CHAPTER 3

The Civil Aviation Analogy

PART II

Cyber Terrorism and Civil Aviation

H. H. Whiteman

Often, when cyber terrorism is addressed in the media, one of the examples provided to illustrate the potential damage that can be done is the possibility of downing aircraft in flight or tampering with air traffic control in ways to cause aircraft to crash. This image of civil aviation as a potential target for cyber terrorists is a chilling one, but it paints a worst-case scenario that, in many respects, misses the point about cyber terrorism. Is there a threat? The answer is yes, but with many qualifications.

1. Cyber Terrorism and Information Operations

If we view cyber terrorism in a narrow sense, it essentially becomes an extension of traditional terrorism into the realm of information technology. Although there is no internationally agreed-upon definition of traditional terrorism per se (the term used in civil aviation is acts of unlawful interference), central characteristics include politically or otherwise motivated use of violence directed at civilians by a group or individual in order to influence public perceptions. Terrorism in this sense can and does apply to the cyber world. There is clearly the potential for individuals with political and/or religious motivations to make use of information technology tools to abuse, tamper, or corrupt IT-based data or control processes, which could result in severe injury or death—rail-switching systems for example. Yet if we limit ourselves to the realm of what I shall refer to as traditional terrorism, we risk focusing on highly unlikely occurrences that constitute the worst-case scenarios. Such focus adds little value in developing a risk-management approach to dealing with the problem.

Cyber terrorism must be considered to include the full range of threats, vulnerabilities, risks, and technological matters that anyone employing IT systems at the core and even on the periphery of their business must contend with today. In Canada, the term that has been adopted to reflect this range of issues is Information Operations, or IO. The current Canadian definition explains IO as "actions taken in support of national objectives which influence decision-makers by affecting others' information while exploiting and protecting one's own information."[1] This definition is admittedly broad and limits itself to addressing national objectives, but it does point to realities that in essence constitute a qualitatively different operational environment that contains many more uncertainties than the one we were function-

[1] See *Canadian Forces Information Operations*, Doctrine Document B-GG-005-004/AF-032 (April 15, 1998), and the Canadian Forces policy document on IO.

ing within only ten to fifteen years ago. Some of the characteristics of this IO environment include:

- information and decision-making architectures not usually included in information technology security are brought into play as potential sources of vulnerability[2]
- traditional conflict and warfare situations, nontraditional forms of conflict, and peace time environments are within the scope of inquiry
- potential scale of harm is huge
- adversaries are anonymous and include everything from individual recreational hackers to organized state-led initiatives
- there is a multiplicity of targets, traditional and nontraditional
- technology employed for attacks is simple, cheap, and widely available
- early warning indicators of attack are available only when voluntarily provided
- remedies or countermeasures are poorly defined and not readily available
- political, temporal, and geographical boundaries disappear

[2] The types of threats involved and their sources vary considerably and both are estimated to be growing at an accelerated pace. See *Critical Foundations: Protecting America's Infrastructures*, Report by the President's Commission on Critical Infrastructure Protection, p. 9, released in October 1997, on increases in information technology expertise and tools. The report is available in its entirety at http://www.pccip.gov/pccip. For a discussion of types of threat and their sources, see *Information Warfare and the Canadian Forces*, document no. 1350-004-D001, Version 1 (May 9, 1996), prepared for Lcdr R. Garigue SITS/ADM(DIS) and T. Romet GDInt/J2 Scientific and Technical, National Defence Headquarters, Ottawa, Ontario, available at ⟨*http://www.dnd.ca/diso/library/lib_e.htm*⟩.

- technological advances create an extremely fluid threat environment[3]

The range of potential perpetrators and intentions in the IO environment is probably the most troubling aspect of this new reality. The availability on the Internet of easy-to-use tools to disable, disrupt, or corrupt systems is astonishing. In addition, the anonymity provided by the Internet may facilitate or encourage individuals to engage in activity or behavior that they otherwise avoid, and there is litle likelihood of being caught. Several high-profile cases involving concerted attacks directed against American government systems were what appear to be the work of thrill-seeking teenagers. The IO environment, therefore, is one of multiple, often unknown attackers, and a wide array of targets, whereas cyber terrorism per se represents a small but potential growth area.

