May 2006

SL-812/09-06

CATSA ACSTA

POSITION PAPER

Air Transport in the Future: 2006 to 2030

Canadian Air Transport Security Authority
Administration canadienne de la sûreté du transport aérien

Canada

CATSA ACSTA

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This paper discusses future trends in air transport and their implications for air transport security in Canada, as well as the policies, procedures and technologies that are anticipated will enable these possibilities. In doing so, the paper provides a wide-ranging, far-looking rationale for CATSA's core strategic priorities by situating them within their proper context: addressing the future of air transport and aviation security. The paper reinforces CATSA's positions and strategic requests by emphasizing how the security challenges facing the Canadian aviation system will expand in scale and scope without increased commitment, capacity and resources for flexible security.

Indeed, exponential growth in air traffic, passenger and baggage volumes and the ensuing increase in airport congestion will pose an inevitable obligation for wholesale transformation in air transport systems throughout Canada and the world. This will entail everything from major airport expansions and better air traffic management to use of smaller "satellite" airports and heightened passenger throughput in every airport, large and small; from expanded management systems and communications networks that enable more decentralized decision-making to the dissolution of traditional "hub and spoke" air systems in favour of tailor-made, on-demand, more flexible "free routing" and "free flight operations."

Exponential growth in air traffic, passenger and baggage volumes and the ensuing increase in airport congestion will pose an inevitable obligation for wholesale transformation in air transport systems throughout Canada and the world.

All layers of security will need enhancement to meet projected growth. Air traffic management (ATM) and navigation will require improvements to protect the overall system from all manner of interference, including electronic jamming, unauthorized communications, and maintenance and control of multiple aircraft routing and flow while in transit. Aircraft security will also need to be heightened to ensure secure operation and flight under all circumstances; notably, to prevent unauthorized pilots from taking control of aircraft, restricting or blocking unplanned trajectories and, should the need arise, literally taking over flight control automatically or from ground-control

All layers of security will need enhancement to meet projected growth.

to return a wayward aircraft safely home. Airport security will likewise need enhancements to prevent any unauthorized access to, interference with, or attack against aircraft or ground systems.

Integration at all three levels will be essential for comprehensive security. Key to this will be greater information sharing amongst the many players operating in the three levels; as well as coordinated use of advanced information technologies, especially communication networks and data processing and information management systems. Such systems could one day enable the uploading, storing and simultaneous sharing of multiple kinds of vital information. Were this to be achieved on a pan-Canadian or even global basis, a single, integrated system could then transmit information on everything from weather patterns, surveillance information, air traffic and airport updates, even specific threat warnings all at once —in real-time —among aircraft, air traffic controllers and security agencies throughout Canada and the world.

This paper affirms that a "risk-based" approach, along with the methods and technologies known to support this, will help address many of these future challenges and threats to air transport security in a cost-effective, sustainable manner. As such, policy and regulatory frameworks must be adapted to suit emerging possibilities and address ever-changing threats.

A "risk-based" approach, along with the methods and technologies known to support this, will help address many of these future challenges and threats to air transport security in a cost-effective, sustainable manner.

"Smarter" security is called for, especially in terms of security screening. Rather than strict prescriptions on the types and manner of searches that screeners must perform, the future of aviation security demands that screening officers be afforded the operational flexibility and training required to adapt to and make authoritative judgements on every-changing situations. They must be conversant with new and evolving technologies and terrorist tradecraft; and, must be adept at sorting through myriad signs and indicators to form quick, accurate assessments and, as needs require, respond appropriately to new threat potential. The range of required skills augurs for 'professionalization' of the screening workforce, whereby screening officers are provided the training and rotation through different areas of security and career progression that allows them to advance into other areas of aviation security.

A "performance-based" regulatory system is also consistent with "smarter" security. We must question the utility of regulations that continue to place strict prescriptions on equipment and procedures when all indications are that future threats will likely involve materials and methods not presently anticipated. A better approach would be to introduce performance-based standards that identify expected outcomes, yet afford latitude in the operational means by which to achieve them. Likewise, CATSA would require the latitude to direct its funds to the areas deemed to be facing the greatest need and/or threat. In short, operational flexibility and financial flexibility are needed to enhance security.

Introduce performance-based standards that identify expected outcomes, yet afford latitude in the operational means by which to achieve them.

This also holds true with regards to technology and methodology. The current regulatory framework imposes specific requirements that arguably could lock Canada into deploying equipment and techniques that, while effective today, could very well prove obsolete and ineffective in the not-so-distant future. It is impossible, in fact, to predict with any degree of certainty or precision beforehand as to which equipment and techniques will become necessary down the road and, so, should be specified under current regulation. Rather, a "technology-neutral" regulatory framework is preferred since this would focus on outcomes, not mandatory specifications. CATSA and its partners could therefore provide more cost-effective security by choosing and implementing new, more appropriate technologies that would more ably address new threats as they emerge.

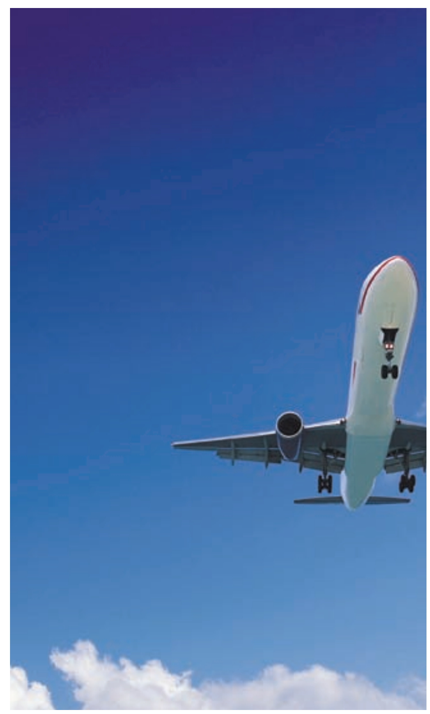
A "technology-neutral" regulatory framework is preferred since this would focus on outcomes, not mandatory specifications.

