and not be left behind. As such, the issues are often framed in terms of how to develop and deploy new technology more quickly. But in this headlong rush, we do also need to reflect on how well, and how wisely we are making use of technology, and whether we are prepared to deal with the collateral consequences of the proliferation of these new technologies….One, how do we prepare for a world where machines are smarter than us? Two, how do we maintain security in an increasingly interconnected world? And three, while we focus on high-tech warfare, how do we avoid being blind-sided by asymmetrical, low-tech warfare, which strikes not just in the battlefield, but in hearts and minds?"

Safeguarding Against Technology

"We are already in that future where a machine can assess and decide in a second what we may take hours or days to evaluate….There are indeed technical measures which we can deploy to help mitigate this future. One example is "explainable AI" – designed to explain how or why particular decisions or actions were taken….Ultimately, humans have to understand and trust the decisions of their computers, so that we will have the confidence to make the most of a more technologically advanced future….With the number of interconnected smart devices multiplying by a factor of say, a hundred, more than today, we need to devise new ways to maintain the security and resilience of our systems….To stay safe, we need systems and processes to protect us from bad actors who are already lurking inside, by seeking them out and acting against them. And when "the system" expands to include many more remote smart devices, we will need new ways of authenticating and verifying the security of smart devices right out at the edge…We will also need to depend more on data encryption, be it for data at rest, or data being transmitted, shared, or processed."

Importance of Collaboration

"While we come from diverse backgrounds, we share common goals. We want to harness the potential of technology and greater interconnectedness to do good, to improve the lives of our citizens, and to better protect our countries and peoples. But these self-same developments present new threats and dilemmas which we will have to collectively confront, particularly as technology continues to advance and pervade every aspect of our lives. Through this conference, I trust that we will be able to share our experiences, develop new ideas, form new friendships, and spawn new practical proposals for cooperation. Let us work together to strengthen our measures for the ethical use of AI; strengthen our cyber defences in a more inter-connected world; and strengthen our national resilience against asymmetrical threats in the physical, cyber, social and psychological domains."

WELCOME ADDRESS BY DR NG ENG HEN

MINISTER FOR DEFENCE, SINGAPORE

EXCERPTS

Impetus of the Tech Summit

"It's been barely a year since the inaugural summit was held and yet we meet under vastly different conditions. I think especially to the delegates of this conference that draw from leaders of defence sciences in Government, business and academia, it is clear that the technological space has become sharply contested….And I think it would not be far off the mark to conclude that a technology race has already started, especially around emerging technologies that will shape our collective futures; and for defence industries, to produce first, new disruptive weapons and platforms for strategic advantage, in all domains of air, land, sea, cyber and space….Countries, especially rivals, will always have differences but there is no cognitive dissonance in meeting and sharing views, even among strategic competitors…. What Singapore and the organisers of this conference can do as hosts is to create a conducive environment to address challenges that confront our collective well-being, which we will have to address together despite our differences."

Challenges on the Horizon

"On the agenda therefore are common challenges. To name a few, the trade-offs between the increasing digitisation of daily lives through the Internet of Things and privacy and security; the ethical conundrums of Artificial Intelligence decision-making with man out of the loop; the impact of increasing automation on jobs that will affect militaries and defence companies; the rules that should govern cyber and outer space, with increasing traffic and the threat of kinetic fall-outs. These problems are complex, and even more so the solutions with hard trade-offs…. And I think here, it is important for leaders in defence technology to be involved in the process early, to have your views clarified and sharpened before they get caught up in the legislative and political machinations of individual countries."

Role of Technology in Reshaping Militaries

"Our militaries today are not geared to respond optimally, if called upon to address these newer, non-conventional challenges. Our organisations and resources are still optimised and allocated towards traditional, conventional threats….Whatever the changes required, one aspect is clear – our militaries will have to do more, sometimes with resource constraints. There will have to be closer interactions between the operational units and the defence technology community, such as yourselves, to optimise resources and improve responsiveness….The militaries that will serve this generation will have to deal with traditional rivalries, as well as expanded challenges related to terrorism, cyberspace, outer space, and the forces of nature. Increasingly, we will need the power of technology to amplify our efforts and improve our effectiveness to deal with such challenges."

CONVERSATION WITH CEOs

(From left)

Moderator: **Prof Alberto Sangiovanni-Vincentelli,** The Edgar L. and Harold H. Buttner Chair, Department of EECS, University of California, Berkeley

Speakers: **Ms Leanne Caret,** Executive Vice President, The Boeing Company, President and CEO, Boeing Defense, Space & Security

Mr Vincent Chong, President and CEO, ST Engineering

Mr Dirk Hoke, CEO, Airbus Defence and Space

Prof Sangiovanni-Vincentelli opined that the world was getting more connected but also much more fragile, as organisations worked in functional silos and had no clear strategies in the adoption of technologies such as artificial intelligence (AI). With that, he started with the question to panellists on "what kept them awake at night?".

Talent as the Most Pressing Concern

The CEOs agreed unanimously that the proliferation of technologies had increased competition for talent, and recruiting and retaining talent were the most pressing concerns they faced. The panellists said it was crucial to clearly articulate one's value proposition and excite talents.

Mr Hoke added that in transiting from traditional to new capabilities, communicating the implications of digital transformation to his employees was key to managing change. He proposed that rather than compete with technology companies to attract top talents in AI, companies could also adopt a hybrid strategy to partner top technology organisations and integrate their novel technologies.

Innovation

Mr Chong said that organisations needed to innovate quickly to deal with the rapidly advancing technological landscape and to remain relevant to their customers. This could be achieved by being open to the adoption of commercial innovations and collaborating across the whole ecosystem. When asked if the USA-China strategic competition would stifle innovation, Ms Caret reframed it as an issue about competing on the speed of innovation and disruption. She explained that Boeing started out small and disrupted others to get to where they were, and that Boeing needed to continue to disrupt themselves before others disrupt them. Hence, the strategy was to create space to promote disruptive innovation through methods such as corporate venture capital arms, and to anticipate and think like a disruptor.

