Air Transport Security

2040 and Beyond


IATA
Strategic
Partnerships

Table of Contents

Introduction

In June 2019, IATA hosted a Blue Skies industry forum at the EUROCONTROL headquarters in Brussels that brought IATA's security Strategic Partners, member airlines, airports, regulators, manufacturers, industry experts and academics together to discuss the future of broad aviation security strategies, as well as the types of threats and new challenges that may be faced in the coming years.

The outcomes of the forum culminated in the production of this White Paper.

The predictions and views expressed in this paper are therefore not necessarily those held by IATA, but rather reflect the topics and trends identified by the participants as possible realities and challenges the industry may face.

This White Paper is issued as a Version One and will evolve along with industry's thinking in the coming years. Its aim is to stimulate discussion within and across the sector and all its actors, ideally to facilitate further development and innovation to help industry and wider stakeholders better prepare and respond to the known threats of today and the unknown, evolving or emerging threats of tomorrow.

Executive Summary

The practical realities of the way Aviation Security measures are implemented and evaluated have seldom changed in recent decades. This is specifically the case when compared to the rate of change and innovation experienced in other parts of the sector. New approaches in the way technology and processes have been introduced continue to improve the safety commitment to the traveling public, yet we still deal with known threats and risks in fundamentally the same way – new and/or additional layers of screening/security. But how about the unknown threats, or the ones that are only beginning to emerge and/or make a noticeable impact?

Arguably, today's ICAO Annex 17 baseline has successfully defended the industry against a repeat of the same form of attack; but does today's baseline provide meaningful defence and perhaps deterrence against the unknown or rapidly evolving threat vectors of tomorrow?

With many believing passenger numbers will continue to grow year-on-year, infrastructure capacity constraints becoming more commonplace, new security threats emerging, and rising expectations from passengers, consumers and investors to evolve the way we do business, there is little choice but to rethink our current approach. Moreover, we should at least take the time and effort to evaluate where we are on the spectrum of change and posit a path in those areas of improvement where required.

The physical security overlay we know today is unlikely to disappear entirely. Arguably, it is an essential base layer to build resilience into our system and to help mitigate the threats that we do not yet know about. However, increasingly, security may become an amalgamation of measures, some physical and others virtual; those that happen at the airport, and others that start as soon as passengers/consumers place an order to travel or ship goods. This evolution of security controls needs to be considered in the context of the future we may be faced with.

In 2040 our lives will be more connected – with a greater reliance on data and automation. The world will continue to change – geopolitically, environmentally and economically. The industry too will change and evolve, becoming increasingly efficient, multimodal and optimized through new levels of connected information. This type of future brings with it numerous opportunities to improve the way we do business. But it also opens us up to new vulnerabilities and greater exploitation of those that already exist.

What is clear, is that the domain of aviation security is perhaps not evolving fast enough. Especially if we are ever going to be viewed as not just a necessary overhead in cost but a silent enabler to growth, connectivity and stability. And thus, without self-evaluation and without organizations taking the time to theorize and challenge legacy tenets, complacency and institutional biases are themselves risks to the industry.

Technology is one part of the solution, but it is not the only one. We need to fundamentally change our thinking and consider how we protect the industry and ensure that the measures we are putting in place are protecting us from the most likely and plausible threats. Measures at airports are an important layer, but they will do little to protect us if future threats come from the sky for example.

While being cognisant of what we need for today, we must start to consider what approaches and mitigation strategies exist to tackle new threats, especially those that need to be urgently developed in the coming years to ensure we stay ahead, or at least in step with, our adversaries – not all of whom may be directly targeting aviation and/or wishing to intentionally cause physical damage or potential loss of life. For example, economic threats could be directly or indirectly the result of climate change and/or activism in many forms and across a wide and diverse range of issues.

At a high level there are several key steps that can help industry better prepare and respond to threats, including improving our agility, resilience and collaboration as well as our approach to regulation and standards development. And, for those threats that are already well known, there is more that can be done. In particular, better investment in technology, improved systems design, contingency planning, mental health support, and improved situational awareness, not least in respect of issues that often revolve around social media and/or new generational causes or concerns that may lead to aviation impacts that may not traditionally have been viewed, and reacted to, from a threat scenario perspective. But will it be enough?

In 2020, building on the work already achieved in 2019, IATA will host a second Blue Skies Industry forum. Participants will again be asked to think-outside-the-box, with the emphasis in 2020 on potentially new, innovative and/or radically alternative mitigation strategies to the evolving vulnerabilities and threats previously identified – those mitigation actions and strategies that we already have, and those that will need to be developed.

This means that innovators, disruptors, academics, activists and manufacturers from within the sector, and importantly from outside it, will be essential participants in this exercise. In addition, it will be critical to the success of the forum to ensure generational and/or aspirational differences are recognised and represented e.g. Generation Z, millennials and others must be actively encouraged to constructively participate. Without their support today, it is unlikely we will be ready to face the reality of tomorrow and deliver on the fundamental promise of the industry to provide safe, secure and relevant air transport to citizens of the world – particularly where an increasing percentage of those citizens are aged under 25 or have yet to even be born.

Three Key Questions

1

What will the future look like?