Finally, we must conceive the possibility that, in the future, aviation transport systems will evolve to incorporate a host of other transport modes (trains, personal aircraft, etc.) and multi-sector, global information networks. This, in turn, will have significant implications for overall system security and, indeed, CATSA's role and place in that system. Aviation security regulations and legislation presently focus only on airports and aircraft, limiting CATSA's activities to the former.

System-wide integration, however, would mean that security is better conceived and addressed starting from the very first point at which aviation passengers and baggage initially enter the overall transport system through until both reach their ultimate, final destination – encompassing whatever mode of transport is used to reach and depart from the airport. All this to say that, in the event, aviation security policies, practices and, consequently, agencies would thus have to provide protection for elements of the system that are located far and away from the traditional confines of an airport.

1.0 INTRODUCTION

This paper discusses future trends in air transport generally and their implications for air transport security, in particular. This discussion relies on studies conducted by experts in order to present short, medium and long-term scenarios, and then we consider the policies, procedures and technologies that are anticipated to enable these scenarios.



Scenario-building regarding the future of air transport has been undertaken by various observers in different countries, most notably the US, UK, Australia, and the EU.[1] CATSA has facilitated a broad visioning exercise for Canada, involving governments, academia, agencies, airports, and airlines . Entitled "Reservation to Destination", it looks at aviation security approaches to the year 2030, focussing on Canada. The exercise took the form of a workshop involving over 40 attendees who developed a model for a multi-dimensional, layered aviation security structure balancing protection with safety and efficiency. The report summarizing the outcomes of this workshop is provided as Appendix A. In this paper, which complements the "Reservation to Destination" report, CATSA discusses broad trends in aviation and other areas that will have an impact on aviation security in the future.

1 See, for example, the 2004 research agenda of the Advisory Council for Aeronautics Research in Europe (ACARE), and the work done by the US Joint Planning and Development Office (JPDO).

2.0 PASSENGER TRAFFIC AND ITS IMPACT

It is generally agreed that aviation in the foreseeable future and beyond will be characterized by increasing volumes – of passengers, of flights, of aircraft, of bags, of freight. This will occur despite advances in information and communications technologies that, in theory, were supposed to better connect people across long distances and mitigate the need for travel. Physical travel will remain necessary for increasingly globalized business, while immigration and other demographic factors will compound the volume of air traffic.

2.1 Projected Passenger Traffic

In the near term, growth in air travel will force a complete rethinking of air traffic management. In Canada, for example, the average annual growth rate of passengers from 2002 to 2017 has been estimated at between 2.8% and 4% for Class 1 airports. Indeed, some Canadian airports are witnessing double-digit growth. The chart below, based on data from Transport Canada, shows projected air passenger traffic in Canada to 2011.

This phenomenon of growth will not be limited to Canada. For example, on a worldwide basis, in 2005 the number of passengers carried on scheduled flights exceeded two billion, which represented an increase of over ten percent from the previous year.[2] European experts are positing an aviation system that, by 2020, will have to accommodate triple the current volume of flights and passengers.[3]

Physical travel will remain necessary for increasingly globalized business, while immigration and other demographic factors will compound the volume of air traffic.

Some Canadian airports are witnessing double-digit growth.

European experts are positing an aviation system that, by 2020, will have to accommodate triple the current volume of flights and passengers.

2 International Civil Aviation Organization (ICAO), “ICAO Update”. *ICAO Journal*, January/February 2006, p. 29.

3 ACARE, “The Challenge of Air Transport System Efficiency”. *Strategic Research Agenda 1*, January 2001, p. 149.

ENPLANED AND DEPLANED PASSENGERS – CANADA 1995 TO 2018

YEAR	TOTAL PASSENGERS (MILLIONS)	FORECAST YEAR		TOTAL PASSENGERS (MILLIONS)
1995	66.14	2004 E		87.48
1996	73.91	2005		92.23
1997	79.52	2006		96.56
1998	82.77	2007		100.05
1999	85.20	2008		103.55
2000	86.00		L	112.32
2001	81.75	2013	M	122.09
2002	78.23		H	131.86
2003	79.99		L	123.92
		2018	M	140.82
			H	157.72

GROWTH RATES IN ENPLANED AND DEPLANED PASSENGER TRAFFIC – CANADA 1995 TO 2018

Years	Average Annual Growth Rates
1995-2003	2.40%
2003-2008	5.30%
2003-2013	4.30%
2003-2018	3.80%

Source: Transport Canada, Aviation Forecasts 2004-2018, September 2005

2.2 Spillover Effects of Increased Traffic

These increased volumes will lead to increasingly serious congestion at airports. Currently, most Class 1 airports are already at or near maximum capacity and cannot accommodate more flights. Consequently, several changes will need to occur in air traffic management processes in order to manage security at the airport of the future:

- Increased efficiencies in passenger flow through the airport will be required to avoid bottlenecks for travellers;
- Increased efficiencies in use of runways and better air traffic management will be required to avoid aircraft bottlenecks; and,
- Increased efficiencies will eventually lead to diminishing returns, therefore airports themselves will have to be expanded – more runways, more terminals. According to one report, "the infrastructure of congested airports will inevitably need to be extended … extensions include: additional runways and terminals, additional gates and stands, new taxiways, extended aprons and parking areas, landing areas for VTOL [vertical take-off and landing] craft and new cargo facilities."[4]

- **Increased efficiencies in passenger flow through the airport will be required to avoid bottlenecks for travellers;**
- **Increased efficiencies in use of runways and better air traffic management will be required to avoid aircraft bottlenecks; and,**
- **Increased efficiencies will eventually lead to diminishing returns, therefore airports themselves will have to be expanded – more runways, more terminals.**

In addition, smaller "satellite" airports could be required to take on some of the spillover from congested Class 1 airports. While these "satellite" airports are ill-equipped to handle large aircraft, they could accommodate growing numbers of smaller aircraft and, thereby, absorb some of the excess volumes facing larger airports.[5] Doing so offers the additional benefit that, given the consequent expansion of destinations (due to use of smaller airports) and flights (due to use of smaller aircraft), it will be possible to better tailor flights to passengers' needs. Observers talk of customized routing and "personal aviation," whereby "customers will seek more flexibility and options tailored to their specific needs increasing the demand for air taxi, charter, fractional ownership, and use of on-demand small low-cost jet aircraft".[6] In the more distant future air taxis, helicopters could shuttle passengers right to the aircraft. Beyond on-demand flights, very large aircraft, accommodating 600-plus passengers, are already being tested, and could help alleviate part of the problem of traffic bottlenecks. Testing and development of lighter and more aerodynamic aircraft will need to continue, given ever-increasing fuel prices and ticket price competition among carriers.