2. Civil Aviation Security, IO, and Critical Infrastructure Protection

The quality of a country's infrastructure is vital to the prosperity and well-being of its citizens. It can be understood as the physical and informational frame upon which an economy depends. Its components include: transportation, energy production and storage, water supply, emergency services, government services, banking and finance, and telecommunications.[4]

The following figures illustrate the critical nature of the transportation sector in Canada. The transportation sector accounted for 3.9 percent of Canada's GDP in 1998 and directly employed approxi-

[3] This list is inspired by the discussion of the nature of information warfare in *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, 2d ed., Joint Campaign (July 4, 1996), pp. 1-17–1-18. Available in its entirety at ⟨*http://www.infowar.com/mil_c4i/joint/joint.html-ssi*⟩.

[4] This follows in part the breakdown used in the October 1997 *Critical Foundations: Protecting America's Infrastructures*, the report by the President's Commission on Critical Infrastructure Protection.

mately 730,000 people, accounting for a 6.4 percent share of total employment. Government spending (all levels) on transportation for the 1997–98 fiscal year was $17 billion; investment in transportation by governments and businesses averaged $18.8 billion per year between 1993 and 1996. In 1997, tourist spending in Canada totaled $44 billion, 40 percent of which was on transportation.

Threats to and the protection of components of the national infrastructure, both physical and informational, have long been part of defense planning and operational activities in both peace and conflict. Over the last few decades, technological advances have brought qualitative changes to large segments of the infrastructure, particularly in the manner in which they operate, the way they are managed, and the extent to which they are interdependent. These changes have resulted in important gains in efficiency of service, lowered costs, and expanded markets, but they have also increased the number and types of vulnerabilities within the infrastructure, particularly from an information management perspective.[5]

One way to view the increased vulnerability of the infrastructure is to examine the change in the context within which the infrastructure operates. It is in this light that the concept of IO becomes useful in

[5] The term National Information Infrastructure (NII) is frequently used to describe the dependency on information that exists in the functioning of the various components of the infrastructure. The United States Army gives the following definition: "A series of components, including the collection of public and private high-speed, interactive, narrow and broadband networks. NII is the satellite, terrestrial and wireless technologies that deliver content to home, business and other public and private institutions. It is the information and content that flows over the infrastructure in the form of databases, the written word, television, computer software, etc. It is the computers, televisions and other products that people employ to access the infrastructure. It is the people who will provide, manage and generate new information, and those that help others to do the same. The NII is a term that encompasses all these components and captures the vision of a nation-wide, invisible, seamless, dynamic web of transmission mechanisms, information appliances, content and people. The global accessibility and use of information in the NII is especially critical given the increasing globalization of markets, resources and economies." From FM 100-6, *Information Operations*, U.S. Army Training and Doctrine Command (October 2, 1995), quoted from *Information Warfare and the Canadian Forces*, document no. 1350-004-D001, Version 1 (May 9, 1996).

analyzing infrastructure vulnerabilities. Much of what has changed in the infrastructure is the way operations are performed, controlled, and monitored. Increasingly, various components of the infrastructure are automated and rely on remote monitoring and control, such as Supervisory Control and Data Acquisition (SCADA) systems, in the conduct of operations. Another aspect of automation in the infrastructure has been the increasing reliance on commercial-off-the-shelf (COTS) information technology products to replace aging custom-engineered systems such as those used in air traffic control.

For decades, the automated systems in use in civil aviation were custom engineered, designed to fail-safe in crisis or unusual circumstances. Although this still holds true today with respect to highly robust system designs, the progressive inclusion of COTS technology in large systems, combined with the greater access and easy-to-use tools that can permit interference (point-and-click virus labs, "how to" guides to hacking, etc.) have raised concerns about how secure civil aviation systems really are.

The short and immediate answer is that, currently, civil aviation systems are quite secure. First of all, most systems still have significant custom-engineered components not easily accessible or understandable even by adept attackers. Civil aviation systems are also inherently robust, having strong backup mechanisms, either built-in or alternate (human), which are regularly tested in the course of circumstances such as power cuts to control towers and erroneous automated flight data. And new systems are, more often than not, engineered or configured within an elaborate security architecture meant to reduce to a minimum the potential for improper use or willful interference. One more very important consideration—related to the robustness aspect—is that the possibility of system failure or breakdown is a central feature of the design in that it is always a consideration and is addressed through the inclusion of redundant or parallel systems and subsystems. Systems are designed with the requirement that there be no single point of failure. In this sense, civil aviation systems are considered extremely hard targets for an IO attack, regardless of its origin.