What will be happening in our world in 2040 – politically, economically, socially – and how will this have impacted the growth and development of the aviation sector?

2

What will the threats to aviation security be in 2040?

Will existing threats evolve and manifest in new ways, or will entirely new threats emerge that challenge the security and economic viability of the air transport sector?

3

How will we mitigate the risks?

How do we plan intelligently for the future today and ensure we are ready and effective in our capabilities to face the challenges of 2040?

Changing geopolitical dominance and increased societal engagement.

Increasingly connected, driven by data, new technologies and rising service expectations.

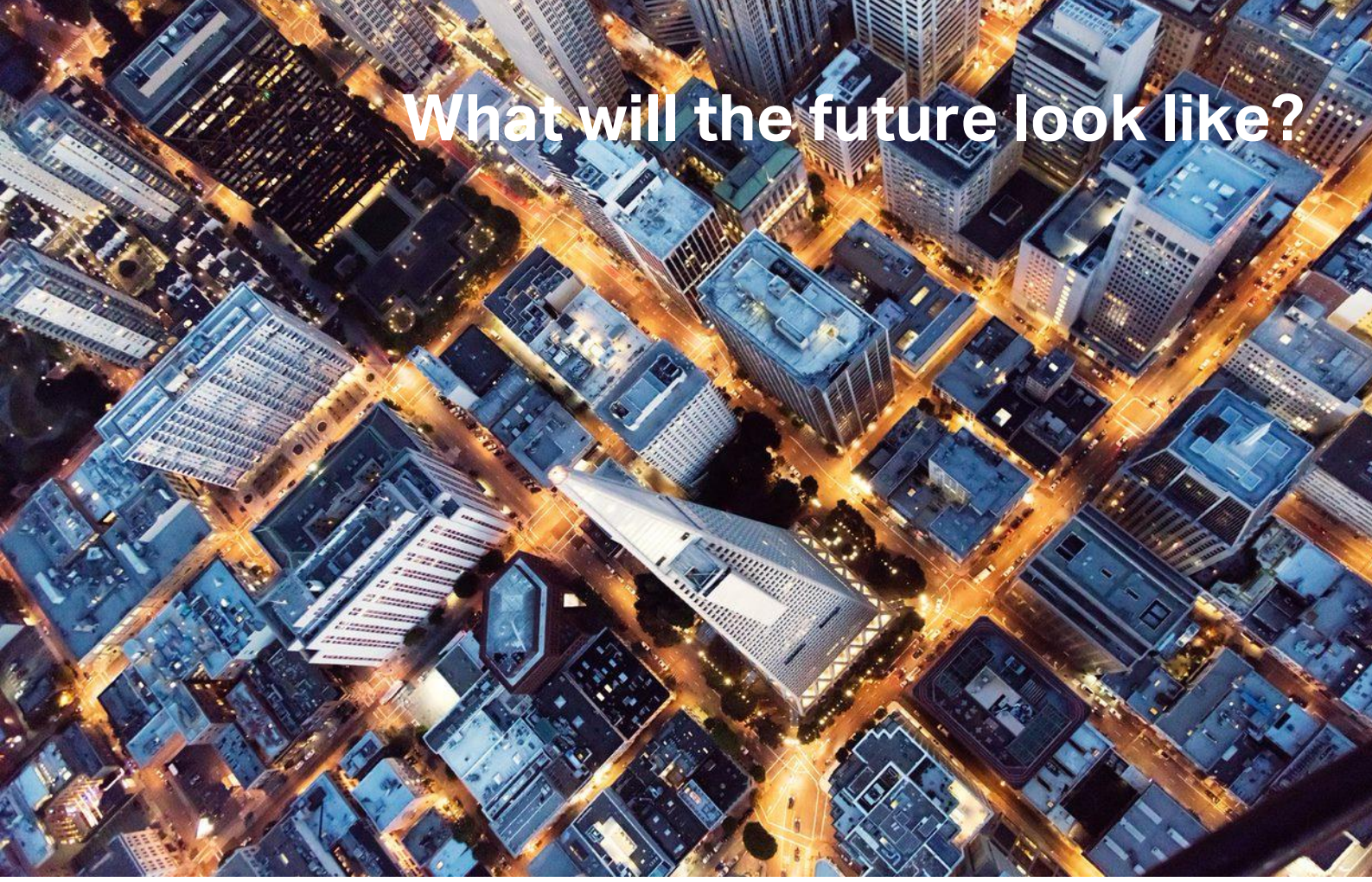
Sustainable, seamless, multimodal transport will be the norm for many and the aspiration for the rest.

Traditional threats such as cyber, insider, and terrorism will remain.

Activism, mental illness, unmanned vehicles and biological threats and infectious disease will be an increasing focus for the security sector.

Agility, trust, standards, capacity building, strategic use of human resources and sensible regulation will be central to mitigation strategies.

Targeted, threat specific measures will also be important.



What will the future look like?

Nine major trends are expected to impact how Air Transport is organized and delivered across the globe in the coming 20 years:

Connectivity and New Technologies

Life in general will be more connected by 2040, with high service expectations. Business and organizations will have an increasingly customer service focus, largely premised on the juxtaposition of privacy versus customised service, with technology integrated and central to every experience.

