Journal of Air Transport Management 69 (2018) 26–37

Contents lists available at ScienceDirect

Journal of Air Transport Management

journal homepage: www.elsevier.com/locate/jairtraman

Are pilots prepared for a cyber-attack? A human factors approach to the experimental evaluation of pilots' behavior

Patrick Gontar[a,*], Hendrik Homans[a], Michelle Rostalski[a], Julia Behrend[b], Frédéric Dehais[b], Klaus Bengler[a]

[a] Chair of Ergonomics, Technical University of Munich, Munich, Germany
[b] Institut Supérieur de l'Aéronautique et de l'Espace, Université Fédérale de Toulouse Midi-Pyrénées, Toulouse, France

ARTICLE INFO

Keywords:
Cyber security
Human factors
Simulator study
Pilots
Trust
Workload
Eye-tracking

ABSTRACT

The increasing prevalence of technology in modern airliners brings not just advantages, but also the potential for cyber threats. Fortunately, there have been no significant attacks on civil aircraft to date, which allows the handling of these emerging threats to be approached proactively. Although an ample body of research into technical defense strategies exists, current research neglects to take the human operator into account. In this study, we present an exploratory experiment focusing on pilots confronted with a cyber-attack. Results show that the occurrence of an attack affects all dependent variables: pilots' workload, trust, eye-movements, and behavior. Pilots experiencing an attack report heavier workload and weakened trust in the system than pilots whose aircraft is not under attack. Further, pilots who experienced an attack monitored basic flying instruments less and their performance deteriorated. A warning about a potential attack seems to moderate several of those effects. Our analysis prompts us to recommend incorporating cyber-awareness into pilots' recurrent training; we also argue that one has to consider all affected personnel when designing such training. Future research should target the development of appropriate procedures and training techniques to prepare pilots to correctly identify and respond to cyber-attacks.

1. Introduction

The exponentially increasing incidence of cyber-attacks is a growing problem in various private and public domains (Wilshusen, 2013). These range from personal cell phones and computers to critical infrastructures—including that of civil aviation (Elias, 2015; Zan, d'Amore and Di Camillo, 2016). A cyber-attack implies deliberate actions "to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and (or) programs resident in or transiting these systems or networks" (Owens et al., 2009, p. S-1). In aviation, the use of complex computer information technology such as that for fly-by-wire or flight management systems has intensified in recent decades. This trend has created potential vectors for cyber-attacks (Sampigethaya and Poovendran, 2013). The interdependence between complex aircraft systems and their integration into a modern airliner can easily propagate the effects of a cyber-attack from one system to another (Haass et al., 2016). Vereinigung Cockpit (2017) gave an overview of how interlinked the different systems in the aviation domain are, and where possible attack vectors might exist (see Fig. 1).

Several national and international aviation agencies (e.g., American Institute of Aeronautics and Astronautics, 2013; European Aviation Safety Agency, 2016; Iasiello, 2014; International Civil Aviation Organization, 2012, 2016; International Federation of Air Line Pilots' Associations, 2013; Lim, 2014) have already acknowledged that the civil aviation domain is potentially subject to cyber-attacks. Cyber-attacks against aircraft are still extremely rare at the time of writing; however, their increasing incidence in the future is highly probable and may lead to catastrophes, especially given the current rate of development in information technologies (International Civil Aviation Organization, 2016). Fox (2016) points out that although nothing serious has happened so far, it is a question of *when* rather than *if*. The vulnerability of commercial aircraft systems was highlighted by the U.S Department of Homeland Security, which was able to penetrate a commercial aircraft via radio frequency communication in 2016 (Biesecker, 2017). The airline industry as well as regulators take this problem very seriously and are following different approaches (American Institute of Aeronautics and Astronautics, 2013; Iasiello, 2014) and also amended regulations (Federal Aviation Administration, 2013; 2014) to try to prevent potential attacks.

However, these approaches focus mainly on technical means to

[*] Corresponding author. Chair of Ergonomics, Technical University of Munich, Boltzmannstr. 15, 85748, Garching, Germany.
E-mail address: gontar@tum.de (P. Gontar).

https://doi.org/10.1016/j.jairtraman.2018.01.004
Received 9 February 2017; Received in revised form 19 January 2018; Accepted 19 January 2018