There is, however, another set of challenges to the vulnerability of civil aviation systems—what has been termed "the insider problem." This has long been a concern in "traditional" aviation security, and one can recall several incidents in which airline or airport employees, or persons posing as such, facilitated or perpetrated acts of unlawful interference with civil aviation. The IO concern that arises is that of the potential for tampering with or modifying source code or specifications included in installation or maintenance manuals, embedded components, and flight management systems, for example, by people having intimate knowledge of a given system. Modifications could be introduced at several points during the manufacturing or maintenance processes, and could result in system failure not addressable by existing backup systems and procedures. The IO issue, in other words, expands the range of potential failures to include some that are not addressed in normal system design. Although such occurrences are deemed to be highly unlikely, windows of opportunity exist and could be exploited by entities on the high end of the threat spectrum—that is, states or terrorist organizations possessing a high degree of technical sophistication.

Some of the specific areas where such opportunities could be exploited include flight management system data, software-based flight control systems (flight control logic), parts manufacturing (specification modification), and maintenance specification modification. Yet, though windows for unlawful interference with these systems do exist, many if not most of them, particularly those involving actual aircraft operations, are extremely well protected, not only by their design and the sheer level of expert knowledge involved but by the administrative processes that are integrated in the elaboration of these systems (multilevel certification by external bodies).

There exists yet another order of potential IO problem areas with regard to civil aviation. These are areas that may be more easily targeted by a recreational or casual hacker or a determined and organized attacker (state or terrorist group)—areas that, if successfully targeted, could disrupt civil aviation operations on a broad scale. These are power distribution, communication lines (telephone), and administrative systems. Some examples of critical, while not particularly complex, systems, include electric power to the control tower (failure over extended period); phone lines, both for tower communications (emergency services access—fire, ambulance, police, weather conditions) and radar (radar data runs on dedicated rented phone lines); electric power for airport lighting, ventilation, etc.; computer reservation systems; passenger manifest data; physical access control; and passenger/baggage matching systems.

Disruption in these areas can have an immediate and significant impact (ripple effect) on the civil aviation system. Given the highly interdependent nature of an infrastructure that often extends beyond national borders, localized disruptions can severely affect larger systems. Disruptions at a major hub such as Toronto can have grave consequences for national systems in terms of flight reassignments and delays, which can result in significant financial losses for the industry as well as potential longer-term effects on passenger and public confidence in the system as a whole. In addition, such disruption can affect the operations of the entire range of service providers and other transportation sector players that feed into the civil aviation system, either directly or indirectly, such as air navigation system, catering, mail and cargo delivery, passenger rail, and cruise ship operations.

In summary, it is clear that IO threats are a matter of concern for civil aviation. The greatest potential threat is not the threat posed to aviation-specific systems, but rather the threat to those systems that support them, such as electrical power distribution.

3. Prevention—Canada's Way Ahead

One of the first questions a policymaker faces is where to focus limited funds and resources to obtain the best result. In addressing current IO challenges, there are two general paths followed, most often in conjunction: (1) to focus on identifying and prosecuting perpetrators, bringing them to justice in the face of tremendous hurdles (technological, jurisdictional); (2) prevention, whereby vulnerabilities are identified and possibly corrected, in areas of information technology and management. Ideally, both the preventive and prosecution components should be pursued, but the preventive route yields potentially greater immediate results in that it ultimately reduces the overall vulnerability of the infrastructure by eliminating system holes and by educating users. Raising awareness levels is a critical component in pursuing the preventive agenda. The degree of sophistication of an attacker needs to be greater in the face of a more secure system that is managed with sound security administration practices (password change schedule, strict access permissions control, personnel screening, etc.).

One question that arises in pursuing the preventive agenda is the possibility of conflict between its objectives and those of the prosecution/administration of justice agenda. Information gathered in the course of an investigation, particularly relating to technical methods and approaches, can often be critical in addressing vulnerabilities, but the necessity of protecting evidence prevents it from being released. In such cases the potential benefits in terms of awareness and the elimination of vulnerabilities can be greatly reduced. Policymakers have to address this issue and develop mechanisms that permit greater access to and distribution of investigation-based information.