4 ACARE, "The Challenge of Air Transport System Efficiency", p. 168.

5 While this is a possibility, it is not considered by all observers to be a desirable one. See for example Transportation Research Board, *Future Flight: A Review of the Small Aircraft Transportation System Concept*, 2002.

6 Satish C. Mohleji and Paul A. Ostwald, "Future Vision of Globally Harmonized National Airspace System with Concepts of Operations Beyond Year 2020." McLean, Virginia: MITRE Corporation, p. 1.

Surface transportation will also be expanded in the hope that it will also accommodate air travel spillover (for short-haul travel). For instance, systems such as high-speed trains (TGVs) and light rail will also connect airports to population centres.

Airports will need to become larger and intake more passengers and baggage. To manage this growing magnitude of air travellers, passenger throughput at existing airports will have to be increased and improved considerably. CATSA and its partners will therefore be developing procedures to move passengers through pre-board screening more quickly and carefully, all without compromising security.[7] Indeed, as described below, some such initiatives are already underway.

The introduction of passenger "smart cards" might facilitate passenger throughput. Cards containing information on the passenger's citizenship, physical features, travel itineraries, financial information, criminal records, even health data, could be combined with biometric identifiers. From the point of reservation to arrival at immigration at the passenger's destination, the smart card data could enable a single security clearance for passengers. A similar card could be used for non-passengers, building on CATSA's Restricted Area Identification Card (RAIC).

In the longer term (after 2015), air traffic management will have evolved to deal with ever-growing traffic and the potential for congestion beyond what occurs in the short- to medium-term. Management systems – combining large databases with algorithms to define options for the user – will need to expand, to handle aircraft arrivals and departures, traffic on runways and approaches, surface traffic, even changes to weather patterns. The effective use of the information generated by these management systems will, in turn, require expanded, secure communications networks linking air traffic control, aircraft, airports, weather offices, security agencies, and others. Satellite communications will likely be the most effective means of networking these disparate users.

CATSA and its partners will be developing procedures to move passengers through pre-board screening more quickly and carefully, all without compromising security

The future Air Traffic Management systems will be information-intensive. That system will move away from central control to more distributed decision-making. Similarly, plans to improve air traffic safety are also demanding increased situation awareness in the cockpit, which must be provided through increased air-to-ground and air-to-air communications in real time.

7 Moreover, with the aging of the Canadian population, air transport security design will also need to take into account the needs of persons with reduced mobility.

According to one observer, "the future Air Traffic Management systems will be information-intensive. That system will move away from central control to more distributed decision-making. Similarly, plans to improve air traffic safety are also demanding increased situation awareness in the cockpit, which must be provided through increased air-to-ground and air-to-air communications in real time. This distributed architecture will rely on characteristics such as precise navigation information and comprehensive global coverage currently not available."[8]

Overall, the traditional "hub and spoke" architecture of air traffic management – where passengers are routed from their departure point (usually a "spoke" airport) through a centre (a "hub" airport) which serves as a huge transfer site, and finally to a "spoke" destination -- will be replaced by more flexible approaches, enabling even more on-demand flight. More flexible approaches include "free routing", where users (airlines, pilots) can plan their routes between an entry point and an exit point, without recourse to the air traffic services. Ultimately, "free flight operations" might also become possible, where pilots take responsibility for determining the flight trajectory, separation between aircraft, and resolution of possible trajectory conflicts. All of these options require advanced automation and decision-making information systems to enable airlines and pilots to design flight patterns more strategically than is currently the case.[9]

3.0 AVIATION SECURITY CHALLENGES

At the same time that these changes occur in aviation, it is expected that the level of available resources that can be devoted to air transport security in Canada will not increase significantly. Security efforts will thus continue to focus heavily on airports themselves. Incremental resources in this area will be devoted largely to the following activities:

8 National Aeronautics and Space Administration, *Aeronautics Blueprint: Toward a Bold New Future in Aviation, 2002.*

9 Arthur D. Little, *Study into the Potential Impact of Changes in Technology on the Development of Air Transport in the UK.* Report to the (U.K.) Department of the Environment, Transport and Regions (DETR), November 2000, p. 47.

- Maintenance and upgrades of already deployed equipment;
- Piloting of new initiatives (canine techniques and beyond);
- Development of modified procedures to make the screening process less predictable and visible to potential terrorists;
- Improved training procedures and tools for screening officers, which in turn could enable the "professionalization" of the screening function; and,
- The possible expansion of screening procedures in order to take into account the areas highlighted by experts to be significant security gaps -- cargo and fixed-base operations (FBOs).

The implications of these projections for CATSA and airport screening are significant. With the expanded use of smaller, regional airports and tremendous growth in air passenger travel, overall demand at airports throughout the country for effective passenger and baggage screening will rise considerably. Both the number of officers and number of screening hours will need to be increased in order to ensure an effective balance between manageable passenger throughput and adequate levels of security. This, in turn, will necessarily lead to higher security costs and, thus, the need for greater financial and other resource outlay for airport screening and security.

Equally vital, greater investment of resources in research and development will also need to occur – ideally in Canada and certainly internationally – in order to create and deploy new screening equipment for detecting new threats. The need is especially great for development of enhanced technologies to address the most oft-cited of these new threats: chemical, biological and nuclear.

The current approach to air transport security is multi-layered. The "layering" is a means of ensuring checks and balances in security – if one layer fails, another can possibly detect and stop the threat. Security needs at the levels of aircraft, airports, and air navigation infrastructure need to be considered, with successive barriers to threats at each of these levels.[10] Security at these three levels would have the following objectives:

- Navigation and air traffic management (ATM) – protect the system from interference including jamming, unauthorized communications, maintenance of control of aircraft in transit
- Airport Security – prevent unauthorized access to, or interference with, aircraft or systems on the ground
- Airborne Security – ensure secure operation of the aircraft; preventing unauthorized pilots from taking control of the aircraft; restricting unplanned trajectories; controlling the aircraft to a safe landing

Longer-term patterns of air travel and the evolution of technology will enable security to begin with the passenger's purchase of her ticket and continue right through to the passenger's final destination.