Technology innovation and adoption will continue at a fast pace. At times, policies, standards and regulations will struggle to keep up.

This adoption will lead to cultural changes in the way we interact with information and each other:

- The general population will be better informed with access to real time information on demand;
- Tolerance for slow, inaccurate or insecure information exchange and/or service delivery will decrease; and
- It will become increasingly difficult for businesses and organizations to control their own narrative, particularly in the wake of any major events or incidents.

> "The world will be increasingly complex, dynamic and fast, as well as considerably more connected."

Facilities and spatial needs at airports may be reduced due to technology enabled optimization. For physical security controls, the increase in computing capacity and the resulting integration of technologies will enable the industry to increasingly automate all aspect of detection and alarm resolution – with virtually zero false alarms across multiple-threat vectors.

At the same time, this will mean that business and industry will be increasingly reliant on technology to deliver services and keep the skies safe. Outages and disruptions to systems (whether intentional or accidental) will cause major havoc for air transport systems, disproportionately impacting more advanced and optimized set ups.

Artificial intelligence will also play a greater role in the operation of the aviation sector. To what extent we see progress by 2040 will largely depend on the ability for regulations and standards to keep pace. However, the technology will be available should industry choose to use it.

Data Protection, Privacy and Cyber

As in today's reality, data in 2040 will be a high valued commodity. It will drive business connectivity and innovation, enable seamless integration of systems and processes, as well as facilitating risk assessments for improved resource and asset optimization.

In this context, concerns over privacy and data protection will continue, and will possibly be the source of a degree of activism as individuals fight for their civil liberties.

Some governments may struggle to strike a balance between security and privacy. While others will rapidly endorse and adopt the use of data both for societal and security purposes. As these differing regimes emerge, compliance with national privacy requirements may become increasingly complex for businesses operating and handling data across jurisdictions (airlines included).

This increased reliance on data and connectivity will further exacerbate cyber security risks. This includes traditional cyber security threats that we consider today (airport systems, on board systems etc.) but also wider system vulnerabilities including remote monitoring and access functionalities that could exist in an entirely different state.

On a more general level, discussions have already begun regarding ownership of cyberspace, which could give rise to sovereign claims and disputes in the coming years.

Changing Nature of Air Transport

Aviation, particularly the short haul sector, will face increasing competition from other modes of transport.

Environmental concerns may also exacerbate this, with social movements increasingly critical of air travel and other modes of transport perceived to be contributing to excessive environmental impact.

Multimodal

Airlines will likely seek to address this by adopting alternative modes of transport into their business models.

Multimodal arrangements are already in place today and provide an example of how this may work in the future. For example, Air France and SNCF (the French rail provider) offer connected end to end train/air journeys on one ticket, and in Hong Kong, passengers can purchase various integrated airline and ferry combination tickets.

The biggest change in 2040 however, will not be that airlines embrace multimodal travel, but rather that multimodal travel will encompass far more than just air and ground transport.

Autonomous vehicles, drones, air taxis and delivery services may all form a part of this connected system. The flow-on effect from this is that the connected passenger or cargo journey may well start at home, necessitating airport like services, security and facilitation earlier in the process.

> "Multimodal is the future of the transport industry."

Aircraft Design

New aircraft design will be high on the list of priorities, particularly in the face of environmental concerns.

It is likely, at least in densely populated regions and hubs, that new small aircraft suitable for distributed modes of air transport will emerge.

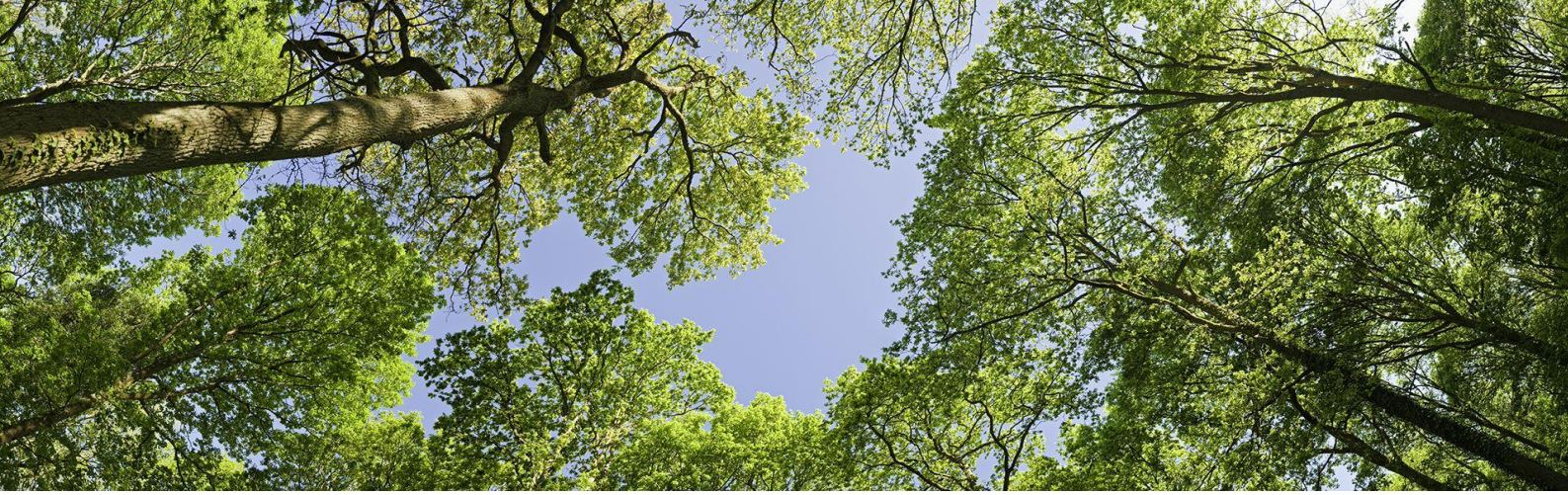
On board design and materials may also evolve, making aircraft faster, but also helping to mitigate against security threats (e.g. on-board sensors for detection of chemical and biological threats, use of more resistant materials that could withstand greater blasts or collisions).

