AUTUMN 2018

ECACNEWS #67

European Civil Aviation Conference Magazine

AVIATION SECURITY

Better, smarter, more innovative

ECAC • CEAC

CONTENTS

ECACNEWS
#67 – Autumn 2018

Publication Director
Salvatore Sciacchitano

Editorial Committee
Salvatore Sciacchitano, Patricia Reverdy, Gabrielle Hubler

Editor
Gabrielle Hubler
ghubler@ecac-ceac.org

Designer
Bernard Artal Graphisme
Cover: © Rawpixel.com - Fotolia.com
Ph: © CEAC

ECAC News welcomes feedback and content ideas from interested parties.

Subscription and distribution requests should be made to communications@ecac-ceac.org

The opinions printed in ECAC News are those of the authors alone and do not necessarily reflect the opinions of ECAC or its Member States.

Printed by Imprimerie Peau.

Follow ECAC on and visit our website **www.ecac-ceac.org**

Aviation Security: the time is now

Alessio Quaranta
Director General, Italian Civil Aviation Authority (ENAC)
ECAC Focal Point for Facilitation & Security

Has aviation security been given sufficient attention and the level of political priority it deserves over the last years? Most probably not, not yet… despite several terrorist attacks and plots in different regions of the world. Aviation security usually hits the newspaper headlines and grabs political attention when there is a crisis, such as long queues at screening checkpoints at the start of the summer holidays or a terrorist attack at a large international airport. At that time, there is a consensus that aviation security represents an essential component of the country's national security and that all the necessary resources should be immediately allocated to protect the citizens. However, as time passes, aviation security gets lower on the political agenda and its importance and contribution to the air transport sector and the economy at large become less prominent.

Terrorist attacks against civil aviation can typically be considered as "black swans", as they lie outside the realm of regular expectations, remain rare, have major consequences, and are often explained a posteriori ("retrospective predictability"). Giving aviation security a higher priority would strengthen our ability to handle black swans, but also show our collective commitment to better and smarter security:

- Better security in terms of the effective implementation of baseline security measures in all regions of the world and the definition of measures based on true risk assessments. And also better security in terms of the system's efficiency to address the constant evolution of the threats.
- Smarter security in terms of designing and implementing security systems that will enable the air transport sector to continue to grow in a sustainable manner. Smarter security in a way that improves the passenger's experience when using our airport infrastructures and our airlines. But also smarter security in terms of enhanced cooperation between States to define a global system where gaps cannot be exploited and the stack of measures does not lead to inconsistencies, overall damaging our objective of protecting aviation.

This edition of ECAC news brings together the perspectives of several European States and international partners of ECAC on some of the most current topics of discussion in aviation security, such as innovation, occurrence reporting, security culture and capacity building. Our international partners' contributions do enrich our reflection on the necessary evolution of aviation security in the year to come and contribute to the dialogue that ECAC has always been keen on promoting and supporting. I hope you will find this edition stimulating, in the weeks leading to the High-level Conference on Aviation Security, where I am convinced several of these topics will be addressed.

Security innovation: towards a better passenger experience

Sander Olivier
Policy Advisor, National Coordinator for Security and Counterterrorism (NCTV), Netherlands

How intelligent security equipment will help us make aviation security better, more efficient and more passenger-friendly.

We all know airport security checks are not much fun and have certainly not become any easier over the past years. The Dutch NCTV (National Coordinator for Security and Counterterrorism) together with Amsterdam Airport Schiphol and KLM are continuously working on improving aviation security. The focus of these efforts lies on making security better, more efficient and more passenger-friendly. So-called 'intelligent security equipment' is the next innovation that will enable us to achieve these objectives. Many developments have taken place over the last years which will help us automate (parts of) the security processes. These concepts are now ready to be trialled and deployed, and promising innovations are around the corner. This article discusses in more detail the Dutch vision for the near future and the results that are already visible at Amsterdam Airport Schiphol.

Over the past years, various terrorist incidents have resulted in a serious increase in security measures at airports. As a result, airport security procedures have become more extensive, more complicated and not always more passenger-friendly. There is a growing awareness that there are limits to the continuous increase in security measures. Of course, it is in the best interests of all stakeholders – governments, airports, air carriers and passengers – to prevent airport security from becoming a victim of its own system. More than ever, there is a need for a system that is robust (future-proof) and, at the same time, can be easily adjusted to current threats (flexible). The secret is to find solutions that offer benefits to all interested parties.

Intelligent and automated security equipment

The key words in this context are 'intelligent security equipment'. Intelligent security equipment will help us make the next step in improving aviation security and keeping up with the growing demand for air travel while maintaining passenger comfort. The use of intelligent screening solutions creates opportunities to automate screening processes, which benefits all involved stakeholders. Screeners can do their work with more focus, more ease and more pleasure and will therefore be more effective. Airports can streamline their security processes and create more screening capacity without the need to recruit more security staff, who are becoming more scarce. Passengers will benefit since there is less need to remove items, which will make security controls less intrusive and more smooth. Altogether, the use of intelligent equipment is expected to improve the overall quality of security by taking away repetitive tasks from screeners. This will result in a more stable and predictable security outcome. Moreover, intelligent security equipment makes it possible to perform tasks that simply could not be done before, as the examples below will show.

Machine learning improves performance of detection software

Recent technological developments have created a stepping stone for the next phase in aviation security. The establishment of new security standards has boosted the development of security equipment that works with automated detection algorithms. This means that most security equipment at airports nowadays is not only a piece of hardware but also runs flexible and adjustable software. At the same time, the science of machine learning rapidly matures and delivers impressive results in the field of detection software development. The fact that detection algorithms have become mainstream and that machine learning techniques can get the most out of these algorithms, has created an environment in which policymakers, airports and manufacturers can start working on improved security processes for both screeners and passengers. The first innovations have already taken place and resulted in major improvements. And there is more to come.

© Schipol Airport

Screener support and passenger comfort

A striking example of the promising results that intelligent equipment can offer is the evolution of automated explosive detection equipment for cabin baggage. The first trials with this type of equipment at Amsterdam Airport Schiphol date back to 2012. At that time, huge and heavy machinery and high false alarm rates were the norm. But since then a lot has changed. Nowadays several machines are available that meet the ECAC C3 standard and allow passengers to keep laptops and liquids in bags thanks to automated detection software. The size and weight of the machines has decreased by 30% and bag search rates have become lower than regular security procedures. Screeners are thrilled to work with the equipment since they feel more confident knowing they are assisted by smart software and 3D imaging capabilities while searching for improvised explosive devices (IEDs). Also, less bags need to be searched, and if a bag does need to be searched screeners are assisted by intelligent software. Frequent travellers who have experienced the ease of keeping laptops and liquids in their bags try to get into one of the smart lanes. Figures show that throughput improved by 10-20%. This convinced Schiphol to deploy this equipment over the whole airport by the end of 2019.

Further automation of cabin baggage screening

The use of automated explosive detection algorithms is just the beginning of the opportunities that intelligent equipment has to offer in our continuous strive to improve security and the passenger experience. Although the automated detection of explosives may currently assist the x-ray screener, it is just a matter of time before it will take over this responsibility. This means that the screener only has to focus on sharp items and guns, which will make his work less mind stretching and more effective. The next step in smoothing the screening process is the automated detection of knives and guns. Machine learning software developers are already working on algorithms that can automatically detect sharp items and other types of weapons (any new threats can easily be added when relevant). It is expected that these types of algorithms can be trialled in the short term. Again, first as a functionality that assists the operator in finding the objects, and subsequently as an automated functionality. This means that the first level of hand baggage screening would be fully automated so that the screeners can focus their efforts on the search for suspect bags. Their work will be enriched and will shift from repetitive image analysis to solving potential alarms and interacting with passengers. Smart image analysis tools like the virtual removal of dense items will help them do this in the most effective and convenient way.

Intelligent solutions for passenger screening

Also in the field of passenger screening, equipment becomes more powerful and intelligent as a result of machine learning techniques. This offers a huge potential to improve screeners' working conditions and, again, passenger satisfaction. Recently, the security scanner alarm rates have dropped significantly thanks to the use of machine learning software. The alarm rates are now nearing those of the walk-through metal detectors, with pat downs only needed on targeted locations. Furthermore, automation of passenger security processes is fostered by improved hardware and software, which allows for more computational capacity. The capability to process large amounts of data in real time opens the door for 'walk-through security scanners', which have become a technical feasible solution. The first proof of concept of a walk-through security scanner has already been trialled at Amsterdam Airport Schiphol. Based on these experiences, it is expected that in the near future manufacturers should be able to deliver ECAC-certified equipment. For the medium term, the goal is to eliminate the need to take off jackets, scarves and shoes. Upcoming wideband technology solutions can make less divesting become a reality. Another promising development for improved passenger experience is shoe scanners, which are designed to take away one of the biggest annoyances for air travellers. Shoe scanning equipment is designed to screen shoes without having to take them off. Equipment manufacturers have been working on shoe scanners – which can be used while standing still or even while walking – for several years now. Ultimately, shoe scanners will be fully integrated in the security scanners and will not require an extra stop in the security process. Current technology is able to deliver solutions; it is just a matter of time to make these technologies fit for operation at airports. The first trials with prototypes of shoe scanning equipment will start soon and will hopefully yield promising results.

© Kirill Zdorov - Fotolia.com

Joining forces towards self-service security

All the above mentioned developments are just the beginning of what is possible. There are many interesting developments underway which will make passengers' lives easier (and that of adversaries harder). The use of smart software on security equipment opens up many possibilities for a more passenger-friendly security system. However, aside from the technical hurdles that still need to be overcome, it is important for legislative bodies on both national and EU level to keep thinking ahead and stay open-minded in order to make these innovations possible. Regulations should be adapted in a timely way if we want to avoid hampering innovations that will contribute to a more passenger-friendly, more efficient and last but not least more effective security system. ECAC can play a significant role in this by proposing standards and developing testing methodologies. Also, to speed up the development of these solutions, it is important for manufacturers to allow specialised third-party software developers access to their equipment. Great results can be achieved when regulators, airports, airlines and manufacturers join hands. The ultimate goal would be for intelligent equipment and automation to lead us to 'self-service security', which would truly be the next level in the passenger experience. ■

Sander Olivier works as a Policy Advisor for the Dutch National Coordinator for Security and Counterterrorism. He has been working in the field of counterterrorism for more than ten years, during which time he was one of the founders of the Counterterrorism Alert System for the Dutch critical infrastructure. Today, Mr Olivier works for the Civil Aviation Security Department in the branch for policy development. In this position he serves, amongst others, as the national representative in several ECAC study groups. His main responsibilities are related to innovation, technology and new and emerging threats. Mr Olivier is the project lead on the Dutch programme that aims to develop a futureproof aviation security system. Under this responsibility, he has been heavily involved in deploying advanced cabin baggage equipment in the Netherlands.

What's occurring? An Irish take on occurrence reporting

Eleanor Travers
Aviation Security Manager, Aviation Authority, Ireland

Do you know what prohibited article is most likely to be found at the passenger screening checkpoint in an airport in your State? Do you know how many staff cause a security breach when they avoid the passenger screening checkpoint queues by entering the security restricted area through a staff checkpoint? Do you know which equipment is most likely to fail on any given day? Do you know which of the unruly passengers are trying to test how the air carrier responds to acts of unlawful interference?

In 2013 when the Irish Aviation Authority was first assigned responsibility for aviation security oversight, the requirement to report security incidents had been in place for many years. Basing its National Civil Aviation Security Programme initially on ICAO Annex 17 and ECAC's Doc 30, incident reporting was recognised as an important requirement.

Despite its longevity as a requirement, it never had the traction enjoyed by safety regulation, in part due to a security culture limiting information to the "need to know". There were other obstacles. Unlike safety, there were no safeguards for reporters, limited access to confidential reporting channels, human factors associated with not wanting to report suspicions of colleagues not to mention, once the report was submitted, limited ability to act or investigate outside of State and police criminal processes.

And everyone was trained. All staff at the airport, crew on board the aircraft, handling staff in the terminals. Latterly this was extended to include cargo and supply chain security personnel. Everyone knew what to do when they found an improvised explosive device.

As the State authority responsible, the Irish Aviation Authority was no different, but working together with the Department of Transport, Tourism and Sport, responsible at State level for aviation security policy, and with an industry cohort committed to improving the aviation security system, the view has changed.

Why did our view change? Ireland has a moderate threat level. Today there is no information that Ireland is a target, and while an attack is possible, it is unlikely. Good to know!! Irish policy goes further – not only do we want to prevent an attack in Ireland, we want to play our part and ensure that Ireland is not a vector for an attack elsewhere.

So how can we ensure the system is effective and how can we learn from our system to modify aviation security regulation and oversight accordingly?

We need security intelligence. Intelligence that tells us not only that the system is working as planned but also identifying the anomalies to that norm that force us to challenge our thinking and approach.

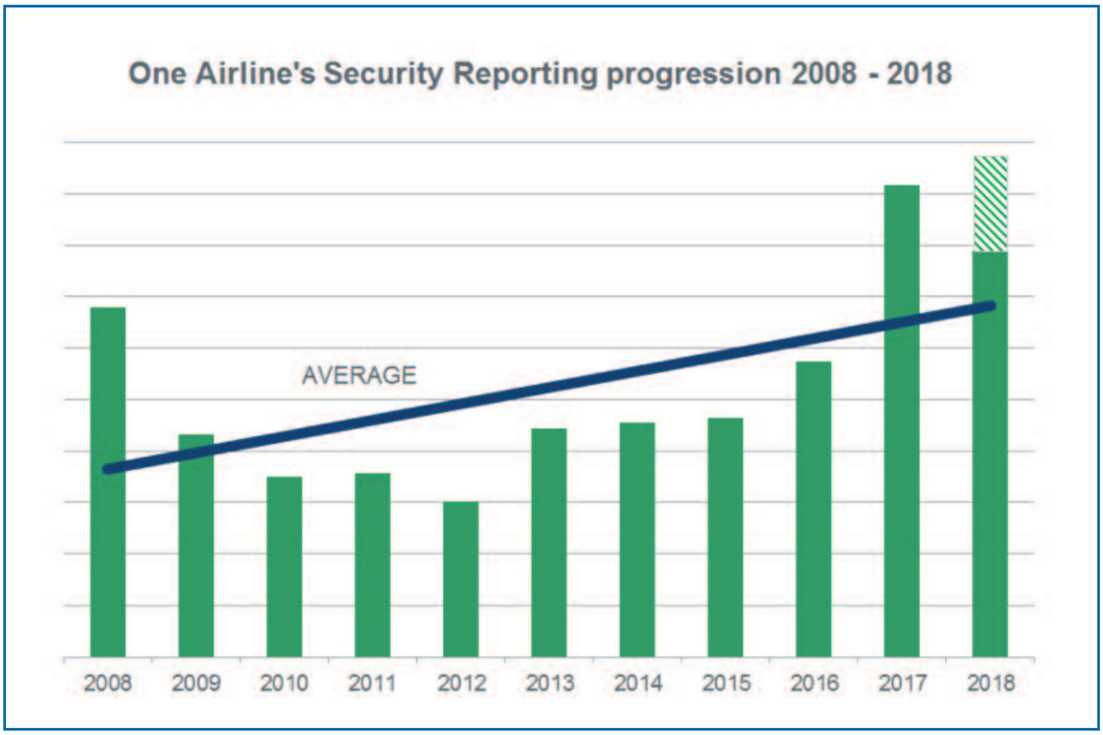
A practical example: pepper spray in cabin baggage is one of the most likely prohibited articles to be detected at a cabin baggage checkpoint in Ireland. In Ireland, it is illegal to carry pepper spray unless authorised to do so and that is limited to An Garda Síochána, the national police. So where was the pepper spray coming from? Firstly, the airports were reporting that these items had been detected. The reports indicated that we had a trend: pepper spray. Once the trend was identified we could act and the airport operators started to examine where the pepper spray was coming from. In all cases to date, the source was inbound – these were passengers travelling to Ireland from States where it is legal to carry such items. With this evidence, communication with passengers can be targeted to ensure that passengers are aware that this material cannot travel in cabin baggage.

A similar trend was identified with gas canisters in hold baggage. While in aviation circles this can be considered dangerous goods for transport by air, we do not discriminate. If the report comes in and a trend is identified, action is taken to address the trend. In this case it was largely passengers travelling to Eastern Europe, information which helps the air carriers in their communications with passengers.

ECAC's mission to foster harmonisation is not the same as standardisation. Systems have slight differences, and in this case, differences help strengthen the system overall. That said, we can only make such statements if we have the evidence to support it.

Has Ireland got it right?

The evidence would suggest we are on the right path, albeit work is needed to progress. The increased



reporting is delivering security intelligence about system performance and effectiveness. It is informing the National Civil Aviation Security Committee about the issues that are identified daily within the aviation regime in Ireland. It is improving procurement planning at airports, communications with passengers and embedding evidence-based decision-making in performance-based regulation. The reports are used to enhance training through everyday examples of security successes and failures.

So did we answer the questions we had asked at the start of this article? For three of them, the answer is yes. We are still working on the fourth. We are also still working on safeguarding the reporting system with provision for just culture being made in the National Programme this year. More reports are needed as we have inconsistency with the level of reporting, not explained by volume or scale.

And when we have this information, where do we share it? Is our experience the same as others? Are there trends that will only appear when we put our collective reports together? And where will that happen? Is there an international forum that can enable and coordinate a reporting process with all the requisite safeguards that are needed?

Maybe the key question is whether we are collectively ready for this. ■

Eleanor Travers is Aviation Security Manager at the Irish Aviation Authority, the State organisation charged with responsibility for oversight of aviation security compliance in Ireland. She is the deputy chair of ECAC's Guidance Material Task Force.

