International Civil Aviation Organization
Latin American Civil Aviation Commission
ICAO/LACAC NAM/CAR/SAM Aviation Security and Facilitation Regional Group (AVSEC/FAL/RG)

WORKING PAPER

AVSEC/FAL/RG/5 — WP/23
27/05/15

FIFTH MEETING OF THE AVIATION SECURITY AND FACILITATION REGIONAL GROUP (AVSEC/FAL/RG/5)

ICAO SAM Regional Office, Lima, Peru, 3 to 5 June 2015

Agenda Item 9: Other Business

CYBERSECURITY: MEETING THE CHALLENGES OF AN EVER-CHANGING TERRORIST PROFILE

(Presented by Jamaica)

EXECUTIVE SUMMARY	
This working paper presents information on recent cyber-attacks perpetrated against non-aviation entities globally and the Jamaica`s experience on this new threat, and calls the attention that it should not be the presumption that the aviation industry is immune in this regard.	
Action:	Suggested action is presented in Section 5.
Strategic Objectives:	• Security & Facilitation
References:	• "Cyber Security Trends in Latin America and the Caribbean", Organization of American States 2014 Report. • "Uniting Aviation", ICAO News Release 2014 • "National Cyber Security Strategy", Government of Jamaica 2015 • "Emerging Threats from Cyber Security in Aviation Challenges and Mitigations", Journal of Aviation Management 2014

1. Introduction

1.1 The ever changing nature of the threat to civil aviation has become increasingly evident as the world moves deeper into the technological era. The increased sophistication with which calculated attacks are carried out on our industry warrants a new paradigm in the way we address these new challenges. A growing concern for the North American, Central American and Caribbean Central, and South America Regions (NAM/CAR and SAM) is the threat of Cyber Terrorism and other cyber-related crimes, and our ability to adequately prevent and respond to critical incidents of this nature. Entities that seek to do harm to air transport are seemingly more minded to engage the industry in the cyber-arena, the real world impact of which being potentially as devastating as a physical attack on an aviation interest.

1.2 Though many of the more recent cyber-attacks have been perpetrated against non-aviation entities, it should not be the presumption that the aviation industry is immune in this regard. In 2013, the passport control system at the departure terminal at the Istanbul Ataturk International Airport and Sabiha Gokcen Airport in Turkey was victim of cyber-attacks leading to a variety of problems at the Airport. Likewise, in 2014, Japan Airline reported that a virus attack on computer terminals within its network resulted in the exfiltration of information relating to approximately 750,000 frequent flyer passengers.

1.3 Cybersecurity challenges have been recognised by ICAO, being proposed as a working document at the 2012 ICAO High-Level Conference for further discussion at the 12th ICAO Air Navigation Conference. This resulted in the formation of a cybersecurity task force to evaluate the extent of the problem. At its 25th meeting the ICAO AVSEC Panel had deliberations on a number of cybersecurity related matters.

1.4 The need for all member states and international agencies to work together was further emphasized in December 2014. ICAO and four international organizations came to an agreement to align their respective actions on cyber-threats. The common goal of the agreement signed by the five major international aviation organizations, as posited by ICAO Secretary General, was to "*work more effectively together to establish and promote a robust cybersecurity culture and strategy for the benefit of all actors in our industry*". The agreement calls on the Signatories, "*…to be more proactive in sharing critical information such as threat identification, risk assessments and cybersecurity best practices*" and for the encouragement of "*…more substantial coordination at the State level between their respective government and industry stakeholders on all cybersecurity strategies, policies, and plans.*"

1.5 The fundamental tenets of the foregoing agreement has been embodied in the required actions herein this working paper. These actions are viewed as necessary for the States within these Regions to overcome their peculiar challenges based in cost and expertise, in order to meet this cybersecurity threat.

2. Overview of cybersecurity in the NAM/CAR and SAM Region

2.1 The Organization of American States (OAS) in 2013, together with other research partners, looked at the state of cybersecurity and certain other developments as it related to cyber-crime in the NAM/CAR and SAM Region. The research assessed what it termed as major trends in the region in terms of cyber threats faced by a broad spectrum of technology users. The results were instructive as it provided for us a picture of the vulnerabilities and challenges faced by the region in safeguarding our critical technology dependent infrastructure.

2.2 The OAS report on Cyber Security trends in the region highlighted significant increases in cyber-crimes and cyber related incidents. These incidents include phishing, financial fraud perpetrated through the use of social networks, defamation and cyber bullying. The increases in cyber-crimes are compounded by the fact that the information and communication technology, to include use of the internet, does facilitate other non-cyber related criminal activities such as arms and drug trafficking.

2.3 The report also highlights a major challenge for policy makers in the area of data gathering: to inform certain cybersecurity related decision-making as there is gross underreporting of cyber-attacks by organizations for a variety of reasons.

2.4 Though the report found that the projections for government activities aimed at addressing cybersecurity needs are positive, it recognised that more work needed to be done in this regard and that greater involvement of other players in particular private sector users of technology systems.

3. Case study: Jamaica

3.1 In November 2014 over 10 Jamaican government websites were victims to a cyber-attack when a weakness in one website being hosted on a common platform was penetrated by a group of cyber attackers. It was known that the scripting platform had a vulnerability point and a patch to correct it had been released, however the website server had not been updated at the time of the attack.

3.2 The website for the Jamaica Civil Aviation Authority was one of the government websites victim to a “denial of service” (DOS) attack. Investigations are currently on going to determine the perpetrators and the Jamaican Government, Communications, Forensics Cybercrimes Unit (CFCU) along with technical assistants from the OAS are working together. Assistance from the International Telecommunication Union has also provided technical expertise in the implementation of the Cyber Incident Response Team (CIRT).

3.3 Cybercrime trends are increasing in Jamaica, and in 2012 the Cybercrime Legislation was updated and in 2015 the *National Cyber Security Strategy* was published which spear headed by a multi-agency task force at the National level.

3.4 Cybersecurity as an aviation topic is new for the aviation security stakeholders in Jamaica, and in February 2015 as part of an initiative between with Jamaica and OAS with technical assistance from the Israeli Government and US Government the topic was introduced as part of a 3 day course on the Insider Threat. The information gleaned in the two hour presentation, brought home the fact that more awareness in the cyber-threat and the use of risk assessments are needed in order to even begin to fight the next generation of threats to civil aviation.

4. Conclusion

4.1 In order for Sates within the Region to adequately and effectively address the sophisticated challenges posed by cyber-threats to its aviation systems, it is suggested that the following actions be adopted by the Meeting in keeping with common goal of the agreement of the five international organizations, Airport Council International (ACI), the Civil Air Navigation Services Organization (CANSO), the International Air Transport Association (IATA), the International Coordinating Council of Aerospace Industry Associations (ICCAIA) and the International Civil Aviation Organization (ICAO).

5. Suggested action

5.1 Sates within the Region should adopt adequate and effective actions to address the sophisticated challenges posed by cyber-threats to its civil aviation systems, and consider adopting the following proactive actions:

a) to develop awareness training courses to address the particular need of cybersecurity awareness;
b) to share cybersecurity information throughout the region through the AVSEC PoC Network; and
c) to include cybersecurity concerns within their States' conduct of aviation security risk assessments.

— END —