CHAPTER 3

The Civil Aviation Analogy

PART III

Past as Prologue: International Aviation Security Treaties as Precedents for International Cooperation Against Cyber Terrorism and Cyber Crimes

Mariano-Florentino Cuéllar

The rise of cyberspace may seem unprecedented, but in some respects it bears a striking resemblance to the development of aviation—a technology that also effectively shrank the world and altered life during times of war and peace.[1] In less than a century, civil aviation went

1. The dictionary defines cyberspace as "the online world of computer networks." (*Merriam-Webster's Collegiate Dictionary*, 1997). For the purposes of this paper, the term "cyberspace" denotes the multifaceted global network of computerized information exchange (including the Internet) made possible by information technology. "Cyber crime" refers to crimes committed within the scope of (or greatly facilitated by) cyberspace. Descriptions of aviation technology suggest the similarities with cyberspace. Martin Sharp, upon completing a flight in the first jet airliner (the de Havilland Comet), declared, "One arrives over distant landmarks in an incredibly

from being exotic to being essential. In the process, states with considerable political, economic, and legal differences were forced to cooperate to improve the security of civil aviation. As the following pages discuss, the extent of this cooperation was unprecedented.

1. Overview

Over the years the system of international law protecting civil aviation security has developed three features, all of which are deeply relevant to the international challenge of policing cyberspace. First, the system combines regulatory authority and criminal enforcement. Second, the system has expanded over time to encompass new threats affecting the security of the network (in this case, civil aviation), and to include an ever growing cluster of nations. Third, the system exhibits what economists term "path dependence": initial focused steps favoring legal cooperation made the system safer, which increased the system's economic value and thereby encouraged countries to take further steps toward legal cooperation even in the face of domestic political opposition. Airspace and cyberspace are obviously different, but certain institutional characteristics of cyberspace mirror those of the international civil aviation network in critical ways. In both cases, the relevant economic activity takes place in a decentralized, interdependent network that needs to be policed in the face of rapidly changing technology. For this reason, the system of international legal cooperation to promote aviation security serves as an engaging precedent for the modern challenge of international cooperation against cyber threats.[2]

short time but without the sense of having traveled." Quoted in ⟨*http://www.skygod.com/quotes*⟩, accessed July 15, 1999.

2. The focus on aviation is the result of a survey of international cooperation and treaty law conducted to evaluate suitable models for cooperation. Among other areas, we surveyed cooperation against narcotics trafficking and money laundering, nonaviation-related terrorism, and economic cooperation in postal services, telecommunications, and resolution of the Year 2000 computer problem. The international law framework governing civil aviation security appeared especially promising as a

Yet, ironically, these emerging cyber threats also point to the shortcomings in the existing aviation security system. Civil aviation depends on networked technology infrastructures to provide electric power, remote sensing capabilities, and communications. All these infrastructures are vulnerable to cyber threats; a disruption in one can cause fatalities as surely as an explosive charge nestled in the belly of an airliner. Accordingly, cyber threats are not materially different from the threats that spurred adoption of the aviation security treaties in the first place. For all the present system's laudable achievements, the framework of international law protecting civil aviation is not fully prepared to address the emerging cyber threats made possible by increasingly accessible technologies. Given that deficiency, draft treaty language is proposed herein that would provide enhanced coverage of cyber offenses targeting civil aviation. In addition to addressing specific threats in the sector, the proposed language illustrates a promising approach to addressing international cyber threats by focusing on an infrastructure that has already garnered considerable international legal attention and by expanding the existing framework to cover the most prominent and unpredictable new threats from cyberspace.

To make these arguments, this part of Chapter 3 proceeds as follows. Section 2 focuses on the structural barriers to international cooperation that states have overcome to build a legal framework improving aviation security. Section 3 describes what legal mechanisms states have used to overcome these barriers in the case of civil aviation security, focusing particularly on the advantages of developing both an enforcement and a regulatory component to improve security. Section 4 concentrates on why the aviation issue gave states a distinctive reason to overcome structural barriers through innovative legal approaches to cooperation. Section 5 then discusses the shortcomings of the system in addressing cyber threats, and proposes draft treaty language to address these shortcomings. Finally, section 6 con-

---

model for cooperation against cyber threats. See sect. 2 below for a fuller discussion. For additional discussion of international legal arrangements that serve as effective analogies for international cooperation against cyber threats, see Chap. 6.

cludes by observing that the use of explicit treaties (as opposed to informal agreements) has given the international civil aviation security system a means to promote deterrence, grow international consensus, and enhance technical cooperation against threats. When existing treaties lay such a foundation, advocates for international cooperation against cyber threats can achieve considerable gains by amending treaties dealing with specific infrastructures (such as aviation) to encompass cyber threats. In contrast, advocates of a comprehensive international accord on cyber threats face far greater obstacles, because even in the twenty-first century, states continue to harbor concerns that broad international crime treaties arouse domestic political opposition and encroach on their sovereignty.

2. Structural Barriers to Achieving International Cooperation

To build an effective international system protecting civil aviation security, states have overcome a number of structural challenges.[3] Both domestic and transnational political developments alter the context for cooperation, often encouraging states to prefer flexible informal agreements instead of explicit treaty obligations. The framework under which international cooperation can achieve a particular goal must frequently contend with technological complexity and innovation. Moreover, all cooperative arrangements are subject to enforcement challenges. Below, I analyze these challenges and explain why the use of explicit treaties—an approach that has characterized civil aviation security—is likely to produce more lasting results.

An initial challenge is the reluctance of states to bind themselves legally through the formal use of an explicit treaty rather than an informal agreement. In civil aviation security, informal agreements have always been supplemented by treaties. It may seem self-evident that a treaty is preferable to an informal agreement: after all, formal

3. In sect. 4, I argue that international cyber crime cooperation faces many of the same structural challenges that have been overcome in civil aviation security.

treaties have been the hallmark of the civil aviation security system and are frequently the capstones of international negotiation to address transnational challenges ranging from environmental protection to migration.[4] Yet informal agreements and cooperative ventures have played an important role promoting cooperation, for several reasons. Informal agreements are more flexible, allowing countries more latitude to change their observance of terms in response to evolving domestic and transnational political developments. In the criminal context, only significant criminal offenses—such as murder and large-scale narcotics trafficking—have been considered extraditable crimes. For a variety of other offenses, a host of organizations and actors still have significant incentives to cooperate through informal agreements. For example, there is no significant multilateral agreement specifically focused on combating credit card fraud. Nonetheless, domestic law enforcement agencies, the private sector, and consumers still have strong incentives to cooperate in addressing such fraud. Although credit card fraud is still a nettlesome problem, some law enforcement agencies and analysts report that projected increases in these offenses have not materialized.