Aviation cyber security in Turkey: methodology and lessons learned from first cyber security exercise

Bekir Dursun
Cyber Security Expert,
Aviation Security Department,
Directorate General of Civil Aviation, Turkey

Serdar Karabulut
Head of Aviation Security Department,
Directorate General of Civil Aviation, Turkey

This article summarises the cyber security structure in Turkey and the methodology, scope and results of the first cyber security exercise conducted in the aviation sector. The main purpose of this exercise was to determine the effectiveness of the preventive measures and the effect of a possible cyberattack on aviation entities. It also aimed to identify vulnerabilities and the level of cyber security awareness in companies, and to evaluate the capability of coping with the threats and measuring the effectiveness of reporting mechanisms.

Cyber security structure in Turkey

Information and communication technologies have become integral parts of our society and economy. In order to eliminate the cyber security risks and vulnerabilities occurring as a result of the widespread use of these technologies, States' administrative structure and governmental organisations must take technical precautions and prepare legal infrastructures to maintain their cyber security.

In Turkey, the National Cyber Security Council was established in 2012. It approved our first National Cyber Security Strategy and Action Plan in 2014 for the period 2014-2016. Within the framework of this action plan, related institutions and organisations were assigned with certain duties and responsibilities. The main objective of this action plan was to be prepared against a possible cyberattack to critical infrastructures and to ensure business continuity is not affected while recovering from the attack, with the least possible loss. Currently, a second action plan is in place, running from 2016 to 2019.

In line with the action plan, the National Computer Emergency Response Team-TRCERT was established within the structure of the Information and Communications Technologies Authority (ICTA) in 2013. The critical infrastructures in Turkey were determined as follows: finance, energy, critical governmental services, transportation, water management, electronics and communication, agriculture and food. Sectoral and Corporate Cyber Emergency Response Teams (CERT) were established in these sectors. The responsibility to act as the sectoral CERT for the aviation sector, as one of the subsectors of transportation, was given to the Turkish Directorate General of Civil Aviation (DGCA) as the regulatory and supervisory authority.

Although the common basis and general layout of the cyber framework in critical infrastructures are defined by the National Action Plan, Sectoral CERTs are still responsible for regulating the sector-specific measures. On 31 December 2015, the Turkish DGCA issued a cyber security regulation consisting of aviation-specific measures, organisation requirements, internal quality control, cyber security culture and training requirements. Airlines, airport operators, terminal operators, ground services, air navigation service providers (ANSPs) and maintenance and repair organisations (MROs) are covered by our cyber security regulations.

To be proactive with regard to cyber security risks, aviation entities in Turkey are mainly responsible for:

- establishing and managing Corporate CERT,
- handling incident response management and coordination,
- performing continuous system testing and inspection,
- establishing a cyber security culture,
- establishing cyber security risk assessment and mitigation processes,
- performing log management,
- gathering cyber security intelligence related to their operations and business reputation,
- establishing a disaster recovery centre for critical systems.

Routine inspections of these entities are performed to monitor compliance with the DGCA requirements. Inspections indicate that significant progress has been made since the start of the initiative and most of the entities comply with the requirements. Furthermore, each entity is required to perform its own penetration tests through State-accredited private/public sector partners.

Aviation cyber security in Turkey: methodology and lessons learned from first cyber security exercise

Cyber security exercise

According to our National Cyber Security Strategy and Action Plan, each Sectoral CERT has to conduct a cyber security exercise for their sector. For that reason, the Turkish DGCA conducted a cyber security exercise for the aviation sector entities in Turkey, which took approximately four months to complete.

AIM AND SCOPE OF THE CYBER SECURITY EXERCISE

The main purpose of this exercise was to determine how effective the preventive measures were and the effect of a possible cyberattack on aviation entities, and to identify vulnerabilities and the cyber security awareness level of companies and their employees. It also aimed to evaluate the capability of coping with cyber security threats and of measuring the effectiveness of reporting mechanisms.

The aviation sector has a very complex structure with various interoperable systems. Considering the complexity and number of players, the scope of the exercise was kept to a limited selective sample from four main areas based on types of operations:

- Commercial air transport operators including all-cargo (35% of the companies that cover 80% of total operation)
- Airport and terminal operators (30% of the companies that cover 75% of total operation)
- Ground handling companies (66% of the companies that cover 60% of total operation)
- Air navigation service provider (100%).

METHODOLOGY OF THE EXERCISE

The following methods were used in the exercise.

Blackbox/greybox penetration tests on operational systems and IT systems: the objective of these tests was to assess the adequacy of the protection systems/methods used and to evaluate whether these systems were operational at optimum efficiency. In this phase of the exercise, sector-related and commonly used information systems were targeted, and various types of test were performed, as follows:

- Cyber intelligence gathering on targeted aviation entities.
- Attacks generated based on information and media reports from previous cyberattacks and gathered information.
- Website defacements such as installing exploit kits in target entity websites/systems in order to spread malicious content that could potentially damage the reputation of the targeted company.
- Attempts to exfiltrate sensitive information.
- Attacks on critical systems and testing national cooperation and escalation procedures.

@http://www.enisa.com

Social engineering tests on employees: studies conducted by the main cyber security service providers and hardware manufacturers show that the weakest link in cyber defence is the employee. Raising staff awareness levels is key to maintaining strength. For that reason, one of the test's main objectives was to assess the cyber security awareness level of aviation personnel by conducting social engineering attacks on randomly selected employees. These attacks, inter alia, included:

- **Phishing emails:** emails with aviation-related content that attempted to collect or transmit data or deceive staff into committing a harmful act.
- **Phone calls:** members of staff were called on the phone by people using fake identities and positions trying to get sensitive information or to deceive them into committing a harmful act.

"Denial of Service" tests on critical infrastructures: the objective of these tests was to evaluate the quality of precautions against a possible "distributed denial of service" (DDoS) attack on critical aviation services to make them unavailable by overwhelming them with traffic from multiple sources.

RESULTS AND LESSONS LEARNED FROM THE CYBER SECURITY EXERCISE

Common findings in this exercise were:

1) Blackbox/greybox penetration tests showed that the configuration quality of the cyber security systems at the companies tested, such as firewalls, log management tools, intrusion detection and prevention systems, needed to be improved to deal with these types of attacks.

Lessons learned: Corporate CERTs and their employees had not reached satisfactory maturity level yet. In order to strengthen the systems and configurations against such attacks, the training requirements for Corporate CERTs were increased by requiring globally recognised cyber security certificates.

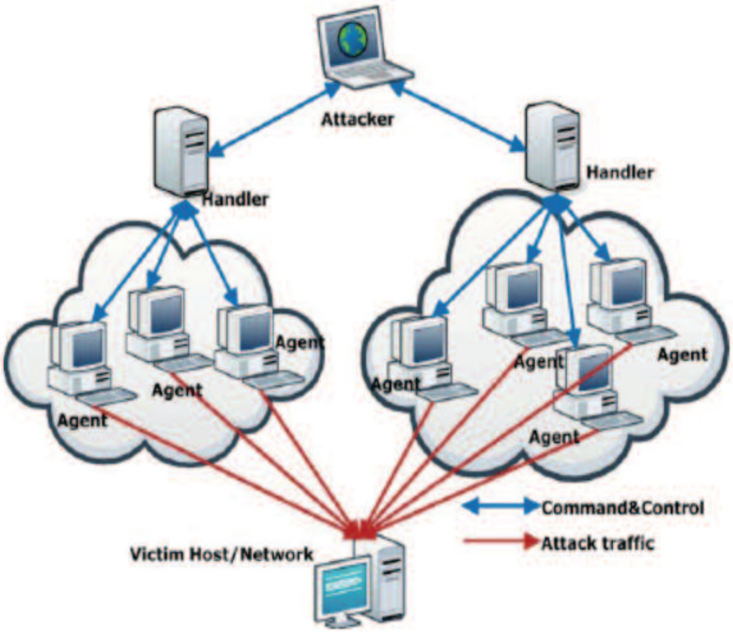
2) In social engineering test results:

- The phishing mail and phone-phishing failure rate amongst participants in aviation entities was over the accepted threshold.

Lessons learned: Although there are international and national training requirements to raise staff's cyber security awareness levels, the effectiveness of the training needs to be increased to reach a satisfactory level according to our standards. In order to enhance cyber security culture among aviation entities and ensure a high level of staff awareness, the training content requirements were reviewed and mandatory cyber security training requirements were increased significantly. Entities were also required to carry out quarterly cyber security awareness testing among their employees.

3) DoS/DDoS tests on many participating companies were not satisfactory.

Lessons learned: Companies rely on the configurations designed by ISPs. The same vulnerabilities were identified at multiple companies using only predefined ISP configurations. To rectify this commonly shared probable vulnerability, a requirement was introduced into Turkish regulation for Dos/DDoS tests on critical systems to be carried out by accredited companies.



@https://www.researchgate.net

Conclusion

As the common use of information technologies in the aviation sector is increasing in all areas of aviation, cyber threats and consequently concerns about the effectiveness of counter measures are increasing in parallel. This applies not only to IT systems but also to operational systems used in aviation.

At the Turkish DGCA, we strongly believe that aviation entities can only protect themselves by collaborating against the ever-growing cyber threat. For that reason, civil aviation authorities in general, and ECAC and ICAO in particular, should rapidly modify existing regulations to encourage international cyber security collaboration among related entities in order to create a solid cyber security framework.

Finally, we would like to thank the stakeholders who joined and supported this first national-level aviation cyber security exercise. ■

Bekir Dursun holds a computer engineering degree and a master's in business administration (MBA) from Cankaya University in Turkey. He has over five years' experience in IT/cyber security. He has been working as a Cyber Security Expert/Engineer in the Sectoral Cyber Emergency Response Team since 2015. Mr Dursun also represents the Turkish Directorate General of Civil Aviation as a member of several working groups, such as ECAC's Study Group on Cyber Security in Civil Aviation and the ICAO Secretariat Study Group on Cybersecurity's aerodromes working group.

Serdar Karabulut has served as Head of the Aviation Security Department since 2011. He is a graduate of Istanbul Technical University, Surveying Engineering Department. Mr Karabulut joined the Turkish Directorate General of Civil Aviation in 2002 where he began his aviation career. He was appointed Director of Security Assessment in 2006. Mr Karabulut has acted as the national coordinator in ICAO and ECAC audits. In 2007, he was certified as an ECAC AVSEC auditor and in 2015 as an ICAO auditor. Mr Karabulut has participated in many airport audits on behalf of ECAC and ICAO both as a team member and as a team leader. He is a member of the National Civil Aviation Security Committee and Border Integration and Management Board. In this role, he oversees the national AVSEC audits and oversight systems, running the screener and instructor certification project, developing regulations in various aspects of aviation security and maintaining the national aviation security programme, and running the Towards One-Stop Security project with ECAC.

Security culture: a personal view and some lessons learned

Yves Mabbe
Corporate Security Director, Cargolux Airlines International

***"Security culture"*: two words used regularly in numerous forums, conferences and symposiums… and often cited as "the most effective way to mitigate the insider threat". Some find these statements "trendy", others do believe there is some truth in this concept. I think I put myself in the second category, despite my usual scepticism.**

Introduction

Allow me to lay down some prerequisites before we get into the core of this paper, just to set up the right mindset. If you are an authority, please understand that you cannot regulate a culture. I know this is a natural tendency but, in this case, you should not even think about it. If you are from an association, please understand that you cannot (or should not) make money of it. Another tendency that should be left aside here. Once this is clear in your mind, we may start the discussions. Oh, and I forgot another essential point that is relevant for any security discussion: out with the politics and in with common sense. In a nutshell, switch the "collaborative and constructive mode" on, thank you.

Culture is often associated with communities. Each community has values, histories, traditions, pillars. Well, the good news is that, in terms of security, we – the authorities and industry – are a community, as we are all fighting in the same corner against the same enemies. We also have the same history, unfortunately built on all the accidents and incidents that have shaped our regulations and somewhere along the line our behaviour as heads of security. So, as a community, we should have a common culture and build it, expand it, promote it together. At the same time, however, we need to recognise that there are differences between the regions of the world. We may have the same need for a security culture but we may have different concerns.

I am very lucky and honoured to have moderated two workshops on security culture. One held in Paris proposed by ECAC in 2016, and one in Nairobi early this year in the framework of the EU-ECAC CASE Project. The first was attended by the same proportion of industry and authority representatives. The second was essentially attended by authority representatives. Both, however, were a success simply because all the participants were operationally driven experts with common goals: to improve security in our countries and in our companies. I was fortunate to have been able to observe the challenges and the differences between the two workshops. In Nairobi, the workshop focused on the basic hurdles we have to overcome to initiate a security culture. In Paris, the focus was on the tools and initiatives we need to take and develop in a collaborative way.

If you want to promote a security culture, there is one fundamental, essential and unavoidable element to respect: top-level management (or political representative) MUST actively support the programme. You cannot develop a security culture if your leaders are considered exempt from your security processes. I recall a representative at a recent workshop who asked me what to do when a highly ranked (or believed so) representative, at a screening point, shouted *"Do you know who I am?"*… The only answer I could think of was to *"tell him that you know him and that you see him as a leading figure who inspires others, and therefore you are sure he will set an example for others on how to behave at a screening point".* This is clearly why leaders should always agree to pave the way for your future culture at the earliest stage of the programme deployment.

During the ECAC workshop in Paris, there was a lot of discussion on the key elements of a security culture programme. Some of the group exercises, which mixed authority and industry representatives, produced an astonishing amount of common sense. Allow me to share the points we raised.

Basic principles of security culture

- Because of the nature, location and cultural differences, there are no 'one-fits-all' solutions.
- We need to move from a purely regulatory tradition (usually linked to sanctions) to guidance provided by regulators after consultation with the stakeholders. The system must be based on **TRUST** between partners.
- A legal framework is needed but it should remain at conceptual level. Security culture must be

adaptive to context: **REALISTIC**. Keep in mind that the culture may be different in two airports/ regions within the same country.

- There are a lot of synergies between safety and security. Security culture could be inspired by the safety culture developed some years ago and which is now in a more mature state.
- All participants recognised that (as for safety) changes to culture take a lot of time. A robust security culture cannot be achieved in several weeks or months.
- Culture must be focused on the human element. Educating staff/ people is the essence.
- Development of an efficient security culture can only take place if all the relevant stakeholders are involved (depending on the level you want to achieve: company, airport, national…). At national level, it should include civil aviation authorities, airports, airlines, subcontractors (handlers, caterers, suppliers, security companies…) and air traffic management. It is a **JOINT** effort.
- An entity that wants to develop a security culture must be ready to share incidents and lessons learned, to change its policies or processes if required, and to increase transparency towards other stakeholders so that each of them can learn from the other's experiences (incidents should NOT be perceived as mistakes or faults).
- There should be a secure platform where security stakeholders can share the lessons learned as well as ideas, performance (good or bad), and even security information for awareness purpose.
- Because of inter-dependencies between all stakeholders, security culture can only work efficiently if it reaches a **GLOBAL** level. If only one stakeholder develops a security culture and none of its subcontractors or partners do so, the impact of messages and improvements will clearly be reduced.

Key elements of security culture

- Security culture can only begin if there is a clear and **SINCERE BUY-IN** from management. Management should have a clear **VISION** and clear commitment. This is a critical prerequisite.
- Security culture could simply start by identifying paths for security improvements by analysing the situation and identifying gaps or inefficiencies.
- Training is only a starting point; security culture requires regular or even daily awareness.
- **JUST CULTURE** is essential. Employees should not be blamed for every mistake but only for those arising from willful misconduct or negligence. Rewarding good behaviour should be promoted but without leading to competition, certainly between companies (competition usually leads to a reduction in transparency, with inefficiencies being hidden to artificially maintain track records).
- Security culture should include a monitoring element to confirm the positive impact of newly introduced elements.
- Security culture should not be nebulous or use fancy but incomprehensible statements. It must be simple and accessible to ALL, from management to staff. To illustrate, you could refer to the successful *"If you see something, say something"* security campaigns.
- Employees should be **EMPOWERED**. They should be given the possibility to decide between 'act' or 'report' when confronted with an abnormal situation (raising a potential security risk). If they believe they could do something to resolve the security situation faced, they should be able to act. If not, they should know how and to whom they should report the situation. They should never leave the abnormal security situation unaddressed or the security question unanswered.
- The national regulatory entity should be the body coordinating security culture initiatives at national level and should act as a guide (NOT as a regulator).
- Security culture cannot be deployed properly if **EFFICIENT COMMUNICATION** is not deployed (employees should know who to

© estherpoon - Fotolia.com

contact, stakeholders should have defined communication channels, and management should clearly communicate on security culture elements…).

- A reporting system is essential. It should include elements like anonymous/confidential reporting, such as exist for whistleblowers or even safety reporting systems.
- ANY report from an employee (or stakeholder) relating to security should be responded to twice. First, an IMMEDIATE 'thank you', and secondly, after investigation/action, ALWAYS go back to the reporter with **FEEDBACK** (within confidentiality/sensitivity limits).

© rdnzl - Fotolia.com

Measurements

Security culture should include a number of key performance indicators. They may vary based on stakeholder nature, culture, etc.