Longer-term patterns of air travel and the evolution of technology will enable security to begin with the passenger's purchase of her ticket and continue right through to the passenger's final destination. Irrespective of the mode of travel used to reach the airport and to leave it, security is envisioned as a seamless, integrated system encompassing passengers, baggage, non-passengers, airports, aircraft, security authorities, billing agents, and other entities in the chain. Perhaps the most succinct characterization of the longer-term environment in air transport is: "move anyone, or anything, anywhere, anytime, on time." [11]

3.1 Security at the Navigation/ATM Level

Canada and other countries will need to assess and address the potential for misuse of air traffic control (ATC) facilities and navigation aids to trigger a collision. We will also need to develop better systems for maintaining radar

10 ACARE, *The Challenge of Security*, p. 195.

11 Mohleji and Ostwald, p. 2.

contact between aircraft and airport, especially for cases when the Secondary Surveillance Radar (SSR) transponder aboard an aircraft is intentionally shut down.

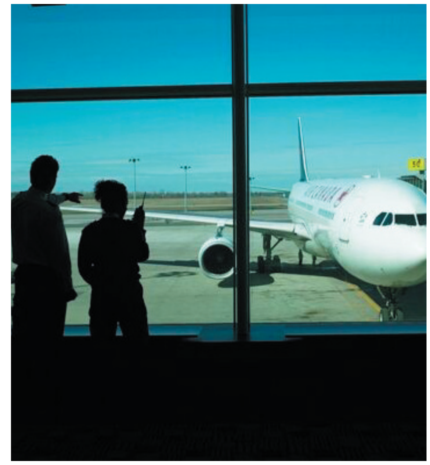
In the longer term, it could be possible to develop tools that detect deviations from the planned trajectory of an aircraft and that take partial control of aircraft from the ground via data link. Similarly, there might be tools to put aircraft into a "protective" mode which performs the predicted flight track until full stop on the runway or onto an airfield.

3.2 Security at the Airport Level

Airport security will be enhanced by considering the potential application of technologies from other domains (e.g. military, policy, special forces, medicine, anti-drug, money laundering, anti-gang). Areas of greatest need and potential for cross-application of technologies include: improving luggage and freight control; detecting nuclear and biological weapons; tightening access control to restricted areas for all personnel and passengers; and sharpening detection of access violations.

We will also need to explore means for neutralizing on-ground aircraft so as to better guard against and prevent unauthorized people from gaining access to a runway, preventing takeoff, and perhaps even taking control of an aircraft at parking. This will need to be supplemented with research leading to effective means for preventing unauthorized persons from stealing aircraft, preventing aircraft from taxiing or taking off without approved by air traffic controllers, and improving runway security more generally. All such needs can be aided through development of systems enabling complete intelligence data sharing and management between airport and police forces.

Beyond the traditional concerns regarding screening for objects and hijacking of aircraft, airport-level security will have a greater focus on biohazards such as



pandemics or chemical/biological threats. According to the Conference Board of Canada, "… we will be poorly protected when we begin to confront non-traditional threats….Canada will not escape the imminent pandemic, and unless the level of global preparedness improves, panic will reign."[12] Indeed, Canada's experience with SARS in 2003 was likely a harbinger of pandemics to come in the near future. It has been suggested, in fact, that an air passenger could travel around the world in less time than is required for the incubation of most communicable diseases.[13] This in turn means that, thanks to the breadth and speed of air travel, dangerous viruses could span the globe and spread among human populations within hours. While aircraft cabin air quality is generally monitored to ensure adequate ventilation and the use of filters effective at trapping bacteria and viruses, passengers sitting in close proximity with carriers of a disease, on long-haul flights or grounded on aircraft with the ventilation switched off are vulnerable.

Airports are a critical portal for people entering and leaving the country.[14] At each of these ends of passenger traffic, therefore, airports must be equipped both to prevent epidemics or health threats from exiting the country to spread abroad, and to prevent health threats from entering the country. Canada's response to terrorism should include a bioterrorism component which, in turn, should recognize that bioterrorism has both security and safety implications. It will be necessary to ensure systems and infrastructures that will both detect intentional chemical and biological attacks on airports before they occur, and that will enable suppression of the chemical/biological agents and treatment of affected persons. The same systems and infrastructures could serve to address pandemics.

12 Conference Board of Canada, *Executive Action: Facing the Risks – Global Security Trends and Canada.* February 2006, p. 4.

13 US House Committee on Transportation and Infrastructure, "Federal Health & Airline Officials Outline New Cooperative Efforts to Prevent Spread of Infectious Diseases on Commercial Air Travel." Press release dated April 6, 2005. http://www.house.gov/transportation/press/press2005/release29.html.

14 Indeed, the Greater Toronto Airports Authority (GTAA) has developed and released its plan to handle pandemics. See GTAA, *Pandemic Influenza Planning: Maintaining Continuity of Airport Operations and Services, 2005.*

Bioterrorism and Biosecurity

[TRANSLATION] "Biosecurity involves the management of all natural and military or criminal threats to health … [which] … includes bioterrorist threats….Bioterrorism is not just a purely military or criminal problem, it also has a public health aspect: like natural infections, it requires surveillance and detection measures related to the protection of public security…in other words, a public health vision can be added to the traditional military or criminal visions of biological weapons, which leads to the notion of biosecurity….Canada's openness toward the health aspects of bioterrorism is all the more interesting given that it is a parallel to North American integration and Canada's desire not to represent a threat to its allies..." [15]

An integrated approach for security at airports, therefore, could incorporate screening for dangerous objects at the same time as screening for dangerous biosecurity threats. Referring to the numerous threats to national security, including terrorism, organized crime, natural disasters, the proliferation of weapons of mass destruction and others, Canada's national security policy states, "All of these threats pose a real security challenge for Canada. Often, they do not exist in isolation from one another. For example, the proliferation of weapons of mass destruction is a problem in itself, but when terrorism is involved, the threat increases dramatically. The danger of pandemics is amplified if groups seek to spread disease deliberately." [16]

3.3 Security at the Aircraft Level

Better prevention and response capabilities will be needed. The starting point is to review and redefine the ultimate responsibilities of different actors (e.g. pilots versus air traffic control) in response to actual security breaches should a hijacker take control of an aircraft.