Although Canada has not yet issued a definitive policy on critical infrastructure protection, the focus in most departments, other than enforcement bodies, appears to be on prevention within the limited budgets available—on vulnerability assessments, system mapping, reviews of IT security system policies, standards, and practices in order to improve the government's preventive posture. Several business-related initiatives are also under way in government that are likely to further the preventive agenda, including the Public Key Infrastructure (PKI) initiative, which will give the government the security it needs to conduct its business electronically in order to improve service delivery. This initiative ties into Canada's e-commerce strategy, which aims to create the conditions for national e-commerce to grow. Some other components of the e-commerce initiative are a policy on cryptography, establishment of a legal framework for digital signatures and electronic documents, and legislation governing the protection of personal information in the cyber domain.

A preventive approach has also been adopted to address threats in the civil aviation security area. Work with the civil aviation industry has been done to ensure that there is at the very least a recognition that the operational environment has changed and that some thought needs to be given to a number of previously unheard of threats that may constitute problems in the future. In Canada, most of the transportation infrastructure is in private hands, and therefore the elements that drive the risk management process in industry are somewhat different from what they are in government. The challenge with industry currently is that of demonstrating a clear threat. While there are few precedents that would compel industry or even Transport Canada to act in order to modify the preventive security posture of civil aviation in Canada, there are certainly enough data (mostly of U.S. origin) to investigate what the IO environment needs in the long run. The point that has to be made to industry is that, though catastrophic failure resulting in mass casualties is unlikely, there may well be incidents that will have some serious economic impact.

Looking at the various arrangements that exist for effective international cooperation in general, the work and structure of the International Civil Aviation Organization (ICAO) provide much food for thought.

4. The International Civil Aviation Organization as a Model for International Cooperation on Cyber Terrorism

The International Civil Aviation Organization was established in 1944, by means of the Chicago Convention, to develop international standards and recommended practices for the aviation industry. Now, over 180 states are parties to this Convention. Its basic objective is the development of safe (including secure), regular, efficient, and economical air transport. Acts of unlawful interference such as terrorism are a primary area of concern, and security is one of its official priorities.

The Chicago Convention as a multilateral international convention specifically addresses preventive security practices for international civil aviation in its Annex 17, adopted by the ICAO Council in 1974. The security standards and recommended practices contained in Annex 17, together with the implementation guidance contained in the ICAO Security Manual, essentially establish the preventive security regime for civil aviation. Once standards are developed, states parties must file a public difference if they do not agree.

Besides the ICAO, there are other multilateral international security conventions in place that deal with response to acts of unlawful interference against aviation. These include the Tokyo Convention of 1963, which established criminal jurisdiction; the Hague Convention of 1970, which removed safe haven and freedom from prosecution; and the Montreal Convention of 1971, which extended the range of offenses that could be pursued. The Convention on the Marking of Plastic Explosives for the Purpose of Detection, which came into force in June 1998, constitutes a departure from these conventions in that it focuses on the prevention aspect.

At this time there is probably little in terms of incidents or trends that would move the ICAO AvSec (Aviation Security) Panel to address the issue of cyber terrorism as a priority, but ICAO has nonetheless achieved much in terms of cooperation and consensus that may be helpful in supplying best practices and guidance for cooperation in the IO field. In fact, the two areas, civil aviation and the information technology infrastructure are similar in many ways: they present major challenges to safety and security; they represent a serious threat to their users if attacked; they have become critically important to national and international commerce; and neither can be contained by national boundaries. The similarities are useful to keep in mind when going over what type of preventive security regime has been achieved by ICAO.

The major elements in the preventive security program that states parties to ICAO Annex 17 observe are the establishment of national organizations, cooperation with other states, establishing preventive security measures, managing response to unlawful acts, and establishing security-related planning and training. As the record indicates, the efforts of ICAO member states appear to have had a positive impact on the state of civil aviation security (Figure 1).

A more detailed analysis of Annex 17 shows that the agreed-upon framework offers many concrete measures, the structure of which could potentially be applied or adapted to counter IO threats.

