Chapter 7
Cyber Threats in Civil Aviation

Calvin Nobles
Independent Researcher, USA

ABSTRACT

Civil aviation faces increased cybersecurity threats due to hyperconnectivity and the lack of standardized frameworks and cybersecurity defenses. Educating the civil aviation workforce is one method to enhance cyber defense against cyber-attacks. Educating the workforce will lead to initiatives and strategies to combat cyber-attacks. Private and public entities need to remain aggressive in developing cyber defense strategies to keep pace with the increasing vulnerabilities of hyperconnectivity. Areas that require immediate attention to safeguard against cybersecurity threats in civil aviation are: 1) Eliminating supply risks, 2) Upgrading legacy systems, 3) Mitigating technological aftereffects, 4) Increasing cybersecurity awareness, 5) Developing cybersecurity workforce, 6) Managing hyperconnectivity, and 7) Leveraging international entities. To safeguard civil aviation infrastructure from cybersecurity threats require assertive, coordinated, and effective strategies and capabilities to defend the network.

INTRODUCTION

Persistent cyber-attacks on private and public computer networks in the U.S. continue to increase annually; consequently, highlighting the cyber security vulnerabilities of critical infrastructures. The number of cyber incidents reported by federal agencies grew from 5,503 to 60,753 from 2006 to 2012 (U.S. GAO, 2015). Increased cyber-attacks and threats led to extensive efforts to improve and safeguard computer networks in the U.S. For example, the National Infrastructure Protection Plan (NIPP) was mandated to develop defensive measures to secure critical infrastructures in the U.S. (Murray & Grubesic, 2012). The NIPP promulgates strategies to prevent cyber threats from manifesting by synchronizing efforts between public and private organizations (Murray & Grubesic, 2012). The U.S. government plays a critical role in providing cyber security, which includes protecting critical infrastructures, increasing cyber security awareness (Murray & Grubesic, 2012), developing cyber-attack capabilities, and disseminating cyber threat information to private and public entities.

DOI: 10.4018/978-1-5225-6195-8.ch007

Cyber criminals exploit private and public computer networks to gain access to sensitive information regarding national security, economic interests (Roesener, Bottolfson, & Fernandez, 2014), military defense plans, military personnel data, and to corporate espionage. Private entities own eighty-five percent of critical infrastructures; therefore, requiring the U.S. government to work strategically and collaboratively with the industry to prevent catastrophic attacks on our prized infrastructures (Murray & Grubesic, 2012). Regarding the civil aviation infrastructure, the Federal Aviation Administration plays a fundamental role in developing strategies and initiating actions to safeguard civil aviation.

Without a doubt, civil aviation is a critical infrastructure that is vulnerable to cyber threats by hackers and malicious actors (Schober, Koblen, & Szabo, 2012). One aspect of civil aviation that lends itself to cyber threats is the interconnected nature of computer networks and communication systems. Researchers refer to this phenomenon as hyperconnectivity (Fredette et al., 2012; Schober, Koblen, & Szabo, 2012). Hyperconnectivity makes it increasingly difficult to safeguard communications and computer systems from cyber-attacks. Critical infrastructure is a system or network of systems that provides vital functions that if disrupted causes socio-economic, financial, political, military defense, or security instability (Tanbansky, 2011). Critical infrastructures are food, water, financial services, healthcare, emergency services, energy power systems, and transportation systems (Kessler & Ramsay, 2013) that provide unique capabilities or services to the populace. Civil Aviation is a subsidiary of the transportation infrastructure and is considered critical infrastructure because of its significance to international and transoceanic transportation, globalization, financial security, international trade, and business. A major cyber-attack on the civil aviation infrastructure will catastrophically weaken and cause international instability.

As cyber innovations continue to expand, civil aviation's reliance on technological advances increases; consequently, making it difficult to protect civil aviation infrastructure from cyber-attacks (Lim, 2014). In the U.S. the aviation infrastructure consists of 450 commercial airports, 19,000 public airfields, multifaceted computer and communication systems Internet protocol enabled aircraft, wireless and sensor networks, supervisory control and data acquisition (SCADA), and cyber-physical systems (CPS) (Abeyratne, 2011; CSAN4, 2013; Jabeur, Sahli, & Zeadally, 2015; Lu et al., 2014; Nicholson et al., 2012; Roadmap to Secure, 2012). The above statement highlights the perplexity and vulnerability of the U.S. civil aviation infrastructure. The purpose of this chapter is to call attention to the cyber security threats within civil aviation from a non-alarmist perspective. This chapter discusses the emerging cyber threats in civil aviation, cyber security frameworks, the implications of hyperconnectivity dependence, educating the aviation workforce on cyber threats, and international and national level strategies for combatting cyber threats in civil aviation.

BACKGROUND

The increase in cyber attacks is indicative of the vulnerable nature of computer systems and networks accompanied by outdated systems and poor information assurance practices. Cyber attacks on critical infrastructures remain of high interest to public and private organizations due to national security concerns. Malicious actors, hackers, and adversarial nations are developing sophisticated capabilities to conduct cyber-attacks. The cyber domain is an attractive option for terrorists because of the low-cost, the ability to remain anonymous, and the opportunity to attack at will (Jarvis, MacDonald, & Nouri, 2014). Current attacks are increasing annually (GAO, 2015) and it is only a matter of time before terrorists conduct a catastrophic cyber-attack on a prized critical infrastructure. The increasing use of technological