As the surest means of providing security, however, efforts will need to focus on preventing threats in the first place. Use of biometrics and enhanced air-ground communication, for instance, will facilitate better cabin monitoring and control, permitting improved prevention and detection against cockpit access and flight control by an unauthorized pilot. New technologies and

15 Julie Auger, "La préparation canadienne contre le bioterrorisme : entre sécurité et santé publique." *Options politiques*, février 2006, pp. 39-40.

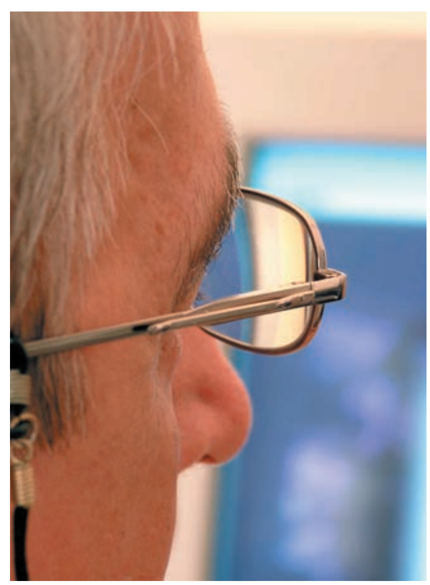
16 Government of Canada, Privy Council Office. *Securing an Open Society: Canada's National Security Policy.* April 2004.

methodologies will also enhance both flight trajectory protection and automatic avoidance interdiction, ensuring that ground zones are better protected from danger in the catastrophic event of an aircraft crash.

An integrated approach for security at airports could incorporate screening for dangerous objects at the same time as screening for dangerous biosecurity threats.

Related to this, from the tragedy of 9/11 we have learned the crucial need to enhance systems for preventing terrorists from using aircraft as weapons against ground population. Key measures here include more effective and sophisticated on-board advisory systems that better alert crew whenever an aircraft deviates from its planned trajectory; or in case of, and in time to prevent, controlled flight into terrain. Also crucial are improved flight control systems on new generation aircraft which, aided by 3D algorithms and comprehensive databases, can literally return a wayward aircraft safely home. If, for any reason, an aircraft inexplicably and uncontrollably deviates from the parameters of its trajectory, such a system would then initiate corrective actions that would immediately restore an aircraft to its proper altitude and heading; or, if required, even automatically – and quite safely – return that aircraft to the ground.

3.4 Data Processing and Systems to Facilitate Aviation Management



Integration will be the key feature of data processing and information systems used for aviation in the future. Overall, experts suggest that there will be greater use of information management systems to optimize the traffic flow of planes at airports, manage runway rates, respond to congestion in holding patterns around airports, manage distances between planes ready to take off and land, and manage departure and arrivals sequences, etc.). Indeed, such systems have been tested for some years in certain European airports. [17]

Better communications networks in turn could enable the uploading, storing and sharing of information on a global basis; users could track weather, surveillance information, air traffic and airport information, even threat warnings using a single system. An emergency response architecture built on this networked system could be created to connect aircraft, airports, security

17 Little, p. 38.

authorities, and other organizations. Networking could also enable the transmission of information between aircraft, air traffic controllers and security agencies in real time, and possibly linking with data gathered by onboard safety and security sensors.

In terms of security, developments in information technologies will enable greater tracking of passengers as they move through the airport to an aircraft (indeed, more futuristic scenarios anticipate tracking of passengers right from their home or office all the way to their final destination).

Data processing capacity will be able to accommodate the huge streams of data that will need to be aggregated to track such flows, and to match them to data on flights, departure gates, baggage, etc. Data processing capacity will expand to better track aircraft movement and passengers within. Non-passenger screening could be expanded to accommodate biometrics.

More robust and integrated data systems will be required to make the data gathered on non-passengers and passengers useful for security purposes. Data gathered by an air transport security body on movements of non-passengers within the airport, for example, are ineffectual unless they can be combined with criminal records, security authorization levels, etc. Finally, simulation devices and models will be required to test the technologies and passsenger/aircraft flow scenarios; this cannot be done in a functioning airport.

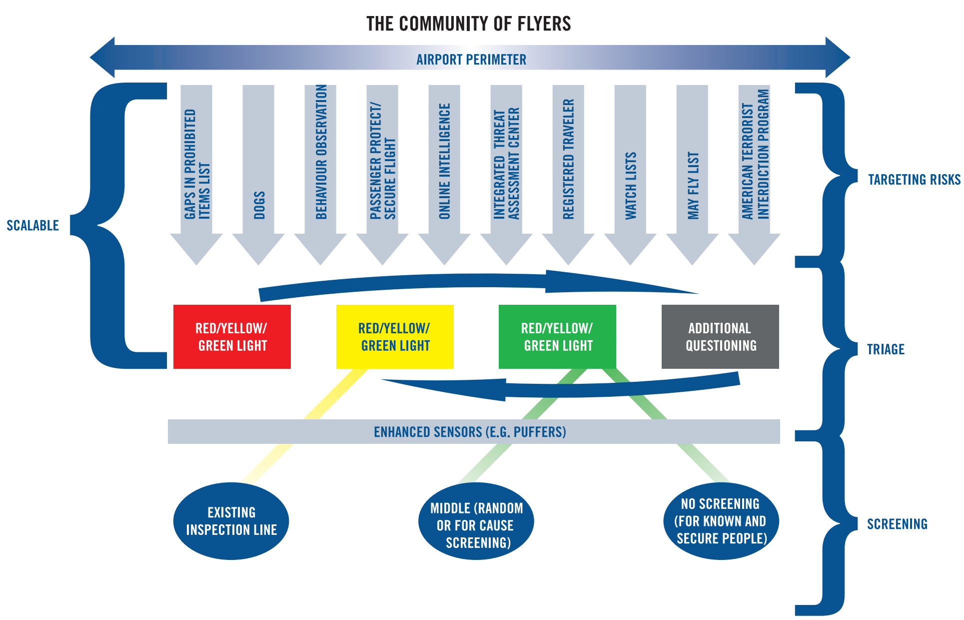
3.5 Toward Risk-Based Approaches

In the slightly longer term, air transport security in Canada could integrate tools and methods adopted in other countries, depending on Canadian regulatory and policy approval. Trials of so-called “trusted traveller” or “registered traveller” programs, as are now occurring in the US and at Pearson International Airport, could be extended to more airports in Canada. Advanced techniques for behaviour observation, or “behaviour pattern recognition,” will continue to be developed, improved upon and implemented in a greater range of countries, and could eventually be tried in Canada.