Maintaining Customer Focus and Designing Systems for Maintainability

The panellists also discussed two key ingredients for success. On evolving customers' needs, Ms Caret emphasised the importance of establishing constant dialogue with their customers to ensure they were not innovating in silo. On designing systems for maintainability, Ms Caret and Mr Hoke mentioned the use of model-based engineering and having a single source of data in digital twins as their engineering approach. Mr Chong cited how DSTA applied design thinking up front to ensure the Littoral Mission Vessel would be modular and easily maintained, thus allowing state-of-the-art technology to be incorporated constantly over the vessel's lifespan.

ONE-ON-ONE DIALOGUE

The one-on-one dialogue with Dr Steven H. Walker provided attendees insights into how the US Defense Advanced Research Projects Agency (DARPA) maintained its track record of delivering game-changing and novel technologies for operations.

DARPA's Success Formula

Dr Walker brought up a few contributors of DARPA's success over the years. First, DARPA strove to take on projects that could "change the world", rather than those providing incremental impact. In particular, they had the autonomy to pursue high risk endeavours, to the extent of even making mistakes along the way. Second, he emphasised the importance of closely partnering academia and industry to invest in dual-use technologies for both national security and commercial applications, where the access to a large pool of resources allowed them to advance a field significantly. Third, Dr Walker shared that DARPA hired people for their ideas. In addition, DARPA employees were hired on a term basis subject to renewal. Dr Walker opined that such transiency created an urgency for the staff to make a difference in a short span of time. Careers would not be impacted by failures, and that liberated the employees to experiment freely, take risks and strive for change.

Willingness to Terminate Projects

While the US developed the best technologies, Dr Walker opined that the DoD's ability to transit technologies to capabilities quickly could be further enhanced. Besides adopting a phased iterative approach to capability development, he added that the ability to terminate a project was just as important as the ability to start one. Such a mindset had allowed DARPA to stay focused on identified areas and thus achieve significant breakthroughs.

Next Bound of Technologies

Dr Walker highlighted three areas as the next bound of technologies. He opined that biotech would be a game changer in the future, and added that we needed to establish the dual use cases of biotech, and develop understanding of biotech outside of the military context. Next, he highlighted that high performance electronics and computing at the edge would also allow new paradigms of operations in warfare. He also noted that hybrid warfare would continue to transform future warfare. In the areas of fake news and social media, he added that these had huge potential for collaboration with the industry to deploy solutions such as big data analytics at scale.

Trust between Human and Machine

In conclusion, Dr Walker opined that trust between humans and machines would be a key factor of the third wave of AI and that AI could only continue to improve as humans place more trust in AI technology.

(From left)
Moderator: **BG Gaurav Keerthi,** Assistant Chief Executive, Cyber Security Agency of Singapore
Speaker: **Dr Steven H. Walker,** Director, Defense Advanced Research Projects Agency, US Department of Defense (DoD)

PANEL DISCUSSION -
WILL ARTIFICIAL INTELLIGENCE MAKE SOLDIERS SMARTER?

Dr Pierce focused the panel introduction on how AI could make soldiers smarter, shifting the panel past the question of "will".

Potential of AI in Grey Zone Scenarios

Dr Pierce painted a grey zone scenario where disaster had struck and disrupted critical infrastructure, and insurgents were taking advantage of the instability. The panellists discussed the potential of AI to assist the headquarters (HQ) and a deployed outfield unit. Dr Altshuler shared that the HQ could tap AI to perform sentiment analysis on tweets and these could be used to generate heat maps and sieve out potential terrorist attacks. Dr Brynielsson described the use of natural language processing for automated intelligence brief and reporting, and shared that pre-trained language models could be deployed at the edge with low computing power. Mr Husain suggested the use of a medium altitude self-stabilising and self-piloting balloon to restore high bandwidth cellular communications, the use of commercial drones to create a real-time surveillance system with object detection and automated prioritisation of events, and the use of autonomous flying aircraft to perform automated despatch of solutions, such as delivering life-saving equipment.

Explainable AI to Combat Adversarial Attacks

Dr Brynielsson highlighted the rapid advancement of adversarial AI research, and that AI classifiers were vulnerable and easily fooled, using examples that showed images, sound and textual content being misinterpreted. Hence, there is the need for AI to be "transparent", i.e. explainable, in order for humans to trust it. The panellists discussed that explainable AI would be key to one's ability to seize AI opportunities and deal with the vulnerabilities.

Collapse of the OODA Loop as the "Biggest Implication"

Mr Husain opined that AI had largely been used to solve perception problems. The greater potential of AI, which was still relatively untapped, was in its applications for industrial and military AI, specifically in the concept of 'hyper-war', where the 'Observe, Orient, Decide, Act' (OODA) loop would be collapsed due to AI applications in areas such as predictive maintenance and detection of zero-day cyber threats using static analysis. Dr Altshuler said that the main benefit of AI was in prioritisation; in military scenarios, systems would filter huge amounts of data, perform automatic tracking and prioritisation, and present information to the human to make decisions. The panellists agreed that the use of AI would not make soldiers obsolete. It would instead redefine their roles in the future. Soldiers could become more proficient if they were technically skilled and able to make use of AI to their advantage.

Managing the Perception of AI for Military Use

Citing the outcry over accidents involving autonomous vehicles, Dr Altshuler felt that education and evidential data would be key to managing the perception that AI for military use was benevolent. Mr Husain added that in reality, military outfits such as the US DoD were keen on non-lethal applications of AI, with one of the biggest use cases being predictive maintenance.

Moderator

Dr Brian Pierce
Office Director, Information Innovation Office, Defense Advanced Research Projects Agency, US Department of Defense (DoD)

Speakers

Dr Yaniv Altshuler
Co-Founder and CEO, Endor

Dr Joel Brynielsson
Research Director, Swedish Defence Research Agency

Mr Amir Husain
Founder and CEO, SparkCognition

PANEL DISCUSSION -
CAN SMART AND SECURE CO-EXIST?

Mr Chang opened the session by inviting Mr Sikkut to share the digitalisation journey of Estonia which included their adoption of best practices in cybersecurity. Mr Chang added that it was not a case of if, but when cyber incidents would happen and that aspects covering people, processes and technology would be required to mitigate them.

Government's Role in Cybersecurity

GEN (Ret.) Alexander shared a lesson he learnt as Director, National Security Agency – when they could not see where the cyberattacks were coming from, they were basically performing incident response and could not defend the nation effectively in cyberspace. He added that a paradigm shift was essential in which companies and the government worked together to achieve collective defence through common standards.

