Cybersecurity in Aerospace: A Military Perspective

Amit Kumar Bhargava

INTRODUCTION

Advances in science and technology have improved everything over the decades, but some improvements or advances are constructive for the world and some are destructive for people. Cybercrime is destructive and is an example of how we improve our technology every day. In today's world, weapons of war such as fighter planes, mission control systems, and defence secrets are digitally processed.

On the other hand, improving and controlling technology creates a problem of very large-scale cyberattacks and cybercrime**.** India reported 1.16 million cyberattacks in 2020, and the number of attacks is growing rapidly. India was the second country to be attacked in the Asia-Pacific region, after Japan.[1] Reducing these attacks requires understanding all aspects of cyberattacks and improving cybersecurity at all levels. Cybersecurity can be

[1] US military forces, *The Changing Role of Information in Warfare*, at https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1016/MR1016.chap10.pdf

Flight Lieutenant **Amit Kumar Bhargava** is a serving officer of the Indian Air Force.

defined as the set of measures to defend against cyberattacks and their consequences, including the implementation of necessary measures. Future warfare will not only be about technology, it will be "contactless" warfare, where "smart soldiers" fight invisibly against "smart weapons". Drones, missiles, EMPs and laser weapons change the whole concept of warfare.[2]

Figure 1: Cybersecurity In Aerospace: A Military Perspective

Source: Gettyimages.in.

Aerospace power is based on the integration of aerospace and information systems to achieve strategic military objectives. More powerful engines, lighter and smaller aircraft, smart weapons, radar and stealth technology, navigation and targeting systems, spatial communications and surveillance, precise positioning and navigation, ballistic missiles, and more has changed the nature and application of aerospace power in military doctrines over the last century.

Aerospace Cyber Security is about keeping safe, secure, strong operations and is the most significant for any military operations.

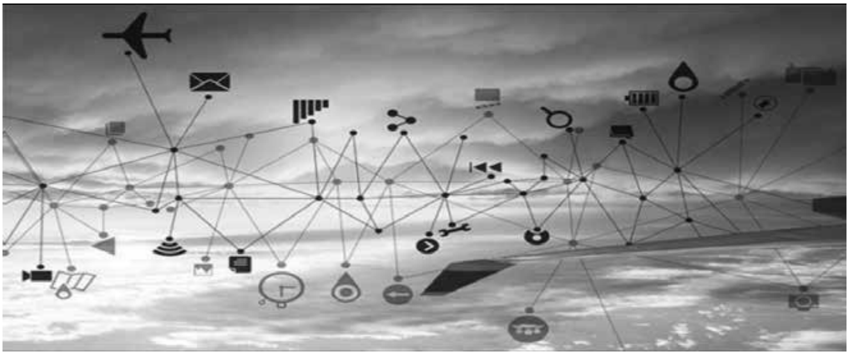
[2] Nikolche Milkovski, et al., "Information as a strategic resource critical to military operations and defence of the Nation", *International Scientific Journal* 355.40:355.45, pp. 107-119.

Advances in technology and successful digitisation carry several benefits to aerospace, but also pose challenges in managing cyber vulnerabilities in this complex environment.

CYBERATTACKS, HOW BIG IS THE PROBLEM?

Today's military weapon systems rely heavily on composite software and advanced connectivity to execute their tasks. Advances in Cyber skills allow many cutting-edge capabilities (automated attack, sensor synthesis, communications, etc.) giving the airborne weapon an advantage over possible challengers. But they also produce likely opportunities and encouragements for enemies. For illustration, a cultured attacker could notice and exploit weaknesses in avionics software, aircraft support systems, or source chain to obtain information or disrupt processes. Probable risks are not restricted to the latest and most cutting-edge systems. A large portion of the Air Force's inventory is comprised of older aircraft, which are also under attack from developing cyberthreats and should continue to be alert.

Figure 2: Cyberattack Network



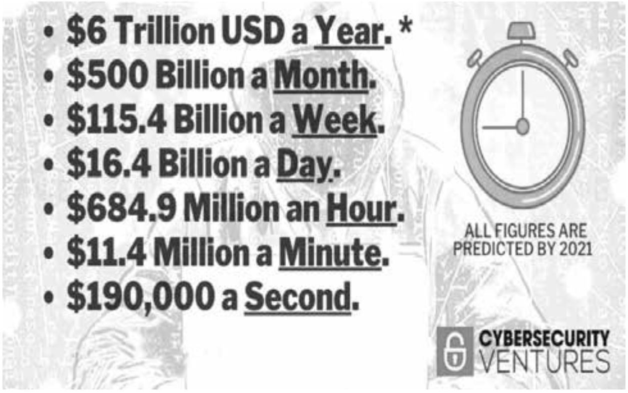
Source: Gettyimages.in.