Combined, these various methods form the core of a risk-based approach to air transport security, one that simultaneously enhances the quality of airport operations, screening performance and the effectiveness of aviation security. According to one authority, "risk-based airport security would mean a reduced focus on finding bad objects and an increased focus on identifying potentially bad people – those most worthy of additional scrutiny. Screening resources would then be applied in accordance with a passenger's risk category."[18]

Risk-based airport security would mean a reduced focus on finding bad objects and an increased focus on identifying potentially bad people – those most worthy of additional scrutiny. Screening resources would then be applied in accordance with a passenger's risk category.

The diagram below shows CATSA's scenario regarding the community of flyers and the risk-based security approach that could be exist in the airport of the future.



18 Robert W. Poole and George Passantino, *A Risk-Based Airport Security Policy*. Los Angeles, Reason Foundation, 2003, p. i.

The table below summarizes the trends in aviation and the security issues that could arise in the future.[19] Possible security responses, on a macro level, are also presented.

Summary of Trends and Responses

Airport Level		
TRENDS	IMPLICATIONS FOR AIR TRANSPORT SECURITY	POSSIBLE AIR TRANSPORT SECURITY RESPONSES
Due to increase passenger traffic: Very large aircraft On-demand travel More regularly scheduled flights Increased usage of satellite airports in metropolitan areas Increased capacity of metropolitan airports; larger airports Rapid proliferation of communicable diseases; potential for pandemics as more people travel together in close quarters	Bottlenecks at PBS lines due to large volume of passengers; larger crowds in airport could create greater passenger vulnerability Increased uncertainty with respect to daily traffic flows through PBS and baggage through HBS Need to determine whether smaller airports can accommodate PBS, HBS and NPS infrastructure; if not, can screening be done airside Need to develop systems and infrastructures to detect biohazards and treat them either before passengers leave the country or enter their destination country/region	Expanded human factors planning and design to streamline passenger flows and increase throughput Passengers encouraged to reduce hand baggage on the aircraft Limit mingling of passengers and non-passengers in airport, for all but essential functions; separate entrance and access protocols for passengers and non-passengers starting at the entrance of the airport Expanded deployment of card readers and sensors to detect movement of non-passengers, passengers, and bags Use of radio and other frequencies, secured, to enable tracking of bags and people within airports Possible Air Transport Security Responses Luggage separated from passenger at check-in to go through series of remote checks; luggage boarded automatically in explosion-proof containers Development of "wide area access control" to detect any intrusion within hundreds of hectares Development of sensor technologies based on work underway in nuclear industry and drug detection, e.g. multi-sensor detection to detect explosives or particles on humans Development of complete information system fed by data from intelligence and police enabling identification of undesirable persons from ticket reservation to airport Expanded quarantine facilities in airports, and PBS and HBS equipment that can detect prohibited items, trace biological/chemical weapons, or passengers carrying communicable diseases

19 Based in part on the work of ACARE.

Aircraft Level		
TRENDS	**IMPLICATIONS FOR AIR TRANSPORT SECURITY**	**POSSIBLE AIR TRANSPORT SECURITY RESPONSES**
Due to more aircraft accommodating higher passenger traffic: Dynamic, real-time air traffic management systems to deal with potential congestion, delays Expanded use of GPS by pilots for CNS (Communication, Navigation, Surveillance) Enhanced power of computers capable of centralized or dispersed operation. Speed of proliferation of diseases and development of bioterrorist weapons	Potential for even greater damage when aircraft fly in close proximity of each other Potential for hijackers or terrorists to take control of aircraft More crew on board larger aircraft; more employees servicing aircraft; need for more non-passenger controls at aircraft level Spread of pandemics or diseases, or acts of bioterrorism on board aircraft (chemical or biological threats to passengers and crew)	Use of algorithms to predict flight paths and calculate deviations in order to identify aircraft being hijacked Collaborative flight planning by all users Automated control of aircraft in case of deviation from approved trajectory; pilot-free aircraft for certain roles (e.g. non-passenger flights) Anti-missile, aircraft-level systems developed to make aircraft less vulnerable to short-range, ground-launched missiles Non-lethal devices on board aircraft to neutralize terrorists without threatening passengers' lives Biometric controls in aircraft preventing control by unauthorized pilots or other staff On-board video monitoring to detect hazardous behaviours New propulsion technologies for greater protection to aircraft against short-range missile attacks; sophisticated detection and jamming facilities attached directly to aircraft Security and safety sensors embedded in aircraft and better onboard computers to transmit information in real-time to controllers or security agencies Deployment of bioaerosol detectors and frequent changing and inspection of air filters on board aircraft

Aviation System Level

TRENDS	IMPLICATIONS FOR AIR TRANSPORT SECURITY	POSSIBLE AIR TRANSPORT SECURITY RESPONSES
Biohazards, pandemics due to greater traffic and globalization	Screening for health risks required before passengers leave country and as they enter destination country	Introduce ways of ensuring “health integrity” of passengers as they leave their country of origin e.g. “smart cards”
Improved capacity of databases for integration and warehousing of large amounts of data from various sources	Coordination of health information across borders required	Introduce techniques to enable simultaneous screening for both health and security threats
Real-time data processing, which could enable intelligence data management system between airports, police forces, and medical	Possibility to create data warehouses and virtual networks, to aggregate data gathered from passenger smart cards, RAIC, etc.	All stakeholders (airlines, manufacturing industry, unions, and government bodies) could adapt their security processes to allow the possible implementation of additional defensive capabilities to address newly-identified threats, and provide security training to all crewmembers.
Expansion of secure/encrypted communications networks to link airports, aircraft, security partners		Air traffic control undertaken from a virtual airport tower which may be located at a remote, highly-secure facility, perhaps controlling a cluster of airports these facilities would also have intrusion protections, layers of NPS
		Simulation and crisis management tools to anticipate future threats and design appropriate responses
		Airport-level security management system to coordinate all necessary components; as well, security management systems to coordinate all elements of aviation

4.0 IMPLICATIONS FOR CATSA

Just as the tools, training, and intelligence at our disposal must enable CATSA to anticipate threats, so, too, the policy and regulatory frameworks must be adapted to suit emerging realities. CATSA believes that the regulations, measures, standards and orders imposed by government on aviation security operators do not provide CATSA with these attributes, and, moreover, these measures are not adapted to the airport of the future.