The panellists discussed the government's critical role in developing infrastructure and ensuring good cybersecurity practices.

Dr Chan said that businesses strive to create innovation and value, and achieving a balance between these and cybersecurity might be challenging. While cybersecurity is important, it should not impede innovation. Mr Hwang said that there would be a role for the government to ensure that the economy was secure as smart and secure would be costly for small businesses.

Trust in Technologies

A lack of trust from the public would hinder the adoption and usage of technology, despite the best cybersecurity strategies. The panellists discussed various perspectives of smart and secure across countries despite technology transcending geographical boundaries. Dr Chen elaborated that countries had different views on how technology might be used for good or bad, and Dr Chan added that cultural norms and perception of technology would differ across generations.

Co-existence of Speed, Smart and Secure

The panellists expressed different views on the co-existence of speed, smart and secure. Mr Hwang opined that only two of the three attributes could be accomplished due to the opposing forces and that painful trade-offs needed to be discussed.

Moderator

Mr Bill Chang
Country Chief Officer, Singapore and CEO, Group Enterprise, Singapore Telecommunications Ltd

Speakers

GEN (Ret.) Keith Alexander
Founder, Chairman and Co-CEO, IronNet Cybersecurity

Dr Vivian Chan
Co-Founder and CEO, Sparrho

Dr Chen Ning
Chairman and CEO, Shenzhen Intellifusion Technologies Co., Ltd

Mr Tim Hwang
Director, Harvard-MIT Ethics and Governance of AI Initiative

Mr Siim Sikkut
Chief Information Officer, Government of Estonia

Mr Sikkut added that smart should not be recklessly fast and that software should be built as small, smart and secure components, prior to scaling up. In contrast, GEN (Ret.) Alexander opined that speed, smart and secure was achievable through software capabilities supported by cloud technologies and 5G. Dr Chen listed the Internet of Things, 5G and AI as the three major technical breakthroughs that would enable the design of a fast, smart and secure infrastructure.

Mr Hwang commented that while we may be prepared to deal with threats in the kinetic domain, this might not be the case in the non-kinetic domain where we need to be ready for "cyber wars of the future".

PANEL DISCUSSION -
THE GOOD AND BAD OF DRONES

Moderator

Ms Ngiam Le Na
Deputy Chief Executive (Operations), Defence Science and Technology Agency

Speakers

Prof Dario Floreano
Director of Laboratory of Intelligent Systems, Swiss Federal Institute of Technology Lausanne and Director, Swiss National Centre of Competence in Robotics

Mr Florian Guillermet
Executive Director, Single European Sky ATM Research (SESAR) Joint Undertaking

Mr Adam Welsh
Head of Public Policy, APAC, DJI

Ms Ngiam opened the session with a brief history of drones. While civilian drones started only in the 2000s, they have grown exponentially and are set to become a mainstay of the modern world. Under this backdrop, she posed the question of "are drones opportunities or challenges?" to the panel and audience.

More Opportunities than Challenges

The panellists and audience agreed that drones presented tremendous opportunities. Mr Guillermet highlighted that the drone business was developing so fast that we could not possibly foresee what new applications would emerge in two years' time. Drones were evolving into multi-purpose platforms with the ability to perform a wider range of services. Reinforcing this view, Prof Floreano revealed that his lab was working on a new class of drones called soft robotics. They are based on new materials, origami structures, and new fabricating techniques that enable drones to resist collisions instead of avoiding them, and with bio-inspired features such as adaptive morphology to adapt their shapes to constrained spaces, perceptual intelligence to navigate their environment, and energetic autonomy to enable swarm of drones to work collectively. Mr Welsh added that drone proliferation was driving innovations and growth in technologies such as sensors and data analytics.

The panel was cognisant of the challenges associated with drones. However, Mr Welsh reckoned that "you can put the genie back in the bottle" but the world would not be ready to give it up. Banning drones would not stop the advent of malicious acts. Instead, drone manufacturers should work closely with regulators to set industry standards for safe and secure drones such as remote identification, geofencing and cybersecurity. Mr Guillermet added that developing a UAS Traffic Management system would be key to systematically integrate drones into the airspace and take care of 99.9% of flying activities of cooperative drones. This would allow regulators to focus on countering the remaining 0.1% associated with uncooperative or malicious activities, which could be mitigated with strong enforcement and counter-drone technologies.

Singapore's Smart Nation Vision

Ms Ngiam explained that drones would be an integral part of Singapore's Smart Nation vision but our urbanised landscape coupled with highly dense airspace made drone operations challenging. Mr Welsh felt that Singapore could turn its small size into an advantage as it had excellent mapping information compared to bigger countries, which was essential for supporting drone operations. Prof Floreano added that there were a lot of opportunities for drone delivery of emergency supplies in Singapore's congested urban areas and busy harbour. Going forward, Singapore could invest in educating and attracting the next generation of talents to innovate on new drone capabilities, steps that smaller European countries had taken to leapfrog their drone capabilities as they sought to develop the next generation of capability instead of trying to play catch up. Mr Guillermet suggested that it was also critical to establish an ecosystem and progressive regulatory framework to enable drone services to flourish. Mr Welsh commended Singapore for taking a balanced approach to allow for innovation and experimentation of drone services through sandboxing without undue regulation.

PANEL DISCUSSION -

WILL SMALL OUTDO BIG IN SPACE?

Space Renaissance

Following Prof Sir Sweeting's summary of the history of space, panellists discussed the possibilities of the New Space, where access to space and applications using space were affordable and no longer dominated by governments of developed countries. Particularly, Mr Winetraub shared that his lunar landing attempt had inspired the younger generation.

Mr Schingler described the current developments as a space renaissance, with companies sprouting up and attracting the best engineers, as well as people taking risks and inventing new and novel capabilities.

Mr Suchet agreed and added that the evolution in space had lowered the barriers to entry and extended the economic sphere of influence beyond scientific and defence purposes.

Challenges of Mega-Constellations of Small Satellites

The panellists deliberated on the challenges posed by mega-constellations of small satellites, with Mr Suchet pointing out space traffic management and debris control as key issues that needed to be addressed.