Establishing national organizations to develop and implement plans and procedures. The national organization should participate by: designating an administrative authority, establishing a security program, reviewing national threat level and adjusting as necessary, defining and allocating tasks between state, operators, etc., establishing airport security committees, ensuring the development of contingency plans, ensuring the development of training programs, conducting background checks on those implementing security, requiring operators providing service to implement security programs, and promoting security R&D. Many of these measures could be applicable in the establishment of a national IO security program. A national organization would be necessary to manage, guide, and focus development and to provide a conduit for information exchange. An international organization, similar to the ICAO, would of course also be required in order to harmonize and coordinate the efforts of national organizations.

Cooperating with other states to adapt their security programs: by making written programs available to other states, including appropriate clauses in bilateral agreements, meeting requests of other states for special measures, cooperating in the development of training programs, and cooperating in security R&D. These measures, in addition to fostering compatibility and adding the benefits of world-class knowledge and experience, would promote participation and cooperation and help to ensure that less privileged states reap the same security rewards as wealthier or more technologically advanced states.

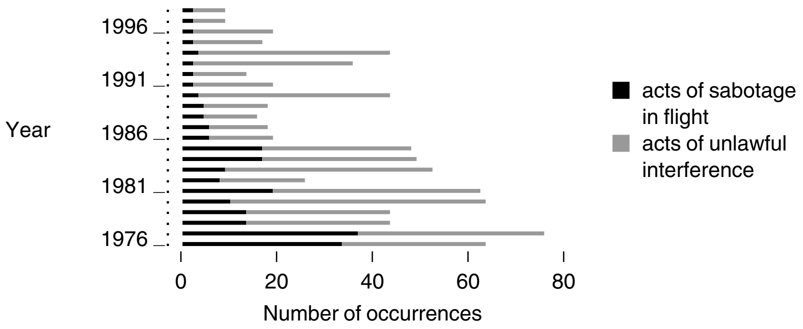

Fig. 1. ICAO figures, 1976–1996.

Establishing preventive measures to prevent weapons, explosives, and other dangerous devices from being introduced by any means whatsoever: by preventing unauthorized carriage of weapons; conducting pre-flight checks to discover suspicious objects; surveying, inspecting, and testing to ensure security implementation; controlling transfer of passengers and goods to prevent introduction of weapons; establishing identification and access control procedures; and ensuring that design and construction of facilities take account of security needs.

This is probably an area where the IO threat would pose the most challenge. Concrete measures that address operational issues must be developed if an international convention is to mean anything. The pace of technological change makes this requirement particularly difficult to address, and this is where increasing awareness through structured programs focusing on industry/government consultations and cooperation can produce significant results, such as standard industry-wide strategies to present and address issues and problems.

Managing response to unlawful acts: by taking measures for safety of persons subject to acts of unlawful interference, exchanging information on incidents with other states, providing the ICAO with information as soon as possible after such incidents; expeditiously notifying all implicated states and the ICAO; and reevaluating security to remedy weaknesses subsequent to incidents. It is imperative to mitigate harm caused by incidents as expeditiously and efficiently as possible.

These measures are meant to ensure that response by the concerned community is as swift and complete as possible.

Miscellaneous measures from other ICAO Annexes that are relevant to security: broadcasting warnings if subject to unlawful interference; establishing training programs to minimize the consequences of unlawful interference; permitting tax/duty free importation of security equipment; assisting, on a priority basis, aircraft subject to unlawful interference; notifying rescue centers, operators, other aircraft operating in the vicinity; establishing emergency plans for threats, fires, sabotage, natural disasters, etc.; and periodically testing plans and revising them as appropriate.

The first thing to examine if ICAO is to be considered, if not as a model, then certainly as a source of best practices and lessons learned, is what forms the basis for consensus. Why has ICAO been successful in obtaining consensus and building agreement on security issues? There is general agreement that unlawful interference with civil aviation is deemed by all to be contrary to the public good and to the main objective of preserving human life. The stigma of terrorism is a long-lasting one for any state or industry associated with it (e.g., *Achille Lauro*—U.S.$ 300 million immediate direct loss), and those that carry the stigma pay a heavy price. This general, unconditional agreement—that terrorism is to be done away with and its perpetrators brought to justice—is the fundamental underpinning of consensus building within ICAO on the security front.