As an example of the advantages and limitations of informal agreements, consider the case of money laundering. In spite of an apparent consensus on the deplorability of money laundering and narcotics trafficking and a great deal of international interest, the international agreements covering these activities have not proved to be entirely suitable models for international cyber crime cooperation. The major international mechanism currently addressing money laundering enforcement is the Organization for Economic Cooperation and Development's (OECD's) Financial Action Task Force (FATF).[5] Under OECD auspices, the work of FATF centers on promoting the adoption and implementation of a basic document containing forty major recommendations to enhance laws against money laundering. This doc-

4. See sect. 3.

5. For a discussion of the creation of the FATF, see FATF, Tenth Annual Report, July 2, 1999.

ument does not have the binding force of a treaty, but a large number of OECD members (including the world's ten largest economies) have made a political commitment to implementing the forty recommendations.

Although FATF has achieved some noteworthy results, money laundering presents a striking opportunity for countries to expand formal cooperation to address the problem meaningfully. Among its achievements, FATF has developed a standard definition of the money laundering offense (though not all its predicates), and has provided technical assistance to members and nonmembers attempting to develop anti-money laundering measures; it has also instituted a system for mutual evaluations of member countries. The use of an international agreement such as FATF does not mean that treaty law gives states carte blanche with respect to dirty money, but the absence of a treaty means participants retain considerable flexibility to choose their enforcement strategies. After all, money laundering can have a large number of predicate crimes, including terrorism, narcotics trafficking, fraud, and arms trafficking. And without a specific treaty-defined conception of predicate offenses, combating laundering activity can mean different things to countries depending on their predicate offenses. Moreover, the financial system has grown increasingly global and efficient in transacting its business. Although FATF's membership constitutes an important bloc, international movements of money allow numerous jurisdictions with smaller economies and strict bank secrecy laws to play a role in money laundering, and even the members of FATF themselves vary in the strength of their bank secrecy laws. As a result, it has become more difficult to control illicit financial flows through regulation or criminal investigation that targets a single national financial system.[6] At the same time, lucrative criminal activity

6. Examples of transnational money laundering activity abound, but a simple hypothetical case serves to illustrate the principle. As long as money laundering within and across national borders persists—activity that can take place in Japan, Switzerland, and a myriad other locations—financial regulation and investigation targeting only Japan could hardly dent such a system. The best that such a domestic strategy

has a more global scope, and can spread its negative externalities over a greater proportion of countries.

The persistent reliance on international agreements arises because obstacles to cooperation counterbalance incentives for treaty use. Although crimes such as money laundering have negative externalities for many states (where crime becomes more profitable), the activity can generate large returns for other states, especially bank secrecy havens whose bank balances swell with potentially ill-obtained money. Finally, economic interests (in this case financial institutions) within the states can perceive a threat from treaties that explicitly or implicitly impose additional requirements on their behavior. As a result, significant multilateral treaties to control money laundering have been out of reach, and interested parties have instead turned to informal agreements. Thus, although the FATF recommendations serve as an auspicious beginning, most recently extending even to Internet banking transactions and Internet gambling, they lack a reliable enforcement mechanism even for member states, let alone for nonmembers. For these reasons, this paper supports treaty language to complement the preventive system in the aviation context (discussed in section 5 below), and a broader treaty (discussed in Chapter 6 of this volume) to cover cyber threats beyond aviation.[7]

Technological complexity and change can also become structural obstacles to cooperation, making specific treaty language harder to define and exacerbating the need for preventive as well as enforcement approaches. In light of these obstacles, centralized technical organizations, though they do not guarantee success, make an important contribution to the advancement of safety and security goals. In the context of aviation security, the International Civil Aviation Organi-

---

could achieve would be to increase the costs of the initial placement of resources in a domestic financial institution.

7. Even the preventive system that characterizes aviation has a nexus to treaty law (see sect. 2 above). Both the civil aviation context and the other areas of international cooperation surveyed in this project suggest that treaty commitments change states' political incentive and encourage cooperation even beyond the provisions of a treaty.

zation plays such a role. The ICAO lacks the power to sanction members for noncompliance with treaties or its own regulations, but it serves as a forum of exchange and consultation.[8] With more and better information, key member states can then coordinate their activities or act unilaterally. Generally, treaties dealing with civil aviation and other commercial matters, such as telecommunications, postal cooperation, and the commercial aspect of civil aviation, give rise to an international organization of some type.[9]

Compliance is a further obstacle to cooperation. In this regard, it appears that specific, narrowly drawn offenses have created a regime where compliance is the subject of less controversy. Information is easier to gather and analyze when offenses are clearly defined—compare aviation, for example, to narcotics enforcement, where offenses are wide-ranging but where even a system of "certification" by the United States (backed by threatened sanctions) does not appear to lead to long-term enforcement solutions in countries that are the source of narcotics. Consider also the difficulty of monitoring a country's adherence to the FATF's 40 Recommendations against money laundering. The recommendations are quite broad, and although it may be possible to monitor cash flows, information on aggregate money laundering activity is notoriously difficult to obtain.[10] Since the variable of most direct interest to compliance cannot be monitored directly, assessing compliance requires an analysis of countries' policies against money laundering. Yet even this is not enough, because policies as they exist in theory and as they are implemented in practice may vary considerably, so that a team of experts has to travel to a country to

8. The history of the ICJ provides an apposite illustration of this difficulty. See, e.g., Shabtai Rosenne, *The World Court: What It Is and How It Works* (Norwell, Mass.: Kluuwer Academic, 1989), discussing the limitations faced by the ICJ in building legitimacy for its interpretation of ambiguous provisions in treaties.

9. Hence the Chicago Convention, discussed below, led to the ICAO.

10. See, e.g., Vito Tanzi, "Money Laundering and the International Financial System," IMF Working Paper no. *96/55* (1996). Although the FATF recommendations are not a binding obligation on the same order as those of a formal treaty, countries may have an interest in complying for diplomatic and economic reasons.

find out how a policy is being implemented. The breath of the agreement (that is, its inclusion of financial institution regulation as well as criminal investigation as an aspect of anti-money laundering policy) increases the work of the evaluation team and also the probability that its evaluation will not be accurate.

Finally, the threat of international sanctioning activity can play a positive role in achieving common goals. For example, although the G-7 (now G-8) is not formally empowered to enforce treaty obligations, it coordinated to punish countries that do not comply, as in the 1982 G-7 punishment of Afghanistan by denying it landing rights when it failed to extradite or prosecute the hijackers of a Pakistan International Airlines plane that landed in Afghan territory. As we shall see below, these threats of unilateral or multilateral sanctioning also help enforce ICAO standards and recommended practices, given the organization's lack of extensive tools to compel members to implement the guidelines.[11]

3. International Cooperation to Achieve Civil Aviation Security

Since the time aviation became commercially viable, air safety has been a compelling objective for a large number of states around the world.[12] Given the magnitude of the structural challenges discussed above, it is hardly surprising that the architecture of the current international civil aviation system took shape over most of the twentieth century, beginning with blanket agreements that established a frame-

11. See Pierre de Senarclens, "Governance and the Crisis in the International Mechanisms of Regulation," *International Social Science Journal* 50 (1998): 91, arguing that effective global governance depends on the coordinated action of states in support of international regulatory regimes, since most international organizations are not powerful enough to induce compliance by themselves.