They discussed the need for accurate orbit data to be shared for improved situational awareness. In specific high risk scenarios, active space debris removal could also be applied. However, the panel noted that accurate orbit information could be abused and active debris removal could be misused as anti-satellite weapons.

Risk Management

Regarding the perception that New Space could take higher risk, the consensus was that it adopted a different approach in managing risks. One of the methodologies is to have a portfolio of projects, focusing on minimising risks for larger projects but allowing room for failure for smaller ones.

Mr Winetraub highlighted that instead of providing redundancies within the system, which would not have prevented the failure anyway, SpaceIL engaged with stakeholders to manage expectations and maintain a positive perception of the project even after their hard landing on the Moon.

He also mentioned that flexibility on performance requirements had helped to manage the project's schedule and cost risks. Risk management in New Space was also about having resilient satellite architectures to cope with component failure, disaggregated systems resilient against satellite failures, and frequent technology evolution resilient to obsolescence.

Big Satellites Here to Stay

The panellists concluded that while there was increasing emphasis and interest on small satellites, there would always be a need for bigger satellites due to constraints imposed by the laws of physics. As Mr Schingler put it, small satellites may outdo big in sheer numbers, but they are unlikely to replace big satellites in terms of capability. However, shifting the laws of economics in space would open game-changing applications and determine how space could continue to evolve.

Moderator

Prof Sir Martin Sweeting
Founder and Group Executive Chairman, Surrey Satellite Technology Ltd

Speakers

Dr Liao Shengkai
Senior Engineer, University of Science and Technology of China

Mr Robbie Schingler
Co-Founder and Chief Strategy Officer, Planet

Mr Lionel Suchet
Chief Operating Officer, France's Centre National d'Etudes Spatiales

Mr Yonatan Winetraub
Co-Founder, SpaceIL

PANEL DISCUSSION -

THE BRAIN AS THE NEXT FRONTIER

Moderator

Dr Anthony Tether
Former Director, Defense Advanced Research Projects Agency, US Department of Defense

Speakers

Prof Alexander Kaplan
Head of Laboratory and Professor, Moscow State University

Honorable Zachary J. Lemnios
Vice President, Government Programmes, IBM

Dr Geoffrey Ling
Professor of Neurology, Johns Hopkins University

Dr Shinji Nishimoto
Senior Researcher, Japan's National Institute of Information and Communications Technology

Dr Eunsoo Shim
Senior Vice President, Samsung Electronics

Combining Human Brain and AI

Dr Tether started the discussion with each panellist sharing his work in neuroscience. The panellists observed that the discipline of neuroscience was starting to converge with AI developments. Instead of just advocating autonomy to a machine, placing the human brain and AI together could result in new exciting breakthroughs to overcome the limitations of humans and machines.

Potential of Invasive BCI

Demonstrating that the new age of brain-computer interfaces (BCI) had arrived, Dr Ling presented videos of astonishing success stories. They feature a woman with a BCI brain chip implant who was able to learn to control a robotic arm; a man with a similar implant being able to 'feel' with his robotic arm's fingers; a woman without any form of flying experience flying a flight simulator by thinking of flying, and a man who showed enhanced ability to recall words after the transfer of neural code. Dr Ling concluded that BCI was no longer science fiction and the possibilities would be limited only by our imagination.

Potential of Non-Invasive BCI

Dr Nishimoto shared his research on encoding brain activities by allowing subjects to watch a movie and recording the brain signals such that the model could decode semantic experience from brain activities. He shared that combining brain models and machine learning achieved a significant improvement in transfer learning compared to just using brain models. This approach of using cortical representation to guide machine learning had the potential to create more human-like AI systems.

Challenges

In the panellists' discussion, Prof Kaplan said it was impossible to fully comprehend the inner workings of the brain accurately by decoding signals in non-invasive neurophysiological sensors and highlighted that the grand challenge was to develop a less invasive technology which would be key to increasing societal acceptance in the proliferation of BCIs.

Dr Shim highlighted the challenges of decoding the brain due to noise and that every brain was different. He showed a Samsung neural processor for AI and said that they were researching to optimise the AI algorithms for executing on small units. He added that the other challenge was emulating the neuroplasticity of the brain, which allowed human brains to learn new connections. This meant that every human brain was different, and even for the same brain, it would vary at different points of a human's life.

Dr Ling opined that neuroplasticity of the brain could be the game changer as it would enable our brains to rewire themselves to communicate effectively with BCIs. With that, there would not be a need for researchers to understand brain signals, and yet be able to attain the holy grail of non-invasive man-computer symbiosis.

PANEL DISCUSSION -

ARE AGILE DEFENCE ESTABLISHMENTS POSSIBLE?

Agility in Defence Establishments

Ms Chan presented that although the agile manifesto was formed in 2001, agile adoption at scale had not been easy. She showed a diagram to illustrate that doing agile was not the same as being agile and that behavioural shifts were never realised by directives alone. The panellists shared their experiences in adopting agile in their respective organisations, and the cultural changes required. Dr Hong shared Samsung's 12-year journey, starting from the adoption of a few 'process-led' agile practices to building agile core teams that led the agile transformation to a corporate-wide level.

Dr Hokazono elaborated on the agile strategies that ATLA was starting to adopt, including leveraging innovation funds and rapid prototyping programmes. He contrasted the commercial sector with defence establishments which were typically slower and less open to collaboration due to sensitive technologies.

Fail Fast and Fail Safe

Mr Lynch shared his experience with the DDS, where he drove multiple digital efforts to transform the US DoD. He spoke of the need to have verticalised teams aligned to delivery and execution, with the organisation providing the required tools and environment for teams to move fast, citing the Joint Enterprise Defense Infrastructure as one such conducive environment. He emphasised the importance of bringing safety and security teams into the onset of development, strongly leveraging automation to achieve agility even for safety critical systems while advocating failing fast and safe.

Empowering Technical Teams

The panellists spoke of the need for organisations to empower staff. Dr Roper advised management to massively delegate to facilitate power at the edge, put thoughts into writing routinely and maintain positive energy to invite staff to contribute. Mr Lynch stressed on empowering technical teams to make decisions and take on risks, even waiving policies if needed. He asserted that instead of policy people, technical people should be making technical decisions on technical problems.