The success of the aviation security screening system depends also on the establishment of a security culture that is rooted in the traveling public, the service provider and the government's oversight organization. When aviation security has become a culture in the mind of every passenger and when the aviation security measures are deep-rooted in every level of aviation operations and imbedded in every routine of the screening process, success is guaranteed.

4.1 "Smarter" Security

As transport evolves, so, too, must recruitment and training for screening staff. Screening officers in the future will need to be trained to adapt to changing situations; for example, with capacity crunch anticipated at major airports, screening officers will need to be able to detect bottlenecks and respond to them with new techniques for throughput management and passenger flow. Under such circumstances, CATSA questions the effectiveness of regulations that prescribe the number of screening lines, the number of screeners, and the time screeners can spend in one function.

Ultimately, creating a pool of qualified security professionals that can rotate through different areas of security could strengthen Canada's ability to move trained resources to where they are required.

If automation of the most basic screening functions occurs (e.g. x-raying of carry-on baggage, metal detection on passengers, etc.), then screening officers will nonetheless be required to deal with cases that machines cannot resolve. To make optimal use of integrated databases and data warehouses that combine data on passenger movements through the airport with baggage movements, criminal data, travel arrangements and other security-related information, screening officers will need to be conversant with information technologies and adept at combining discrete bits of information to arrive at a complete picture of a potential threat. Screening officers with such skills will be in demand for other types of employment in the security field. Ultimately, creating a pool of qualified security professionals that can rotate through different areas of security (e.g. security guards, retired police, IT security professionals, etc) could strengthen Canada's ability to move trained resources to where they are required.

4.2 Regulate Outcomes, Not Outputs

The threats of the future, in the airport of the future, will likely involve materials and techniques that have not been anticipated by policymakers. Consequently, CATSA questions the utility of regulations that prescribe the specifications of explosives detection and x-ray equipment, and the types of searches that screening officers must perform. As passenger throughput increases generally, with possible ebbs and flows at different points during the day, it would be more effective to introduce performance-based standards that identify the outcomes to be achieved rather than the means to achieve them.

In the absence of higher revenues to cover the costs of more screening hours or the acquisition of equipment that detects new threats, CATSA would require the latitude to direct its funds to the areas where they are most needed.

Moreover, the growth in passenger traffic and the investments required in Canada's air transport and security infrastructures will be significant. CATSA itself will be facing zero growth in its appropriations to deal with the passenger traffic growth that is foreseen by Transport Canada. In the absence of higher revenues to cover the costs of more screening hours or the acquisition of equipment that detects new threats, CATSA would require the latitude to direct its funds to the areas where they are most needed. Funding flexibility – whether or not combined with higher revenues – will therefore be essential to deal with the air transport challenges of the future.

4.3 A Technology-Neutral Framework

The current regulatory framework imposes specific requirements with respect to equipment and techniques that might be effective today, but could be obsolete in the not-so-distant future. It is impossible, however, to predict exactly which equipment and techniques should be captured in regulation. A technology-neutral regulatory framework, which focuses on outcomes and not specifications, would be more appropriate in the future environment.

Regulation as specific as these examples is problematic for several reasons: it can easily be superseded by new technologies, thus locking Canadian aviation security into outdated equipment and techniques; it does not allow for the implementation of new equipment and technologies, even for piloting; and it does not consider future threats such as chemical, biological, or radiological. A more technology-neutral framework that identifies the desired outcomes, rather than equipment parameters, would enable CATSA and its partners to provide effective security in the airport of the future.

4.4 Integrated transportation, integrated security?

In a long-term "reservation to destination" environment, the airport will be but part of the passenger's overall travel experience. Security of passengers and bags could be conceived of from the point where the passenger enters some transportation system (e.g. shuttle buses or trains) to reach the airport, and continue right until the passenger reaches the final destination. Aviation security regulations and legislation focus on airports and aircraft. It is unclear whether, in the future, regulations could envision a security system that could exist outside the airport, for example on a shuttle taking the passenger directly to the airport.

Even when the discussion is restricted to airports, experts predict that the types and functions of airports will be differentiated. Satellite airports serving business commuters might be a lower level of target to terrorists than large international airports. Passengers that pay a premium for quick point-to-point travel might expect adapted or expedited security measures. If the concept of "air taxis" takes flight, then security requirements might need to be revisited even further. Screening lines, expensive x-ray equipment and walk-through metal detectors might be unfeasible, or unreasonable, for these rapid alternatives to trains or buses, and could make future aviation developments uncompetitive vis-à-vis other modes of transport.

System-Wide Information Management creates opportunities for another type of integration: the aggregating of access to databases and data warehouses that link airport authorities, airlines, air traffic managers, and potentially security information. These information systems will have nodes that are located outside airports, but, given the wealth of sensitive data and information they contain, they could be extremely vulnerable to outside attack. Aviation security policies and practices will therefore have to anticipate protection for elements of the system that are located away from airports and airlines.

