SYSTEMATIC THREAT ASSESSMENT

A PROCESS FOR ADAPTING SECURITY MEASURES BASED ON EMERGING THREAT RESEARCH

ABSTRACT

The Systematic Threat Assessment (STA) project conducted by the Center for Adaptive Security Research and Applications (CASRA) aims to produce highly relevant information and training material for airport security providers and serves as an additional source of information for relevant authorities in Switzerland. The main features of the STA are its structured process, its expert network and its timeliness. The constant scanning of different sources and the associated analysis allow the identification of novel threats in an early stage.

This process facilitates the prompt elaboration of countermeasures such as the development and implementation of adequate training methods within airports in order to facilitate the awareness of security staff regarding the latest threats. Embedded within effective and efficient structures for personnel selection, training and assessment, as well as a supportive work environment, such a process can arguably provide crucial benefits.

CASRA

The Systematic Threat Assessment (STA) is an essential part of a long-term research project of the Center for Adaptive Security Research and Applications (CASRA) which is funded by the Swiss Federal Office of Civil Aviation (FOCA). The main project goal is to increase the threat detection performance at airports by combining up-to-date intelligence with competence of security officers through changes to current training programs which are implemented at airports.

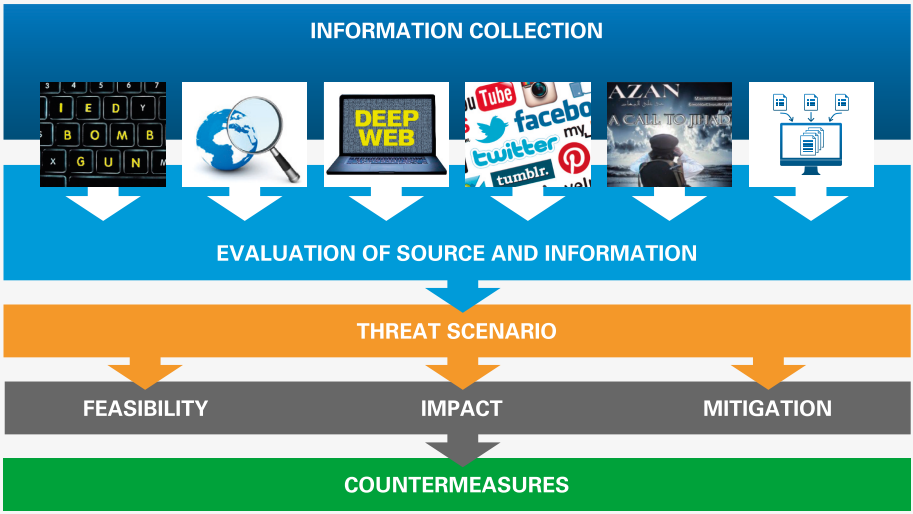

FIGURE 1: SYSTEMATIC THREAT ASSESSMENT PROCESS

The definition or adaptation of training measures for security officers should ideally be based on information on recent incidents as well as new and emerging threats to stay in tune with current and future threat scenarios. Therefore, an intelligence-based approach for the definition of different training measures, and potentially also other countermeasures, was established. In a two-step procedure, information is first collected from different sources and then analyzed and assessed with regard to a number of factors to determine the threat potential of a scenario. Within the scope of the STA process, different public and non-public Internet channels are systematically scanned for information that might be relevant for aviation security. The choice of sources that are taken into account is of high importance for the quality and conclusiveness of the analysis. Therefore, the scanning process and the sources were defined with great care. Figure 1 gives an overview of the STA process.

WEB ALERTS

An important part of the STA is to find and collect information on aviation and airport specific security incidents. For this purpose, a large number of so-called Web Alerts were set up with different publicly available web content detection services. Such tools allow the subscription to keywords and keyword combinations, for example 'IED + aircraft'. Whenever the subscribed keyword combination appears on the Internet, an automatic alert message is sent out by the web content detection service.

FIGURE 2: INSPIRE MAGAZINE NR. 13: «THE HIDDEN BOMB»

One example was the information that a new *Inspire* magazine was published by al-Qaeda at the end of 2014, which led to an evaluation of the so-called «Hidden Bomb» (Figure 2). In this manner, a large number of web alerts are constantly being generated and have to be evaluated by CASRA analysts.

To this end, an intelligence analysis process was established in which the raw alert content is rated and categorized in order to separate relevant from irrelevant information.

SURFACE WEB SEARCHES

By means of search engines and meta search engines, more detailed research on the relevant information is then performed in the Surface Web, the regular Internet. An example was the TSA report on Thermite based improvised incendiary devices (IIDs) from the end of 2014 (Figure 3).

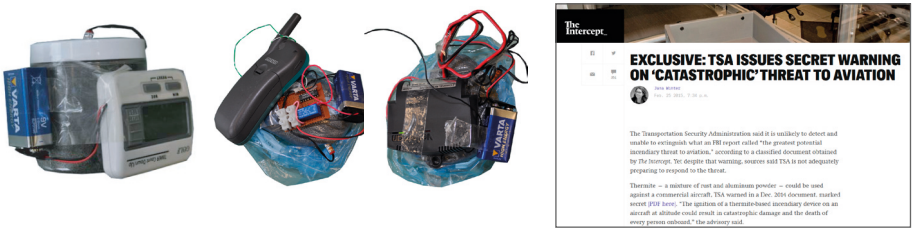

FIGURE 3: THERMITE BASED IMPROVISED INCENDIARY DEVICES

DEEP WEB SEARCHES

This procedure is also applied for certain anonymity networks in the non-indexed part of the Internet, the Deep Web (e.g. the Tor network), where the availability of threat objects and components can be assessed (e.g. 3D printed handguns, Figure 4). The Surface Web and Deep Web searches not only provide information about past incidents, they also reveal information related to the planning and preparation of attacks.