However, despite the focus on this kind of development, it is unlikely that by 2040 there will be widespread adoption. Thus, airspace and aviation infrastructure will need to continue to cater to mixed fleets of varying aircraft types and sizes.

Airport Development

New aircraft types and changing modes of transport may impact the type and location of infrastructure required, potentially expanding beyond today's existing airports and flight paths. This may also have an impact on how airports are designed and utilized and resultant customer experience requirements or expectations.

Airports currently under development may be able to factor these considerations into planning and design. Existing airports however, may face more challenges in adapting to new operating requirements. In this context, it is important to note that there are no new major airports being constructed in the West, thus Europe and the United States may suffer the greatest impact.



Nationalism, Geopolitical and Policy Evolution

2040 may bring with it diffusion of political power, with the United States and Europe increasingly sharing the global political stage with Asia and other emerging economies.

Facilitated by growing populations, the air transport markets in Asia (as well as other parts of the world) are reasonably expected to continue to grow, as will their influence in the development of standards and norms for the industry.

At the same time, we may see a continuation of today's nationalism and protectionism trends by states both in terms of industry and business, as well as information sharing. And while more data may be available than ever before, it is uncertain whether this information will be openly shared between states in order to facilitate harmonized and streamlined air transport processes.

For aviation security, this may make reaching global recognition and agreement more difficult. The trend of imposing extraterritorial measures is likely to continue in this type of climate.

Widening Capability Gaps

Existing economic disparity and disproportionate regional population growth will exacerbate capability gaps going forward. This may be evident across several sectors, but for aviation, gaps between countries in terms of aviation security and facilitation capabilities are already apparent.

Some states are advancing rapidly, making the most of intelligence, data and new technologies, whereas others continue to struggle to meet existing baselines and global best practices. It is inevitable that some countries will be left behind. They simply won't have the infrastructure, funds, resources or political support to effect major change.

Whilst the gap exists today, it is expected that it will widen in the coming years, possibly resulting in a two-speed security and facilitation system.

On a much larger scale, these social and economic gaps could also lead to increased social unrest and uprisings.

> "Despite the Air Transport system being an increasingly evolved ecosystem where actors collaborate in an effective and mutually supportive fashion, the world will be even more divided in terms of technology, capability, funding and operational delivery."

Environment and Sustainability

Climate change and questions over sustainability will have a major impact globally. Some governments will adapt well, proactively planning to address the issues. Others however, will not have the political influence or resources to act in time.

As a result, some cities may literally be under water by 2040. Others may be facing increased resource shortages and significant changes in quality and way of life. This in turn will likely result in an increasing number of displaced persons and possible conflict, providing ideal breeding grounds for social unrest and potentially terrorism.

For the transport sector, an increase in the number of severe weather incidents will result in more cancellations, delays and disruptions to the global system.

Increased political pressure and activism may force the hands of many governments to start reducing emissions and improving the way businesses take responsibility for their impact. A sustainable transport system will be the primary goal in many states. Strict regulations could follow for both businesses and individuals, which in turn may help drive innovation.

Terrorism

Terrorist attacks in public places (not just airports) are likely to continue over the next 20 years. Attack methodologies will no doubt evolve, with continued use of readily available objects and substances (e.g. vehicles and guns) expected in the context of attacks on public spaces.

With increasing ease of access to information via the internet, lone wolf, or small locally planned attacks will be far more commonplace than large scale organized operations. These attacks may be instigated and supported by well-known terror groups, though their direct involvement in planning may be difficult to establish.

Terrorists may start focusing on other aviation targets, such as cargo, catering, stores and general aviation. As airport security and defence systems improve, attacks against softer targets, such as landside, may also increase.

State actors (or their proxies) may also become more active, using disruption of the aviation sector to achieve their political objectives, potentially via economic and operational disruption rather than direct violent action.

Passenger growth and the need for larger capacity will drive the social and cultural growth of airports. With more passengers and staff, terrorists may seek to exploit the insider element and may more easily be able to do so.

Activism

Activism is on the rise, and in many states may be the new means by which citizens try and effect change on political and social regimes. Human rights, freedom of speech and movement, as well as environmental and quality of life issues may dominate activism activities in the coming years.