- A possible option could be to measure **EFFICIENCY LEVELS**, especially on a specific process (for example, the number of security tests passed/failed before and after a change in the security culture).
- As for safety culture, security culture should involve a clear reporting system and – also as for the safety culture – a key indicator could be the number of reports raised.
- As security culture in aviation also aims to efficiently increase passenger protection, passenger surveys could be a tool to measure the efficiency of the security culture (similar to a 'Felt Safe?' survey performed amongst users): organise **SATISFACTION** surveys.
- Other surveys/questionnaires could also be used in case of non-compliance with a procedure, such as checking with the concerned employee when he received his last security instruction, feedback or briefing… (or in other words: when was he confronted with one of your security culture initiatives).
- A possible key measurement could be **SELF-PROMOTION**. Is security culture amongst employees improving without any input from management or security teams? – i.e. do staff members speak about security or security improvements without being prompted to do so by management? Does the system work without external supervision?

I remember that the United States representative who participated in our Paris workshop was able to demonstrate the efficiency of basic security training on the identification of 'abnormality' and how to react/report it, given to airport cleaning staff. The efficiency of the training was established when they received the statistics on the number of criminality-related incidents at the trial airport – they had drastically reduced.

End note

So, after handing out all these tips and advice, what about me? Am I able to develop a robust security culture in my *own* company? Well, I must admit this is certainly a daily challenge. But when, in the same week, on the one hand my CEO complains that he was not *"screened to the adequate standards at a screening point and that I should address this issue with the subcontractor because it is not normal"*, and, on the other hand, the cleaning lady informs me that the previous night she *"found my office open and immediately asked a security guard to come and lock the door because it was not normal"*, then I think we may be on the right track, as the entire staff spectrum **does** know what is 'not normal' in security terms and **does** know how to address the concerns. Maybe a security culture starts then… with a little bit of education.

Wishing you all safe and secure skies. ■

Yves Mabbe began his career in aviation 30 years ago and has spent more than half of them in managerial positions. Most of this time has been in flight operations but he has also covered other areas such as quality control, diplomatic and regulatory affairs. He finally joined the aviation security community in 2007. He worked for air traffic control, then passenger, express and now cargo airlines. For several years, he actively represented the express industry in ICAO, Asian, United States and EU AVSEC regulatory forums and meetings. He is a member of A4E's Safety and Security Committee and IATA's Cargo Security Working Group and Cargo Border Management Board. He is one of the longest-serving members of the ECAC Guidance Material Task Force (since 2009) and has participated in ECAC workshops on explosive detection dogs, RNBC, security culture and cargo screening.

Implementing a security culture? A practical approach

Andrew Murray
Security Regulation Manager, Gatwick Airport

Writing an article about the practical steps we have taken at Gatwick Airport to build our security culture was never going to be easy. Arguably, it could be said that we didn't seek to follow a structured programme of activity to systemically build a culture, principally because a culture cannot be built. Instead it has to be nurtured and encouraged by providing the correct environment from which it can grow. Then comes the question of how you measure or assess its development. One strong indicator of our security culture at Gatwick lies within the following story.

From day one, the cleaning supervisor noticed Tim as being friendly, easy going and really keen to get on with the job. In fact, it wasn't until the end of the first week that he realised the level of Tim's keenness. His unbridled enthusiasm included his desire to always volunteer for any aircraft cleaning duty rather than other jobs in and around the airport, air bridges or stands. Tim was always first on board to clean, after the flight deck and cabin crew had deplanned, eagerly getting on with the prepping of both first and business class cabins. Cleaning the flight deck was the least popular job as ground engineers often had a moan at operatives that got in their way or inadvertently touched the controls. But Tim never seemed fazed and often accessed the flight deck as soon as he could.

Tim's supervisor had managed many cleaning crews before and knew that operatives came from all walks of life with a huge range of diverse backgrounds, life experiences and interests. But he had a gut feel about Tim that something wasn't quite right. Tim's passion for photography wasn't known until he started talking about it in the crew room, nothing unusual about that hobby, thought the supervisor, until he was tasked to work with him, covering the first wave of turnarounds that included both short and long-haul aircraft.

Being questioned by the airport security duty manager wasn't something the supervisor expected in a normal working day – but having caught Tim taking pictures of a number of aircraft flight decks led him to follow his gut instinct, fuelled by his general security awareness training, and make a call to the airport security team. The supervisor's worst fears of some type of hostile reconnaissance appeared to be warranted as, after various checks with the police and counter terrorism border policing teams, steps were taken to redeploy Tim to a less sensitive non-airport cleaning operation.

Ah... I hear you say, did this really happen? Absolutely, the only details that have been changed is the name of the individual concerned. Why did the supervisor make that call to the security team? It's a good question, and part of the answer is because he, like all pass holders at Gatwick, is required to complete an online generic security awareness course. This enables all pass holders to understand the security sensitivities of working at an airport that is part of the United Kingdom's critical national infrastructure.

Community engagement

Our culture drives us to target the wider airport community, which we call the "Gatwick Family", with key security communications. As an early hook-in to encourage our community to think security, we have produced a hard copy document that recognises that not everyone has easy access to the internet via a smartphone. This means that a range of contractors, cleaners, in-flight caterers and many other staff can receive a basic security message that sets out some fundamental principles, such as how to report an unattended bag, or suspicious activity, together with guidance on maintaining ac-

Welcome to Gatwick Airport

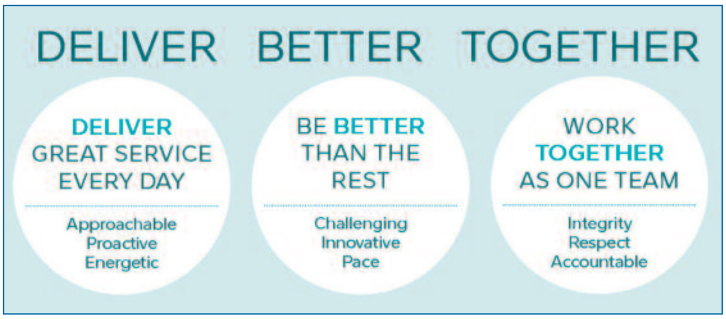
Everything you need to know about working here

YOUR LONDON AIRPORT Gatwick

cess control, protecting against tailgating and even information on how to prepare for security when presenting themselves to staff search.

We don't believe there is a one-solution-fits-all-airports approach to developing and defining a good security culture. It is certainly not formulaic; rather a series of on-going actions, activities and behaviours that continually seek to remind all staff at all levels of the need to think security.

Balancing security compliance against cutting queues whilst ensuring the highest levels of customer service is no easy task. With new threats, technology, fluctuating budgets, processes and people – nothing endures but change. Yet we aviation security entities are committed to embedding a stable, consistent, reliable security culture. Be warned, if you don't like a challenge you are possibly in the wrong job. Luckily at Gatwick, we are values-led and performance-driven. This means that we are passionately committed to delivering a security product that protects our customers, staff and stakeholders. This in turn has promulgated our security culture, because in order for us to deliver effective security people need to know not only what to do but why they are doing it. We do this by ensuring that every single employee across all aspects of our security operation has a clear set of objectives that can be measured, tracked and delivered. This has empowered our teams and created some healthy competition in their performance. Whether it is customer feedback or covert test results, we love to track and trend data and use it to drive improvements as we compete to grow as a leading provider of airport aviation security.



DELIVER BETTER TOGETHER

DELIVER GREAT SERVICE EVERY DAY
Approachable
Proactive
Energetic

BE BETTER THAN THE REST
Challenging
Innovative
Pace

WORK TOGETHER AS ONE TEAM
Integrity
Respect
Accountable

Define your values

Integrity, respect and accountability are just three of our core values that form part of our Gatwick DNA. These values are evidenced through our behaviours in and around the business, which form some fundamental foundations that contribute to our security culture.

We believe passionately in maintaining our values and will actively encourage all staff to display the behaviours that evidence them. Provided it is done professionally and constructively, we will call out those colleagues who don't adhere to our values of delivering better together. But much more importantly we continually seek out ways to communicate and engage all our people, with particular emphasis on the need to continually drive the security message. This means seeking out and engaging on many different media channels and avenues, but what works particularly well is what we call "Heads Up". It is certainly not rocket science; the management team simply takes time out to arrange a small gathering of front-line staff from across the business at various operational and non-operational locations to talk about key issues that support and promote our security culture. Whether it is changes in security regulations, process, threat level or topics of discussion that help evidence what good looks like – it is all part of the way we do security.

Recognition

One of the most enjoyable aspects to our Heads Up sessions is the opportunity to reward and recognise those within our organisation who either go the extra mile or indeed, consistently and quietly deliver a professional security service to our passengers and staff.

It is a real opportunity to pick out those individuals at Gatwick who can sometimes go unnoticed as they just get on and do a great job without any noise or show-boating. We love it, because a simple thank you can go a long way in keeping people motivated in a role that can be incredibly demanding.

Lead by example – transmit but also receive

It is important to lead by example when it comes to security culture. Taking the opportunity to display good security leadership at every level throughout the organisation is a must. At Gatwick, we will often open a meeting, even if it is not a security meeting, with a security and safety "moment". This is nothing more complex than taking a few minutes to highlight good security practice or awareness of a particular incident and the learnings that can be taken from it. Security cultural leadership is also about "behavioural "leadership. At Gatwick, all managers are actively encouraged to be seen and engage with front-line security staff. We take a dim view of security managers who are not known because they don't engage with security officers. It is a delicate balance; with such a large workforce, it is likely that not all the staff will know all the managers. But at the very least we expect operational managers to make themselves known to security staff at every opportunity. We often use the word "walkabout"; this is not a reference to an Australian outback sabbatical! Instead it is a term that describes our approach to getting out into the operation to either witness a process, location or engage staff, rather than disappear into a meeting room and make isolated decisions. As security leaders within our business, we also seek to influence the security behaviours of all our stakeholders, contractors and even visitors, with appropriately targeted face-to-face communication to offer friendly guidance on a range of security practices, from ensuring IDs are displayed correctly, temporary pass holders are adequately escorted, the risk of tailgating is mitigated, or even politely checking and challenging individuals whose behaviour raises suspicion. Linked very closely to driving our security culture is our ability to listen to our security officers. It is a cliché but communication is always a challenge in any large organisation. We devote a huge amount of effort to continually review our current processes to ensure we are capturing the views of all staff. We conduct regular "voice of the employee" surveys to help us identify areas of our security operation that could be improved; whether that's uniforms, rest rooms, briefings or rosters – we are always willing to listen to better understand whether things can be done differently. We respect and understand the diversity and hands-on experience of our workforce and are keen to capture any great ideas from within, hence we launched our "ACES" (Any Clever Exciting Suggestions) initiative. Examples of successful ACES ideas that have been designed and delivered include changing some low-level solid panels to segregate passengers after the walk-through-metal detector to transparent panels to enable parents and children to keep sight of each other, strategically placed mirrors that enable team leaders to keep sight of any building queues in staff search areas, through to designing small plastic collars that have been placed around some of our emergency stop buttons on cabin baggage screening roller beds in order to reduce accidental emergency activation. All of these ideas and actions came from our front-line operatives.

Stakeholder buy-in

The United Kingdom government requires all airports to operate a Security Executive Group (SEG) and a Risk Advisory Group (RAG) together with the Airport Security Committee. This may appear bureaucratic, however the principal objective is to ensure that all the airports manage their key security risks (both current and emerging) by regularly reviewing, discussing, challenging and updating their risk registers. Gatwick's approach to risk management is further enhanced by ensuring we continuously build and maintain our professional working relationships with all our key security stakeholders. We do this by taking every opportunity to "reach out" to encourage open and honest de-

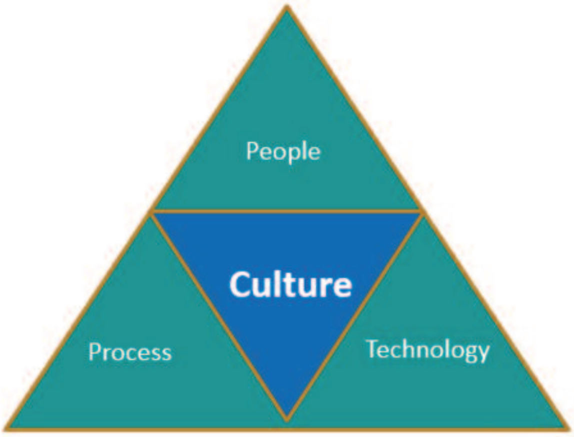
PROJECT SERVATOR
My job is to help keep you safe.
I am friendly but I also work hard, searching for things that could put others in danger.
Together, we've got it covered
If you see something suspicious
Call 101
In an emergency always call 999
SUSSEX POLICE
YOUR LONDON AIRPORT Gatwick

© Gorodenkoff - Fotolia.com

bate. This could mean either grabbing a quick coffee with a senior official from any of the control authorities or even just making a quick assurance call regardless of operational peaks or troughs. By doing this we start to break down barriers and build a truly open and honest style of multiagency threat and risk management. At Gatwick, we pride ourselves on a relaxed but delivery-focused approach to security leadership. We love to leave rank and status at the door such that we can constructively and appropriately challenge the status quo. This leads to a succinct and sensible approach to developing our risk register. The SEG enables our CEO and COO to evaluate and assess the work of the RAG, who in turn, may seek buy-in from the top in order to, perhaps, seek funds to trial, build or design processes that will strengthen our portfolio of security risk mitigations. The RAG also enable key security stakeholders to gain assurance that security of the airport is being effectively managed, whether that's by conducting a quick wash up of a previous incident or whether its understanding that all security aspects have been and are being considered as part of a new landside constructive project. In summary, the RAG process helps build and develop the highest levels of security leadership by working collaboratively with all airport security stakeholders in creating a secure forum for open and honest dialogue.

I'm sure Gatwick is no different to many "modern" operations, as intrinsically linked to our overall way of doing business is our fairly informal way of communicating. In others words, we don't stand on ceremony and in fact dislike bureaucracy and red tape. In contrast, we fully endorse good old-fashioned face-to-face conversation that leads to operational delivery. If that means hunting someone down to get things done then, so be it. Of course, calendar management is key – making time to engage those that make things happen in our business is critically important. Actively managing the message means doing the groundwork to get people onside even before the official meeting. This means selling the concept of security and getting buy-in prior to the formal approval process. It is not about bypassing governance, it's simply about educating and warming up the audience prior to the show! This could simply mean a quick word with the COO, business leader, project sponsor or project manager will pay dividends in getting a security process or project delivered that will further enhance the overall security culture.

People, process and technology together form the key components of a security culture. At Gatwick we have been fortunate in benefiting from a healthy capital investment programme that has enabled us to develop world-leading security processing mechanisms such as our central search security facility, remote screening rooms together with state of the art external vehicle control posts.



April 2018
Your Magazine
p6
COMMON SENSE
WE'RE OPENING BRITAIN'S FIRST AIRPORT SENSORY ROOM
p8
SLOT GAMES
THE CHALLENGE OF ALLOCATING OUR AIRLINE SLOTS
p10
FLYING HIGH
OUR NEW AIR AMBULANCE PARTNERSHIP
The 90-year-old who just loves working at Gatwick
p4
GOING STRONG
YOUR LONDON AIRPORT
Gatwick

However, even if you are fortunate in having the best security technology and processes in place, the development of your security culture will be severely hampered if you have not invested the time and energy into taking your people with you on this journey. Capturing the views of all staff, embracing diversity and providing a safe, supportive and collaborative working environment is all part of the process. Communicating and celebrating the successes of the wider airport community helps to drive this message, whether it's recognising the "going strong" efforts of older members of the ground and passenger handling agents or whether it's highlighting the attentive efforts of security officers outside of their working remits – it all counts towards building a strong security culture.

People create a culture

In many ways, the security culture at Gatwick is a by-product of our commitment to keeping people safe, delivering excellent customer services and cutting queues. Whilst components such as performance management, accountability, risk and threat management, governance, compliance and incident reporting all help to create the engine of security, it's the quality of the drivers that dictates the direction of travel. By driver, I mean people leaders, line managers and supervisors. It's a cliché but it's true, your organisation's security culture is only as good as the people within it and their ability to manage the emerging threats and risks to aviation, balanced against a backdrop of ever challenging financial and commercial challenges. ■

Andrew Murray is accountable for the delivery of Gatwick Airport's Security Compliance and Assurance programme. As Head of the Security Regulation team, reporting up to board level on all aspects of the UK's National Aviation Security Programme, he intuitively understands the challenge of defining and implementing aviation security regulations against a backdrop of ever changing commercial and operational demands. A well-developed sense of security consciousness enables him to furnish the wider airport operation with a high degree of security assurance. Mr Murray's unique extensive aviation career history, balanced against his time working for the UK government' s Department for Transport (DfT) Aviation Security Regulation and Compliance team as a senior inspector has provided him with a well-balanced, informed, pragmatic approach to leading the multiple aspects of threat, risk and compliance management. A subject matter expert in his field, he frequently represents Gatwick in both domestic and international security arenas including Department for Transport and ECAC capacity-building projects in Morocco, Ghana and Kenya.
Post 9/11 led to changes in the aviation industry where the UK government sought to identify key individuals who could offer an industry approach to compliance assurance and stakeholder engagement. As senior aviation security inspector for the DfT, Mr Murray held lead auditor responsibilities for all British Airports Authority (BAA) airports and all UK air carriers, leading a team accountable for aviation security compliance assurance together with threat & risk management.

Brussels Airport: managing the recovery after a terrorist attack

Wilfried Covent
Senior Security Expert, Brussels Airport

22 March 2016 – 07h58. Brussels Airport is hit by terrorism. Two explosions are heard during peak operations in the public terminal.

Gradually it became clear: there had been two explosions inside the terminal close to the check-in desks, inflicting significant fatalities, casualties and destruction in the landside area of the building. The nature of the explosions indicated a coordinated and planned terrorist attack. Sixteen people died and over one hundred and fifty were hurt.
Our thoughts were – and will always be – with the victims, family, friends and relatives.