FIGURE 4: 3D PRINTED HANDGUNS

SOCIAL MEDIA

The fact that a large amount of relevant information also originates from online networking services or file sharing platforms shows the importance of paying particular attention to social media as well. This is why Internet identities that are well known for regularly uploading and sharing relevant content (e.g. manuals for the manufacturing of IEDs) are followed and monitored by the CASRA STA analysts in order to stay up-to-date about novel weapon types and attack techniques. Social media were also the source of the radio-controlled improvised explosive device (RCIED) scenario evaluated by CASRA in 2015 (Figure 5).

FIGURE 5: RADIO-CONTROLLED IMPROVISED EXPLOSIVE DEVICES (RCIEDs)

RADICAL PROPAGANDA

In the same context, radical propaganda magazines represent another important source of information taken into account in the STA process. Radical propaganda magazines that are available online in different languages are procured and scanned for relevant content such as manuals, ideas or concrete calls to action (see Figure 6).

FIGURE 6: EXAMPLES OF PROPAGANDA MAGAZINES AND THE OBJECT FROM DABIQ NR. 12 CAPTIONED: «IED USED TO BRING DOWN THE RUSSIAN AIRLINER»

THIRD-PARTY SUPPLIERS

As an addition to the large amount of information that is collected by the CASRA STA analysts themselves, threat reports from third-party suppliers in the field of web and technical intelligence services are included in the STA.

This further supports the validity and conclusiveness of the sourcing of content. Information that is considered relevant is integrated into the STA database.

SCENARIO EVALUATION AND COUNTERMEASURES

FEASIBILITY	IMPACT	MITIGATION
Is a threat scenario feasible, i.e. how easily are the necessary expertise and required materials available?	How high is the damage potential in terms of human, psychological and economic consequences?	To what extent are damage minimizing measures already implemented and what still needs to be done?

However, due to the large amount of raw material, a process needed to be defined that leads to a more conclusive list of potential threat scenarios. Subsequently, these scenarios are evaluated and assessed with regard to feasibility, impact and mitigation. This evaluation methodology is a derivation of the approach proposed by the ICAO for risk assessment (International Civil Aviation Organization ICAO (2012). *Risk Context Statement – Abridged Version)* with modifications to suit the process capabilities available.

In order to answer technical aspects of these questions, CASRA may rely on the expertise of supporting companies and competence centers at federal level. The knowledge that is gained within the framework of the particular evaluations is documented in threat reports that are sent to the relevant authorities who complement the information provided by CASRA with other information sources in considering the adaptation of existing and unpredictable measures (see Figure 7).

Research has shown that visual knowledge of threat items and their appearance in X-ray images is one essential prerequisite for good X-ray detection performance at airport security checkpoints (see e.g. Schwaninger, A., Hardmeier, D., & Hofer, F. (2004). Measuring visual abilities and visual knowledge of aviation security screeners. *IEEE ICCST Proceedings, 38,* 258-264). This knowledge has to be acquired and maintained through regular computer-based training (CBT). This is why, besides possible regulatory adaptations of security processes based on gained knowledge from the STA, effective countermeasures also involve the implementation of new threat objects within TIP and CBT libraries, as well as the creation of e-learning modules to provide deeper knowledge about new and emerging threats.

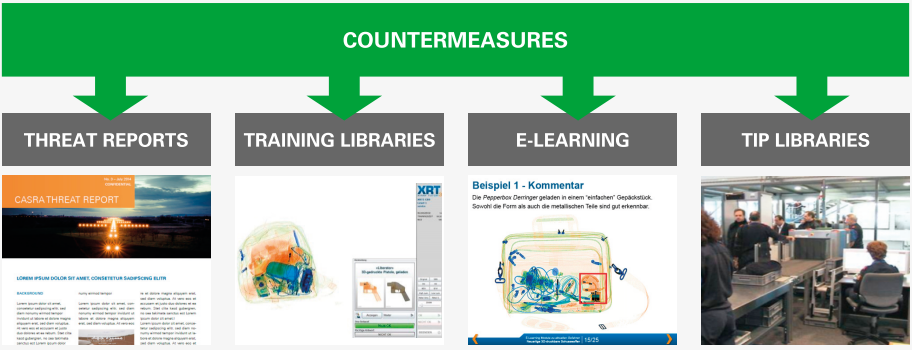

FIGURE 7: DIFFERENT COUNTERMEASURES

Finally, it should be noted that any process of threat assessment needs to have an effective and efficient transmission into a security chain that pays due attention to and supports the human factor. Starting from personnel selection, going through training and assessment, and further into the figurative "trenches" at the checkpoint, many aspects need to be considered to allow airport security officers to excel at what they do. For example, recent research has shown that the organizations that provide security screening services should pay attention to factors such as emotional exhaustion and job satisfaction to give their employees the environment they need to be good at what they do (Baeriswyl, S., Krause, A., & Schwaninger, A. (2016). Emotional exhaustion and job satisfaction in airport security officers - Work-family conflict mediator in the job demands-resources model. *Frontiers in Psychology, 7,* 1-13).

CASRA
Thurgauerstrasse 39
8050 Zurich
Switzerland

Phone: +41 (0)43 336 01 01
Fax: +41 (0)43 336 01 00
E-mail: info@casra.ch
Web: www.casra.ch