



# SPEECH

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

---

## **Opening address by Senior Minister of State for Defence Dr Mohamad Maliki Bin Osman at the Ministry Of Defence Internet of Things Challenge at the National Design Centre on 25 September 2016**

25 Sep 2016

Ladies and Gentlemen,

Good afternoon, it is very exciting to be with all of you here today. I would first like to extend my heartiest congratulations to all the teams here at the MINDEF Internet of Things (IoT) Challenge. The Ministry of Defence organises annual IT-enabled innovation events involving employees and the public and this year's theme is IoT. The IoT sounds like something out of a sci-fi movie but it actually refers to a network of interconnected devices where data can be intelligently harnessed to enhance operation effectiveness and improve service excellence. I hope that you have found the programme exciting and that the rigorous process of proposal submission and selection, the customised Design Thinking Workshop, and the two-day hackathon have been a good learning experience.

"Disruption" and "disruptive technologies" have become buzzwords in the fields of engineering and technology. The technology that we see as modern conveniences, have the power to change industries and the way we live. Consider this: technology has placed information in the palm of our hand; we are now able to read the news, check on facts, and find a place to have dinner all with our smart phones. But these conveniences have also irrevocably disrupted industries that once specialised in publishing. For instance, the Yellow Pages telephone directory, once a familiar sight in many homes has now evolved into an online portal.

Technology, combined with commercial ingenuity, has also led to the growth of the sharing economy, where online platforms and apps such as Uber and Airbnb have given people the opportunity to become small-scale business owners. The collective power of these individuals who rent their cars or homes is challenging the way the taxi and hospitality industry work. Similarly, retail owners face fierce competition from Amazon and Taobao, which sell a wider range of products at cheaper prices online. Technology has pushed traditional industries to change the way they operate in order to thrive and IT innovation is crucial.

The Internet of Things (IoT) is another example of recent IT megatrends, and is poised to change the way we live, think, and work. The IoT is a network of physical objects – devices, vehicles, buildings and other items – embedded with electronics, software, sensors, and network connectivity that enables them to collect and exchange data with each other, often without the need for human intervention. The IoT allows objects to be sensed and controlled remotely across networks, creating opportunities for more direct integration of the physical world into IT systems, and resulting in improved efficiency, accuracy and economic benefit.

By infusing everyday objects with connectivity, we will be able to better gather information and exchange data to improve lives. At the national level, iDA's Smart Nation Platform (SNP) will enable everyone and everything, everywhere, to be connected and many sectors of society will be able to benefit from this interconnectivity. For instance, the LTA tracks the real-time location and arrival times of buses using sensors installed in over 5,000 vehicles and uses the information for transport planning to better meet commuters' demands.

I spoke about connectivity as a key enabler for IoT solutions. Of course connectivity also comes with challenges. Cyber attacks are real. Similar to governments worldwide, the Singapore government has been the target of highly sophisticated cyber attacks for years. Let me quote two examples that happened outside of Singapore, but could potentially happen here if system designs are not strengthened with robust cyber security measures.

First, the hack on the US Office of Personnel Management in 2015, which affected 22.1 million people, resulted in the theft of Social Security numbers and other information about current and former government workers, applicants, contractors and spouses of those who underwent background checks for security clearance. My second example occurred in February this year. Computer security researchers in UK demonstrated how a certain electric car's mobile app can be used to remotely hack its in-car systems. The app interface (API) uses only the vehicle identification number (VIN) to control car features remotely, without authenticating the user login through passwords. The researchers were able to hack into features related to the car's current battery life and air conditioning. A malicious hacker could easily turn on the car's air conditioning from the opposite side of the world, draining the battery and making the car inoperable. Therefore, it is important that we create solutions that are securely connected, so that we could harness cutting-edge technology without compromising security.

### **Harnessing Technological Innovations**

The Ministry of Defence is no stranger to harnessing new technologies to improve its processes and operations. This includes exploiting the Internet of Things in the areas of Logistics, Building, and Soldier Health and Safety. Imagine how the SAF could use and benefit from such technology. For instance, there could be sensors on vehicles to optimise their utilisation and to reduce downtime by using predictive analytics to schedule maintenance appointments and order spare parts in advance. Similarly, buildings and infrastructure design could harness IoT technologies such as video analytics to enhance our ability to detect security threats. The IoT also has the potential to deliver enhanced soldier care and training. For example, wearable technology could be used to monitor soldiers' vital signs during training, and identify those who are unwell.

### **Crowdsourcing to Co-create A Better MINDEF/SAF**

MINDEF understands that to keep up with the rapid changes in technology, it has to continually look for new ways of problem solving and tap on brightest minds in the field. Since 2014, MINDEF has organised annual IT hackathons, to crowdsource ideas and co-create prototypes for mobile applications and data analytics solutions. MINDEF is open to new ideas and wants to tap on a broader range of external experts and partners. This year, MINDEF has reached out to the Institute of Higher Learning to encourage students to submit IoT ideas. I am heartened to see that we have participants from our universities competing against, and learning from the IoT practitioners from start-up companies.

### **Engaging Science and Engineering Talent Pool**

I would also like to encourage you to think about the IoT and use of technology in defence in particular. MINDEF has always been committed to building up a strong science and engineering talent pool to support Singapore's needs through the Defence Technology Community, or DTC, for short. The DTC has been invaluable in procuring military assets and gear, and enhancing them to suit the SAF's operational requirements. Many of the DTC's contributions also extend beyond the military such as the Infrared Fever Screening System which was Singapore's first line of defence against the deadly SARS virus, and the Marina Bay Floating Platform which has been the venue for numerous events including seven National Day Parades and the F1 Night Race. These are but two of the many accomplishments of the DTC, and I hope that these examples will inspire all of you to dream big and help the local tech community soar to greater heights in the next 50 years.

**Conclusion**

I hope that the IoT Challenge has inspired you to think more deeply about how we can harness technology to better our lives and that of our fellow Singaporeans. I wish all the teams the best of luck and look forward to seeing these innovative projects. Thank you.

**News Release:**

- MINDEF Internet of Things Challenge to Crowdfund Ideas and Co-create Solutions to Improve Work Efficiency and Training Safety (MINDEF\_20160925001.pdf)

National Archives of Singapore