The Internet of Military Things

AJ Poulter
Principal Computer Scientist – Data Science Team

Matthew Mackay
Senior Analyst – Cyber and Novel Effects Team
Introduction

The Defence Science and Technology Laboratory (Dstl) is an executive agency of the United Kingdom Ministry of Defence; our role is to ensure that innovative science and technology contribute to the defence and security of the UK.
Contents

• What is the Internet of Military Things (IoMT)?
• Benefits of the IoMT for Defence
• Cybersecurity Challenges
What is the Internet of Military Things (IoMT)?

- Gartner define The Internet of Things as “…the network of physical objects that contains embedded technologies to communicate and sense or interact with their internal states or the external environment”.
- Cisco highlighted that in 2016 that while the world’s population stood at 7.4 Billion, the number of connected devices reached approximately 16.28 Billion
  - This is set to further increase with the IoT estimated to reach 50 billion connected devices by 2020 (Manyika et al; 2015);
- The IoMT is the application of Internet of Things (IoT) technologies and concepts to the military domain
Benefits of the IoMT

• Military IoT adoption is still in its infancy, however defence companies and the armed forces are eager to prepare, understand and leverage the IoT.

• The US Defense Information Systems Agency (DISA), for example, argues that the IoT will “result in an explosion of capabilities on our sensitive unclassified and classified networks” (Seffers, 2015);

• There are clear military benefits from the use of IoT devices for the armed forces, ranging from vehicle maintenance to personnel monitoring to stock control.
Source: Connected Soldier (Fraga-Lamas et al; 2016: 10)

Source: IoT Fleet Management (IoT Now Magazine; 2016)

Blue Force Tracking
The US Army take the concept even further with the idea of the Internet of Battlefield Things (IoBT)

Thousands of dynamically composed devices with sensors across the battlefield, exploiting autonomy & AI to provide situational awareness & meet mission goals
Cybersecurity Concerns

• A number of high profile attacks, for example the Mirai botnet attack, have shown that many IoT networks are insecure
  – Risk of compromise or loss of data from the device
  – Risk of false data spoofing from the device
  – Risk to the physical device
  – Risk to the networks into which the device is connected

• Before IoT devices are used in the military environment, the risks they pose must first be properly understood and suitable mitigations put in place
Summary

• The use of IoT devices in the military environment has the potential to provide real benefits
• However, numerous examples have demonstrated that IoT devices are often susceptible to cyber attacks
• The risks that these systems pose must be fully understood and mitigated before they are implemented within the Military and MOD environment.