Not all cyberattacks are successful, but all have a significant impact on the aviation industry. Due to the sensitive nature of the industry, airlines and defence contractors are particularly vulnerable to cyberthreats. Hackers in this space are often more sophisticated than hackers in other industries, and breaches in this space can have significant national security implications. Cyberthreats are growing faster than ever, aviation is not pervasive. By country, cybercrime is expected to cost US$6 trillion globally in 2021, making China the world's third largest economy after the United States and China.[3]

GLOBAL CYBERCRIME DAMAGE COSTS

From a military perspective, all weapons, including fighter jets, mission control systems, missiles, and drones, are increasingly embedded in digital technology. The computers that control weapons depend on data in the same way that human life depends on oxygen. Digital military data is the military representation of important information, facts, concepts, and instructions that form the basis of strategic or tactical decisions in the military. Our weapons platforms and communication networks exist in the physical dimension, but most data is generated, processed, stored and protected in the cyber domain.

Figure 3: Cybersecurity Spending



- $6 Trillion USD a Year. *
- $500 Billion a Month.
- $115.4 Billion a Week.
- $16.4 Billion a Day.
- $684.9 Million an Hour.
- $11.4 Million a Minute.
- $190,000 a Second.

*Source: cybersecurityventures.com

[3] Centre for Strategic and International Studies (CSIS), "Significant cyber incidents", at Washington, D.C._ 220906_Significant_Cyber_Incidents.pdf

In 2003, countrywide security data was stolen by Chinese software experts from the China Lake Naval Air Weapons Station, including data on nuclear armaments testing and design, and data on secret aircraft.

In April 2005, Chinese software experts penetrated National Aeronautics and Space Administration's network, controlled by Lockheed Martin and Boeing, and obtained data about the Space Vehicle Discovery Program.

In August 2006, Chinese software experts compromised the US Division of Defense network. A senior Air Force officer publicly stated:

> "In March 2008, Chinese hackers broke into the Department of Defense's Joint Strike Fighter Project and stole data related to F-35 fighter jets. South Korean officials claimed China attempted to infiltrate the South Korean embassy and South Korean military networks."

In May 2008, the newspaper (*Times of India*) stated that Indian administrators suspect China of installing malware into administration computers. The representatives of government say the spirit of the Chinese attack is to examine and plot India's official networks.

From January 2009 to February 2009, software experts confronted Israel's Internet organisation during a military aggression in the Gaza Strip. A French Navy plane was on the ground after its military database was infested with the "Confickr" virus. Navy bureaucrats alleged someone in the Navy had utilised his infected USB stick in February 2012. According to media reports, in March 2013, Chinese hackers stole classified information about the technology on board his F-35 Joint Strike Fighter. India's Defence Research Institute was hacked and thousands of documents were uploaded to servers with IP addresses in Guangdong, China. According to data recorded in National Aeronautics and Space Administration's Aviation Safety Reporting System (ASRS), there were close to eighty events of GPS signal noise or aircraft malfunction between 2013 and 2016. In March 2022, hackers affiliated with the Pakistani government targeted an Indian government official for espionage.[4] One cybersecurity researcher has observed hackers hacking into the networks of at least seven Indian State Load Balancing Centres (SLDCs) that monitor the operation of power grid controllers. According to SLDC, he controls the SCADA system, and researchers suspect he may be involved in the PLA-related hacks. In August 2022, a hacker targeted his website for the National Energy Agency of Ukraine, which is responsible for overseeing Ukraine's nuclear power plants. Officials said the attack was carried out by Russian hackers.

An Aviation Expert, along with two others, attacked the networks of Boeing and US and European defense companies to steal sensitive military and export control data. The trio stole gigabytes of data on 32 US projects, including 220 MB related to F-22s and 630,000 digital files related to C-17 freighters.[5]

Consider potential security vulnerabilities. All wireless communications and protocols should be considered at a high risk of exposure.

Scale of the problem: We have looked at many examples of reported incidents, but the name of the incident seems like the iceberg rule that we can only see reported cyberattacks. What about data and non-data attacks? Were reports received or

[4] Ibid.

[5] Indian Computer Emergency Response Team, "Cybersecurity in Aerospace", at https://www.cert-in.org.in/Downloader? Pageid=5&type=2&filename=CIPS-2017-0121.pdf

not approved? Or are we following the 80/20 rule? 20 per cent detected and 80 per cent not detected?[6] Nobody Knows!