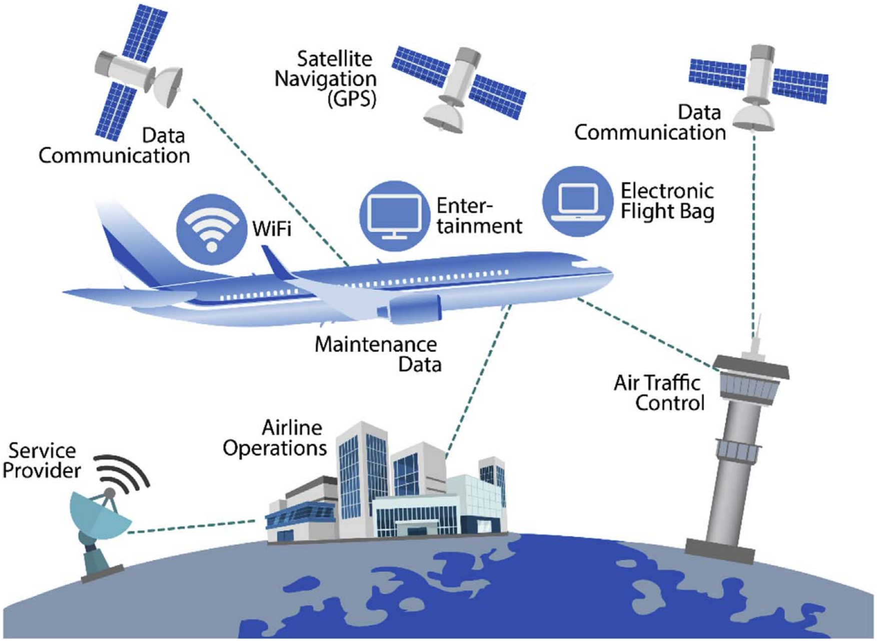

Fig. 1. Visualization of interlinked systems in the civil aviation domain showing several potential vectors for cyber-attacks. The figure is based on Vereinigung Cockpit (2017).

render potential attacks technically improbable. Very recently, a patent was granted to Boeing, in which the inventors suggest a new system to evaluate pilots' response to cyber-attacks in a simulation environment (Nguyen et al., 2017). In their description of the evaluation system, Nguyen et al. (2017) argue that "… because the pilot is such an integral part of the operation and control of the aircraft, pilot reaction to a cyber-attack is important" (p. 7). Besides erecting formidable technical and organizational barriers to eliminate security hazards before they reach the cockpit, we agree with Nguyen et al. (2017) that the human operator has to be integrated as a defense layer (Boyce et al., 2011; Langton and Baker, 2013), if not as the last line of defense (Vereinigung Cockpit, 2017). In this context it is important to distinguish between *safety and security*. Piètre-Cambacédès and Chaudet (2010) analyzed the usage and definition of both constructs extensively. They found not only that several researchers fail to explicitly define what they mean by one or the other, but also that very different definitions are used in different domains. Coming from the human factors domain, we favor the distinction from Firesmith (2003, p. 2) who defines safety as "the degree to which *accidental* harm is prevented, detected, and properly reacted to." Common safety issues might arise in the context of fatigue (Caldwell, 2012; Rosekind et al., 1994), loss of manual flying skills (Haslbeck and Hoermann, 2016), complex task switching (Gontar et al., 2017a,b), or technical malfunctions involving effortful problem solving and decision-making (Mosier and Fischer, 2010; Orasanu and Fischer, 2014) as well as intense team-communication (Gontar et al., 2017a,b). Firesmith (2003, p.14) defines security as "the degree to which *malicious* harm to a valuable asset is prevented, detected, and reacted to." Security is often seen as a technical challenge, although a successful cyber breach could evoke pilot reactions resembling those to a safety problem. However, from a human factors perspective, we think that pilots perceive differences between a cyber-breach-induced malfunction and a purely technical one. We point out these differences in the next section.

1.1. A human factors approach to cyber-attacks

Unfortunately, researchers have neglected human operators' response behavior in earlier cyber security research (Mancuso et al., 2014; Proctor and Chen, 2015). Horowitz and Lucero (2016) and Heiges et al. (2015) used a scenario with a manipulated navigation system showing false waypoints. Their main interest, however, was in investigating which security requirements would be usefully satisfied in engineering tools. Human factors analysis showed pilots' explicit wish for technical support during a cyber-attack as well as their concern about making ill-informed decisions. The major issue is that a successful attack exposes pilots to great uncertainty (Dutt et al., 2013; Hirshfield et al., 2015). Although individual cues might be ambiguous during the very infrequent occasions when technical malfunctions occur, pilots can normally apply procedures to solve the associated technical problems. Faced with a purely technical problem, pilots can also anticipate not only their own course of action but also the aircraft's behavior when, for example, a hydraulic system is leaking. The pilots know that they will receive an alert that hydraulic pressure is too low, maybe followed by another alert that the fluid level is also too low. Further, the pilots (depending on the aircraft type) might receive information from the aircraft system about how the specific technical malfunction will affect the aircraft's performance. In the example of a hydraulic system burst, the pilots can anticipate how this malfunction will affect their future flight—that their high-lift system will move slower, for instance—so that they can prepare mentally. When pilots face a cyber-attack, in contrast, they do not know whether the cues are trustworthy, or clear cues that an aircraft-borne system is under a cyber-attack might be absent. The pilots know neither whether the problem is solvable with their checklists and procedures, nor whether they will experience another problem right afterward. If pilots automatically follow their procedures in such cases, one can imagine potential attackers exploiting that knowledge to manipulate the pilots' behavior. Handling cyber-attacks, which are likely characterized by ambiguous cues lacking clear response options, becomes very effortful and also difficult for the pilots. The cue-clarity model that Orasanu et al. (1993) developed helps to understand how *cue-clarity* and *response option* availability can affect pilots' decision-making and performance.

1.2. An issue of cue-clarity

Cue-clarity describes a cue's clearness or ambiguity. An example for a clear cue could be a 'green hydraulic low pressure' warning in the abovementioned loss of a hydraulic system, while an ambiguous cue could be something like 'expect weather changes on-route'. Indeed, Dismukes et al. (2007) argue that weather information displays