The emergency operation began immediately after the attack, with one goal only: to rescue the people. Thanks to the heroic actions of the firemen, medical/security services and many volunteers from amongst staff and passengers, a quick response was organised. Professional and agile teams on-site managed the crisis. Although there had been no previous training to cope with such an event, the collaboration between all parties involved, from the crisis centre to the rescue teams on-site, was efficient, showing that the regular crisis management training and the contingency plans in place had contributed to a successful rescue operation.

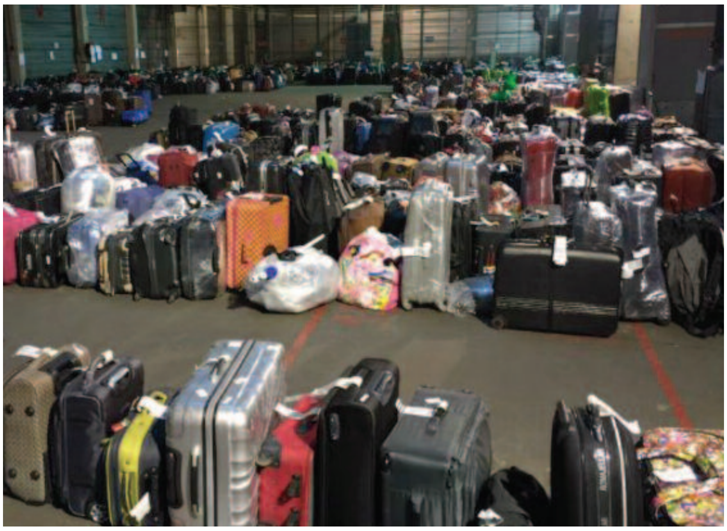
Immediately after the attack, the airport was placed on lockdown for both departures and arrivals. Over 5000 passengers were stuck in the airside part of the terminal and began to self-evacuate towards the apron. Bussing operations on the apron were organised to pick up people and bring them to a technical hangar, which was used as a temporary central assembly point. After registration, people were transported to different 'friends & relatives reception centres' in the area surrounding the airport.

Over 10 000 pieces of baggage from aircraft were left behind. Baggage belts, gates, waiting areas, shops and the departure hall were deserted. More than 6000 cars in the car park in front of the terminal were not accessible to the public. We had to handle the consequences…

On 22 March, Brussels Airport recommenced its cargo flights, and passenger flights began on 3 April. Passenger flight capacity was limited because all the check-in capacity had been destroyed. Progressively, the number of flights increased to reach 100% capacity by 2 June, in time for the summer peak beginning at the end of June.

The biggest change affecting passengers and staff after 22 March was accessibility. As a result of the new landside security standards, pre-check tents were installed to control passengers and staff before entering the terminal building. However, with the increasing number of passengers weeks after, it became clear that such a 100% static check was causing a lot of queues, affecting the smooth passenger flow and resulting in additional safety concerns.

In close cooperation with the authorities, a new landside security concept built on a multi-layered security approach was introduced. Key elements included:
- infrastructural measures (protection);



© Brussels Airport Company

© Brussels Airport Company

- technology (e.g. intelligent cameras); and
- human factor elements (e.g. behaviour detection monitoring).

This concept, based on risk management principles, with visible and less visible measures, contributed to a high level of security while optimising the efficiency and the comfort of the passengers.

Due to the new security measures, the 'kiss & fly' zone in front of the terminal is no longer available for cars. A new drop-off zone close to the terminal was created and a new parking card allowing visitors to park for free for 30 minutes in the front parking area, less than 50 metres from the terminal, was launched.

The story of the recovery is a story where people made the difference.

Based on team work and empowerment, including extensive stakeholder management, we were able to manage the crisis. With one common goal in mind – creating and spreading a new positive vision – we made the right decisions even under pressure, working in a decentralised, rapid and efficient way and creating agile teams able to 'think outside of the box'.

And communication was key. Both internal and external communication, as well as information management, were essential for a successful recovery. The huge media attention also required professional spokesmanship and extensive conversation management on social media.

We also emphasised the importance of taking care of our people: the airport community. From the beginning, it was clear that this was not going to be a sprint but a marathon. A lot of people showed signs of trauma. From the first day we took a combination of collective and individual initiatives – psychological support - and we still do!

Brussels Airport will never be the same following 22 March 2016. But we are back, and stronger than ever!

Security is clearly embedded in our vision and supported by an ambitious investment programme. We strongly believe it is possible to combine better security with better customer experience. But 'zero risk' does not exist, and there will always be a part of unpredictability. All public spaces are a possible target for terrorist attacks. Good coordination with the public authorities is therefore crucial, as well as assigning clear roles and responsibilities.

All security measures taken in the landside area should be the result of continuous security risk assessment based on local threats and defined in real time. A 'one-size fits-all' solution does not exist. This approach is supported by most stakeholders, including ICAO and the European Commission.

The security approach must be proportionate to the threat airports face, and must continue to deliver open, accessible and expedient air transport services to the travelling public. ■

Wilfried Covent has a rich career spanning almost all the key organisations in the aviation security industry, including the police, airlines and cargo, and he is currently Brussels Airport's Senior Security Expert. At the beginning of his career, Mr Covent was Police Commissioner with the local police in Belgium. In 1994, he became involved in the aviation security industry. He first joined the (previous) Belgian Airline SABENA as the airline's Security Manager. A few years later he switched to the air cargo/express industry to become Aviation Security Manager for DHL Express Europe. In February 2010, Mr Covent started to work in the airport environment as Head of Security at Brussels Airport. Recently he moved to a Senior Security Expert function within Brussels Airport. In this function, he has been appointed as Chairman of the ACI EUROPE Security Committee (Airports Council International – representing +/- 500 airports in Europe).

Making an impact through capacity development

Dan Micklethwaite
Director General of Civil Aviation, United Kingdom

As United Kingdom Director General of Civil Aviation, I deal with the full range of issues impacting on civil aviation, but security will always be top priority. The successful and disrupted attacks of the past few years are a reminder that aviation remains an attractive target for terrorists.

We need to redouble our efforts to get ahead of the threat, and in the United Kingdom we are doing this through our new **Aviation Security Strategy.** Our strategy sets out a new proactive approach across six core themes:

- **Confident** – understanding risks to improve our collective confidence in the security of the aviation system.
- **Comprehensive** – taking a holistic approach to disrupt and deter terrorists.
- **Concentrated** – taking a data-driven approach.
- **Collaborative** – government and industry working in partnership.
- **Cooperative** – working with international partners.
- **Capable** – building capability and security culture.

> We recognise that the terrorist threat is a global one which we need to tackle together.
> The United Kingdom remains committed to working with other States, industry and global bodies to protect aviation.

A key theme of our cooperative work focuses on the importance of **sustainable capacity building** and promoting a positive security culture, principles which feature heavily in ICAO's 2017 Global Aviation Security Plan (GASeP), which aims to increase cooperation between and within States.

Improvised Explosive Detection Kits donated by the United Kingdom government to airports overseas for use in x-ray training

Since the unanimous passing of UNSCR 2309 in 2016, the United Kingdom has spent over £10 million on our overseas capacity-development programme. We work with our international partners, including ICAO and ECAC, to improve aviation security. Our emphasis is on providing expertise, training and support covering a wide range of subject areas and threats.

Since November 2015, we have delivered over 200 training courses, enhancing the skills of over 3000 security staff at overseas airports, including screening staff, specialist operators and security managers. We are also developing more innovative training capabilities, including a series of animated training films for use by host States and computer-based training (CBT) software for x-ray screeners. To improve security, we have provided over 200 explosive trace detection machines for use by airports in priority locations and engaged with over ten host States to develop their capabilities through the United Kingdom counter-MANPADS programme, working closely with international partners to prevent duplication. We underpin our work through regional workshops, having recently hosted meetings with host States and international partners in sub-Saharan Africa and South Asia.

Most importantly, the United Kingdom capacity-development programme **seeks to deliver sustainable improvements in aviation security,** rather than just providing short-term benefits that dissipate or become out of date.

To this end, over the past three years we have more than doubled our spending on aviation security around the world, expanding our global network of aviation security liaison officers in priority locations to work with host States. Since November 2015, we have completed over 350 specialist assessments in over 25 countries covering more than 55 last points of departure (LPODs).

Our assessments consider security performance across the airport using criteria based on ICAO baseline standards, taking account of the threat and risk in each location. We use these assessments to identify potential vulnerabilities within host State aviation security capabilities, and most importantly to inform our capacity development work overseas.

Most States, of course, do not have such an extensive network and infrastructure. But we believe that many more States and organisations can participate effectively and add considerable value to our collective efforts – by creating capacity-development programmes appropriate to their resources, and cooperating across regions to maximise our common effort.

We have an opportunity in the coming year, with the **Second ICAO High-level Conference on Aviation Security (HCLAS/2)** and the 40th ICAO Assembly in 2019, to make security a strong focus of multilateral aviation work. The United Kingdom will do all it can to promote progress on the GASeP, not just through capacity-development work, but also to help boost ICAO's work on insider threat and security culture, as well as strengthening the Universal Security Audit Programme, as these provide a crucial underpinning to the improvements we all wish to see.

So as we approach the ICAO High-level Conference on Aviation Security in November, I would encourage all to give aviation security the attention it requires and to invest in sustainable capacity-building projects. This is fundamental to achieve the objectives of UNSCR 2309, and will help all States to implement the GASeP quickly and effectively. It embodies the ICAO principle of No Country Left Behind (NCLB), and we should be aiming for aviation security to become the most visible example of how we can deliver on the NCLB principle.

In doing this, it is crucial that we share a common approach to **good practice in capacity development,** so that our programmes deliver sustainable results. For any capacity-development project, large or small, to be delivered efficiently and effectively the following elements are necessary;

- **Buy-in** - successful capacity building requires the full engagement of the host State. Any proposal for assistance has to be accepted by them, and address an agreed need. It is important to appreciate the host nation's appetite for change and understand the political dynamics that might affect the delivery and success of any programme. It is also important to understand what other capacity development is being undertaken either by the host State or with support from other international partners; capacity-development efforts should be complementary to maximise impact, minimising duplication.
- **Careful scoping** – capacity-building initiatives need to be properly scoped to maximise the chances of getting the project work right and delivering new capabilities. It is difficult to get visibility of host skill levels or an understanding of the processes and practices they actually use if we have not established good relationships first. The focus needs to be on what changes we are trying to make, as skills cannot be taught in isolation. There is no value in training staff in a new skill unless they can use it in their day-to-day work. Host State stakeholders should help define their needs, so that they have ownership of the project from the start.
- **Resourcing and funding** – staff and funding must be secured at the start for the duration of a project. If an initiative is withdrawn prior to completion, this can significantly affect the confidence of participants regarding future support.

Local trainers delivering a new training programme after the United Kingdom's "train the trainer" project at the host's academy

Making an impact through capacity development

We have learned lessons on what works well and delivers sustainable and lasting improvements. Our most successful capacity-development projects have adhered to the following basic principles:

- **Start small and keep it simple**
  Capacity building could require the introduction of a change in security culture. This can seem daunting for senior staff, who may fear it will undermine their authority and also disrupt the efficiency of their organisations. We have addressed these concerns through the use of small scale pilots to prove concepts and deliver results. These allow new ways of working to be tried, tested and agreed before they are rolled out more widely. They also avoid the risk of threatening existing capabilities and practices should the concepts fail or take longer than expected to realise.
- **Think about sustainability and an exit strategy from the start**
  Capacity building is about equipping the country in question with the capability to deliver effective security. Therefore all capacity development needs to be prepared and delivered through the lens of the host State's ability to deliver measures and use new skills self-sufficiently. We have ascertained that an exit strategy, agreed with the hosts, is an important part of the programme scope. This helps to manage expectations from the outset and gives the host State time to scale up their own funding or resource.
- **Monitor and evaluate**
  All capacity-building projects should be monitored on a regular basis to ensure the project is fit for purpose, giving value for money and delivering the required impact. It is important to collect evidence of changes in performance, capability, processes and attitudes delivered by the projects as these 'outcomes' provide the confidence that the new capabilities are being used and becoming embedded. This evidence should be used to reassure all stakeholders, and the host State, that progress is being made. Monitoring and evaluation allows us to learn lessons from previous projects, and implement those lessons for the future.
- **Deconflict with partners**
  We as the international community need to complement our work, and not duplicate and conflict. We have learned that engagement with other donor states and international organisations to support each other's work and ensure they are not delivering similar projects is critical before a project gets off the ground. We have worked with ICAO to upskill aviation security inspectors in partner States and have supported ECAC's capacity-development activities through the framework of the excellent CASE Project, including the provision of expert speakers at workshops, counter MANPADs work and the development of a training DVD on air cargo security. We have also seen modern security equipment donated by the international community remaining unused by host States, either because the training has not been provided or the technical support was not available.

Successful capacity development is as much about the journey as the destination. Over the years, the United Kingdom has learned that attention to the journey of delivering capacity-building projects will determine the project's success or failure. We recognise that whilst delivering capacity projects can be very difficult, it is essential given the threats we face, and it should be incumbent on all Member States to work collectively to secure the global aviation network. ■

Training DVD on air cargo security produced jointly with ECAC through the framework of the CASE Project

Dan Micklethwaite was appointed as United Kingdom (UK) Director General for Civil Aviation (DGCA) in summer 2016. He is responsible for overall UK policy on aviation. Mr Micklethwaite previously held a number of senior positions at Her Majesty's Treasury (the UK's economics and finance ministry). During the last four years, he was the principal adviser to the Chancellor of the Exchequer on UK transport policy, and oversaw the UK national transport budget. Prior to that Mr Micklethwaite held the roles of Head of Strategy and Head of Economic Growth, also at the UK Treasury. He also spent some time working as a consultant at Deloitte earlier in his career.

The CASE approach

In his article, Dan Micklethwaite mentions the "buy-in" of the Partner State at the top of the list of the prerequisites to achieve efficiency in the implementation of aviation security capacity-building actions. This required buy-in is first and foremost political and administrative since all departments and individuals involved need to be fully committed if the action delivered for the benefit of the concerned country is to produce all the expected outcomes and also deliver sustainable results. This assessment is totally confirmed by the three years of implementation of the EU-funded and ECAC-implemented CASE Project, and it is hard to imagine a capacity-building initiative that would not rank the buy-in of Partner States as the most important factor of success, albeit not the only one.

Based on ECAC's experience in the implementation of capacity-building activities, one of the best ways to achieve this is to use experts from the region of the scope of the Project, as they are the most familiar with the needs of their region and understand best what methods and ideas are most likely to be successful.

Regional expertise and experience are as valuable as lessons learned from past activities, therefore factoring in local specificities and environments (e.g. constraints on resources, sharing of responsibilities between various entities involved in aviation security) is absolutely crucial to provide technical support in a relevant manner.

In its early stages, the CASE Project initiated this good practice by inviting regional speakers to its multilateral workshops (e.g. cargo and mail security, explosive detection dogs). By the beginning of the third year, this strategy was expanded to national operational activities. At the time of writing, the CASE Project has already benefited from the experience of experts from the following States: South Africa (for an activity in Namibia), Kenya (for two activities in Ghana), Benin, Cameroon and Niger (all three for two sub-regional activities in Côte d'Ivoire which involved experts from the Democratic Republic of the Congo and the Republic of the Congo in addition to the representatives of the host State).

Meanwhile, several good practices have been adopted by the Project to ensure an efficient implementation of activities which are delivered partly by regional experts. These good practices ensure consistency with those delivered exclusively by experts from ECAC and ECAC Member States. They are designed to provide the same standards of quality for the beneficiary Partner States, as initially African or Arabian experts cannot be already familiar with ECAC methodology and tools in training and coaching. For example, a good practice applying to the management of regional experts is that they have been, so far, systematically teamed up with an expert from the CASE Project team. This does facilitate the familiarisation with ECAC procedures and training materials. Another example is that the performance of the expert from a Partner State is assessed after the mission by his/her senior teammate from ECAC, using exactly the same evaluation criteria as the ones used to evaluate experts released by ECAC Member States. This does contribute to a have a common pool of experts that perform to the same standards.

As this trend is to continue, the next major step would be to rely on the skills of regional experts for activities other than training. In the months to come, ECAC will extend further its cooperation with regional experts, starting with secondments of regional experts to the Project team.

The European Union-funded CASE Project delivers capacity-building activities in the field of civil aviation security in Africa and the Arabian Peninsula. ECAC is in charge of its implementation over the course of four years (November 2015-October 2019). ■

More information on the CASE Project :
https://www.ecac-ceac.org/ec-ecac-case-project

Antoine Zannotti
CASE Project Coordinator

ICAO second High-level Conference on Aviation Security: topics and goals

Sylvain Lefoyer
Deputy Director, Aviation Security and Facilitation,
Air Transport Bureau, ICAO

In November 2018, the International Civil Aviation Organization (ICAO) will convene its second High-level Conference on Aviation Security (HLCAS/2), bringing together senior government officials from around the world to engage in important discussions on countering threats to civil aviation.

In the six years since the last High-level Conference on Aviation Security, numerous aviation security initiatives have been undertaken, leading to significant accomplishments. These range from the passage of high-level legal instruments to the concrete application of appropriate countermeasures at airport checkpoints. The unanimous adoption of United Nations Security Council Resolution 2309 (2016) in September 2016 and the ICAO Council's approval of the Global Aviation Security Plan (GASeP) in November 2017 demonstrated States' commitment to ensuring aviation security around the globe. During this HLCAS/2, Resolution 2309 (2016) and the GASeP will feature prominently in the discussion.