Need to Adapt Defence Acquisition Policies

The panellists also discussed the lack of openness in military systems which limited the ability of ageing systems to be upgraded quickly as technological trends progressed. Citing that the consolidation of defence contractors posed a national security concern, Dr Roper proposed a new paradigm of defence acquisition that would shift towards schedule, architecture, and design, instead of the conventional cost, schedule and performance. The discussion included the need for defence acquisition processes to speed up in order to be quick ingestors of technologies, with Dr Roper advocating an early connection with promising companies so that they develop commercial products with a responsibility in national security.

Managing Change

The panellists also recognised the need for organisations to manage change, such as in managing potential friction points between agile and non-agile teams.

Moderator

Ms Gayle Chan
Director Digital Hub, Defence Science and Technology Agency

Speakers

Dr Hong Won-Pyo
President and CEO, Samsung SDS

Dr Will Roper
Assistant Secretary of the Air Force for Acquisition, Technology and Logistics, US Department of Defense (DoD)

Dr Hirokazu Hokazono
Deputy Commissioner and Chief Defense Scientist, Acquisition, Technology & Logistics Agency (ATLA), Japan's Ministry of Defense

Mr Chris Lynch
Former Director and Founder, Defense Digital Service (DDS), US Department of Defense

SUMMARY PLENARY

(From left)

Moderator: **Prof Daniel Hastings,** Head, Aeronautics and Astronautics Department, Massachusetts Institute of Technology

Speakers: **Dr Eric D. Evans,** Director, Lincoln Laboratory, Massachusetts Institute of Technology
Mr Lim Chuan Poh, Chairman, Singapore Food Agency
BG (Res.) Prof Jacob Nagel, Visiting Professor, Technion-Israel Institute of Technology
Prof Alex Zelinsky, AO, Vice-Chancellor and President, University of Newcastle

Prof Hastings began with a hype curve to foster discussion on whether the panellists see the current state as hype or reality. Dr Evans explained that the key was to create a greater overlap between operational and technical communities, citing the example of setting up a counter-improvised explosive device task force in Afghanistan which allowed ops-tech teams to work on broad problem statements together quickly to meet real operational needs within weeks. Mr Lim added that funding and adoption were good indicators of whether technology was real or hyped up.

Facilitating the Mobility of Talent

The panellists concurred that talent was critical, especially in today's global environment where top talent was in demand and highly mobile. It would be challenging, if not impossible, to compete with technology companies through attractive pay and benefits. Hence, they advocated increasing access to talents by facilitating the flow of talent across government, industry and academia.

Prof Zelinsky explained that the system has to be flexible, which means enabling talent who had left the government to rejoin it without having to restart from scratch. Mr Lim emphasised the importance of an open talent strategy to access the global talent pool.

Dr Evans added that it was important to adopt novel approaches, such as allowing talented individuals in specific areas but without security clearances to work off-site along with security-cleared staff, and transit the knowledge to them. Mr Lim commented that it was important to empower talent to work on challenging problems and relieve them of bureaucracies within organisations.

Building Trust

A recurring theme of the summit was building trust in order for technology to be adopted. The panellists discussed their perspectives with Mr Lim opining that trust was independent of technology and was a slow process which required investment up front.

BG (Res.) Prof Nagel posited that trust between humans and machines with AI continued to be a challenge, with commendable efforts made in areas such as explainable AI. He cited autonomous vehicles as an example where AI might override human decisions.

Prof Zelinsky opined that applying AI to break the OODA loop must be for self-defence to protect human lives, as AI should not be responsible for human casualties when making offensive decisions.

Need for Agility in Asymmetric Warfare

The panellists agreed that agility was paramount due to the speed of evolving threats. BG (Res.) Prof Nagel noted that new threats did not need to arise from the latest technologies, citing how Israel had been experiencing a shift from high to low intensity conflicts in what was dubbed as a "war between the worlds", often against "weapons of the weak". In such an environment, it was critical to have flexible systems that could be adapted and reconfigured quickly.

Prof Zelinsky added that open standards and architecture are needed in order to be agile, citing how proprietary solutions had resulted in silos that hindered agility.

In order to stay ahead and develop game-changing technologies for the future, the panellists discussed the factors that had led to DARPA's success, which were summarised as DARPA's ability to recruit top talent; empowering these talent to make decisions; equipping them with the necessary resources, and immersing them in a culture of pursuing "world-changing" concepts while being cognisant and tolerant of a high failure rate.

The panel opined that every country would not be successful in replicating DARPA, but needed to adopt and contextualise its best practices. Given the rapid evolution and proliferation of technologies, the panel concluded that it was imperative to focus on innovations and reiterated the need for the global defence technology community to work together to tackle common problems.

ENGAGEMENTS

The second Tech Summit opened doors to promote the exchange of ideas, greater collaboration and partnerships. Singapore's Minister for Defence Dr Ng Eng Hen met with information experts Dr Brian Pierce, Office Director of the Information Innovation Office at the Defense Advanced Research Projects Agency (DARPA), US Department of Defense (DoD); Mr Amir Husain, Founder and Chief Executive Officer of SparkCognition; Mr Tim Hwang, Director of the Harvard-Massachusetts Institute of Technology Ethics and Governance of Artificial Intelligence Initiative; and BG (Res.) Prof Jacob Nagel, Visiting Professor at the Technion-Israel Institute of Technology. They discussed threats in the information space and the approaches to address them.

In addition, Dr Ng also met US DoD officials – Dr Will Roper, Assistant Secretary of the Air Force for Acquisition, Technology and Logistics;

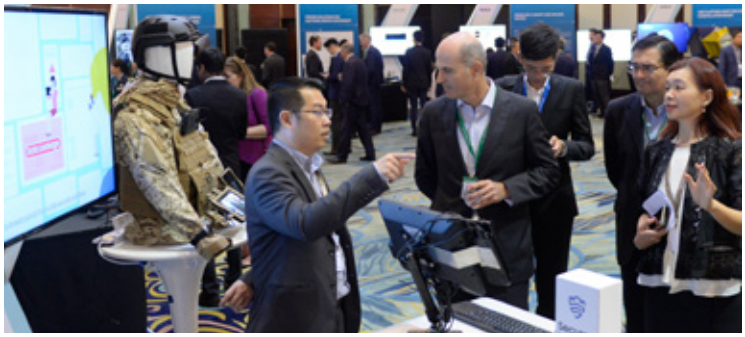
Dr Steven H. Walker, Director of DARPA; and Ms Heidi Grant, Director of the Defense Technology Security Administration on the sidelines of the summit. During the meeting, they discussed advancements in defence technology and its global implications while also reaffirming the breadth and depth of the bilateral defence relationship and strength of Singapore-US defence technology cooperation through professional exchanges.