4.5 International Cooperation and Collaboration

As the Conference Board of Canada states, "…our limited weight and influence will hinder our ability to control global trends and events. The transnational nature of current risks to human security requires stronger intergovernmental coordination at a time when multilateral arrangements are weak and global governance is increasingly constrained.[20]" Most of the future trends described in this paper will emerge first in other countries and Canada will follow. Nonetheless, it is not appropriate to assume that the transportation environment in other countries translates well into Canada. If, for example, our trading partners implement, and expect Canada to implement, behaviour-based or voice detection techniques, could these techniques be transposed to Canada? Canada's multicultural and multilingual context might lend itself poorly to techniques developed in other countries, where common cultural understandings of gestures and language make it more straightforward to detect

As the Conference Board of Canada states, "…our limited weight and influence will hinder our ability to control global trends and events. The transnational nature of current risks to human security requires stronger intergovernmental coordination at a time when multilateral arrangements are weak and global governance is increasingly constrained."

20 Conference Board of Canada, Executive Action: Facing the Risks – *Global Security Trends and Canada.* February 2006, p. 5.

unusual behaviours. Thus, while sharing best practices and adopting techniques developed by other countries, Canada will also have to consider uniquely Canadian approaches that respond to Canadian imperatives.

Canada's proximity to the US requires Canadians to be close to, or involved in, the development of that country's security infrastructure; if not, US requirements will, de facto, be imposed on Canada. Moreover, it is likely that international bodies like ICAO and IATA will play an important role in facilitating technology standards that in turn enable communications systems interoperability and data compatibility. International bodies will doubtless continue their role in developing international standards for screening and aviation security techniques.

Canada could take a page from the lessons learned by Australia in developing international approaches to aviation security. In the latter country, CATSA observes in a background paper, "the Government of Australia has arrived at the conviction that airport security at home is directly enhanced by monitoring and improving airport security in other countries….As such, Australia is launching a host of initiatives to build the intelligence capabilities and enhance the airport security capacity" of its trade partners.[21] Similarly, Canada's aviation security experience, expertise, and infrastructure could be provided in some way to other countries, in the spirit of sharing best practices and recognizing that aviation security takes place in a borderless world. CATSA itself has made some strides in this area, having created the International Forum for Security Screening in Aviation (IFSSA), and having built bridges with counterparts in Israel, the US, and other countries. As well, CATSA's learning and training programmes could be offered in other countries seeking to build or expand their aviation screening systems.

21 CATSA, *Backgrounder: Implementing the Wheeler Report in Australia*. May, 2006, p. 7.

5.0 CONCLUSIONS AND RECOMMENDATIONS

Perhaps the most succinct conclusions concerning aviation security in the future could be drawn from the work of Stephen Flynn, a US security expert. Flynn observes that the management of security risks will always be necessary, given that it will be impossible to design perfect security that is perfectly in step with emerging threats and technologies. Recognizing, however, that security measures are perceived by passengers to be irritants, future security will need to be integrated with measures to mitigate other threats such as pandemics, criminal activities in airports, illegal immigration, etc. These multiple-benefit solutions will involve greater coordination among government agencies, private stakeholders, and the travelling public. Such a vision, in turn, will promote the "policy coherence" consistent with the government's goal of horizontal policy management.

Seven Principles for Security in the New Environment [22]

1. There is no such thing as fail-safe security, and any attempt to achieve it will be counterproductive. Ultimately, our goal must be to manage the threat of acts of terrorism on our soil.
2. Security must always be a work in progress, to reflect changes in technologies and threats.
3. Security requires forging and sustaining new partnerships at home and abroad.
4. National coordination, resource support, and leadership by the government are essential.
5. Emergency preparedness can save lives and significantly reduce the economic consequences of terrorist attacks.
6. Security measures have deterrence value.
7. Security measures will have derivative benefits for other public and private goods: by augmenting our tools for detecting and intercepting terrorists, Canada will augment its tools to handle criminal acts such as narcotics and migrant smuggling, cargo theft, and violations of export controls. Similarly, public health investments to deal with biological agents will enable security and health authorities with more effective tools to manage global diseases and pandemics.

22 Stephen Flynn, *America the Vulnerable.* (New York: Harper Collins, 2004), pp. 165-168.

In this vision of multiple-benefit solutions, CATSA would continue to be one layer of an integrated security system that would include other security agencies, government departments concerned with transport, health, public safety, foreign affairs, immigration and customs, airport authorities, airlines, and others. Cooperation and collaboration at even greater levels would be required to design, test, and implement techniques and tools that address, for example, both the health and security dimensions of air travel. The kinds of information- and intelligence-sharing approaches that CATSA has developed to better deliver its mandate, described in the CATSA paper *What We Need to Know and Why*, will have to underlie future information systems, communications networks and databases that integrate security, immigration, health, and other key information, while safeguarding citizens' privacy. The transition toward a more risk-based policy and regulatory framework will be essential to ensure more operational flexibility for security organizations like CATSA in the new environment. Regulations and other restrictions that currently limit CATSA's ability to participate in research and development, piloting of new systems and technologies, and partner with organizations in Canada and abroad to share infrastructures and best practices, will need to be revisited. In this context, CATSA will require the following:

1. The flexibility to explore further the implications of trends in aviation on security, including:

- the ability to conduct ergonomic, time-motion tests of optimal screening configurations
- the ability to introduce alternative screening processes that continue to ensure maximum detection of threat objects and terrorists
- the opportunity to become involved in the development, testing and deployment of new equipment and technologies for screening

2. A technology- and process-neutral regulatory framework that focusses on optimal results, rather than prescribed processes and equipment. By focussing on desired outcomes, the Government can help ensure that aviation screening and security authorities and partners can implement the equipment and techniques necessary to meet future imperatives of passenger growth, airport congestion, new threat items, technology evolution, and other issues raised in this paper. This regulatory framework, in turn, will require revisiting the Security Screening Order, the Aerodrome Security Measures, and other regulations that affect CATSA, airport authorities, airlines, police and security agencies, and numerous other stakeholders.

3. The ability to expand its network of partnerships both in Canada and abroad. CATSA wishes to deliver its screening mandate effectively for today and the future. In that light, CATSA must be able to build partnerships with organizations involved in transport (air and other modes), security (screening, policing, and other aspects), learning and training (of screening officers and other security professionals), infrastructure, health and safety, and other areas that overlap directly or indirectly with this screening mandate. These partnerships in turn will enable CATSA to acquire and share information and intelligence about emerging security threats, trends in transportation, and best practices in screening and aviation security.