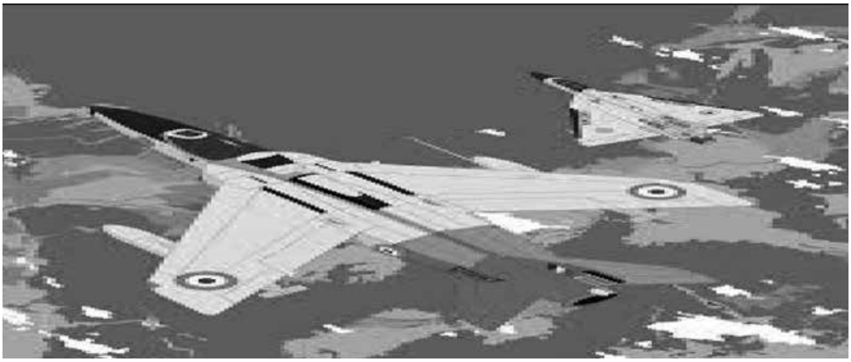
WHY CYBERSECURITY IS IMPORTANT IN AEROSPACE OPERATIONS?

Intelligence has always been a key issue in military operations. "If you know your enemy and know yourself, you can fight hundreds of times without fear of danger. If you know yourself, even if you don't know your enemy, the odds of winning and losing are the same. If you don't know your enemy or yourself, any battle is sure to put you in danger." (*The Art of War*, Sun Tzu) WuThe. The term "full band supremacy" suggests that "military forces can conduct rapid, sustained, and synchronous operations with forces sized for specific situations, access and having freedom means being able to conduct operations in all dimensions: land, sea, air, space, and information." Particularly in air forces of the world, because of its ability to carry out tasks with speed and flexibility, information handling for operations becomes even more sophisticated and critical. There are many systems and processes that are critical to the Air Force's capabilities. An enemy always attempts to interrupt, distort, or terminate the data necessary to support the military's ability to fight and sustain its operations, or both. The possible susceptibilities of the information systems that support war operations and sustainability efforts are quite different, as are the consequences of disrupting those systems.[7]

[6] Industry Intelligence Report, "Cyber Threats to the Aerospace and Defence Industries 2016", at www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-aerospace.pdf

[7] E. Matania, L. Yoffe, and T. Goldstein, "Structuring the national cyber defence: In evolution towards a Central Cyber Authority", *Journal of Cyber Policy*, 2017, vol. 2, issue 1, 16-25.

Figure 4: Cybersecurity in Aviation



Source: datascience.aero.

DIRECT IMPACT OF DATA INTERRUPTION

If an opponent were to exploit these susceptibilities, the effects could expose them in a number of ways:

- Damage or distortion of data.
- Interruptions of various sorts.
- Compact weapon efficiency.
- Reduced sortie rates.
- Reduced target discrimination capability.

War assets like radars, aircraft, missile systems, tanks, aircraft carriers, submarines, all at the heart have a computer and use computer networks to communicate among themselves. All these computer-operated war assets are governed by the data, or rather information which flows in the electronic circuit boards and networks. To win any war, absolute control over such data is mandatory. The merits of the digitisation in weapon systems don't come without the risks of information security. The enemies are on the lookout for vital data with every possible illegitimate cyber technique. With the recent advancement like IACCS, IMPACT, ICATS, E-MMS, IMMOLS, etc., secure data management will be the biggest challenge put in front of the leadership. Our ultimate aim of ‘cursor over the target’ will only be possible if all the digitised building blocks are ‘Information Secure’ and are available on demand.

Information networks and applications such as communication systems, air defence systems, and logistics network in military organisations. It covers all areas of operations, administration and maintenance, and this reliance will only increase in the future. Nationwide networks use a variety of media, including fibre optic cable, unshielded twisted pair, satellite, and other wireless channels and technologies such as MPLS and VoIP. These media will have their own inherent susceptibilities, which may reduce the network susceptible to attack. These network disruptions lead to disruptions that seriously disrupt the integration between air traffic and facilities.

Easy-to-use operating systems, antivirus software, browsers, firewalls, intrusion-detection systems, encoding software, etc. Most of them are of foreign origin. Similarly, the most important hardware components of high-end computers (motherboards and processors) and network elements (switches, routers, modems, and network cards) are also foreign-made. This software/hardware may contain pre-programmed malicious “backdoors” to perform a pre-programmed hostile activity.[8]

PREVENTION FROM CYBERATTACKS/CRIMES IN AEROSPACE

Security of data. In armed forces data security is paramount to ensure security of operations and thereby the nation. The operation data loss can jeopardise the organisation interest and will be a big threat to national security. Data can be backed up using a variety of hardware and software technologies. Common tools include antivirus, encryption, firewalls, two-factor authentication,

[8] US military forces, n. 1.

software patches and updates. Various technologies are used to ensure the security and privacy of operational data.

Figure 5: Prevention pictures

Source: istockphoto.aero.