12. Mark W. Zacher with Brent A. Sutton, *Governing Global Networks: International Regimes for Transportation and Communications* (New York: Cambridge University Press, 1996), p. 94: "In probably no other international industry is safety or the prevention of accidents a bigger issue than it is in air transport."

work for international air travel.[13] But if the scope of what was considered to be a safety concern changed over the years, the concern over safety did not change. Early in the twentieth century, countries sought to limit dangerous accidents and commercial crimes.[14] By the middle of the century, terrorism had become a threat throughout the world.[15] The interest in reining in aviation-related terrorism resulted in an incremental series of treaties beginning with the Convention on Offenses and Certain Other Acts Committed on Board Aircraft in 1963 (the Tokyo Convention). Although the present cooperative regime provides a coherent framework for extradition, investigative and regulatory cooperation, and technical assistance, the process that has produced these arrangements thus far suggests that the system may continue to change over time. In succeeding decades, states turned their attention to activities that upset the idealized framework chiseled early in the century. The first such agreements were concerned with airborne threats to aircraft in flight. Later, states agreed that threats to aircraft in flight need not originate in the air, and they developed conventions addressing threats to aircraft preparing for flight, navigation systems, and airports.

13. This discussion only highlights the most significant international civil aviation agreements. For a more all-encompassing discussion of relevant agreements through the late 1980s, see Paul Stephen Dempsey, *Law and Foreign Policy in International Aviation* (Dobbs Ferry, N.Y.: Transnational Publishers, 1987).

14. Commercial crimes were a concern long before terrorism was. For a discussion of the role of commercial crime control in nurturing the infant aviation industry, as it had nurtured crime control in the marine shipping and rail transport domains, see Frederick C. Dorey, *Aviation Security* (New York: Kluuwer, 1983), pp. 106–9.

15. Aviation-related terrorist activity was at first more common in Soviet-bloc countries, but by the late 1950s, Western nations increasingly became the targets of such terrorism. Robert A. Friedlander, *Terrorism: Documents of International and Local Control* (Dobbs Ferry, N.Y.: Oceana Publications, 1984), p. 324, describes the growing interest of the United States and Western Europe in safeguarding aviation security following high-profile aviation security breaches targeting them.

Early Cooperation: Paris and Chicago Conventions

The Air Navigation Convention of 1919 (the Paris Convention) was the first major attempt to develop rules for international civil aviation. The principal objective of the Paris Conference was to establish a system for major countries to consult each other and agree on standards governing transnational civil aviation.[16] To this end, it was attended by representatives from nearly every region of the world, although the initial agenda was set primarily to reflect the interests of European countries.[17] In fulfilling its objective, the Paris Convention had three major substantive concerns. First, it settled much of the ambiguity concerning countries' rights to their airspace; although the treaty included language emphasizing the importance of rights-of-access to nonhostile aircraft, the right of a country to control its airspace was recognized as well. Second, it established a framework for allowing civil flights to occur between countries.[18] Third, it authorized the creation of the International Commission for Air Navigation (ICAN), and airlines created the International Air Traffic Association, to develop safety and technical standards. Significantly, the Paris Convention continued the approach taken in the law of the sea, which distinguished between civil and military vessels requiring access to ports. Like many treaties dealing with economic activity, the treaty depended crucially on countries' interests in maintaining positive reciprocal relations.[19] Unilateral and multilateral sanctions against noncompliance were contemplated.

The Paris Convention was amended several times after it came into force. Because its primary focus was overall cooperation, it did not create obligations that could have any direct relevance to cyber crime

16. Air Navigation Convention, Paris, October 13, 1919, 41 Stat. 1687.

17. Ramon de Murias, *The Economic Regulation of International Air Transport* (Jefferson, N.C.: McFarland, 1989), emphasizes the interest of European nations in creating a reliable system to transport cargo and people across medium-haul routes.

18. This early system preserved virtually all authority that each country had to regulate civil aviation within its borders.

19. This is the case absent greater, countervailing, interests.

or other types of criminal offenses; nonetheless, the parties confirmed that states had jurisdiction to address offenses taking place in their airspace. In instances where offenses occurred over international waters, the country of registry was granted jurisdiction.[20] The system of international cooperation established under the Paris Convention set the stage for future arrangements that targeted criminal offenses against aircraft.

The Convention on Civil Aviation in Chicago in 1944 (the Chicago Convention) sought to fill in the gaps left by the Paris Convention (and its amendments) in establishing an international regime to facilitate transborder civil aviation activity.[21] Negotiated along with the creation of the United Nations' International Civil Aviation Organization (ICAO), the Chicago Convention and its various components constitute the major international civil aviation convention still in force for the United States. As with the Paris Convention, the primary safety-related objectives of the Chicago Convention concerned the prevention of accidents.

The safety measures contemplated by the Chicago Convention were far-reaching. The accord addressed air navigation rules, and led to the further development of the ICAN through the creation of an Air Navigation Commission. It also established a framework to promulgate and evaluate rules on technical equipment, practices for transporting dangerous goods, rescues in cases of accidents, joint investigations of accidents, and even joint financing of air navigation facilities

20. Given the early stage of aviation and the still-nascent concept of airspace, the simple approach to jurisdiction over crimes taken in early civil aviation conventions is understandable.

21. Convention on International Civil Aviation, Chicago, December 7, 1944, 59 Stat. 1693, 84 UNTS 389. Technically, this is only one of several agreements reached in Chicago at the gathering known as the Conference on International Civil Aviation, but it is the broadest in scope. The other three agreements include: (1) the Interim Agreement, dealing with provisions having effect before the Convention took effect; (2) the International Air Transport Agreement; and (3) the International Air Services Transit Agreement—collectively referred to as the "Chicago Convention." See, e.g., Stephen D. McCreary, "The Chicago Convention: Article 22 and the SFAR 40 Episode," *Journal of Air Law and Commerce* 54 (1989): 721, 722.

in Greenland and Iceland. Yet in the area of crime control, the Chicago Convention merely affirmed the Paris Convention's assignment of jurisdiction over criminal acts on board aircraft. If the act was committed while the aircraft was flying over a country's airspace, that country had jurisdiction; if the aircraft was flying over the high seas, which was considered international airspace, the country of registry had jurisdiction. The structure of the Chicago Convention resembled that of the Paris Convention, although the Chicago treaty included a provision allowing an international organization—the ICAO—to issue the equivalent of advisory regulations, known as "Standards and Recommended Practices" (SARPs).[22] In the period following World War II, the system provided enough flexibility to encompass a significant growth in international cooperation to prevent accidents. Just as the growing reliance on cyber systems has engendered broad interest in protecting the integrity of cyberspace, the marked increase in aircraft size and in the volume of air travel played an important role in spurring such cooperation.[23]

The issues addressed at the Chicago Convention highlight some of the similarities and differences between international civil aviation and cyberspace. In both cases, countries have had to overcome technical hurdles to promote efficiency in the network and to reduce accidents. In the aviation context, countries supported the establishment of an international organization (the ICAO) as a means of marshaling, analyzing, and maintaining technical information to service the international civil aviation system.[24] Of course, one significant difference

22. See Eugene Sochor, "From the DC-3 to Hypersonic Fight: ICAO in a Changing Environment," *Journal of Air Law and Commerce* 55 (1989): 407, describing the regulatory nature of ICAO SARPs and their evolving effect on the international aviation industry.