The HLCAS/2 will be the culmination of AVSEC Week – five days dedicated to understanding the current state and future of aviation security, and exploring avenues for effective improvement. The first day of this week will focus on industry engagement and will comprise multiple tranches of workshops, SkyTalks, and facilitated debates. The second ICAO Global Aviation Security Seminar (AVSEC2018), open to government officials, industry and other stakeholders, will take place the following two days. During interactive sessions through AVSEC2018, participants will explore the complicated issues surrounding aviation security information-sharing.

HLCAS/2 participants will then discuss and produce recommendations on policy issues and a framework for aviation security, as well as related actions by States, industry and ICAO. Key topics addressed during the HLCAS/2 will include current risks and threats to aviation, new approaches for managing these risks, the status of the GASeP, achieving synergies with other areas in aviation, and ensuring sustainability of aviation security measures. Through the advanced submission of working papers, Member States and selected organisations and associations will be able to seek specific actions related to these topics. Interpretation and translation will be provided in six ICAO languages.

Aviation security threat and risk context

Following the first HLCAS in 2012, the ICAO Global Risk Context Statement (RCS) was developed. Now published as ICAO Doc 10108 (Restricted), this document is updated annually using evidence-based risk assessments, and includes possible mitigating actions that States may implement in their risk-based security programmes. The RCS acknowledges that risks vary from region to region, but the interconnectedness of aviation requires that all States remain aware of current threats and adapt their countermeasures accordingly.

The current threats facing civil aviation are continuously evolving. Concealment methods for improvised explosive devices (IEDs) have become more creative and concealed items harder to detect. Chemical, biological and radiological (CBR) agents are an increasingly worrisome threat. Decentralised recruitment and attack-planning make detection and prevention exceedingly difficult. The insider threat, constituted by risks arising from employees working in or for the aviation sector whose role provides them with privileged access to secured locations, secured items or security-sensitive information, remains a growing concern. Corruption or compromise of employees at all levels – from airport staff to security personnel to pilots – provides potentially unfettered access to the target, unless appropriate screening and security controls are implemented.

The HLCAS/2 will address these ongoing and emerging threats and the need to conduct individualised risk assessments reflective of unique situations. The conference will also encourage States to more comprehensively address insider threats and enhance information-sharing on threat and risk.

Improving aviation security risk management

To substantially reduce the probability of an act of unlawful interference being successfully carried out against civil aviation, members of the aviation security community must implement multi-faceted approaches. Through a robust security culture, employees who might otherwise be susceptible to coercion or corruption may be deterred from becoming an insider threat. Current, evolving, and new threats must be continuously monitored and the intent and capability of potential perpetrators must be accurately reported. Rapid growth in remotely piloted aircraft systems (RPAS), increasing interconnectedness of data in the cyber realm, and emerging terrorist attention to CBR weapons are the most pressing, but not the only, threats faced by aviation security professionals.

Focusing on the resilience of the aviation system, authorities must ensure the resilience of redundant critical systems, support contingency planning, and conduct appropriate exercises. The HLCAS/2 will emphasise the importance of an enhanced security culture, and the sharing of best practices, and highlight data driven risk management systems.

Status of the GASeP

The GASeP provides the foundation for ICAO, Member States, industry and other stakeholders to work together in enhancing and improving aviation security worldwide. Central to the Plan is a global commitment to achieve aspirational goals by raising the level of implementation of Annex 17 – *Security*. The extent of effective implementation (EI) for all critical elements, as documented through the Universal Security Audit Programme, serves as an indicator of the global international civil aviation security posture; the Plan identifies ambitious targets for years 2020, 2023 and 2030. A review of the current global and regional EI rates will be presented during HLCAS/2, with a view to taking the necessary actions to improve these rates in the appropriate areas.

Assistance efforts have been identified as a key component in improving aviation security in many States. The ICAO Secretariat continues to coordinate with donor and recipient States to identify security deficiencies, prioritise assistance efforts, and ensure the effectiveness of these efforts. These initiatives result in budgetary considerations and a pressing need for additional and sustainable resources.

The GASeP's core content presents a multi-year approach to enhancing and reinforcing aviation security. Its roadmap, however, is a living document that will be adjusted and enhanced as actions are completed, additional items are identified, and best practices set out. The HLCAS/2 will be invited to consider the future evolution of the GASeP, which may include incorporation of the security-related provisions of Annex 9 ahead of the 40th Session of the ICAO Assembly in 2019.

Achieving better synergies across the aviation disciplines

Aviation security is not a standalone sector; safety, air navigation, law enforcement, and counter-terrorism organisations are just some of the entities whose goals align in keeping people and goods safe and secure. Perpetrators have a multitude of motivators such as ideology, politics, criminal gain or mental instability. However, they often employ similar tactics, techniques and procedures as they seek to exploit vulnerabilities in the aviation sector.

Similarly, expansion of pre-boarding passenger data availability, often discussed in terms of facilitation benefits, may be highly useful in enhancing border and aviation security efforts, particularly in the context of counter-terrorism efforts.

© hin255 - Fotolia.com

ICAO second High-level Conference on Aviation Security: topics and goals

© bychykhin - Fotolia.com

ICAO has completed several key collaborations with other entities whose goals are aligned, although their areas of expertise and mandates may differ. These include other United Nations agencies, such as the Counter-Terrorism Executive Directorate (UNCTED), the Office of Counter-Terrorism (UNOCT), the International Organization for Migration (IOM), the World Customs Organization (WCO) and INTERPOL, and international industry associations such as the International Air Transport Association (IATA), Airports Council International (ACI) and many others. The conference will be encouraged to recommend this model of integration at the Member State and international organisation levels to achieve a coordinated and holistic approach to aviation security matters.

Ensuring sustainability of security measures

The aviation system remains a choice target for attacks by a spectrum of bad actors. In addition to structured terrorist cells and transnational organised crime syndicates, the growing concern of self-radicalised individuals or returning foreign terrorist fighters (FTFs) represents an increasing threat. This has resulted in new kinds of would-be assailants who continue to evolve their attack methods while still revisiting tactics previously used.

Responding to the threat posed by the continuously evolving potential attacker must be carefully considered. Simply adding new technology to the existing kit at a security checkpoint may result in more problems than it resolves as queues get longer, flight schedules are affected, revenue generation decreases and tempers flare. Integration of adaptable countermeasures must be emphasised to ensure the vulnerabilities are mitigated without negatively impacting the industry they are designed to protect.

The Conference will be encouraged to expand efforts to identify new ways to mitigate security risks and share best practices for achieving sustainability.

Conclusion

Member States and selected organisations and associations are strongly encouraged to submit working papers suggesting actions, or information papers identifying perspectives and experiences, as they relate to the HLCAS/2 topics. As ICAO prepares for the 40th Assembly, scheduled to occur in 2019, these inputs will be immensely important in defining the next chapter in aviation security. ■

Sylvain Lefoyer has been Deputy Director in charge of aviation security and facilitation in the Air Transport Bureau of the International Civil Aviation Organization (ICAO) since 1 March 2017. He leads teams responsible for developing aviation security and facilitation policy, Standards and Recommended Practices (SARPs), conducting audits of Member States' aviation security activities, assisting States that are unable to address deficiencies highlighted by those audits, and implementing the Traveler Identification Programme (ICAO TRIP) Strategy.

Mr Lefoyer has extensive experience at the senior executive level in policy and regulations development, strategy, oversight, critical incident management and organisation development in aviation security and facilitation.

Previous to his role in ICAO, Mr Lefoyer's career in transport safety and security spans more than 25 years in the French ministry of transports. He held various positions, such as Deputy Regional Director for ground transport safety, security and defence in the Regional Directorate for Equipment and Urban Planning in the Paris metropolitan area, and as Deputy Head of Aviation Security and Defense in the French Directorate General of Civil Aviation (DGAC). Prior to that, he enhanced his career in air traffic management from 2005 to 2011, in risk prevention and management from 2002 to 2004, and in maritime transport safety and security from 1992 to 2001.

Mr Lefoyer holds a master's degree in electronics from Paris University and a master's degree in public administration from the *École des Ponts ParisTech*.

New Zealand priorities for the ICAO second High-level Conference on Aviation Security

Chris Ford
Deputy Director, Civil Aviation Authority, New Zealand (CAANZ)

As I write this article I am also contemplating my travel to Montreal in November this year for the second International Civil Aviation Organization (ICAO) High-level Conference on Aviation Security, where I will be leading the New Zealand delegation.

Essentially that requires over a day of travel, transiting multiple airports, and includes 13 plus hours on a single transoceanic flight. This serves to highlight that I live in a remote set of islands in the middle of the Pacific Ocean. New Zealand is indeed home to the All Blacks, the Rugby World Cup (currently!), hobbits, and kiwis. It is also a remote, oceanic State, surrounded by vast bodies of water. Our nearest neighbour is some three hours flight-time away.

“Flight is a vital part of our collective national identity”

What this means is that we are absolutely, critically dependent as a State on a safe, secure, and efficient aviation system. Flight is a vital part of our collective national identity. It connects us with our friends and family across the globe. It is estimated that at any one time there are one million New Zealanders living abroad – out of a total population of some 4.7 million. Aviation enables us to see the world, and broaden our understanding of the people in it. Needless to say, we are a proudly pluralistic nation, represented by people from many different parts of the world and from varying backgrounds.

Aviation is also essential to our economy and our resulting social and collective national well-being. Our tourism sector, which is dependent on aviation, is a major export earner and driver of growth for New Zealand, directly contributing around six per cent of New Zealand’s gross domestic product. It is also our largest source of foreign exchange and employs approximately eight per cent of our workforce. We are conscious that, for many tourists, we are a discretionary destination. For those who travel a long way to visit our shores there are many other countries they could choose to go to instead of flying for over a day to visit us: ones that are also cheaper to fly to. Acknowledging these factors, we need to make sure our aviation security system, while protecting the travelling public as its first priority, also provides value for money, an appropriately facilitated passenger experience, and supports on-time departures so we remain an attractive destination for airlines and their passengers. In recognition of the importance of these factors, our government and public accountability reporting systems include measures such as maximum queue length time targets and any departure delays caused by security that ensure we hold ourselves to account on these matters.

“Safe and secure skies – to help New Zealand fly”

Accepting the need to take facilitation into account, at the Civil Aviation Authority of New Zealand we are fundamentally guided by one mission: *Safe and secure skies – to help New Zealand fly*. This statement recognises that for New Zealanders to flourish – socially, economically and globally – we must have an aviation system, it must be safe, and it must be secure.

Despite the fact that New Zealand is geographically remote, we are acutely aware that we are part of an international aviation system. While the threat to aviation varies from place to place, it is also extremely mobile and threats can quickly cross regional and State boundaries. A prime example is the attempted terrorist plot reported in the international media against an aircraft operating out of Sydney, Australia, in July 2017. Australia is one of New Zealand’s closest neighbours in terms of both geography and aviation security operations. In New Zealand, we were incredibly thankful that the plot was disrupted, and that our neighbours avoided what could have been a catastrophic loss of life. We were also reminded of an important lesson: we cannot afford to be complacent.

© Liam Mackinnon

Ambitions for the ICAO High-level Conference on Aviation Security

Taking this context into account, New Zealand has three ambitions for the High-level Conference on Aviation Security in Montreal in November this year.

STRIKING THE RIGHT BALANCE

The first is to recognise the need for balance. That is, balance between performance-based and outcomes-based aviation security standards, and prescriptive ones. However, when using the terms performance-based or outcomes-based or prescriptive it is also important to clarify what I mean.

Firstly, prescriptive standards. This term refers to standards that set specific technical or procedural security requirements that must be complied with by States. Such a standard expressly determines the means by which an appropriate level of security assurance is attained. In such cases no choice is left to the State regarding the means by which this level of assurance is reached. A State's compliance with the Standard can be directly assessed by comparing whether or not the specific technical or procedural security requirement expressed in the Standard is applied and present.

Secondly, performance-based or outcomes-based standards. This is an approach that focuses on desired, and measurable, outcomes, rather than prescriptive processes, techniques or procedures. In this case, performance-based or outcomes-based standards lead to defined results without specific direction regarding how those results are to be obtained.

In any case where performance-based or outcomes-based standards are applied, there are two considerations that need to be taken into account. The first is the need for clear guidance material for States on options by which the required desired and measurable outcomes may be delivered, and factors States should take into account to ensure this delivery. In this regard, ICAO – and the guidance material it provides – is critically important to support achievement of the required outcomes and the ongoing validity of any performance-based or outcomes-based standards. The second is the need for transparency at a State-to-State level: the means by which a State may choose to deliver on performance-based or outcomes-based standards, and its rationale for its chosen approach, must be apparent to its international partners and ICAO in such a way that collective confidence in the international security system is maintained.

Each State and the international aviation security system may benefit from a different mix of performance-based and prescriptive standards. No single approach is appropriate. No single approach is robust. Why? Because we must remain flexible, agile and considerate of our differences. Aviation is an international, network business, with complex inter-relationships between States and industry partners. As noted above we must acknowledge that threat and risk environments can and do vary globally while recognising the critical importance of a strong international security system. Reflecting this international context we see a variety of different aviation security delivery models in different States. There are also varying levels of awareness and capability between States. Meanwhile, aviation remains a favoured terrorist target, with new and emerging threats expected as the norm. We face conscious and adaptive adversaries who are continually looking to identify and exploit vulnerabilities in our global security system.

In such a setting, promoting a balance between performance-based and prescriptive standards is the only way to support all States to best manage their specific threat and risk environments, within the wider global environment. Moreover, the flexibility enabled by this balance promotes innovation and efficiency in passenger facilitation, without compromising security. Flexibility can potentially produce better security outcomes, by embedding quality and continuous improvement in security delivery processes.

That's not to say that prescriptive standards are not desirable in some cases, but we need to undertake very careful analysis and consideration of all relevant factors before concluding this in any one case. Balance is key to ensuring sustainability, and what good are our security systems if they are not sustainable? Risk-based measures that appropriately take into account varying threat and risk environments, and the proportionality of counter measures can contribute significantly to the sustainability of our aviation security systems.

PROMOTING ICAOs' GLOBAL AVIATION SECURITY PLAN (GASeP)

Our second desire is to endorse and promote ICAOs' Global Aviation Security Plan (GASeP). This is the strategic document that guides States and industry stakeholders towards ongoing and continuous aviation security enhancement. New Zealand considers it appropriate to comprehensively endorse the GASeP's existence, and the importance of all States working in partnership with ICAO and industry to implement it.

The ICAO Assembly first agreed in 2016 that there was a need to develop the GASeP, to replace the Comprehensive Aviation Security Strategy. The GASeP aims to foster a greater commitment from all parties – including States, ICAO, and industry – to enhancing global aviation security. This is an important pursuit. International air passenger traffic is forecast to continue growing as are air cargo volumes. That's assuming that we sustain a safe and secure aviation system, in which the public have confidence. The ongoing enhancement of our systems in the face of conscious and adaptive adversaries and constantly evolving threats is critical if we wish to maintain that confidence and support international travel, trade and connectivity. Without question, the GASeP will yield benefits, and prevent human, immediate financial, and longer-term economic losses.

In light of the ongoing threat and risk environment, aviation security must remain a priority for all States. This was highlighted by the United Nations Security Council's Resolution 2309 (2016) on aviation security, fully supported by New Zealand, and adopted in 2016 at the time when New Zealand was chairing the Security Council. We remain committed to the principles of the GASeP, the need for States to implement it, and for ICAO to support its members on that journey. To that end we support the intent of ICAO for the High-level Conference to recommend a vision for the future evolution of the GASeP.

ADVOCATING FOR SMALLER NEIGHBOURING STATES: NO COUNTRY LEFT BEHIND

Finally, New Zealand will also be advocating for its smaller neighbours. This takes us back to the need for balance as a means to support sustainable and continuously improving aviation security systems. We must remain cognizant and considerate of differences between States. Consider, for example, the aviation security system required at an airport from which you can fly to 180 destinations in 90 countries on flights offered by 90 airlines. Is the same system necessary for a small island airport which has only one or two departing international flight per week? Of course not. But smaller States are also not immune from threats and risks and equivalent outcomes must be delivered. In our part of the world, there are potentially some smaller States who face capacity and capability challenges at the levels of both operational security service delivery and regulatory oversight that we do not. As a result, these States may have difficulty achieving full compliance with all ICAO aviation security standards, and the intentions of the GASeP. Notwithstanding these challenges there is a high degree of commitment and willingness on the part of relevant States to achieve necessary levels of compliance and ensure they play their part in our global aviation security system.

This highlights the importance I have referred to above for a mix of performance-based and prescriptive standards, to allow States to achieve ICAO compliance in a way that is most appropriate to their threat and risk environment, while also recognising that they are part of a global aviation system.

New Zealand recognises it has a responsibility to support its developing neighbours, and takes that responsibility very seriously. I am proud to say that we have, and continue to provide, a range of aviation security support to our Pacific neighbours, and have done so in a sustainable way. What I mean is that we have built capacity, not simply filled gaps. We have trained trainers. We have provided screening equipment and the expertise to maintain that equipment, and will continue to do so. We have sent uniforms, vehicles and radios and personnel to advise how to use these. We have established relationships and we have helped align processes, procedures and systems with international standards, and supported the development of increased oversight capability. For New Zealand, the strength of these relationships and working together with our smaller neighbours for the collective benefit of all is a crucial element of any effective and successful capacity and capability-building efforts.

