Cybersecurity in aviation: a regulator's perspective

Modern military aircraft and their supporting ground systems have become increasingly reliant on computer systems for safe and efficient operation, making them targets for cyber-attack. The Military Aviation Authority (MAA) is implementing enhanced requirements for cybersecurity, to evaluate and counter this threat to air safety.

Background

The use of computers in aircraft and their supporting systems is not a new phenomenon, the ability to implement complex functions in software and improve them without changing the hardware has been an attractive attribute in aircraft design for several decades. Previous generations of computers utilised on aircraft tended to be bespoke, isolated systems with novel components. As such, attacks on these computer systems would require physical access and use of specialist equipment and knowledge.

Traditional security measures (such as physical access controls) were effective against such attacks and the computers themselves were limited in their ability to affect aircraft safety. Modern computers are far more powerful and versatile than those of earlier generations. Improved programming techniques now allow them to be used with confidence for safety-critical functions.

Previously, the requirement for military applications drove the cutting edge of computer technology, whereas more recent developments are designed to meet the needs of complex civilian applications such as safety control systems, entertainment and communication systems. Whilst the use of available 'off-the-shelf' software and hardware components in military systems represents good value for money by leveraging on the billions of pounds being invested in the civil sector, as a direct consequence it may increase the systems' susceptibility to cyber-attack.

The threat of cyber-attack on military systems is multifaceted and can include incidental attacks not specifically aimed at military systems. An example is a ransomware attack, which encrypts general IT systems and demands payment to unlock the data. The WannaCry ransomware attack of 2017 infected an estimated 300,000 computers worldwide, leading to a lock-down of the UK National Health Service computer system at an estimated cost of £92 million and the cancellation of 19,000 appointments.

Of specific concern to military systems are state-sponsored attacks, multiply directly from government teams or from covert groups with access to state resources operating under directed intent. Such attacks are likely to be aimed at reducing or impeding military capability or securing access to sensitive information. The attackers themselves are likely to have access to sophisticated technology and intimate knowledge of previously-undisclosed

vulnerabilities.

An example of an alleged state-sponsored attack is the infamous Stuxnet virus of 2010, which targeted Iranian nuclear enrichment facilities. This virus spread through PCs operating Windows software, infecting an estimated 200,000 computers. However, it had limited noticeable effect on these machines unless they were connected to a specific type of Siemens control system used in the operation of the Iranian centrifuges.

Once connected, the virus could target the precise motors in use and control their rotational speeds. The attack was subtle in its approach, doing nothing at first but then periodically speeding up and slowing down the equipment, wearing out the motors whilst the cause remained particularly difficult to pinpoint. Deemed highly successful, the attack resulted in a reported 30% drop in output and may have destroyed up to 1000 (10%) centrifuges used at the site.

New civil aviation requirements for cybersecurity

The European Aviation Safety Agency (EASA) has published two notices of proposed amendment (NPA) related to cybersecurity. NPA 2019-01 'Aircraft cybersecurity' was added in February 2019 and NPA 2019-07 'Management of information security risks' added in May 2019.

NPA 2019-01 introduced the new acceptable means of compliance (AMC) 20-42 which detailed changes to various existing certification specifications (CS) that now include new cybersecurity requirements. For example, CS 25 (large aircraft) will introduce a new clause, CS 25-1319, which requires applicants to protect against 'intentional unauthorised electronic interactions that may result in adverse effects on the safety of the aeroplane', whilst demanding that 'security risks have been identified, assessed and mitigated as necessary'.

NPA 2019-07 has a wider scope, introducing new draft regulation to cover the direct (aircraft specific) and indirect effects on air safety caused by a cyber event impacting the normal functioning of the European Aviation Traffic Management Network (EATMN).

MAA cybersecurity requirements

In 2015, the MAA formally recognised the risk posed by cyber-attacks by updating its default airworthiness code, Defence Standard (Def Stan) 00-970, to introduce requirements for assessing cyber risks to airworthiness. At the time, there were no equivalent requirements within civil regulation, although civilian standards for assessing cyber risks to safety had been published. Therefore, these civilian standards, RTCA DO-326 and DO-356, were introduced to a single clause in part 13 of Def Stan 00-970 and tailored for the military requirement. Def Stan 00-970 is invoked for both type airworthiness (through regulatory article (RA) 5810) and changes to type design (through RA 5820).

The MAA endorses the wider Defence principle of ‘as civil as possible, as military as necessary’. In line with this, Def Stan 00-970 is currently undergoing transformation, as reported in a previous article titled MAA transformation of the design and airworthiness requirements for service aircraft (Defence Standard 00-970). Basing its requirements on recognised civil airworthiness codes to which military deltas are applied, where necessary.

Initial MAA focus is to provide updated guidance on the assessment of cybersecurity considerations on type airworthiness and changes to type design. As the new EASA AMC 20 42 is based upon the same civilian cyber standards as previously embodied in Def Stan 00-970, the MAA is seeking to introduce both this new AMC and the updated CS clauses to the equivalent parts of Def Stan 00-970, with necessary military deltas applied. For example, introduce CS 25.1319 to the large aircraft standard, Def Stan 00-970 part 5.

Further reviews of MAA cybersecurity policy are anticipated and are likely to include:

- consideration of overarching MAA regulation of cybersecurity, applicable to all military air safety-critical and safety-enabling systems, including a new RA for cybersecurity and/or updates to existing MAA regulation. This work will embody the overarching cybersecurity framework requirements of the US National Institute of Standards and Technology (namely: identify, protect, detect, respond and recover), but with a specific focus on air safety

- embodiment of cybersecurity requirements into MAA regulation and guidance where they relate to wider air safety, such as Air Traffic Management requirements in Def Stan 00-972 and continuing airworthiness

- working with the other cybersecurity regulators and the Regulated Community to establish best practice for cybersecurity in military aviation platforms and their supporting systems

The MAA is mindful that impending Brexit outcomes may bring changes to national civil aviation requirements and is liaising with the Civil Aviation Authority with respect to their ongoing cybersecurity work.

Summary

Cyber-attack poses a significant threat to the safe and efficient operation of modern military aviation systems. By supplementing existing civil regulation where necessary, the MAA must now equip the Regulated Community with cybersecurity regulation that, by design and sufficient through-life support, will ensure our critical systems and infrastructure are appropriately protected from this non-traditional, emerging threat.