These kinds of protests – where airports, airlines, or the sector are the target – have the possibility to significantly disrupt operations, but also risk lives. 2019 events in Hong Kong provide a good example of the disruption that activism can cause to the air transport sector.

Moreover, large-scale drone activity targeted towards airports during 2018 and 2019, helped raise awareness of the potential collision and ingestion risk that aircraft face when drones invade the airspace (even if not the intention).

While these kinds of protests have remained peaceful in today's context, it is likely that more radical elements within these groups may stray towards direct and combative protest styles. There is also a chance that the lines between activism and terrorism further blur.

Health and Disability

An increasing aging population in many countries will change the way in which airports and airlines cater for their passengers. As air travel becomes more comfortable, it is also more accessible for those with disabilities, thus numbers are expected to increase. With many states implementing new and increasingly strict requirements regarding the rights of passengers with reduced mobility (which take into consideration factors such as age as well as disability), the aviation sector may need to do more to provide for these passengers. New services may be required, and facilitation will become more complex – including, potentially, an increasing requirement to screen/secure medical/age related apparatus, medicines and/or other items that require new, additional and/or time-consuming screening processes.

Mental illness issues, or at least acknowledgement of them, is increasing in society in general. In addition, the long-term impact of technology immersion as part of day to day life has yet to be fully understood and may further exacerbate the issues. For aviation, with an increasing number of crew, staff and passengers, the issue of "mental illness" will be a challenge for the aviation industry both in terms of facilitation and prevention/resolution of incidents.

From a more general health perspective, the interconnectivity provided by air transport, growing ease with which tickets can now be booked and an increase in passenger numbers provides a vehicle for faster spread of illness, contagions and possible pandemics. Airlines and governments already take steps to manage this today, but efforts may need to be stepped up in the future, particularly if this becomes a viable threat vector for terrorism or extreme activism.

What does this mean for the way people, baggage and cargo travel?

To what extent the trends discussed will influence the development of the aviation transport sector is still unknown.

The generally held 2040 industry vision (for both passengers and cargo) is one of personalized, seamless, non-intrusive, integrated journeys facilitated by digital identification, self-service options, automation and rapid technology development. Intelligence based decision making, data, connectivity and harmonization are all central to this vision.

There is a level of consensus that the capacity and technology already exist to deliver this end to end seamless experience. However, there remain several critical uncertainties with regards to the pace of change:

- Regulatory, policy, privacy issues – to what extent and at what pace will national and international regulatory bodies be able to develop robust and comprehensive regulatory frameworks?
- Geopolitical issues and collaboration between states – will the world be increasingly fragmented/multipolar, or will the pendulum swing back towards international collaboration?
- Data availability – to what extent will states/stakeholders/individuals be willing to share data?

Depending on how these elements evolve, we may not have achieved the idealistic industry vision by 2040, but rather may be faced with slower, incremental change, i.e. a progressive evolution of today's reality.

That may mean less standardization, collaboration and information sharing between states; remaining regulatory and privacy barriers; technology unable to be implemented to its fullest extent; and customer attitudes and willingness to accept innovation having moved little from where they are today.

These two scenarios are not distinct and different futures, rather an evolution along the spectrum. Thus, the vulnerabilities, threats and mitigation strategies discussed in the following sections are those that remain plausible and possible in both.

What will the threats to aviation security be in 2040?

What are the likely vulnerabilities and threats in 2040 and which actors will be involved?

Vulnerabilities

In 2040 vulnerabilities will exist that could be exploited by those seeking to do harm or simply disrupt. Some of these vulnerabilities already exist in today's transport system, others will evolve with industry growth and technology development.

- 2040 will bring with it a heavy reliance on data, connectivity and automation. While this vulnerability exists to some extent today, the situation will be much more critical in 20 years' time.
- In some states increasing passenger numbers will exacerbate reliance on data and connectivity, while in others it will result in capacity constraints and significant congestion landside.
- Delayed roll out or development of critical technologies, particularly in certain parts of the sector where adoption may be slower – such as cargo, stores and vehicle screening and security - may create opportunities for those with mal intent to infiltrate or compromise the system.
- As a public space, often the jurisdiction of different agencies, deployment of effective technologies, as well as ability to respond to landside security threats will remain challenging for security services.
- Despite increasing automation being critical to future operations, people will always be part of the security system, and thus will remain a resource that can be exploited. As more and more aviation related activities move off airport, or become virtual, the pool of people within scope, as well as their location, also changes.
- Activism and disruptions at airports or targeting aviation will remain a vulnerability that can be used by those with mal intent. However, prevalence may increase in the future as individuals become more aware of the impact that can be achieved.
- Mental health issues, which as noted, are a growing societal problem, may result in direct threats to aviation security, or may simply provide a larger group of individuals who are more vulnerable to exploitation.

Actors

Many of the actors that pose a threat today will do so in the future – terrorist organisations, insiders, lone wolves.

However, activists and state actors may play a more widespread role in the future.

Threats

It is expected that eight key threats will dominate the 2040 landscape:

- Cyber
- Insider
- Terrorism
- Activism
- Autonomous/Unmanned Vehicles
- Air Cargo and Supply Chain
- Mental Illness
- Biological and Infectious Diseases

Cyber

While not new, the possible impact of cyber security threats will be greater in 2040 thanks to the increased reliance on technology, connectivity, data and Artificial Intelligence (AI). Cyber-attacks may evolve from low scale/annoyance to sophisticated crippling incidents.