All of us have a duty, as part of ICAO and part of the global aviation security system, to provide what support we can, in the spirit of ICAO's own initiative: *No Country Left Behind.*

In closing, New Zealand recognises that it is part of an interconnected global aviation system; one in which threats and risks are continuously evolving and can rapidly cross regional and State boundaries. Acknowledging this there is a need to ensure an appropriate balance of performance-based and prescriptive standards, and an approach of continuous aviation security enhancement in a manner that allows all States, small and large, to reap the benefits of a safe, secure and efficient global aviation system. ■

Chris Ford is Deputy Director Aviation Infrastructure and Personnel within the Civil Aviation Authority of New Zealand (CAANZ). In this executive role he is accountable for oversight of New Zealand's aviation security system and its linkages to New Zealand's wider national security system. He is also accountable for the oversight of New Zealand's air traffic management system. Mr Ford represented New Zealand on the International Civil Aviation Organization (ICAO) Aviation Security Panel from 2004 to 2012 before taking up his current executive management role. He was vice chair of the Panel from 2010-2012. He is also a past chair of the Asia Pacific Economic Cooperation (APEC) forum experts group on aviation security. Prior to his career with CAANZ, Mr Ford was a member of the New Zealand Police in a range of criminal investigation and transnational crime and national security roles. Mr Ford is a graduate of the Melbourne University School of Business Leadership Development Programme, and the Harvard University John F Kennedy School of Government Senior Executives Programme on National and International Security. He holds a Graduate Diploma in Arts (Philosophy) from Victoria University of Wellington and is currently studying towards a master's degree in philosophy, politics and economics, also at Victoria University.

COMPLIANCE MONITORING

Effective training for AVSEC inspectors and auditors: the Canadian experience

Meaghan Campbell
Senior Program Officer, AVSEC, Transport Canada

John Velho
Chief of International Operations, AVSEC, Transport Canada

For aviation security insiders, there may be nothing more frustrating than going through a security screening line and seeing screening officers displaying poor screening techniques, paying little attention to the activity at the screening point or using security technology ineffectively. Equally disconcerting is knowing that with proper training and oversight, these security gaps could be reduced, if not eliminated!

But witnessing such deficiencies should not just result in corrective actions applied to the screeners – the public face of aviation security. Rather, it should result in a wider view that includes a look at the supporting framework that is in place – including proper training and oversight, as it is these elements that help to reduce security gaps.

A PhD thesis could be written on the importance of professional competencies within the entire aviation security community – from screening officers to primary security line partners – but we have decided to focus on one area in particular. We believe one of the cornerstones of an effective aviation security programme is effective training of those professionals conducting oversight – AVSEC inspectors and auditors.

ICAO and the importance of oversight

ICAO maintains that aviation security oversight plays a vital role in States helping to ensure the effective implementation of security-related Standards and Recommended Practices (SARPs) contained in the Annexes to the Chicago Convention. Aviation security practitioners agree with the international civil aviation body, asserting that oversight is a key component in establishing, maintaining and sustaining a strong and effective aviation security programme. However, an effective aviation security oversight regime necessitates properly trained professionals whose abilities and expertise are respected by industry and who are fully equipped to deal with different facets of the security programme within civil aviation.

We believe that aviation security inspectors and auditors are the front line of any oversight programme. They are responsible for conducting activities such as inspections, audits, surveys and tests to proactively ensure that those entities identified in the National Civil Aviation Security Programme (NCASP) with AVSEC responsibilities are meeting their obligations as required by the State. Inspectors and auditors are also the public face of the oversight programme – engaging with those delivering the AVSEC programme, playing an important educational and outreach role. When effective training is lacking for inspectors/auditors it can lead to a weakness in the oversight programme and consequent vulnerabilities in the system. This means that whenever a security incident occurs, the first reaction is to examine if those persons responsible for oversight did their job properly, as it is society's expectation that States exercise their diligence through competent staff in order to ensure that security is effective.

ICAO rightfully requires that Member States establish minimum knowledge and experience requirements for personnel performing State aviation security oversight functions. Providing training to AVSEC inspectors to acquire, maintain and enhance their competencies is also considered a critical element – along with the provision of appropriate on-the-job training.

Training of inspectors/ auditors – assessing the needs

Transport Canada (TC), the national civil aviation authority in Canada, would go further, however, and assert that the minimum requirements for AVSEC inspectors should be consistent among States but also generic enough to allow flexibility for a State to recruit and train individuals in accordance with their operational requirements and depending on the State's current infrastructure in terms of aviation security resources, political initiatives, technology, etc. In sum, training requirements that reflect local realities.

Further, training should derive not from a set of requirements but from something that is continuously assessed. We must ensure that individuals still possess the knowledge, skills and behaviour required for their function, especially in a world that evolves rapidly with regard to threats, technology and volume of passengers.

Where to start

How can States ensure that the training requirements for those individuals who play such a key function in the oversight programme include today's skills and the competencies needed to fulfil their responsibilities and be proficient in their work? This is a common challenge for all organisations conducting oversight activities. So where should they start?

A strong governance framework is essential for any effective training programme. In the field of aviation security, this framework should be established in order to ensure that training is given the attention and degree of formality that is required within an AVSEC organistion. It should provide a consistent and common set of expectations to be adhered to by AVSEC executives in order to ensure that learning needs are met and that actions and key activities linked to learning development and learning delivery are clearly laid out. That's correct! People who make decisions need to be accountable for learning, especially for training that is directly link with a State's AVSEC obligations and responsibilities.

Roles, responsibilities and accountabilities associated with the analysis, design, development, delivery and evaluation of technical training should also be defined in the governance framework for training. Further, a process for the identification of deliverables and priority-setting for training activities along with the allocation of adequate resources for the design, development, delivery and evaluation of training are needed in order to succeed. Supporting systems such as a learning management system or a content management system should not be forgotten as they form the infrastructure to support e-learning and allow for the tracking, monitoring and reporting of training activities. These systems should also provide a formal process to report on performance and satisfaction. Careful when considering these systems, especially those that support e-learning design and delivery, since these do require different skills than the usual resources.

The experience of Transport Canada

Transport Canada has established a national standardised approach for recruiting aviation security inspectors as well as minimum training requirements. The recruitment process includes a generic work description for AVSEC inspectors that outlines key required knowledge, skills, activities, responsibilities and work conditions. A competency profile has also been created that outlines the core business and technical competencies required for conducting security oversight activities. Transport Canada has also established a Learning Continuum and a formal, structured on-the-job training (OJT) programme that provides a learning schedule based on a modular approach grouping specific areas of competencies (i.e. security screening oversight, inspections and enforcement).

The AVSEC Learning Continuum has been adopted as a learning framework for aviation security inspectors and reflects the commitment of the government to provide the best possible training programme in the area of aviation security. Characteristics of the Learning Continuum include learning that is organised by area of expertise (e.g. specific training paths for general aviation security and air cargo security) as well as skill sets (e.g. inspection and enforcement, security screening inspections). Learning is divided into core, mandatory, advanced and refresher training. For each of the mandatory core learning modules, prerequisites are required, participants take part in courses (e.g. classroom training, workshops, virtual classroom, e- learning etc.) and complete associated pre- and post on-the-job training/learning activities and all modules are to be completed in a specified sequence.

As the learner gradually, and successfully, completes each mandatory core learning module they are able to exercise their delegation of authority (powers) in a progressive manner, based on the guidelines distributed by Transport Canada. When the mandatory core learning modules are fully completed successfully, only then does the learner have the power to exercise their full authorities. A policy is also in place that establishes a process for meeting training requirements that must be met prior to obtaining inspector's credentials. The entire process is managed by an internal training group within Transport Canada, which is the entity responsible for all technical training in the department. This multimodal training group offers expertise in educational design, training systems, e-learning design and multimedia, which in return works with modal groups such as AVSEC to deliver a National Civil Aviation Security Training Programme.

In considering who is best to deliver the training in the AVSEC Learning Continuum, Transport

Canada has identified and implemented a novel approach. Aviation security subject matter experts (SMEs) work together with educational specialists to develop and deliver training. This approach ensures that the educational needs of the adult learner can be addressed in the course design based on established pedagogical best practices and knowledge in order to help ensure the best possible outcome. SMEs provide their expertise to ensure that the material addresses the most recent threats and risks, and develops the practical skills and competencies needed for conducting oversight activities. There is no certification process for the SMEs or the educational specialists, rather they are chosen on the basis of having met key competencies through education, background and experience required for the role, which exceeds a formal certification process.

Transport Canada recognises States' obligations to have a standardised approach in the certification of aviation security instructors. However, a State should not solely rely on such a process to ensure that training is effective and instructors are indeed qualified to deliver an AVSEC training programme. Transport Canada believes that instructors should possess the qualifications of the subject being taught, which goes beyond certification. Qualifications should address the level of core competencies for different areas of responsibilities within the aviation security regime to ensure that instructors have the proper knowledge, skills and experience in the subject being delivered. The traditional way of granting a certificate to an individual through a generic certification process is often misrepresentative and doesn't confirm the ability of the instructor to actually teach a specific subject. This often results in poor training.

© No-Te - Fotolia.com

The role of on-the-job training

In creating and maintaining a workforce of qualified and effective inspectors/auditors, Transport Canada has had to evaluate what is most critical in all AVSEC training programmes e.g. ICAO courses, State training programmes, academia. All are important, but we believe that on-the-job training is what makes the different between good training and effective training!

According to training specialists "Structured on-the-job training is the planned process of developing task-level expertise by having an experienced employee train a novice employee at or near the actual work setting." [1]

OJT programmes can range from a 'structured' programme to an informal 'follow Joe/Jill around' method. OJT is a common means of training or retraining workers and may seem simple and straightforward; however, doing it effectively requires more thought and preparation than simply having someone follow an experienced worker around and watch what they are doing.

While structured OJT has many features in common with other forms of structured learning, it is distinct in other respects. For example, it emphasises one-on-one contact between seasoned and novice employees as the primary means of conveying learning. In addition, structured OJT is often thought of as involving both learning and practising at the same time.

An unstructured environment may perpetuate bad habits and create trained employees who are not given the same information, skills or evaluated to the same standards. It is only through planning a structured OJT programme that consistency can be created and maintained. At the very least, all learners who have successfully completed such a programme can be expected to perform at an established level, and they will know what they must do to be successful.

[1] Jacobs et Jones, Structured On-The-Job Training, 1995.

Structured OJT as a learning system – the importance of coaching within an AVSEC regime

The purpose of a structured OJT programme is that it permits new AVSEC inspectors/auditors to learn skills and behaviours through orientation, observation and demonstration, guided practice, feedback, and assessment while working on the job, all of which is done under the supervision of a competent and committed inspector/auditor (coach). It is for these reasons that a structure based on coaching is the approach adopted by Transport Canada.

The foundation of the structured OJT programme is its coaches. Coaches must know and be able to perform the jobs they are teaching and also know how to share their knowledge and skills and demonstrate a positive attitude with the learner.

Choosing the right people to be coaches and then giving them the support they need is key to a successful programme Often, OJT coaches are chosen on the basis of their job experience. But factors that need to be considered when assigning coaches include not only job expertise – both knowledge and experience – but also personal characteristics. Enthusiasm, humour, flexibility, tolerance and patience are just some of the kind of qualitative differences that will set excellent coaches apart from adequate ones. In Transport Canada, just like AVSEC instructors, those coaches assigned to new inspectors are qualified through a process of mandatory training, proficiency requirements and experience.

© Geza Farkas - Fotolia.com

Conclusion

Transport Canada's experience has shown that States should have a policy for all AVSEC professionals promoting a process of continuous learning in order to foster a work environment that encourages and supports professional development and commits to planning for learning as an integral part of their business planning process. Learning needs to be identified and communicated, prioritised and planned for, based on business, organisational, human resources and goals. The impact of learning activities on an organisation's goals should also be measured and communicated.

The next time you travel and see a screening officer chatting with a colleague rather than focusing on the x-ray image, or conducting an inadequate search of the baggage – we hope that you stop to think about what more than the human factor is in play and, by using the lessons learned from our experience, how it might be remedied! ■

Meaghan Campbell is a Senior Program Officer in the Foreign Programs Branch of Transport Canada. She has spent nearly a decade working in various aspects of the aviation security field including air cargo security, security technologies and inspection and oversight. She currently holds the position of Senior Advisor with the International Branch, responsible for many AVSEC files such as foreign inspector training, risk assessments and quality control.

John Velho is Chief of International Operations at Transport Canada. He has extensive experience in the field of aviation security and has been a key resource in the development and implementation of Canada's National Civil Aviation Security Training Program (NCASTP), a programme that he led after the events of 11 September 2001. Mr Velho has since trained over 300 AVSEC inspectors in Canada and has offered multiple workshops around the world in the area of risk management, quality control, screening, security audits, testing, investigations and many other AVSEC programmes. Mr Velho has been with Transport Canada for 19 years and as the lead for the foreign inspection unit, he has championed many security projects at domestic and international airports to mitigate security risks.

The Argentinian approach to covert testing

Oscar Rubio
AVSEC Director, Airport Security Police (PSA), Argentina

Historical background

Annex 17 (Security) to the Chicago Convention has had ten editions and 16 amendments since its entry into force on 22 March 1974. In its subsequent editions and amendments, the Standards and Recommended Practices (SARPs) have established and gradually raised the base of a harmonised international regulatory system that regulates different aspects of the Contracting States' aviation activity with regard to the prevention of acts of unlawful interference against civil aviation.

In October 1989, Amendment 7 to Annex 17 came into force, which included for the first time Chapter 4 under the title "Preventive Security Measures". However, there was still a long way to go before these written measures could be assessed methodically to verify, through demonstrable evidence, their effectiveness.

Amendment 9 to Annex 17, put into effect in August 1997, incorporated the proposals of ICAO´s Unlawful Interference Committee in collaboration with the Aviation Security Panel (AVSECP). As a result, a provision was included obliging the Contracting States to incorporate new provisions with respect to the performance of tests to determine the programme's effectiveness and the measures applied. This standard was part of Chapter 4, "Preventive Security Measures", and was identified with number 4.1.6, which established that *"each Contracting State should conduct surveys in order to identify security needs, conduct inspections regarding the controls of security applied to cover them and organize tests of them to evaluate their effectiveness".*

ICAO defines a security test as "a covert or overt trial of an aviation security measure which simulates an attempt to commit an unlawful act". This article tries to highlight the key principles in establishing a robust covert test programme, the challenges and the successes, and Argentina's experience in this domain.

Current implementation in Argentina

Annex 17 requires the development of best practices and workshops to assist States in complying with the implementation of covert testing programmes. Additionally, with new standards on security measures, the scope of the covert testing programme should be increased accordingly.

Notwithstanding the above, we must understand, under a holistic concept, the purpose of security testing is developped according to its key principles. This is necessary because the personnel and organisations subjected to these oversight activities have a tendency to reject the security testing because testing is perceived as a threat to job stability.

In this regard, we should emphasise that a security test's main objective is to evaluate how effective the application of security measures is, and to identify the breaches, deficiencies or vulnerabilities in the security systems before the perpetrators can discover and utilise them for their own purposes. These weaknesses can be of a material, human or procedural nature, which are the aspects on which any aviation security systems are based.

The security testing will reveal in real time and in a real environment the opportunities available to those who try to compromise the effectiveness of the security system. Similarly, it will assess feasibility. That is why, in order to promote global aviation security through continuously auditing and monitoring the Member States' aviation security performance, the Protocol Questions used by the ICAO Aviation Security Audit Section include some Member States' duties that must be carried out, such as the need to perform the following types of covert testing:

- a) access control to security restricted areas (SRAs) (e.g. detection of attempted access by non-authorised persons);
- b) aircraft protection and aircraft security check / search (e.g. detection of prohibited or suspicious items on board an aircraft, and detection of forcible intrusion);

- c) passenger and cabin baggage screening (e.g. verification of the security staff's capability to detect and deny the introduction of prohibited items);
- d) screening of persons other than passengers and items carried (e.g. detection of unauthorised items);
- e) screening of cargo and mail (e.g. assurance that consignments are effectively screened using appropriate methods);
- f) screening of in-flight and airport supplies (e.g. detection of prohibited items in catering carts and merchandise);
- g) protection of screened passengers, baggage, cargo and mail from unauthorised access (e.g. detection and/or prevention of access by unauthorised personnel); and
- h) airport patrols (e.g. detection of unattended items).

With the aim of strengthening the quality control system, Argentina also amended its National Quality Control Programme (NQCP) through the Aviation Security Regulation N°7 (RSA 7) *"Protocolo de Pruebas de Seguridad"* in July 2017, adding specific written authorisations for those responsible for conducting covert testing, including:

- a) a description of the test pieces and any accompanying cases and tools;
- b) personal information and qualifications of the person carrying the test pieces, to be matched with the person's photo identification; and
- c) duration of the mandate during which the person is authorised to carry test pieces for the sole purpose of conducting covert testing.

Key principles

We could say that security testing has three pillars on which to build its strength. Let's give a brief description of them:

1) CONFIDENTIALITY

Protection of information. The aviation security inspectors and those in charge of carrying out security testing must be vigilant regarding the use and protection of the information obtained in the exercise of their functions. Whoever performs testing should not make inappropriate use of such information for personal benefit, or to the detriment of the legitimate interests of the auditee. This concept includes the appropriate treatment of sensitive or confidential information. Adequate discretion in this regard will allow the security procedures and practices to be enhanced without damage resulting from leaked information.

2) INDEPENDENCE

The impartiality of the security testing and the objectivity of its conclusions. Inspectors must be independent of the entity being evaluated and free from prejudices, conditions and/or the perception of conflicts of interest. In the event such personnel *is* part of the assessed entity, they must maintain objectivity throughout the evaluation process to guarantee that the results and conclusions are based only on the security test conducted.