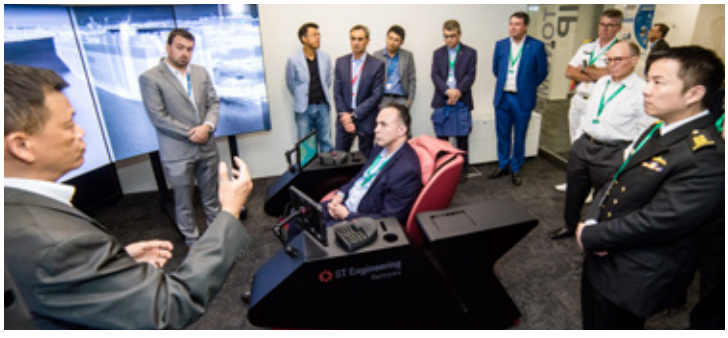
Engagement with Students

As the second Tech Summit brought together many delegates who are experts in their respective fields, it was also valuable for speakers to share their knowledge and insights beyond the summit's panel discussions. For the first time, DSTA organised a student engagement session to pique students' interest in science and technology. Two successful entrepreneurs – Dr Vivian Chan and Mr Yonatan Winetraub spoke with some 160 students from 36 schools on their entrepreneurial journeys as well as passion for science and technology.

TECHNOLOGY SHOWCASE AND SITE VISITS

To foster further dialogue and facilitate collaboration, a technology showcase was set up to feature technology innovations from 13 exhibitors. The exhibits inspired many conversations about technology development and covered topics ranging from micro-satellites, Internet of Things, and to drone detection and classification. In addition, delegates had the opportunity to visit several key technology centres in Singapore to gain insights into initiatives and efforts that are influencing Singapore's defence, security and society. These included DSTA, Singapore Armed Forces' sites, DSO National Laboratories, the Agency for Science, Technology and Research's FusionWorld, Maritime and Port Authority of Singapore's Port Operations Control Centre and Living Lab, Singapore Technologies Engineering's Smart Solutions and Thales' Digital Identity and Security Solutions.





Artificial Intelligence: A Revolution in Military Affairs?

By Michael Raska and Richard Bitzinger

COMMENTARY

At the upcoming Singapore Defence Technology Summit, defence-innovation leaders from around the world will discuss the direction and nature of novel technologies, as well as their impact on the future amid intensifying geopolitical strategic competition.

One of the key questions underscoring the summit is the ongoing debate on whether the rapid diffusion of artificial intelligence (AI) has a revolutionary impact on the future of warfare, and if so, what are the consequences for the development of military organisations and application of the technology.

In theory, the possession of AI technologies equals more effective weapons systems, which in turn results into greater military power, which in turn translates into greater geopolitical power.

AI proponents argue that the application of novel machine-learning algorithms to diverse problems promises unprecedented capabilities in terms of speed of information processing, automation for weapons platforms and surveillance systems, and ultimately, decision-making for more precision firepower.

In doing so, the utility of AI in military affairs seems virtually endless – from real-time analysis of sophisticated cyberattacks and detection of fraudulent imagery to directing autonomous platforms such as drones, and enabling new forms of command and control such as automated battle management systems that analyse big data and provide recommendations for human action.

Consequently, many argue that the diffusion of AI will have profound implications for how militaries adopt new technologies; how on an operational level, militaries adapt to and apply new technologies, and facilitate our understanding of the future battlespace.

At the same time, however, the pursuit of next-generation AI, which will transform computers from tools into problem-solving "thinking" machines, presents a range of complex organisational and operational challenges.

These include the research and development of advanced algorithms that will enable systems to learn from surprises and adapt to changes in their environment, adopting and adapting them into varying force structures and weapons platforms using novel operational concepts, and ultimately, designing ethical codes and safeguards on how to use them.

Complicating these predicaments, we now live in a time when "militarily relevant technologies" are becoming harder and harder to identify and classify.

Technological advances, especially in the area of military systems, are a continuous, dynamic process; breakthroughs are always occurring, and their impact on military effectiveness and comparative advantage could be both significant and hard to predict at their nascent stages.

Moreover, such technologies and resulting capabilities rarely spread themselves evenly across geopolitical lines.

In the Asia-Pacific, for example, the sources, paths, and patterns of new and potentially powerful militarily relevant technologies – based on AI and robotics as well as the ability of militaries to exploit their potential – varies widely.

Paradoxically, the growing strategic rivalry and the contest for future supremacy between the US, China, and to a lesser degree, Russia, shapes different national responses to the same technological breakthroughs, including AI.

In China, for example, the strategic competition for the research, development and acquisition of

cutting-edge AI technologies and robotics for the People's Liberation Army (PLA) to fight and win future "intelligentised wars" is embedded in the concept of military-civil integration (MCI).

While the MCI builds upon established principles of civil-military integration, which have for over two decades promoted the development of dual-use technologies and combined defense and civilian industrial bases, President Xi Jinping in 2016 elevated the MCI into a national-level strategy.

In doing so, PLA's long-term strategic military programs are deeply embedded in China's advancing civilian science and technology base, which in turn is increasingly linked to global commercial and scientific networks.

Yet, critical weaknesses remain. The Chinese science and technology industry still appears to possess only limited indigenous capabilities for cutting-edge defense R&D, and Western armaments producers continue to outpace China when it comes to most military technologies, particularly in areas such as propulsion, unmanned platforms, and defence electronics.

In the US, strategic competition for AI in military affairs are driven by a multitude of priorities, requirements, operating concepts, resources, and strategies - all factors that shape the direction and character of its future military forces.