Today, most of the critical security infrastructure and systems are run locally at airports, often on different networks to other airport systems. In 2040 however, more and more services and processes will occur off airport, remotely, or online, necessitating connectivity with a wider range of public and private networks. This will exponentially increase the possible attack paths available to those seeking to infiltrate and exploit the system.

Basic systems breaches, compromised or tampered data, identity theft, and disruptions (including via deliberate power or systems outages) will continue to be a focus for those seeking to attack the system. All of which have both direct and indirect consequences.

However, there is also a risk that the systems themselves, as an isolated attack or part of a wider plan, will become the target. For example, hacking X-ray or CCTV systems to allow people or prohibited objects to pass through uninhibited. Dormant technology could even be deployed inside such systems before they leave the manufacturing warehouse, giving insiders the opportunity to access data or systems in the future once equipment has been deployed.

Air Traffic Control (ATC) and aircraft themselves are not immune to cyber-attacks. The increased number of aircraft in the sky, as well as new entrants such as drones, will mean that airspace management becomes more autonomous and more connected. There are risks that aircraft themselves will be deliberately targeted, or that ATC systems will be hacked to send incorrect information to pilots, with potentially fatal consequences.

What is clear, is that this is a critical and growing area of concern for the aviation security sector. And there is an urgent need to better understand the real impact and risks so that appropriate strategies and protocols can be put in place to minimize the risks.

Insider

Like cyber, the insider threat is not new but may manifest differently in a more connected and automated 2040. Moreover, the insider threats may or may not be terrorism related. Insiders may present less risk to physical security systems, instead choosing the virtual (cyber) realm as their preferred attack methodology.

As a result, the scope and range of insider threat widens – from those that simply have physical access to restricted areas at airports, to those that have access to systems and data. Importantly, these insiders may work for external companies or subcontractors, not subject to same level of background checks and vetting as those physically working at the airport. Indeed, they may even be in an entirely different country, where rules and regulations around cyber security, privacy and access control differ.

While systems and processes may become more automated, there will always be people involved to make decisions and to take actions when needed. People develop, install, operate and maintain technology. Thus, these people will always be a target that can be exploited. In a security screening context for example, this may manifest via manipulation of X-ray images, records, algorithms and equipment detection levels.

In this context, deliberate exploitation through social engineering may play an increasing role in such attacks, potentially across borders. At the same time, risk may also come from those who make simple mistakes, particularly in a virtual sense, allowing would be perpetrators access to critical systems or facilities.

Terrorism

Terrorist attacks against aviation are expected to continue. As noted above, in 2040 there will likely be an increased focus on the use of insiders and cyber as an attack vector. Traditional attack methodologies (i.e. use of Improvised Explosive Devices (IEDs) and weapons) will probably continue, with targets possibly expanding beyond the aircraft itself (i.e. landside, cargo, critical infrastructure) and new technologies such as drones could be used as a more covert means of deployment, facilitation and/or reconnaissance.

With a more distributed network and an increasing cohort of potential lone wolf attackers, terrorists could seek to opportunistically exploit disruptions caused by IT and power issues, extreme weather events, strikes/protests etc. These types of attacks would likely be low complexity, targeting crowds of people gathered in public areas of airport terminals during such disruptions. Thus, these types of attack may be difficult to predict ahead of time, and as a result, harder to prevent. The more complicated variation of this threat is where terrorists first create the disruption to maximize the impact of an already planned attack.

Use of conventional explosives and IEDs will probably evolve with terrorists using increasingly complex concealment methodologies. There are also concerns that terrorists will focus on development of new weapons which may be able to defeat less advanced security equipment. Slow uptake of new detection technologies in certain parts of the world could therefore increase the risks in these locations. 3D printing is seen as a threat in this regard as it is now much cheaper and by 2040 could be much more widely available allowing organizations and individuals to print their own weapons at home.

Another area of concern is the evolution of the suicide bomber. Rather than carrying explosives, the suicide attacker could be carrying infectious diseases or bacteria (i.e. the individual becomes the weapon). Such attacks may be difficult to detect, and even harder to prevent once the attacker has reached the airport. Impact may not be limited to a single airport, but rather could rapidly spread throughout the interconnected transport network resulting in major worldwide pandemics.

Activism

Political activism has only recently started to touch aviation operations, with protest and disruptions taking place on airport premises making it difficult for security agencies to both protect passengers and protestors as well as carry out necessary security functions.

Perhaps more concerning, are spin-offs from some of the major activist groups. These groups or individuals may be willing to take more extreme action when initial passive protests have little effect. Threats to deliberately, en-mass, target airports and aircraft by violent means for political purposes could have dire consequences for aviation safety and security.

Also, as noted, terrorist organizations could seek to take advantage of such activities (which are generally well publicized), in order to create maximum damage. Thus, this potential combination of violent activism and terrorism is a concerning problem for the future.

Autonomous/Unmanned Vehicles

Although drones and autonomous/unmanned vehicles offer numerous opportunities for the aviation sector, as well as for urban planning and society in general, they also pose possible security risks.