23. Zacher with Sutton, *Governing Global Networks*, p. 92, explains the effect of the growing economic importance of civil aviation on international efforts to regulate damage control problems in the field.

24. Certain specialized international organizations exist to deal with specific aspects of cyberspace policy, such as the registration and regulation of domain names on the Internet.

between cyberspace and airspace is that the latter is more obviously linked to a country's physical territory.[25] Computers allow information to travel without obviously impinging on a state's physical sovereignty; aircraft penetrate the airspace of more than one country in the course of international flights. As a result, the Chicago Convention adopted an approach that was protective of countries' rights to their airspace.[26]

The Growing System of International Civil Aviation Security

By the mid-twentieth century, countries began to express concern about the security component of the international aviation system. Yet these concerns remained secondary to the development of an efficient economic network to manage air traffic. Cold War divisions also hampered any sustained focus on civil aviation security. Even in its first half-century, commercial air travel yielded considerable economic

25. Nonetheless, although transactions in cyberspace may appear to take place in a domain that is devoid of links to countries' sovereign territory, in fact they are taking place in real space. The difference is that the jurisdictional rules in force determine precisely where in real space the transactions have taken place. Depending on the rule, a legal system could recognize that the transactions occurred in the physical location of the user(s) who initiated the transaction, in the location of the server(s) containing the software that received the transaction information, or in the location of the server(s) used to access the Internet. In some respects, the issues raised in resolving such conflicts are no different from the issues raised in the Paris and Chicago conventions concerning countries' jurisdiction over crimes occurring on board aircraft. For an analogous discussion of how existing conceptions of jurisdiction can effectively resolve even complex disputes about the control of cyberspace, see Jack L. Goldsmith, "Against Cyberanarchy," *University of Chicago Law Review* 65 (1998): 1199, who argues that, analytically, there is no difference between working out conflict of law issues and jurisdiction issues in real space or cyberspace.

26. Indeed, in some respects the degree of recognition over sovereign airspace even trumped concern over safety. Sovereignty over national airspace could interfere with safety if an aircraft is forced to adopt longer or more dangerous routes when a country denies access to its airspace (or certain portions of it). Although the Chicago Convention does express in general terms that countries should allow innocent passage to civil aircraft attempting to shorten routes, the principle is subject to numerous exceptions, consistent with the concern over sovereignty.

benefits.[27] Unfortunately, commercial aviation also provided a sterling opportunity for militants to call attention to their causes through terrorist acts. The physical isolation of aircraft allows offenders to attempt to wrest control from the pilots—which, because of the technical complexity of modern aircraft, can place hundreds of passengers at risk. As instances of criminal activity on board aircraft mounted—particularly targeting Western countries—the inadequacy of existing international law on the problem became evident.[28] The Tokyo Convention was the first major effort in international cooperation to turn attention directly to terrorism targeting aircraft.[29] Because it was the first such effort and because of the exacerbated sensibilities that countries possess about criminal enforcement, the Tokyo Convention's objectives were limited to offenses taking place on board aircraft in flight. In essence, it required states to take control of an aircraft that had been unlawfully seized, and to return the aircraft to the control of its lawful commander. Significantly, however, the treaty did not clearly specify the obligations of the signatories beyond simply taking control of the aircraft: the state taking custody of the aircraft was not obligated to punish the hijackers or to surrender them to a state requesting extradition. The Tokyo Convention depended on its signatories to

27. See, e.g., Betsy Gidwitz, *The Politics of International Air Transport* (Lexington, Mass.: Lexington Books, 1980), who emphasizes the degree of political interest in civil aviation that was stimulated by the economic consequences of rapid, relatively safe, routine air travel.

28. Between 1949 and 1985, over 1,500 persons were killed in nearly 90 separate bombings and explosions on aircraft. Indeed, in the period 1970–1979 alone, criminal acts against civil aviation resulted in 1,255 deaths, as well as 1,013 wounded and 33,097 persons who were taken hostage. See Henrik Gam, "Liability Damages for Injuries Sustained by Passengers in the Event of Hijacking of Aircraft and Other Violations of Aviation Security," *Lloyds Maritime and Commercial Law Quarterly* 217 (May 1988). The striking figures for the 1970s (accounting for approximately 80 percent of total deaths) help to explain the continuing salience of the issue even after the flurry of treaties negotiated between 1961 and 1971.

29. Convention on Offenses and Certain Other Acts Committed on Board Aircraft, Tokyo, September 14, 1963, 20 U.S.T. 2941. Although other conventions had dealt with crime issues to settle jurisdictional matters, the major safety concern in previous treaties was the prevention of accidents, not the punishment of willful, malevolent actions affecting the international civil aviation system.

police themselves.[30] As was the standard practice, disputes were meant to be settled by negotiation or arbitration. If two countries were unable to agree on an organization to perform the arbitration within six months of the request for arbitration, then either party could submit the dispute to the International Court of Justice (ICJ), consistent with its statute. Because of the added breadth of later conventions (the Hague Convention and the Montreal Convention), the Tokyo Convention has not drawn significant enforcement interest from signatories.

The Convention for the Suppression of Unlawful Seizure of Aircraft (Hijacking) of 1970 (the Hague Convention) sought to extend the reach of the Tokyo Convention and to provide for a less porous enforcement system for arresting and prosecuting hijackers and related offenders.[31] Nonetheless, the Hague Convention still focused primarily on hijackings, to the exclusion of many other offenses that could potentially affect the safety of the civil aviation system. Whereas the Tokyo Convention simply required states to take offenders into custody, the Hague Convention required parties having custody of the offenders either to prosecute or to extradite them. The Hague Convention further obligated parties to criminalize the act of unlawfully taking control of an aircraft, or attempting to do so.[32] These offenses were to be punishable by severe penalties. Finally, parties were required to assist each other in connection with criminal proceedings instituted under the treaty.

30. Of course, a state might still punish or extradite the alleged offenders if it chose, but it faced no legal requirement to do so.

31. Convention for the Suppression of Unlawful Seizure of Aircraft (Hijacking), The Hague, December 16, 1970, 22 U.S.T. 1641.