3) EVIDENCE-BASED APPROACH

The rational method to reach conclusions of reliable and reproducible control measures in a systematic process. The security testing must be objectively verifiable. In general, testing will be based on samples of the available information, given that the security testing is carried out for a specific period of time and with limited resources. As a result, it is essential to follow up activities appropriately. In this sense, appropriate use of approved test pieces should be made, since this is closely related to the confidence that can be placed in the conclusions and monitoring activities that measure the evolution of the observations. Create a database of all the security testing performed with the respective results, and with this database generate statistics that allow us to make a projection in time and develop a plan to optimise the resources according to the dependencies that will require more or less oversight.

The personnel who carry out the security covert testing must have the appropriate aviation security training established by the national authority as adequate to conduct the procedures, as well as knowledge of the local organisations responsible for implementing the security measures, and the testing should be conducted under their legal authority.

© Jose Luis Stephens - Fotolia.com

© stnazkul - Fotolia.com

Challenges and successes

Security testing carries a great responsibility. The personnel responsible for it should therefore be trained to stop it at any time if the situation becomes out of control potentially resulting in damaging or negatively impacting the normal functioning of the security system, or even more, the safety systems. In practice, a national inspector should be the most prepared person to carry out these activities, but it would be appropriate to analyse the State's current capabilities and maybe develop another specific course for those conducting the security testing. It is worth mentioning that although Document 8973 and the training workshops developed by ICAO suggest and recommend that national inspectors be certified, Annex 17 does not require certification for the State's national inspectors, nor for any other person who carries out this type of control measure. This must be taken into account when States set the basis of their own security testing platform.

Prior to conducting the security testing, it is important for the AVSEC authority and authorised entities to have standardised protocols and procedures established relating to the scope to be assessed, issued by the appropriate authority, in order to guarantee the homogeneity of the different security tests to be conducted. In particular, the authorised entities must have an approved programme establishing how they will implement quality control activities, specifically security covert testing, if applicable. It must be highlighted that procedures are one of the main points to observe, so it is useful to remember that the procedures are carried out by people. But are the people involved in these procedures the only ones who can make mistakes? In principle, yes, when the focus is on evaluating the human factor. But what would happen if the technical resources were the ones to fail? We must be aware in advance that the equipment used has been approved for its use. And even when the technology meets the necessary requirements, it is essential to know if it is verified regularly. When writing the test report, the person in charge of the execution would have to evaluate all the factors that can impact the operation of the security controls.

Following the same reasoning, suppose for a moment that the system to be controlled had the best training personnel it could aspire to, the best preparation, the best technical equipment. What would happen if the procedure itself was poorly designed? If the staff subjected to the security test did not have the necessary rest? If sufficient personnel were not available to implement these procedures?

Taking into account the above hypothesis, the analysis of the results must contain a comprehensive evaluation of all the aspects involved in the security processes, and in this way be able to distinguish the failure that caused the inefficiency, in order to make the most appropriate recommendations and take appropriate remedial actions to resolve the deficiencies.

Experience gained in Argentina

When Argentina revised its covert testing programme to a continuous monitoring approach, it needed to establish a team which could carry out its duties in an unpredictable manner whilst maintaining a pattern. The results of the first activities showed that personnel subjected to covert testing perceived it as a threat to their job stability. This resistance lowered with the security testing covert programme but it should be stressed that security testing is part of the AVSEC culture, including staff promotion for those who duly passed the security testing.

It is essential to develop solid working groups which understand the SARPs to be assessed. But is this enough? In order to truly understand the importance of establishing a team, some key principles should be set out. In the first place, there needs to be clear objectives: the team needs to be able to understand where it is going, the sense of belonging will be enhanced and the unity of the team will be promoted. Secondly, there needs to be defined roles: each member should understand their place in the team, and recognise, value and rely on each other's competencies, facilitating the interaction that will contribute to the operational realisation of the tasks and the related roles that contribute to the team's cohesion.

There is no other way to have a robust security system without establishing a security culture. In general terms, aviation is global, meaning that each State depends on the effectiveness of other States' aviation security systems to provide a common and secure aviation environment.

We cannot underestimate the need to: incorporate effective and risk-based measures that are evaluated on a regular basis to ensure they reflect the changing threat picture; ensure the effective implementation of those measures on the ground in a sustainable manner; allocate resources and promote a security culture; and establish effective national surveillance of aviation security systems.

The civil aviation industry should be able to share the results of the security testing carried out within its own systems in a secure manner, analysing them objectively. The results of internal covert testing must always be reviewed by the appropriate authority to assure impartiality and objectivity, and then reported in the Risk Management Assessment.

Finally, the security testing modality seeks to incentivise the airport community overall, through the personnel that has been evaluated via this procedure. And we must consider that the purpose is not to look for errors in the system, but to test the effectiveness of the security procedures under different circumstances. ■

© Rawpixel.com - Fotolia.com

Oscar Anibal Rubio is AVSEC Director at PSA (Airport Security Police), the national aviation security authority in Argentina. He is a designated member of the ICAO Aviation Security Panel and chairman of the AVSEC-FAL Regional Group ICAO/LACAC for the North American and Caribbean and South American (NAR/CAR and SAM) regions.

Mr Rubio began his aeronautical career in the Air Force in 1994 and then continued working for the PSA. Since 2001 he has been working as an aviation security specialist as auditor and instructor. He was in charge of the application of the National Quality Control Programme.

Currently, as Director, he is responsible at national level for the execution of a comprehensive risk management system and oversight in the development and implementation of national aviation security standards and programmes.

Mr Rubio has regularly served as a certified instructor for ICAO and has participated in many ICAO Universal Security Audit Programme (USAP) audits as an audit team member. This year he has also contributed as team leader to the Aviation Security Audit Section.

Mr Rubio is an officer in the reserves of the Argentine Air Force and holds a law degree from the University of Buenos Aires, specialised in aeronautical law, as well as international law on armed conflicts and international humanitarian law.

Implementation process of key priority outcomes of the Global Aviation Security Plan in the Russian Federation: challenges and success

Vladimir Chertok
Advisor to the Head of the Federal Authority for Transport Oversight, Russia

From the start, the Russian Federation has participated in the development and approval of the Global Aviation Security Plan (GASeP) by the group of ICAO aviation security experts, and therefore decisively supports its implementation.
GASeP approval by ICAO means ICAO's global regulation of the whole sphere of security provisions in international civil aviation is now complete.
At the present time, the three global plans concern aeronavigation, flight safety and aviation security.

The importance of GASeP for the Russian Federation is evident: Russia is a huge country covering 20% of the globe. It has borders with 20 States and is located across 11 time zones. It is evident that the main and most available means of transport in all regions is civil aviation.

At the present time, in accordance with the Russian Federation's approved transport development strategy till 2030, 230 airports are being constructed or renovated. Of these, 80 have international status. Platov, a large new international airport, recently opened in the south of Russia near Rostov-on Don.

In the field of aviation security, the Russian Federation is actively implementing the latest innovative technologies and equipment, many of which have no equivalent in the world. The structure of division of power of public authorities in the field of aviation security is clearly established in the Russian Federation: in legislation, in State security oversight and State services for construction, reconstruction and exploitation in aviation.

Enhanced risk awareness and response

Currently, the Russian Federation is implementing a continuous monitoring approach mechanism in the field of aviation security. The main aim of modernising the system is to efficiently identify problems in security, assess risks that have an impact on threat rise, and manage threat identification in order to lower potential breaches.

In accordance with its federal law, the Russian Federation has established the State Information System on Transport Security, which is a database of all State authorities in the security field across all modes of transport.

This complex information system of control and oversight for transport security has been developed and implemented by the Federal Authority for Transport Oversight. This system allows gathering all the information about risks, analysing global threats, and justifying the recommendations to reduce or eliminate security risks.

The main idea of this risk-oriented approach is to manage risks. It allows timely measures to be taken where necessary and, to a large extent, saves human and financial resources. We constantly control and confirm that this State Information System on Transport Security is effective and continuously improving.

In February 2018, the Russian Federation government established criteria to classify airport activities per security risk category, taking into account the severity of the potential negative consequences and the probability of their occurrence. The frequency of inspections is determined by the risk category determined at the facilities.

In relation to aviation security oversight on aircraft, a procedure of checks and examinations ('frame checks') of the aircraft in the process of their exploitation is in place. A control of the completeness and authenticity of passenger and crew data is conducted in accordance with ICAO directives.

The automated centre was established by the Federal Authority for Transport Oversight to collect operational information and assess risk. The head centre is located in the central office of the Federal Authority for Transport Oversight in Moscow, but local branches are run in all territorial offices overseen by the Federal Authority.

This control centre gathers and processes information and notifications from State inspectors and transport infrastructures' special services. It is the Russian Federation aviation security point of contact and is included in the system of ICAO coordinating centres.

The Russian Federation also shares its experience at the international level by participating in meetings of the ICAO Aviation Security Panel (AVSECP), the ICAO EUR/NAT Aviation Security Group (ENAVSECG), and some ECAC working groups, as well as at EUROCONTROL, the French Directorate General of Civil Aviation and the United States Transport Security Administration.

Security culture and human capabilities development

Considering the new risks emerging in the modern world, the Russian Federation focuses on developing a security culture and human capabilities.

The Russian Federation declared 2018 the Year of Security Culture. The annual plan includes information and prevention events, «open doors» days, and security classes for the public, representatives of State oversight and businesses.

The Year of Security Culture aims to enhance public knowledge and practical skills in the field of security, while State oversight specialists can obtain a unique experience in protecting the population from acts of unlawful interference.

In order to inform the population about aviation security, mass media is used, including specialist journals such as the regular «Transport Security and Technologies».

In order to lower unlawful human interference, automated access control systems with biometrical application technology have been implemented in airports, as well as video monitoring/recording of personnel actions at all stages of screening.

The 'admission to work' system established by the Federal law, «About Transport Security», and the Russian Federation government's special regulations set out the qualifications, knowledge and skills required of personnel.

Special measures have been taken to increase public awareness and create a positive image of defenders among of transport security employees.

On 3 September 2017, national Day of Solidarity in the fight against terrorism appointed by decree of the President of the Russian Federation, Vladimir Putin, a monument dedicated to the transport industry employees murdered while conducting their professional duty to protect was inaugurated at the Russian University of Transport in Moscow. The monument was financed with voluntary contributions from Russian transport industry organisations and citizens.

Improved technological resources and fostering innovation

The Russian Federation conducts an innovative approach to implementing the eight critical elements of the ICAO Universal Security Oversight Audit Program.

The requirements for functional specifications and regulations for obligatory certification of technical systems used in transport security were developed and confirmed by resolution of the Russian Federation government. Five certification bodies on categories of equipment have been established and are fully functioning. Trial laboratories have been accredited.

The work of 16 mobile remote transport security monitoring and oversight centres in the Russian Federation continues, conveying their data to the Federal Authority for Transport Oversight.

In order to objectively control the implementation of aviation security requirements, a system of video monitoring has been set up in aircraft cockpits. Setting-up obligatory video recording systems in commercial aircraft was approved by the Russian government.

© BRIAN_KINNEY - Fotolia.com

In the Russian Federation, innovation technology to built-up aviation security system "Electronic system of security management" (ESpsM) was developed. The system integrates information flow from airport security subsystems, provides a timely identification of threats, manages all stages of reaction, analyses the effectiveness of the measures taken, and provides control and help to the operator in emergency situations.

The Russian Federation supports the ICAO Secretariat's efforts to stimulate innovations in the field of aviation security.

Improved oversight and quality assurance

I would like to express my gratitude to the personnel of the ICAO Aviation Security Audit (ASA) Section and of the ICAO EUR/NAT Regional Bureau. They carry out very important and necessary work on implementing the continuous monitoring approach in the global aviation security system.

In the Russian Federation's national programme, priority was given last year to improving control and oversight activity in the field of transport until 2025. This programme includes seven main guidelines to improve oversight activities.

In April 2018, a list of control and supervision activity key indicators from the Federal Authority for Transport Oversight was confirmed by governmental decree. It showed a drop in the number of victims and injured people resulting from acts of unlawful interference, and of material damage to citizens, organisations and the State.

We focus our attention on developing and implementing a complex system of prevention against the rise in aviation security breaches.

Currently, a mechanism of self-control of the implementation of aviation security requirements is in place in supervised entities. Advanced information technology to objectively and independently assess State inspector qualifications is also used.

In the near future, a pilot training programme project for aviation security inspectors will include virtual modelling of different situations that may arise during the check (as is applied in pilot training with the use of flight simulators).

The system of compulsory certification of all personnel directly contributes to aviation security.

Increased cooperation and support

The Russian Federation participates in ICAO events in the field of international cooperation and exchange of best practice.

At the national level, antiterrorist committees have been established in every entity of the Russian Federation. Their task is to help interested bodies and services prevent security breaches.

Field conferences dedicated to aviation security issues are held approximately every quarter.

Cooperation with other countries to enhance the quality of supervision of aviation security is implemented on a regular basis.

In conclusion

Considering that control and oversight efficiency plays a key role in State's process to proactively adapt to new security threats, the Russian Federation supports the ICAO Secretariat and its Regional Bureau's efforts to implement the GASeP roadmap in the European and North Atlantic Region.

As chairman of the Aviation Security Working Group of ICAO EUR/NAT Regional Bureau, I think and believe that our mutual work to unite States' efforts to improve aviation security provision will be successful. ■

Vladimir Borisovich Chertok is Advisor to the Head of the Federal Authority for Transport Oversight. He graduated from Moscow Aviation Institute. He worked during 30 years at the State Research Institute of Civil Aviation and conducted ground and flight tests of board life support systems, survival and safety for crews and passengers almost in all types of modern civil aircrafts. As a test engineer in test flights flew more than 338 hours.
Currently, he is in charge of state control and oversight for compliance of legislation and international treaties of the Russian Federation in the field of protection from acts of unlawful interference in all types of transport, aviation security and flight safety in civil aviation.
Under the leadership of Mr Chertok, were established the system of state oversight and control and the operation service with the functions of the Crisis Management Center and the Coordination Center for Aviation Security.
Since 2006, Mr Chertok has been the national aviation security coordinator of ICAO audits in the Russian Federation for provision of aviation security in civil aviation, and he is also designated member from the Russian Federation of the ICAO Aviation Security Panel and Chairman of the EUR/NAT AVSEC Group.

The ECAC Network of Chief Economists

Interview with **Ana Mata**

Director of the Management Control and Studies Bureau, Portuguese Civil Aviation Authority

The ECAC Network of Chief Economists was set up in 2016 with the objective of bridging the gap of incomplete knowledge of essential data in the air transport sector. It has the mandate in particular to list existing economic studies, statistics and other relevant materials on issues such as connectivity, taxation, airport charges, traffic data, route potential analysis, economic impact of regulations, air navigation services charges, etc. and to exchange views on permanent or current challenges faced by the aviation community. Chairing the Network since 2017, Ana Mata (Portugal) answers a few questions for ECAC News to present its recent activities.

What is the Network of Chief Economists? How does it relate to the Economic Working Group? How does it function?

The Network of Chief Economists (NCE) reports its activities to the Economic Working Group (ECO). Both ECO and NCE aim to support the understanding of economic issues of common interest to the aviation community within ECAC.

NCE's main goal is to bridge the gap of incomplete knowledge in essential areas related to economic matters. Its priorities are to identify relevant studies, material or data on issues such as, amongst others, connectivity, taxation, airport charges, traffic data, the economic impact of regulations, and air navigation services charges.

Sharing information and exchanging views on those relevant topics is also a priority. To address this challenge, it was considered crucial to establish a common and stable platform to list and exchange the relevant material.

NCE concluded a survey on economic studies and statistical information last year: how was this project led? What were the main outcomes/benefits?

Following Directors General's mandate at DGCA/147 in December 2016, the NCE launched a survey at the beginning of 2017 to identify the data, economic studies and statistics available in ECAC's Member States and, after assessing the results, to establish a common ground and a platform to exchange information.

Meeting of the ECAC Network of Chief Economists in October 2018 in Paris

The survey was designed to gather information on statistics and economic studies produced or co-produced by ECAC Member States, and it was divided into three parts: respondent profile, sources of statistical information, and information on the production of economic studies and statistical production for the period between 2011 and 2016.

With a response rate of 72.7% (32 out of 44 Member States), the survey also compiled the Member States' perspectives on the most relevant topics for the coming years.

More generally, what have been the NCE's main achievements so far?

In conducting its annual work programme, the NCE now aims to have an overview of existing studies available in ECAC Member States and to identify what new studies and statistics need to be developed to provide Members States with the relevant information on key economic issues.

Furthermore, and in line with the NCE's Terms of Reference, the group considered creating a common platform where that information could be shared. For that purpose, a dedicated page was created for the Network on the ECAC website, where studies and statistics recently published by Member States could be uploaded (on a yearly basis).

It was also decided to develop a forum allowing the members to exchange views and additional information. These exchanges would initially take place via email and an interactive platform could be developed as a further step.

The NCE is currently working on a survey related to airport charges and levies: What are main economic issues currently before the NCE? And more generally, what issues (if different) do you believe will become the air transport economics questions of the next decade? What topics do the Member States consider most pressing to analyse?

Following the results of the previous survey, a second survey was launched with the aim of presenting an overview of the airport charges' regulations and models applied at ECAC level, with a view to further developing research around airport taxation issues.

From the comments of the 32 Member States which responded to the survey, it was possible to conclude that most States are interested a further analysis of airports' charging models (e.g. cost–based vs price cap, single till vs dual till), the modulation of charges, and a benchmark analysis of the charges.

Regarding the areas that Member States consider most pressing to analyse on economic related issues, Member States have shown an interest in developing connectivity topics, airport and air navigation charges, and capacity and air fares related issues.