A consensus analogous to the one that exists on civil aviation terrorism is difficult to achieve in the area of IO threats, in spite of the similarities noted above. A consensus for IO may be more difficult because of the remoteness of the threat to human life: the existing body of incidents that can clearly make the link between IO-type attacks and the loss of life is probably not sufficient to make the case in favor of basing consensus on the protection of human life. Moreover, we do not have any internationally accepted definition of what constitutes IO threats or even cyber terrorism.

Yet there are sufficient data to support at least a partial agreement on the basis of the potential for serious harm—individual, social, and/or economic. The case can be made that potential widespread disruptions in economic activity brought on by an infrastructure attack, regardless of source, are serious enough to pursue international cooperation.

It is also noteworthy that ICAO has been successful in building consensus on commercial matters. One positive result has been the harmonization of minimum regulatory standards and practices (in no way related to security) that facilitate international aviation. The underlying consensus-building motivation on commercial issues has been a belief in an open system in which interoperability is the norm. The creation of an international voluntary regime that would establish minimum standards for a secure infrastructure environment might go part of the way in addressing a common response to IO-type threats, permitting the establishment of a baseline for managing risk in the IO environment. Some examples of elements that could constitute this sort of regime include consumer protection laws extending to the cyber domain, the existence of a national IO threat information clearinghouse, making cyber crime a punishable offense under law, having open access to strong encryption, and having information and data handling and storage standards.

The list of ICAO preventive security measures becomes relevant here. An international regime could take the form of an ISO-type approach to basic quality standards that businesses and/or countries could strive for. This would in effect create a preventive regime framework standard against which companies and countries could be assessed.

The IO threat is so broad and the interdependencies it underscores (power distribution, telecommunications) so numerous that addressing it sectorally, such as in an ICAO-type forum, may not be practical. Because the IO operational environment cuts across all economic activity, it could probably be best addressed in an international forum with a broad mandate, and in international organizations such as the International Organization for Standardization (ISO) and the International Telecommunications Union (ITU). Nonsector-specific business organizations could also be considered, although the grounds for consensus may be somewhat at odds with what could be possible within an international state-based entity. Some business organizations that are currently addressing issues surrounding e-commerce include the Alliance for Global Business (AGB) and the International Chamber of Commerce (ICC).

5. Government and Industry

One of the difficulties in addressing the issue of IO-type threats and, by extension, critical infrastructure protection in Canada is that most of the components of critical infrastructure are now managed not by government but by private entities. The main thrust in Canada for commercializing the management of much of the infrastructure was to increase efficiency and to have the users of the systems—not all taxpayers—foot the bill. This push has also included an effort to reduce the regulatory burden on these entities. So the challenge we face in Canada at this juncture is to convince industry, without resorting to regulation, that IO threats are a problem and that critical infrastructure protection is a new part of the equation of doing business. This places the onus on industry for action and requires that government act not as a regulator and enforcer but as an enabler and facilitator. This is certainly the route the Canadian government has taken with regard to electronic commerce.

The transportation industry in Canada recognizes that IO threats, at the very least, are one more item to consider in managing risks. The problem is that very few probably realize the extent to which these threats could rapidly become serious problems affecting their operations. Keeping industry abreast of these developments through security awareness and consultation forums is part of our role as a government; where danger to the public is not voluntarily addressed by the private sector, government can implement enforceable requirements.

Cooperation with industry is central to developing a workable approach to tackling the IO issue. This not only includes those areas dealing directly with infrastructure but also must involve manufacturers and providers of IT services. Consultation forums involving all levels of government and a cross-section of industry may prove beneficial for airing problems, devising common approaches, and sharing best practices. This strategy worked very well for Canada in preparing for and addressing the millennium-bug problem. Raising awareness in government, industry, and the general population was key to achieving the critical mass necessary for significant remedial action to be undertaken and central coordination permitted to maintain focus. The same sort of vehicle could be considered for the IO issue.

Canada is in the process of developing a national policy on critical infrastructure protection that will very likely include a significant role for private industry in supplying expertise and guidance to government and those entities that manage our critical infrastructure. The policy is also likely to support the creation of a Computer Emergency Response Team or CERT-type body that could serve as a clearinghouse for information and advice on system vulnerabilities and solutions. None of this is yet defined or agreed upon, but one thing is clear: government and industry will have to work in partnership to address this issue successfully.