32. The convention makes it an offense for any person on board an aircraft in flight to "unlawfully, by force or threat thereof, or any other form of intimidation, seize or exercise control of that aircraft." Hague Convention, art. I, 22 U.S.T. 1641, at 1644 (1970).

The Montreal Convention and Modern Developments

By 1971, it was apparent that hijacking was not the only threat, or perhaps even the major threat, to the international civil aviation regime. Terrorists could forgo the technical difficulties involved in hijacking a plane, and could threaten passengers and aircraft through interference with the air navigation system, or while planes were on the ground. The 1971 International Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (the Montreal Convention) had the goal of broadening the scope of international legal authority to deal with terrorism targeting civil aviation.[33] In particular, the Montreal Convention sought to protect air navigation facilities and aircraft (along with their passengers) on the ground from terrorist attack. It went considerably further in specifying aviation-related offenses to be criminalized, to include unlawfully and intentionally performing an act of violence against a person on board an aircraft in flight if the act is likely to endanger the safety of the aircraft. Parties also were required to criminalize the placement of explosive devices on aircraft, the destruction or damage of air navigation facilities, and communication of information known to be false that could thereby affect the safety of an aircraft in flight.[34] Whereas the premise for the Hague Convention appeared to be that the most dangerous threats to aviation safety were inside the aircraft, the Montreal Convention recognized that aircraft were simply elements of a civil aviation system that could be disrupted in a number of different ways; damaging an air navigation facility or providing false information to a pilot could be just as lethal as harming the pilot while the plane was in flight. As in the Hague Convention before it, parties were required to apply severe penalties to these offenses, to prosecute or to extradite

33. Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Sabotage), Montreal, September 23, 1971, 24 U.S.T. 564.

34. The Convention also bound parties to criminalize any attempt at such offenses or acting as an accomplice.

the offender, and to assist each other with relevant criminal proceedings.

Because of its somewhat broader scope compared with other treaties on international civil aviation safety, the Montreal Convention could have greater applicability to cyber crime than earlier conventions. Its concern with protecting air navigation systems could be applied to the deliberate use of computers to sabotage an information network essential to the proper function of a navigation system.[35] Since the Montreal Convention also covers offenses involving the provision of deliberately false information to aircraft with the objective of affecting their safety, then certain offenses involving the use of computers to provide false information to aircraft could also be covered.[36] Yet for all the foresight of the Montreal Convention, some potential cyber offenses might well fall outside its coverage, such as a cyber attack designed to cause delays and inconvenience rather than specific disruptions in safety.

Addressing Gaps in Coverage or Enforcement

Over the years, the world has seen a decline in terrorist acts targeting civil aviation.[37] Although general improvements in safety practices and technologies have contributed to the decline, it is likely that the antiterrorism treaties have also yielded some results. They reflect a nearly global consensus deploring aviation-related terrorism. What had be-

35. An "air navigation system" includes sensing equipment, radio and communications equipment, and related technology.

36. Subsequent amendments to the Montreal Convention explicitly criminalize offenses targeting airports (even if these do not directly affect air navigation systems). Protocol for the suppression of unlawful acts of violence at airports serving international civil aviation, supplementary to the convention of September 23, 1971. Montreal, February 24, 1988, TIAS.

37. Michael S. Simons, "A Review of Issues Concerned with Aerial Hijacking and Terrorism: Implications for Australia's Security and the Sydney 2000 Olympics," *Journal of Air Law and Commerce* 63 (1998): 731, 732, indicating that, although terrorism remains a threat for civil aviation and other critical infrastructures, the incidence of annual terrorist activity targeting civil aviation has declined.

gun as a passing reference to crime in early treaties dealing with civil aviation grew to encompass offenses against aircraft in flight, aircraft on the ground, air navigation systems, and airports. The system of treaty law addressing these offenses grew in fits and starts, amid considerable substantive disagreement between countries, some of whom occasionally sympathized with the political goals of offenders.[38] Nonadhering countries have been reluctant to extradite or punish their own citizens, or individuals whose goals are admired.[39]

Countries most concerned about civil aviation–related terrorism have responded to the situation in two ways: through unilateral action and through cooperation with countries that share the degree of concern over terrorism. Unilateral action involves the threat of restricting the access of offending countries to domestic airports, as well as notifying domestic and international passengers using U.S. facilities about airports judged to be unsafe (based on the home country's own safety standards). The U.S. Department of Transportation notifies passengers in U.S. airports when certain airports are not in compliance with a predetermined antiterrorism safety standard, and the Secretary of Transportation possesses legal authority to block air traffic between the U.S. and a certain jurisdiction if that jurisdiction's safety violations are significant enough. The U.S. has also been viewed as part of a de facto enforcement system in instances where states decide not to accept safety and security regulations arising from the ICAO standard-setting process. In a similar vein, the G-8 countries have undertaken a coor-

38. Of course, in most cases, a country that is not in compliance will present a treaty interpretation under which the noncomplying country has in fact discharged its obligations. See, e.g., *Case Concerning Questions of Interpretation and Application of the 1971 Montreal Convention Arising from the Aerial Incident at Lockerbie, Libyan Arab Jamahiriya v. United States of America*, 1992 I.C.J. 114, 1992 WL 190214 (Request for Provisional Measures) (where Libya argued that its refusal to extradite suspects involved in the destruction of a Pan American Airlines flight over Lockerbie, Scotland, was in compliance with the Montreal Convention).

39. For example, offenders' goals could be popular with key domestic constituencies. Hence, a country's leadership may prefer to violate international law instead of strictly adhering to the existing conventions, especially when there is ambiguity in the text.

dinated effort to deny landing rights to airlines from countries that do not cooperate with measures against civil aviation–related terrorism, particularly those that fail to comply with obligations under the Hague Convention and the Montreal Convention. The threat is not idle. As noted earlier, in 1982, the then G-7 punished Afghanistan by denying it landing rights when the country failed to extradite or prosecute the hijackers of a Pakistan International Airlines plane that landed in Afghan territory. The threat of denied landing rights in G-7 countries also played a role in pressuring South Africa to prosecute hijackers who attempted a coup in the Seychelles in 1981.[40]

These reactions to gaps, or compliance problems, in the existing civil aviation treaty regime are instructive in two ways. First, compliance issues recur even when countries ordinarily recognize the value of a particular goal. Second, countries occasionally use access to an international network as a means of furthering safety-related goals. In the case of civil aviation, the network is the international system of conventions and the denial of access is the denial of landing rights. These insights are relevant for the regulation of cyberspace, a context where the ability and willingness of states to regulate varies considerably.

4. Why Aviation Is Distinctive

We have chronicled how governments gradually moved from a safety-centered approach in protecting international civil aviation to a concept focusing increasingly on security against willful, destructive activity.[41] The concept of security itself then evolved from one focused

40. John F. Murphy, *Punishing International Terrorists: The Legal Framework for Policy Initiatives* (Totowa, N.J.: Rowman & Allanheld, 1985), pp. 18–20.