However, unlike during the Cold War, spending on military R&D is now dwarfed by its commercial equivalent. Consequently, the US military is no longer the primary driver of technological innovation. Accordingly, the Pentagon aims to streamline its science and technology engines, such as the Defense Advanced Research Projects Agency (DARPA) enterprises to support sustained research in fundamental technologies and quickly leverage emerging technical opportunities in the commercial sector, including AI and cyber.

In doing so, the US military aims to tap on all potential sources of technical advantage from traditional industrial base, non-traditional suppliers and academia to help create competitive advantage by means of translating technical capabilities into solutions and concepts that would turn into capabilities to outmatch any threat.

Overall, how nations and their military-industrial complexes can leverage advanced military and dual-use technological innovation will have a significant impact on military capabilities and acquired advantages.

Some countries, including Singapore, may possess the resources to acquire advanced military technologies – either through indigenous R&D efforts or through acquisition from foreign suppliers – and others will not; some will have the means to systems-engineer advanced commercial technologies into effective military systems and others will not.

The main factors for success will not be technological innovation per se, but the combined effect of sustained funding, organisational expertise (i.e. sizable and effective R&D bases, both military and advanced commercial) and institutional agility to implement defence innovation. This means having people, processes, and systems in place capable to deliver innovative solutions in advance of need, while maintaining existing core capabilities.

At the same time, however, the diffusion of technological innovation will continue to create new strategic dynamics. Alliances may become more closely interconnected through technology-sharing and interoperability imperatives, while traditional strategic concepts such as deterrence will be tested through the emergence of different types of conflicts brought by new technologies.

All of these factors, in turn, will have likely have a significant impact on regional security and stability.

It is therefore critical to assess the relative abilities of regional militaries to access and leverage new and emerging critical technologies such as AI, their likely progress in doing so, and the impediments they may face, ultimately with an eye toward how it will affect relative gains and losses in regional military capabilities.

While the Singapore Defence Technology Summit may only scratch the surface of the debate when it comes to the future of AI and defence-innovation, it may advance what is bound to be a broad, multi-decade-long dialogue.

Michael Raska is Assistant Professor and Coordinator of the Military Transformations Programme at the Institute of Defence and Strategic Studies, a constituent unit of the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore.

Richard A. Bitzinger is a Visiting Senior Fellow with the Military Transformations Programme at the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore.

AI in Defence Innovation

By Zoe Stanley-Lockman

Executive Summary: *As the second Singapore Defence Technology Summit approaches, military applications of artificial intelligence (AI) will be a topical theme of discussion for global thought leaders who have gathered in Singapore. This commentary introduces some of the opportunities and challenges AI poses to militaries as context for the city state's investments in AI and emerging clout as a defence innovation leader.*

Over the past five years, rapid developments in artificial intelligence (AI) – particularly in deep learning – have brought AI to the fore. When DeepMind's AI beat the top human player at the complex logic game *Go* in 2017, the achievement was hailed as AI's "Sputnik moment".

Humans are growing more accustomed to hearing about and interacting with AI – be it in the form of virtual assistants, benefits such as accurate and reliable disease diagnoses, or warnings about dystopian futures of uncontrollable machines or job displacement.

More than 30 countries – including Singapore – have issued national AI strategies, not to mention the various international and regional organisations that have introduced AI principles and guidelines for their member states to follow.

Today, one need not even be an expert in machine learning to reap its benefits; AI services or hardware like accelerators spawn a range of off-the-shelf solutions available to individuals or organisations. While this type of AI democratisation creates more scope for mutually beneficial cooperation and innovation, some fear it simultaneously lowers barriers for malicious uses of the technology.

Nevertheless, the adoption of AI is not straightforward. As is the case for adoption of any new technology, access rarely translates to absorption. Instead, creating an advantage is dependent on a number of variables, including resources, institutional culture, and organisational structures. Adding a layer of complexity, one must also consider that AI is still a relatively new domain that poses challenges not only in the breadth of its future societal impact, but also in its comprehensibility to humans who cannot necessarily understand algorithmic reasoning.

Despite the accelerating pace at which AI has achieved milestones over the past several years, most organisations are still in a phase of priming themselves for eventual transformation, rather than substantially transforming today.

Singapore's Military AI Clout

Militaries are no exception. While anecdotal exploitation of AI may be possible for many, only few will have the capacity needed to strategically leverage AI.

The Singapore Armed Forces (SAF) has already made strides as an early adopter, most notably through innovative AI-enabled training methods and investments in laboratories focusing on AI analytics and robotics.

For one, Singapore's Defence Science and Technology Agency collaborated with the SAF to develop the Fleet Management System, which harnesses data analytics, machine learning and Internet of Things sensors to help diagnose issues, detect anomalies and perform pre-emptive rectification of systems. To help answer critical questions about military applications of AI, including the speed of decision-making, operational safety and accountability, Singapore has also established itself as a hub where technology and innovation leaders from around the globe can convene.

In the forthcoming Singapore Defence Technology Summit, human-machine collaboration will be one of the main themes that delegates will explore to advance the understanding of how AI can transform defence establishments ethically and securely.

What does it mean for soldiers to be augmented by AI technology? How can trust in AI be nurtured? How do we determine accountability when AI is involved? These are some of the complex, but nonetheless important, topics that the summit seeks to examine.

Explainable Algorithmic Reasoning

Such opportunities for dialogue and discourse are important because as it stands today, the nature of AI is highly sophisticated and ever-evolving. Humans are not always capable of understanding how an AI achieves its goal because the algorithm's reasoning

is not necessarily explainable to humans. In fact, improving the explainability of AI is a research area that has received significant attention.

For example, the US Defense Advanced Research Projects Agency has launched the US$2 billion "AI Next" campaign to, among other goals, improve contextual reasoning skills of machine to better match – and be comprehensible to – human reasoning.

Bias in data has also proven a near-insurmountable problem that decreases the utility of an AI's algorithm. In relation to security and defence, these types of challenges have significant implications for the decision-making process.

For instance, if a demographic is over-represented in a dataset used to train an algorithm to be used for surveillance, then that algorithm may end up prioritising irrelevant characteristics when identifying threats. If an algorithm sends that information in a way that is only comprehensible to another machine but not to human operators, then there is no way for humans to act on that information. In turn, this can increase reliance on machines, as will other traits such as speed and reliability.