Drones and other land and water based autonomous vehicles may be used to:

- breach perimeter and airport drainage systems to deposit prohibited items and weapons airside;
- conduct reconnaissance activities in support of possible attacks;
- cause major disruption to airport and airline operations (either in isolation or in swarms); or
- directly target an aircraft or airport facilities with the intention of causing mass loss of life.

While military grade hardware is not readily available today, it is expected that by 2040, technology will have significantly progressed such that advanced drones, and other autonomous vehicles can be more easily obtained and used as weapons or delivery systems designed to harm or disrupt.

In particular, concerns sit with the development and expansion of fully autonomous vehicles, which will require no human operator, and may be more difficult to defeat. By 2040, this type of technology is expected to be commonplace.

Although solutions exist today to deter, detect and defeat rogue and nuisance drone operations, they are often deployed in isolation, are difficult to integrate, pose potential safety risks and require specialist operations. Critically they may not be fit for purpose when it comes to dealing with large scale, coordinated and imminent attacks.

Thus, this is one area where further research and development is required so that the aviation sector is better prepared to deal with this emerging threat.

Beyond this, the lack of, or fragmented, drone regulations globally may pose a risk in the future, with terrorists able to take advantage of differences in international laws, both in terms of proliferation and transfer of the technologies as well as their use.

Cargo and Supply Chain

Cargo operations are not expected to fundamentally change between now and 2040. Cargo and goods will still be carried on passenger and dedicated freighter aircraft, and certain commodities will still have to be shipped in certain ways.

However:

- the increased demand for rapid delivery, driven by growth of e-commerce, may mean more cargo is transported by air;
- drones will increasingly be used to transport cargo, especially over short distances and to remote locations;
- the increasing service nature of the industry will likely mean customers have more information and control than ever before about when and how their cargo travels (including autonomously); and
- due to the increased demand, cargo may come from increasingly unreliable sources (i.e. unknown shippers).

Given that technology development for effective palletized cargo screening is unlikely to be deployed universally by 2040; and the fact that by this time terrorists will probably be able to easily track and trace their cargo throughout the journey; will mean cargo is a much more attractive way to attack a passenger aircraft than it is today.

Freighter aircraft are not immune to this threat either. For example, should terrorist organizations or individuals be able to track their cargo and detonate over a city or critical infrastructure, the impact of such an attack could be enormous.

The supply chain itself may continue to be exploited for the shipment of weapons and componentry. While difficult to detect today, this could become more complicated in the future if adequate technology or robust risk-based solutions are not routinely deployed.

Mental Illness

As noted previously, mental illness is on the rise. This manifests as both a vulnerability, but also a possible direct threat.

In terms of aviation security specifically, there is concern over the rate of mental illness amongst flight crew. Most of which today is unreported and untreated, increasing the risk that flight crew suffering from mental illness could pose a security risk to the aircraft.

This risk could be exacerbated by working conditions such as longer working hours/shorter breaks, shortage of flight crew to meet growing demand and fear of stigma or reprisals if they seek support.

However, it is not just flight crew that may pose a risk in this regard, any aviation sector worker not receiving treatment for such conditions could pose a personal risk (tampering with security systems or aircraft, as has already occurred), or be more susceptible to social engineering attempts and exploitation.

Passengers with untreated mental illness will continue to cause security concerns both at the airport and on board, and it is likely the number of incidents will increase as we move towards 2040.

Biological Threats and Infectious Disease

As discussed previously, there is concern that in the coming years terrorists could move away from use of conventional IEDs towards use of biological weapons and infectious diseases.

Today these types of weapons are considered too volatile and difficult to transport, thus have not received much focus. However, in the future, drones or the terrorists themselves could be the distribution mechanism for such attacks.

More concerningly, passengers could even be used as the distribution method, having been infected before they reach the airport.

These kinds of attacks may initially be difficult to detect, and even more difficult to contain and trace.

How will we mitigate the risks?

How do we begin to mitigate the security vulnerabilities and threats that the aviation sector may face over the next 20 years?

Industry has started to address these challenges, but not necessarily in a concerted and coordinated manner. As the world evolves, industry must collaborate towards a common goal; to make air transport a safe and sustainable mode of transport for passengers and goods throughout the world.

In this regard there are some general steps that can be taken to help industry and governments better prepare and respond, including:

Improving Agility

The sector needs to be quicker at identifying, assessing and responding to threats and vulnerabilities. At the heart of this is the need to improve risk assessment and risk management.

Preserving Trust

Recognition of security measures and regimes across borders is the basis for the entire international aviation security framework. Its continuation is essential to the protection of the sector. Increasingly, inter-organizational cooperation will be required, with a need for agreed mechanisms to better share passenger and cargo information between states, government organizations and private stakeholders.

Developing Standards

While standards for certain elements of the global aviation security system exist today, more work still needs to be done. In particular, the speed at which standards are adopted and upgraded needs to be improved. More targeted research and development and better routes to market need to be established, to ensure that technology, once developed, can be readily deployed in airports and aviation facilities globally.

Capacity Building

Increasing capability and technology gaps in certain states are a threat to the preservation of international recognition and the integrity of the global network. More work needs to be done to bridge these gaps and ensure that the security baseline is increased globally in a sustainable and efficient manner.