41. Of course, the complexity of the international aviation system ensures that there is always a relationship between safety and security. Since accidents can cause failures in the system, governments have cooperated to develop a comprehensive system to reduce the probability of accidents. Security breaches against the system can then attack either the underlying technology of the system (that is, hijacking an airplane) or the procedures and technologies designed to reduce the safety risks in the system (providing false information to air traffic controllers). Thus some of the efforts to reduce safety problems can have a collateral, if indirect, effect on reducing security

primarily on protecting aircraft to one focused on protecting the technological network on which aircraft depend to operate safely and efficiently.

Looked at in the context of international cooperation in other areas involving safety and security, aviation security seems to be distinctive, in five ways. (1) This area of international law has steadily grown over time to encompass more offenses. (2) The responsibilities imposed on signatories are very specific and the network being protected is technologically complex. (3) As a matter of law, the system has both a prevention and a law enforcement component. (4) A growing number of countries have signed on to the regulatory regime. (5) Finally, acceptance of the treaties has coincided with greater security.

Here is some of the evidence: at first, countries were most interested in the basic rules of airspace; they could not agree on how the system should function under the best of circumstances, let alone on how they should cooperate to address intentional damage to the system. This was the subject of the Paris Convention in 1919. Through Annex 17 to the Chicago Convention of 1944 (which created ICAO), states have committed to observing ICAO's standards on preventive security—unless they specifically and publicly reject them. ICAO may lack direct capacity to enforce its guidelines, but the information it generates allows key countries with large aviation markets to impose (or threaten) restrictions that serve as a de facto enforcement mechanism. About 180 countries and 23 international organizations participate in ICAO, which provides technical assistance for preventive security measures.[42]

Since 1989, ICAO has offered technical assistance on aviation security to 132 states. Because the framework exists and appears to work, these programs are funded by donor states. Fifteen such states have contributed nearly $5 million to the program since 1989. In 1963, the Tokyo Convention only went as far as to establish criminal juris-

threats. The context of cyber crime and security may involve similar relationships between safety and security.

42. ICAO, The International Civil Aviation Organization: Annual Report 1999.

diction over the interference with aircraft while they were in flight,[43] but there is now also a law enforcement component to the system, enacted by the Montreal Convention, now signed by 174 countries. Indeed, since treaty membership is usually the most controversial element of any legal regime, this level of membership may understate the total number of countries that voluntarily cooperate in aviation security–related law enforcement—contrast this to the 79 countries that have signed the Hostages Convention, and the 144 countries that have signed the Narcotics Convention.[44] Since adoption of the civil aviation treaties, sabotage and acts of unlawful interference have steadily declined; in 1998, for example, ICAO reported only about ten acts of unlawful interference and basically no acts of sabotage.

Aviation is distinctive for both psychological and economic reasons. The psychological reasons include the ready availability of graphic images, high casualty to incident ratio, and high mortality to casualty ratio. There are at least three economic reasons why civil aviation security engenders considerable international interest: (1) the growing economic significance of international air transportation in absolute terms, (2) the indirect benefits of air transportation, and (3) network externalities.

During the last four decades, air transport has become an increasingly important economic sector in terms of total revenue.[45] Civil aircraft manufacturers in the U.S. and Europe have become major industries. Security threats afflicting civil aviation place these economic sectors at risk. Moreover, civil air transport provides indirect economic benefits by lowering transportation costs, increasing the diffusion of labor, and allowing for redundancies that allow transport to proceed when surface or seaborne routes are blocked. Finally, the

43. U.S. Department of Transportation, FAA Website, International Programs, ⟨*http://www.faa.gov/international*⟩ (accessed June 19, 1999).

44. United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, December 20, 1988, T.I.A.S., 20 I.L.M. 493 (Vienna Convention).

45. See, e.g., Dempsey, *Law and Foreign Policy in International Aviation*, and de Murias, *The Economic Regulation of International Air Transport*.

principle of network externalities applies to international civil aviation, thereby raising the value of a portion of the network to the extent that the entire network grows.[46] The notion of network externalities is straightforward. Certain goods and services increase in value to the extent that a greater number of users are included in the network. For example, the value of telephone networks increases as more people can be reached on the network. The value of e-mail communication also increases as the number of e-mail users grows. In the aviation context, if certain portions of the network are considered unsafe, the remaining portion of the network loses value; so that if there is a spate of terrorist attacks on airports in Africa, for example, and aircraft flying to Africa, then the entire international civil aviation network is less able to provide efficient transportation to Africa. This makes the network itself less valuable.[47] Even beyond the economic considerations, aviation security is an appealing objective because of the psychological significance of breaches in aviation security, due in part to the sense of empathy that many people who use the international aviation system feel when confronted with an aviation disaster.[48]

To some extent, these elements of the aviation sector have analogues in the context of cyber crime. Cyber networks are growing in economic value.[49] And as the networks grow, the economic activity beyond information technology is increasingly dependent on cyber

46. Although passengers may not feel network externalities when they buy a ticket to fly between two geographic points, everyone else in the system benefits from network externalities. An airline investing in aircraft finds these more valuable if there are more safe airports that they can fly to, and governments can secure a similarly greater benefit (at the margin) when investing in aviation infrastructure as the network grows in size and scope.

47. See generally, Nicholas Economides and Lawrence J. White, "Networks and Compatibility: Implications for Antitrust," *European Economic Review* 38 (1994): 651, discussing network externalities in the context of antitrust analysis.

48. For a review of the psychological research on the salience of aviation versus other types of disasters, see Richard Nisbett and Lee Ross, *Human Inference: Strategies and Shortcomings of Social Judgment* (Englewood Cliffs, N.J.: Prentice-Hall, 1980).

49. For example, as of June 2000, the stock market capitalization of information technology companies in the U.S. far surpasses the price-earnings ratios that many financial analysts consider most acceptable.

networks. Moreover, network externalities almost certainly play a significant role in the development of information technology networks. Although cyber crime does not necessarily inspire analogous psychological reactions, certain developments could be framed in a manner that would help the public perceive the salience of cyber security breaches and the implicit threat to their safety.[50] The perception of cyber insecurity decreases the network's value. Users of information technology could be "hijacked," and in the midst of a cyber attack they might feel as helpless as if they were on an aircraft that had been hijacked. A plane could crash when given faulty information. Water could be poisoned though interference with purification systems. Policymakers can emphasize the analogy between civil aviation security and cyber security to help build the domestic political consensus that often serves as a precursor for international cooperation in damage control.

5. Applying the Civil Aviation Precedent to Cyber Threats

The existing framework of international law covering civil aviation security is laudable but not entirely adequate to address cyber security breaches. In civil aviation there are indeed ways in which cyber threats could elude coverage under the existing legal framework. But there may be ways in which we can bring such threats under the scope of the international treaties protecting civil aviation.

