Systematic Threat Assessment: how to adapt security measures based on the research on latest threats

To prevent acts of unlawful interference against civil aviation, knowledge about new threats is of fundamental importance when it comes to the adaption of airport security measures in an efficient and effective way. But which sources have to be tapped into and how must different emerging threats be weighted? The Center for Adaptive Security Research and Applications (CASRA) has developed and implemented a Systematic Threat Assessment to detect and prioritise latest threat scenarios and to develop appropriate defence strategies. Florian Schmid, Systematic Threat Assessment Project Manager at CASRA, explains more.

The Systematic Threat Assessment (STA) is an essential part of a long-term CASRA research project 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 based on very regular changes to current training programmes which are implemented at airports and unpredictable adaptations of the screening level. 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 analysed and assessed with regard to a number of factors to determine the threat potential of a scenario.

**Scanning of different sources**

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 on the source categories of the CASRA STA.

"An important part of the STA is to find and collect information on aviation and airport specific security incidents."

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. 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 categorised in order to separate relevant from irrelevant information. 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. This procedure is also applied for certain anonymity networks in the Deep Web (e.g. the Tor network; see infobox on page 63 for more information). 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. In summary, this extensive internet analysis provides a valuable overview about key elements of threat scenarios such as the items and threat objects used, the availability of required items, and previous successes with similar operation methods.

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 contents (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. In the same context, radical propaganda magazines represent another important source of information taken into account in the STA process. More than a dozen radical propaganda magazines that are available online in different languages are procured and scanned for relevant contents such as manuals, ideas or concrete calls to action.

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.

Assessment of threat scenarios
Information that is considered relevant is integrated into the STA database. 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 the following three specific factors:

- **Feasibility**: Is a threat scenario feasible, i.e. how easily are the necessary expertise and required materials available?
- **Consequence**: How high is the damage potential in terms of human, psychological and economic consequences?
- **Existing mitigation measures**: To what extent are damage minimising measures already implemented?

In order to answer technical aspects of these questions, CASRA may rely on the expertise of supporting companies and competence centres at federal level. So far, this collaboration has resulted in a valuable network of experts whose assistance may be called upon if necessary. 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.

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. 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, countermeasures also mean the implementation of new threat objects within the CASRA TIP Libraries as well as the image libraries of the training program X-Ray Tutor 3 (XRT3) which has been installed in more than 30 countries at more than 600 airports. Additionally, specific and up-to-date e-learning modules for the CASRA Learning System (CLS) are developed in order to provide a deeper knowledge about new and emerging threats to airport security screeners.

**Case Study: ‘3D printed guns’**

The example of 3D printed guns illustrates how the Systematic Threat Assessment operates from the first information up to the implementation of Fictional Threat Items (FTIs) of 3D printed guns in the X-ray training system XRT3 and the e-Learning platform CLS at airports.

In May 2013, news channels reported the fabrication of the first working 3D printed gun called the Liberator. Comprehensive CASRA internet research showed that 3D files of different gun types could easily be downloaded on various file sharing platforms. In addition to that, a Deep Web evaluation of known marketplaces revealed the recent emergence of arms dealers who already sell printed 3D guns and deliver their products at a low price worldwide.

Within the framework of the STA and thanks to the collaboration with relevant Swiss authorities, CASRA was able to manufacture a number of different 3D guns in order to assess this novel threat scenario. In this manner, large-scale X-ray experiments with regard to their detectability, an evaluation of existing security measures as well as ballistic tests were conducted with the support of airports and federal competence centres. The results led to a report on this threat and the implementation of new FTIs showing different models of 3D printed guns into the training programme XRT3. In addition to that, e-learning modules for airport security personnel were developed and implemented in the CLS.

**Summary**

The STA supports CASRA in its efforts to produce highly relevant and up-to-date training material for airport security providers worldwide.

The STA supports CASRA in its efforts to produce highly relevant and up-to-date training material for airport security providers worldwide and it also serves as an additional source of information for relevant authorities in Switzerland. The main strengths of the STA are its structured process, its expert network and its timeliness. The constant evaluation of automatically generated news and the associated open source 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 sensitise security staff on latest threats.

It is worth emphasising that the security technology used at airports is currently evolving in the direction of multi-view and 3D imaging. In a newly launched project, CASRA is investigating the changes brought about by these technologies with regard to the human-machine interaction. As threat defence continues to take on new forms, it demands an assessment of the potential changes in required skills and training. These changes will arguably reshape the role of security officers at airports and influence the focus of STA.

---

**Deep Web and Tor network explained**

The expression ‘Deep Web’ (also known as Deepnet, Invisible Web or Hidden Web) stands for the part of the internet content which is not indexed and therefore not retrievable by standard search engines. The indexed part of the Web which is retrievable by standard search engines is known as the Surface Web. The Deep Web is estimated to be hundreds of times bigger than the Surface Web. As a part of the Deep Web, the Tor network, accessible only by the dedicated Tor browser, enables users to surf the internet and publish content anonymously. Therefore it is used by a wide variety of people for both legal and illegal purposes.