- **Validation.** Validation is the act of confirming that a claim made by or about an entity is true and genuine. It performs important functions in organisations such as: securing access to corporate networks, protecting user identities, and ensuring users are who they say they are. Validating information can present unique challenges, especially man-in-the-middle (MITM) attacks. Most cryptographic protocols include some form of endpoint authentication to prevent MITM attacks.
- **Data encoding or encryption.** Encryption is an effective method of preventing unauthorised access to complex data. Its solutions protect and maintain data ownership throughout its lifecycle, from source to endpoint. Encryption helps thwart attacks such as packet sniffing and theft of storage devices. The organisations need to ensure that their encryption schemes are effective, easy to use for both users and administrators, and easily extendable to accommodate new electronic records.

Also, the number of keys owned by each user should be kept to a minimum.

- **Data screening or masking.** Screening or masking replaces sensitive data items with unidentifiable values. This is not actually encryption technology. However, it is not possible to return the original value from the masked value. Anonymise files or use strategies that mask personal identifiers such as names and social security numbers and suppress or simplify quasi-identifiers such as date of birth or the PIN code. Data masking is therefore one of the most prevalent approaches to anonymising live data. The main advantage of this method is that it reduces the security cost of data delivery. We recommend masking data before communicating outside your organisation for legitimate purposes.[9]
- **Access regulator.** After validation, a user may enter an information system, but that access is subject to access control policies typically based on the privileges of each authorised user. This is a powerful and flexible approval mechanism for users. It provides sophisticated authorisation controls to ensure users can only perform authentic activities, such as data access, cluster administration.

Importance of observing and auditing. Security monitoring or observing collects and examines network events to detect intruders**.** Auditing means that operating system user activity is recorded in chronological order**.** Maintain a log of all data access and changes**,** these two-security metrics are also used to measure and assure operating system security. Intrusion detection and prevention technology for all network traffic is very complex. A data network security system must quickly detect anomalies and identify appropriate alerts on disparate data. A data security event monitoring system consists of four modules: data

[9] Nikolche Milkovski et al., n. 2.

collection, integration, analysis, and interpretation. Data collection includes security and network device logs and event information. The data integration process is done by filtering and classifying data. Data analysis determines correlation and association rules to capture events. Data interpretation makes decisions, predicts network behaviour, and provides knowledge-based visual and statistical results in response to events.

Data retention. Data retention states to maintaining access to data and files over time. At the very least to survive, you need to store your data in one safe place, in multiple places, and in the file formats that are most likely to serve you well in the future.

The importance of data retention cannot be over-emphasised. Lost data is like it never existed. It is important to remember that data is the building block of everything and comes in all shapes and sizes. Data can be lost in several ways, including natural disasters, war, data breaches, or simply carelessness or degradation. Data loss, whether personal data or data loss within an organisation, can occur on a small or unrelated scale, and can also occur on a large or national or global scale. Environmental protection, research, health security, etc., can be adversely affected, with potentially permanent consequences. And security, economic development, and culture.[10]

RECOMMENDATIONS

- **Training.** Training is an integral part of human resources development programme in almost all organisations. In IAF training for cybersecurity will be effective to secure data and organisation.
- **Be Prepared for cyberattack.** Establish a crisis management team to monitor crisis situations and appoint a coordinating

[10] N. Yasar, F. M. Yasar, and Y. Topcu, "Operational Advantages of Using Cyber Electronic Warfare in the Battlefield." SPIE Defense, Security, and Sensing, International Society for Optics and Photonics, 2012.

officer as a "Point of Contact" to coordinate security policy compliance of the formation.

- **Cybersecurity in air traffic control.** Air traffic control, a critical function for any aerospace operations, is therefore subject to being targeted by attacks. There is a need to follow defined standards for cybersecurity in general.
- **Securing air traffic controllers and crew.** Crew and air traffic controllers are exposed persons who are important to protect.
- **Keep an eye on third party.** Third party involvement is a risk of cyberattacks. Every organisation has come to depend on third parties for their routine operational requirements. Notwithstanding the profits these relationships promise, however, dependence on third parties also exposes organisations to a higher level of risk.

CONCLUSION

Information warfare is of increasing importance both in the military as a whole, and in the Air Force, in particular. To combat myriad threats, it is imperative that the IAF have a clearly defined roadmap. Cyberwarfare capabilities will play an important role in future combat, but unlike other technologies used in warfare, cyberwarfare expertise is not yet confined to the military. Both military and civilians rely on information technology. Ultimately, a nation's supremacy in cyberwarfare will largely depend on its ability to combine military and other efforts. Any defence organisation must compulsorily instrument and sustain the best information security system to have the competitive edge over the enemy as digitised data is so vulnerable to losses while being highly important for the legitimate users in operations.