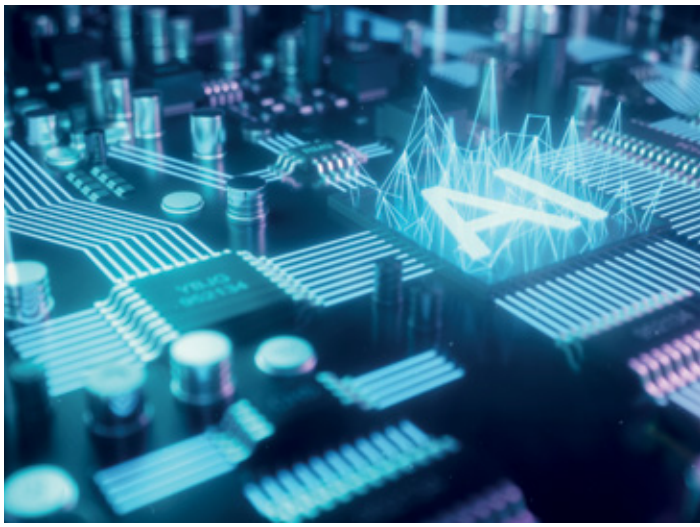
Hence, the development of guidelines and principles around AI ethics and safety, as well as investments in understanding algorithmic reasoning so as to be explainable and accountable to humans, are fortunately priorities amongst technical and policy communities around the globe.

However, not all consider how those guidelines translate to military contexts, or if they should at all. Only a handful of defence ministries, including in Singapore, are prioritising military AI ethics principles to guide the development and deployment of any AI-enabled capability.

In Singapore, for Singapore

In addition to overcoming these challenges, each country's military will have to contend with other roadblocks related to their own resource constraints, institutional culture, available talent, and political will.

Singapore has its advantages. Not only has Singapore launched the Model AI Governance Framework, the first of its kind in Asia, but the government has also set a high level ambition of having each ministry and government agency launch at least one AI-related project by 2023, funding AI training for the workforce, and offering incentives and a warm investment climate for AI start-ups and small and medium-sized enterprises.



Because no development of militarised AI will be purely conventional, these foundations in the commercial base and government adoption are critical to any strategic usage of the technology.

Given its small size (both in terms of population and geographical area), Singapore can also more readily scale up AI efforts than others. Having recently added digital defence as the sixth pillar of Singapore's total defence concept, the SAF is laying the groundwork for greater focus on cyber capabilities, big data, and related AI developments.

Early test cases from the SAF in leveraging AI for training serve an important role of familiarising the ranks with new technologies, which may set the tone for the SAF's ambitions to continue deploying AI for other tasks. More broadly speaking, Singapore's civilian investments in emerging technologies and in the Smart Nation concept will help establish the country as an AI middle power.

But ultimately, relying on AI alone is not enough. Even if some tasks are relegated to machines, a military is still only as good as its people who develop, collaborate with, or are augmented by those machines. Recruiting, training, and retaining personnel to make use of AI will be necessary.

Not only does this depend on the availability of talent, but also the willingness to engage in military affairs.

Zoe Stanley-Lockman is Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies, a constituent unit of the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore.

TESTIMONIALS

"I would say that it is extremely important to have the best possible knowledge in the room, coming from scientists, researchers, government officials, military and the industry. So I think the Singapore Defence Technology Summit gives the foundation for insightful discussions not just to talk about the future, but also to shape the future and make it real."

Rear Admiral Thomas Engevall, *Deputy National Armaments Director, Swedish Defence Materiel Administration*

"The Singapore Defence Technology Summit is fantastic because it brings together a number of different people from very diverse fields and environments – industry, government and universities. Not only are they very bright people but they also bring forth different perspectives for enriching discussions. The discussion with the CEOs was very interesting for me because I saw that one of the major problems or challenges that they are facing is talents. Today, searching for talents and training people in robotics, AI and new technologies is the number one priority and as researchers and professors at universities, I think it's a duty for us to train, grow and retain those talents."

Prof Dario Floreano, *Director of Laboratory of Intelligent Systems, Swiss Federal Institute of Technology Lausanne and Director, Swiss National Centre of Competence in Robotics*

"The big value in a conference like this is to really get cutting-edge thoughts from over the world, and not only were those people present here – very impressive delegates and attendees – but the atmosphere was such that it really bred that kind of open exchange. One of my biggest takeaways is that this new wave of technology is coming. Artificial intelligence, for example. There are a lot of challenging questions around cyber: How do we deal with attribution? How do we deal with issues of proportionality? These are all cutting-edge questions and this conference explored so many of them... It really added to my own knowledge."

Mr Amir Husain, *Founder and CEO, SparkCognition*

"It's important to ensure that technology is accessible because I think that it can be applied in many different places and doing it right often requires many different types of perspectives. So, it's critical for the military, industry and academia to collaborate with one another. DSTA is really interested in thinking long-term around the technologies, and that requires lots of perspectives. Holding the Singapore Defence Technology Summit is a far-seeing approach to think about long-term strategy, and I admire DSTA for making the investment for this event."

Mr Tim Hwang, *Director, Harvard-MIT Ethics and Governance of AI Initiative*

"In a dynamic and complex world, it is crucial that the military keep abreast of technological developments to continuously strengthen our capabilities... We are working very closely with the Defence Technology Community to build the Next-Generation Singapore Armed Forces (SAF), one that is more responsive to the realities of digital warfare and more capable in every domain. The Tech Summit has indeed generated many insights into how we can leverage emerging technologies to make the SAF more effective and future-ready."

Lieutenant-General Melvyn Ong, *Chief of Defence Force, Singapore*

"It's really a top collection of delegates. Industry and academia are producing new technologies and platforms which can be adopted by non-state actors and used potentially as threats, so these cannot be ignored by defence and national security agencies. There is also a rule of opportunities to take such technologies and adapt them at a reasonable cost and get a competitive advantage for the military capability."

Prof Alex Zelinsky, AO, *Vice-Chancellor and President, University of Newcastle and former Chief Defence Scientist, Australia*

Organised by:

Strategic Partner:

Platinum Partners:

Gold Partners:

Event Organisers:

www.dsta.gov.sg/techsummit

DSTA
Defence Science &
Technology Agency