Strategic use of Human Resources

Automation and increased use of AI certainly have a significant role to play in securing the sector in the coming 20 years. However, continued use of human intervention and management for critical tasks will need to be balanced against automation, technology and processes to ensure we don't become overly reliant on one or the other.

Sensible Regulation

In addition to security impact, it is important that the operational impact of any new security regulations is well thought through. This will ensure that reduction or removal of one vulnerability does not lead to the creation of another. This also means that government organizations within and across states need to work together, rather than in a siloed nature, to ensure that new regulations and requirements are considered as part of the bigger picture.

In addition to these general steps, there are already actions that can be taken against the vulnerabilities and threats that we know about.

Cyber and Insider Threat

Integration of Security and IT

In order to combat the cyber security and insider threats (particularly exploitation of increased connectivity and automation), IT and Security need to become better integrated. Rather than treating these as two separate functions (as most do today), cyber experts should be integrated into security teams so that they can provide specific advice and counter measures to the cyber security threats aviation security operations are faced with.

Systems Testing

Increased systems testing is essential. This means tests of physical security systems, but also virtual systems. Red teaming could play an important role in this regard.

Contingency Planning

Despite increased automation and reliance on technology, contingency planning will remain important to business continuity. Plans will need to be in place to cater for major IT incidents, power outages and equipment failures, particularly those caused deliberately as they may be more complicated and take longer to resolve.

Security Culture and Training

Security culture and training will need to evolve to consider the wider scope and possible new attack vectors. Staff outside the organization (i.e. vendors and their subcontractors, possibly in multiple countries) may all need to be upskilled in this regard.

Security by Design

Systems should be designed with cyber security and insider concerns in mind. Where possible, critical systems and equipment should be isolated in terms of power and networks. Protocols should be employed, where practical, to help compartmentalize and protect critical data.

Professionalization of the Industry

Human factors will still have the greatest influence on security outcomes when it comes to cyber and insider threats. Thus, there remains merit in attracting and retaining the right people. Recruiting those with good operational IT skills could be challenging with competition from other sectors. Professionalization of the industry could be one way to help this, developing clear career pathways and certification.

Cargo

With the ability to track and trace cargo from point A to point B, screening technologies, particularly those for palletized/containerized cargo need to be rapidly developed. Failure to prioritize this will see cargo become an increasingly attractive attack vector.

Increased cross border compliance and information sharing will also be a critical piece of the solution, allowing industry and regulatory bodies able to better identify and manage high risk cargo before it flies.

Autonomous/Unmanned Vehicles

There is an urgent need to invest in research and development, for both detection and defeat technologies for use against autonomous/unmanned vehicles.

Capability to intercept such vehicles before they reach restricted air space or airport facilities would also be beneficial, however may be more challenging to achieve.

Successful integration of these vehicles, particularly drones, into traditional airspace could help airports and authorities more quickly understand which pose a threat and which do not. There is therefore a need to facilitate this integration as fast and as seamlessly as possible. Importantly, harmonization of national and international requirements will be central to this.

Mental Illness

Response and mitigation strategies will differ significantly between staff/crew and passengers.

For staff and crew, improved awareness, detection and support will be critical to addressing emerging issues. Cultural change will also be needed, allowing employees to more confidently report and seek help, so that those affected get the treatment that they need.

The situation for passengers is more complicated as it relates to wider societal issues. However, staff within the sector should receive appropriate training so that they are better able to identify possible problems and act accordingly before situations escalate. Staff working at key pressure points in the passenger journey (security, boarding, on board etc.) may need specific training to help rapidly deescalate potential issues.

Exploitation of Disruption

In order to reduce the likelihood that disruptions are exploited, improved situational awareness and inter agency cooperation will be required when it comes to demonstrations and planned activism activities.

Importantly, security measures may need to be stepped up in order to make it harder for terrorists or violent activists to take advantage of such situations.

What Next?

Although the guiding principles and mitigation strategies identified in this paper provide a good starting point, they may not be enough. While it is unlikely that the threats of 2040 will be fundamentally different from those we are presented with today, they may manifest in a myriad of ways.

Those who seek to do harm will likely look to exploit emerging vulnerabilities created through our increased reliance on data, automation and technology. At the same time, perpetrators may return to older and more established attack methodologies. As a result, industry must be prepared for all scenarios.

Importantly, in this connected and technology driven future, the threats, but also the opportunities to mitigate them, may come from outside the traditional aviation security sector.

It is clear that this is only the beginning and further work needs to be done to better assess the most plausible threats and risks and identify and develop the comprehensive mitigation strategies that will be needed going forward.

> Are our assumptions about how the world will change realistic? Have we identified the real threats? And do we have what we need to mitigate them?

In 2020, IATA will host a second Blue Skies forum. This forum will bring together aviation security stakeholders, as well as innovative thinkers from all generations, disruptors, academics and manufactures from around the globe to answer these questions. These key stakeholders will help us think about what we have and what we need to develop in the coming years to mitigate both the known and unknown security threats our sector will face.

Blue Skies 2020 - working together today to deliver a safe, secure and sustainable tomorrow


IATA


IATA
Strategic
Partnerships