EXCERPTS FROM NCE TERMS OF REFERENCE
(August 2016)

« **1. The Network of Chief Economists has the mandate to:**

- Identify and list existing economic studies, statistics and other relevant materials on issues such as connectivity, taxation, airport charges, traffic data, route potential analysis, economic impact of regulations, air navigation services charges, etc.
- Share information on economic studies they intend to develop.
- Exchange views on permanent or current challenges for the aviation community with regard to methods (e.g. data collection, surveys, studies, strategic intelligence).
- Establish a platform for exchanging afore-mentioned studies, statistics and relevant materials as well as national and international data sources.
- Provide analysis in order to support policy discussion in the Economic Working Group, as requested and subject to resources being available.
- Share information on the impact of new technologies for air transport economics and the impact of macro issues on the air transport sector such as globalisation and migrations.

2. The Network of Chief Economists shall report on its activities to the Economic Working Group on an annual basis. This report may also include recommendations for further activities to be undertaken by the Network and/or on issues to be discussed at Directors General meetings. This report should include the draft work programme of the Network for the upcoming year. »

READ MORE
https://www.ecac-ceac.org/documents/10202/234214/TORs+and+Rules+of+Procedures+Network+Chief+Economists+%28August+2016%29.pdf/c74bea7b-2c48-48ed-af8f-7a76e413c98e

Ana Mata has been Director of the Management Control and Studies Bureau in the Portuguese Civil Aviation Authority (ANAC) since 2008, and Coordinator of the Economic Regulation Directorate since 2014. Her main activities relate to airport and air transport economic regulation as well as monitoring the civil aviation markets, and assessing the quality and availability of data. She also conducts several studies including the Statistical Yearbook and economic studies on the competitiveness of civil aviation areas and their impact on the Portuguese economy.
Ms Mata joined the civil aviation authority in 2000, working as head of the Air Transport Licensing Department. Ms Mata has a postgraduate degree in I&T – business engineering, a master's in management and strategy from the Lisbon School of Economics & Management, and a degree in business management from the University Institute of Lisbon.

European Parliament host to ECAC's 36th Plenary Session

Strasbourg, 10-11 July

Directors General of ECAC Member States gathered with high-level representatives from a range of ICAO Member States and international organisations, including ICAO, the European Commission, EUROCONTROL, EASA, IATA, and ACI EUROPE, on the occasion of ECAC's 36th Plenary (Triennial) Session at the European Parliament in Strasbourg.

Chaired by ECAC President Ingrid Cherfils, the Plenary Session heard addresses by ICAO Council President Olumuyiwa Benard Aliu (above), ICAO Secretary General Fang Liu, Ukrainian Minister of Infrastructure Volodymyr Omelyan, Director General for Transport and Mobility of the European Commission Henrik Hololei, and the CEO and Director General of IATA, Alexandre de Juniac.

Recalling ECAC's mission to promote safe, secure and sustainable air transport, ECAC Executive Secretary Salvatore Sciacchitano introduced the strategic topics of the discussions to be held on the first day of the Plenary, which focused on defining Europe's ambitions for next year's 40th ICAO Assembly Session. Aviation security and facilitation, safety and air traffic management, and aviation and the environment were each debated in panel sessions whose members included senior figures in European aviation and beyond. The meeting also welcomed addresses from ECAC's sister regional organisations (ACAO, AFCAC, LACAC), ICAO States (Israel, New Zealand, Singapore, United Arab Emirates, United States) and international organisations.

The meeting considered the reports on ECAC's activity since the previous triennial session in 2015, and adopted the work programme and budget for the next three years. It re-elected Ingrid Cherfils (Sweden) as ECAC President, and Patrick Gandil (France) and Alessio Quaranta (Italy) as Vice-Presidents, and elected Silvia Gehrer (Austria) as Vice-President for a first mandate. The Coordinating Committee was also pleased to welcome its newest member Bahri Kesici (Turkey). The full membership of ECAC's Coordinating Committee is available on the ECAC website.

For more information on ECAC's 36th Plenary Session, please visit https://www.ecac-ceac.org/web/ecac-36/welcome

ECAC Member State Portugal hosts Directors General summer meeting

Ponta Delgada, 30 August-1 September

For their annual meeting hosted by a Member State, ECAC Directors General were generously welcomed by the Portuguese Directorate of Civil Aviation in Ponta Delgada in the Azores, for three days of intense discussions.

On the first day, the meeting heard opening addresses from high-level Portuguese representatives Guilherme d'Oliveira Martins, Secretary of State for Infrastructure, and Vasco Alves Cordeiro, President of the Regional Government of Azores. Ana Amorim da Cunha, Regional Secretary for Transport and Public Works, and Luis Ribeiro, Chairman of the Portuguese Civil Aviation Authority, supported by former representative to the ICAO Council Helena Faleiro, presented the main principles and figures of air transport in Portugal and in the Azores, underlining the specific public service obligations applicable in the region.

For the fourth year in a row, ICAO Secretary General Fang Liu joined the ECAC summer meeting, where she delivered a substantial keynote address on ICAO's achievements, current priorities and forthcoming major initiatives, in which ECAC Member States play a critical role. She also joined the European discussions on security, safety, CORSIA advancement and air traffic management, providing her global perspective on the matters.

Under the leadership of ECAC President Ingrid Cherfils, the meeting focused on key aviation challenges, such as the urgency to address the capacity crunch in air transport with short-term mitigation measures and a longer-term sustainable strategy. On this critical matter, EUROCONTROL Director General Eamonn Brennan provided the facts and figures concerning the specific ATM challenges faced by Europe over the summer period. Austria's Director General (international) Silvia Gehrer presented the priorities of the current EU Presidency held by her country until the end of the year, while Director General for Mobility and Transport (DG MOVE) Henrik Hololei provided the meeting with the European Commission's perspective on aviation evolutions, EU policies and external relations. Other key players from the European aviation community, such as EASA Executive Director Patrick Ky, shared their most significant developments since the last ECAC Directors General meeting in May, and all actively contributed to the discussions. The meeting also launched strategic discussions on the European priorities for the 40th ICAO Assembly next year.

Spain will host the next ECAC Directors General Special meeting in 2019.

ECAC highlights ECAC-AFCAC cooperation at ICAO's third Security and Facilitation Symposium • Niamey, 18 July

Executive Secretary Salvatore Sciacchitano delivered a presentation on ECAC's cooperation with the African Civil Aviation Commission in aviation security, at the third ICAO Security and Facilitation Symposium, held in Niger. During a session on harnessing synergies to address the challenges of aviation security and facilitation in Africa, Mr Sciacchitano highlighted ECAC and AFCAC's shared activities in the security, facilitation and environment domains, and the importance of promoting mutual understanding on policy matters amongst States. He also spoke about the CASE Project and the activities organised within the framework of the Project to support ICAO's No Country Left Behind initiative, the AFI SEC/FAL Plan and GASeP implementation.

ECAC contributes to ICAO Global Aviation Gender Summit

Cape Town, 8-10 August

Deputy Executive Secretary Patricia Reverdy participated in the first Global Aviation Gender Summit organised by ICAO and the South African Civil Aviation Authority. Attended by over 500 participants representing both regulators and industry stakeholders in the fast-evolving sector of air transport, the Summit represented an excellent opportunity to discuss gender equality in the sector and the importance of education – especially science, technology, engineering and mathematics (STEM) education – for younger generations. Ms Reverdy contributed to the panel focusing on leadership and equality, underlining the specific roles of both mentoring and coaching in supporting the professional development of young professionals.

#TimeIsNow
Global Aviation Gender Summit
Cape Town, South Africa | 8 to 10 August 2018

Events to come

NOVEMBER

5/ 7th meeting of the European Aviation Environment Working Group (EAEG/7) (conf call)

5/ 3rd Environmental Programme Management Group (EPMG/3), Paris (DGCA)

6/ 183rd meeting of the Coordinating Committee (CC/183), Paris

7/ 39th meeting of the Common Evaluation Process (CEP) Management Group (CEP-MG/39), Paris

7/ 7th meeting of the Economic Working Group (ECO/7), Paris (DGCA)

7-8/ EaP/CA Project workshop on cargo and mail screening, Luxembourg

8/ 9th meeting with security equipment manufacturers involved in the Common Evaluation Process (CEP) of security equipment (CEP-Manuf/9), Paris

13/ Workshop on General Aviation Accident Investigation, Valletta

13-14/ 8th meeting of the European Aviation and Environment Working Group (EAEG/8), Paris

14/ 49th meeting of the group of experts on accident investigation (ACC/49), Valletta

14-15/ CASE Project regional workshop on behaviour detection, Accra

14-16/ Best Practices on Covert Testing, Skopje

16/ 28th meeting of the Security Programme Management Group (SPMG/28), Rome

16/ 9th meeting of the European Aviation and Environment Working Group (EAEG/9), Paris

28-29/ EaP/CA Project workshop on training and certification, Paris

DECEMBER

2-3/ CASE Project workshop on vulnerability assessments (CASE-WSVA/2), Amman

4/ 11th ECAC Forum of Directors General (FORUM/11), Paris

5/ 151st meeting of Directors General of Civil Aviation (DGCA/151), Paris

10-11/ 2nd ECAC Environmental Forum (ENVFORUM/2), Paris

11-12/ Workshop on Insider Threats, Dublin

18-19/ 10th meeting of the European Aviation and Environment Working Group (EAEG/10), Paris

Executive Secretary joins international debate on policy solutions to aviation development impediments at ICAO World Aviation Forum

Fortaleza, 17-19 September

ECAC Executive Secretary Salvatore Sciacchitano participated in a high-level interactive discussion panel addressing public policy solutions to aviation development impediments during the session on "Promoting investment for aviation development" at the fourth ICAO World Aviation Forum (IWAF/4) held in Brazil. Mr Sciacchitano shared some of the conclusions reached at the ECAC/EU Dialogue with the air transport industry in Rome last year, highlighting the strong interest in investing in aviation despite the risks, and that private capitals are available. He underlined that while there are resources, some constraints, such as the infrastructure capacity crunch, regulatory fragmentation and restrictive provisions for market access, limited their mobilisation.

EaP/CA IN BRIEF

Project Steering Committee meets in Kazakhstan

Astana, 27 June 2018

The Committee discussed the implementation of activities from July 2017 to June 2018. In relation to planning security activities, the Project Steering Committee supported the implementation of new security activities that will focus on the following areas:

1) Strengthening the capabilities of beneficiary states to implement compliance monitoring activities.

2) Providing support to beneficiary states in reviewing and improving national civil aviation security programmes.

3) Enhancing knowledge on best practices in implementing aviation security measures and mitigating existing current threats to aviation security.

Cargo and mail security mentoring activity for Kyrgyzstan

Paris, 28-30 August 2018

The main objective of the mentoring activity was to review Kyrgyzstan's legal framework in the field of cargo and mail security, and to provide proposals to amend and further develop the regulatory requirements, taking into consideration ECAC Doc 30 Recommendations.

In the course of the mentoring activity, the security expert from the Latvian Civil Aviation Agency, together with the officials of the Kyrgyz Civil Aviation Agency, examined the provisions of the aviation law, the National Civil Aviation Security Programme (NCASP), the National Civil Aviation Security Training Programme (NCASTP) and the National Civil Aviation Security Quality Control Programme (NCASQCP). As a result, several modifications to the draft aviation security law and national programmes were proposed in order to further strengthen their cargo and mail security regime.

News from the JAA Training Organisation (JAA TO)

Albanian CAA receives in-house training courses from JAA TO

Paula V. de Almeida, *JAA TO Director*

July and August were very active months for staff at the Albanian Civil Aviation Authority (CAA). After the Training Needs Analysis (TNA) – a new programme provided by JAA TO exclusively to the CAAs of ECAC Member States –, the Albanian CAA requested JAA TO's services for a few training courses considered to be relevant to the Albanian CAA inspectors. Some courses have already taken place. We interviewed the CAA Executive Director, Krislen Keri, and talked to others in the CAA to find out how the training is going so far.

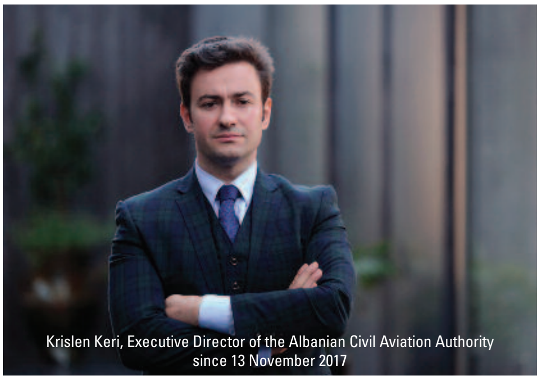
Interview with Krislen Keri, Executive Director of the Albanian Civil Aviation Authority (CAA)

1. Mr Keri, what are the CAA of Albania's goals and priorities for the coming years?

Mr Keri: The Albanian civil aviation sector is undergoing some major developments as the Albanian government seeks to develop two additional airports, one in the north of the country and one in the south. These objectives come at a time when the Albanian air transport market has witnessed a considerable increase in traffic numbers, and the aim is to offer airport services diversification. However, a strong industry needs a strong regulator and we are working hard to achieve full compliance of national regulations with the *acquis communautaire,* in order to achieve European standards in aviation regulation.

2. How has JAA TO helped CAA Albania in the achievement of such goals? Did the Training Needs Analysis (TNA) help?

Mr Keri: We believe that a major contribution to a strong regulator is an adequately qualified staff. For this, the Albanian CAA has paired with JAA TO to tackle staff competencies' needs. The ICAO TNA tool was part of this process. Through this joint exercise, we managed to do a full gap analysis of our staffing needs and technical competencies and then moved on to a tailor-made training solution. We are in the process of organising five in-house training courses for 50 people, and all of this within six months, giving us a chance to reach the latest developments in the field.



Krislen Keri, Executive Director of the Albanian Civil Aviation Authority since 13 November 2017

3. How have the courses been so far?

Mr Keri: The feedback from our inspectors is great. Some of them have gained new knowledge of their functions and others are updating their knowledge in specific fields, according to best international practices.

4. What is the next step?

Mr Keri: According to best international practices, training is not all that is needed to gain the appropriate competencies to exercise our duties. Other major components are on-the-job training (OJT) and the transfer of best experiences from qualified European inspectors. Thankfully, in this regard we have already collaborated with the Italian CAA (ENAC) via a Memorandum of Understanding signed between our two organisations. We are especially thankful to ENAC Director General, Alessio Quaranta, for this joint undertaking, which will help us accomplish the next steps.

CAA Albania takes the "ICAO & EASA Safety Management System Requirements – Introduction" course

During the week of 24 July, JAA TO trained the professionals from the Albanian CAA. The "ICAO & EASA Safety Management System Requirements – Introduction" training was a three-day course. Its objective is to develop and implement an effective Safety Management System (SMS), and this is one of the biggest challenges in modern aviation organisations. The course delivered that week at the Albanian CAA provided its delegates with the opportunity to meet such challenges head on.

Participants learn with the JAA TO-qualified instructor Bas

We asked CAA Albania why they had asked for this specific course, and they replied: "The Albanian CAA identified this as one of the courses needed for a better qualified and efficient staff, able to exercise its national regulatory competencies and fulfil the requirements of international organisations such as ICAO and EASA", said Megi Xharo, International Relations, CAA Albania, on behalf of the team. "We recommend this course to staff starting out in the regulatory aspects of civil aviation, as it serves as a basis to better understand and fulfil ICAO's and EASA's requirements in safety management", said Ms Xharo.

The JAA TO-qualified instructor, Bas, provided them with the tools, knowledge and methodology to successfully implement an SMS in their organisation.

CAA Albania takes the "Human Factors/Crew Resource Management" training course

In the second week of August, JAA TO delivered another training course at the Albanian CAA. This time, training was on "Human Factors/Crew Resource Management".

Delegates at the Albanian CAA during training class and assignments

"I believe this course is very important, as human factors affect human performance daily. Awareness is raised about human performance limitations and the factors that affect it, so we can improve human performance. The training course is interesting as it covers many issues, such as the history of crew resource management, stress and workload, sleep and fatigue, human errors, and threat and error management", said Erjon Tema from the Albanian CAA.

"I highly recommend this course to all inspectors, to help raise awareness of all the factors affecting human performance and how to better apply these methods", he added.

Why JAA TO and why in-house?

"I personally believe that JAA TO is one of the most important training organisations in the field of civil aviation", said Mr Tema. "JAA TO is one of the most accredited training institutions in the field of civil aviation. We have had a great experience throughout the years, with many of our inspectors continuing to improve their skills to become more efficient in accomplishing our goals, and we are looking forward to completing the rest of the courses", said Ms Xharo on behalf of the team.

JAA TO delivers training course at the Albanian CAA

Asked why the Albanian CAA chose to have the training course delivered at their location, they said: "This course, as well as some other important courses, are currently underway in the Albanian CAA. I believe it is cost effective and a unique and interesting idea."

If your company or CAA would like to have an in-house JAA TO training, submit your request to: https://jaato.com/trainingoutside/

ECACNEWS provides an overview of the activities of the European Civil Aviation Conference. ECAC makes no warranty, either implicit or explicit, for the information contained in this document, neither does it assume any legal liability or responsibility for the accuracy or completeness of this information.

Opinions expressed in signed articles are the author's opinions and do not necessarily reflect those of ECAC. Reproduction in whole or in part of all unsigned material is freely authorised. For rights to reproduce signed articles, please contact the ECAC Secretariat.

ECACNEWS is published by the European Civil Aviation Conference (ECAC)

FOR MORE INFORMATION,
PLEASE CONTACT:
ECAC Secretariat
3 bis, Villa Emile Bergerat
92522 Neuilly-sur-Seine Cedex FRANCE
Tel. : +33 1 46 41 85 44
Fax : +33 1 76 73 98 57
secretariat@ecac-ceac.org
www.ecac-ceac.org