Filling the Gaps in Existing Aviation Security Treaties

The growth in the scope of the international civil aviation security system illustrates a gradual progression that filled in gaps left by previous accords. For instance, the Montreal Convention finally reflected

50. For a discussion of the psychology of framing information in a manner that increases its salience, see, e.g., Daniel Kahneman and Amos Tversky, "Choices, Values, and Frames," *American Psychologist* 39 (1984): 341.

the growing international consensus that aircraft safety could be indirectly threatened by undermining air navigation systems. Yet, although the international civil aviation system has achieved impressive results, the existing legal framework does not provide coverage against all major cyber threats. Today the advent of cyberspace and the increasing relevance of information technology again creates a gap between what the treaties cover and the nature of the threat.

Some of the existing civil aviation security treaties could be found to impose legal obligations relevant to cyber crime. For example, the Montreal Convention specifically covers instances where a person "communicates information which he knows to be false, thereby endangering the safety of an aircraft in flight."[51] More generally, it requires members to punish offenders who interfere with the safety of the air navigation system, which includes the sabotage of an air navigation system through computer viruses, transmission of inaccurate information, or related technologies. Other malicious attacks against aircraft in flight or on the ground, or against air navigation systems, are also covered.

Nonetheless, in most cases such obligations are quite circumscribed in comparison to the range of offenses targeting civil aviation that could arise through, or benefit from, information technology. In particular, the current treaties generally do not cover the use of computers to target critical infrastructures necessary for the security of civil aviation. As with virtually all international terrorism treaties, the focus is on malicious—not reckless—conduct. Thus, for example, two academics who recklessly and unlawfully interfere with an air navigation system would not necessarily commit an offense under current treaty law.

Moreover, the current international treaty law does not cover reckless or malicious cyber attacks against critical infrastructures collaterally affecting civil aviation security.[52] Such attacks could signifi-

51. Montreal Convention, art 1(d), 24 U.S.T. 564.

52. The only exception to this is if the attacks were considered de facto attacks on the air navigation system.

cantly and adversely interfere with the commercial or economic efficiency of the international civil aviation system, and thereby interfere with safety. If, for example, a cyber attack penetrates airline reservation systems, terrorists could learn the identity, destination, and itinerary of any passenger, allowing individuals to be targeted while they make their way through the network.[53] Reckless or malicious cyber attacks could also affect collateral infrastructures, upon which the international civil aviation system depends, such as electric power grids.

Although gaps in the system exist even beyond cyber terrorism, cyber offenses are particularly threatening in terms of their potential to damage a number of the infrastructures upon which civil aviation depends. In many cases, computers pose a new enforcement challenge. Illegal information or reproductions (of currency, for example) can be transmitted throughout the world in seconds. The combination of expertise and malevolent intent can disable the vital computer networks. Accordingly, it could be argued that cyber crimes merit enhanced punishments and increased provisions for transnational law enforcement cooperation. For these reasons, it is probably easier to reach international consensus on the cyber offenses than on changes to other aspects of international law governing civil aviation security.

Specific Changes to the International Treaty System

Minor changes to an existing treaty could address cyber threats currently not covered. The Montreal Convention provides a vehicle to achieve this, because it already presents a politically sustainable and legally coherent framework concerning prosecution or extradition.

53. Interference with airline computer systems could also put passengers at risk by changing air traffic patterns, concentrating passengers in certain locations, and interfering with maintenance schedules and crew assignments. A recent computer malfunction at Phoenix's Sky Harbor Airport highlights the damaging consequences of problems with maintenance and pilot crew schedules. The computer malfunction delayed flights on one airline for nearly a day.

Although using an existing treaty is not the only way of achieving this result, it is the most straightforward.[54]

The language below would go a considerable distance to address the core cyber threats not currently covered. Although the format I offer is designed to follow Section 1 of Article I in the Montreal Convention, the language easily could be adapted to stand on its own:

> 2. Any person commits an offense if he unlawfully, and intentionally or recklessly,[55] engages in any of the following conduct to commit an offense specified under section one of this Article[56] or to adversely interfere with a significant aviation infrastructure without legally recognized authority, permission, or consent, if such an act is likely to endanger the safety of the civil aviation system:[57]

54. The goal of this language is not the Montreal Convention per se, but rather the body of international law that pertains to civil aviation security. Another alternative that achieves this result would be a separate treaty, though such a vehicle would probably attract more attention and political debate than an amendment to the Montreal Convention.

55. The addition of the word "recklessly" extends the provision to instances where individuals unlawfully engage in prohibited conduct, mindful of the danger it poses yet with a complete (that is, reckless) disregard of the consequences of their actions. Example: two college professors of computer science seek to test whether a new theoretical approach to breach computer security works as predicted; they infiltrate a computer network used to transmit air traffic information and hinder its ability to rapidly transmit information. The professors are so eager to complete the test that they put aside their knowledge of the activity's risk to civil aviation. Even if the professors did not undertake the activity with malice (that is, with the general intent of causing harm), their recklessness would constitute an offense under this language if damage results.

56. This refers to the first section of the article defining offenses in the Montreal Convention. The goal here is to extend the recklessness standard to instances where cyber systems are compromised in the course of committing one of the original offenses in the Montreal Convention, such as "destroy[ing] or damag[ing] air navigation facilities or interfer[ing] with their operation." Montreal Convention, art. 1 (d), 24 U.S.T. 564.

57. The "significant aviation infrastructure," defined in detail below, refers to critical infrastructures that, if compromised, would adversely affect civil aviation. Although civil aviation security would be threatened even by a noncyber attack to such an infrastructure, cyber attacks against these infrastructures deserve coverage in an international treaty for two reasons: (1) cyber attacks can be more easily undertaken across national boundaries; (2) a cyber attack against these infrastructures can have more insidious consequences for aviation safety because it could be timed, localized,

(1) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data or programs in a cyber system with the purpose of causing, or knowing that such activities would cause, said cyber system or another cyber system to cease functioning as intended, or to operate with a significantly reduced capacity to perform its intended function;[58]

(2) enters into a cyber system for which access is restricted in a conspicuous and unambiguous manner;

(3) interferes with tamper-detection or authentication mechanisms.[59]

The following definitions would complete the picture:

1. "Cyber system" means any computer or network of computers used to relay, transmit, coordinate, or control communications of data or programs.[60]

2. "Adversely interfere" means any conduct with a meaningful likelihood of causing a "significant aviation infrastructure" (defined below) to cease functioning as intended, or to operate with a reduced capacity to perform its intended function.[61] A "meaningful likelihood" means an identifable and nontrivial change in probability beyond what would arise in the normal course of operating the civil aviation system or a "significant aviation infrastructure."

3. "Significant aviation infrastructure" means any interconnected network of physical devices, pathways, people, and computers used to maintain, power, supervise, or operate air navigation facilities or airports, and without the proper function of which civil aviation security would be adversely affected; including but not limited to electric power grids, meteorological equipment, water and fuel

---

and coordinated to exert maximum damage on aviation. Example: interrupting an airport's access to electric power is always dangerous, but it is far more so in the case of a crowded airport, at peak periods of take-offs and landings, on a rainy evening.

58. This clause focuses on direct interference with cyber systems affecting civil aviation, either directly or collaterally (through interference with other critical infrastructures).

59. These two clauses allow coverage of offenses involving breaches of security, even when data are not significantly altered.

60. This defines the potential target of cyber attacks.

61. The goal of this definition is to explain the most worrisome type of interference with critical infrastructures that indirectly affect aviation. Note that the definition of adverse interference here parallels Section 2 of the proposed treaty language.

supply networks, airline reservation systems, and information systems used to transmit information relevant to civil aviation safety.[62]

4. "Civil aviation system" means any aircraft in flight, or preparing for imminent flight, air navigation facilities, and airports.[63]

In conjunction with the existing prohibitions of the Montreal Convention and its previous amendment (extending coverage to airports), this new language addresses the two major cyber security problems with the existing international treaty system. First, the new language makes clear that cyber attacks interfering with infrastructures that affect aviation, such as electric power, constitute offenses under the treaty. Even interference with computer reservation systems would be covered, as long as such interference placed safety and security at risk. Second, because of the unique threat posed by cyber attacks, the new language specifies that an unlawful cyber attack endangering the civil aviation system is covered under the treaty even if the perpetrator is reckless rather than malicious.

Although this last element is controversial, a growing number of intentional cyber attacks may have been undertaken recklessly rather than maliciously, yet caused (or had the potential to cause) significant damage to critical infrastructures. The legal standard of recklessness involves a deliberate disregard of the risk involved in a certain action even when it is known, which involves an element of deliberateness far beyond that involved in negligence.[64] The goal of this language is to address enforcement through prosecution and extradition rather than regulation, but the proposed changes extend the reach of this

62. This definition specifies what critical infrastructures are protected by the treaty language. The objective is to strike a balance between wide coverage (including most infrastructures on which civil aviation depends) and narrow application (maintaining focus on civil aviation).

63. This is just a convenient shorthand to refer to the specific aspects of the civil aviation system that are already covered by the Montreal Convention (aircraft in flight and air navigation facilities) and a previous amendment (airports).

64. In common law systems, negligence is generally viewed as the failure to consider a risk that a person should reasonably have considered. Civil law legal systems make analogous distinctions.

regime to matters that are regulated outside transportation agencies. Accordingly, this proposal would also require states to build domestic consensus among government agencies charged with protecting non-aviation infrastructures such as energy and telecommunications.

This proposal illustrates the selective expansion approach in action. The proposal's expansion of international criminal liability is consistent with the objectives of established treaty law. The focus on cyber threats is consistent with cyber technology's potential to lower the cost of threatening a key economic infrastructure. The focus is international because the protected infrastructure (civil aviation) is, and because the nature of cyber technology poses the threat that criminals and terrorists might stretch an offense across geographic boundaries and political borders. To address the threats, the selective expansion approach uses the same path-dependent logic that resulted in the international aviation security laws that the proposal seeks to enhance. Treaties of narrow scope reduce initial opposition and encourage signatories to change their prevention, safety, and enforcement practices. States enhance prevention and observe the treaties to avoid politically costly controversies over treaty interpretation, or sanctions that might impede their use of a valuable technological network such as the international aviation system. In contrast, proposals to radically expand international criminal liability for cyber offenses would be far more likely to arouse opposition on sovereignty grounds.[65] Once the precedent is established with narrower treaties, politicians are likely to find it less costly to support further expansions of international criminal liability, regardless of whether such expansions protect airspace or cyberspace.

65. See Dan M. Kahan, "Gentle Nudges vs. Hard Shoves: Solving the Sticky Norms Problem," *University of Chicago Law Review* 67 (2000): 607, arguing in favor of incremental changes in criminal liability to reduce the prevalence of "sticky norms" against the imposition of the new liability.

6. Conclusion

The international experience with aviation security indicates that, even though treaty law is not infallible, it is nonetheless an important component of international enforcement and prevention. Covering certain offenses with a treaty furthers the applicability of a legal standard and encourages participants to share information. This leads to specific political consequences that advance underlying goals of safety and security:

- *Deterrence of specific offenses*. Treaty law allows for extradition or prosecution to loom larger, marginally enhancing deterrence against cyber terrorism and cyber crimes targeting civil aviation. Potential offenders would find it marginally harder to assume that jurisdictional difficulties would allow them to evade punishment if they are caught.
- *International consensus for legal cooperation*. Treaty law reflects international consensus, encouraging law enforcement and security cooperation, for which still other treaties provide the framework. If a treaty defines an offense, the authorities of signatory countries are more likely to cooperate in addressing the offense.
- *Enhanced prospects for technical cooperation beyond the confines of the treaty*. Treaty law is a starting point to encourage international consensus on objectives for technical cooperation to avoid the offenses in question, even if such cooperation is beyond the scope of any single treaty. If countries sign a treaty recognizing certain conduct as offensive, it is probably more likely that both public and private research will focus on developing solutions to the offenses.[66]

66. Separate arrangements dealing exclusively with technical and investigative cooperation also exist.

These benefits arise from more than the normative impact of treaty law. Rather, there is a political connection between expanded treaty law and some of the objectives highlighted above. Once expanded prohibitions are legally in place, it is difficult for countries to retreat from them. Because gains and losses tend to be perceived asymmetrically—meaning that people value the avoidance of a loss more than the corresponding gain—a country is more likely to suffer greater scorn for terminating recognition of offenses than for not initially recognizing them.[67] Interest groups supporting cooperation (such as security and safety firms, special prosecution and investigation units, and transportation firms) develop in response to new opportunities. Finally, since countries are sensitive about their sovereignty on criminal justice matters, and extradition or prosecution of offenders poses complications in the context of domestic politics, countries develop a strong incentive to improve prevention approaches.

Thus, the regulation of cyberspace raises difficult but surmountable challenges. The universe of users is expanding far more rapidly than in the case of other communications technologies developed during the twentieth century, such as television, radio, and the telephone.[68] Hardware and software change vertiginously in months, and transactions can take place over a multitude of national jurisdictions. Given these developments, there is room for original and principled thinking in policing cyberspace. Such thinking played an indispensable role in negotiating the treaties that govern civil aviation security, and as with aviation, part of the challenge is a political one—generating a consensus that a certain network is valuable enough that everyone might be adversely affected if it suffered at the hands of criminals or terrorists.

67. To see this, just imagine what the international response would be if a current member of NATO seceded from the NATO constitutive treaty. Presumably, the consequences would be much more severe in terms of political, economic, and diplomatic costs than if the country had not joined in the first place. This intuition is consistent with the research of cognitive psychologists on how gains and losses are valued by people. See, e.g., Kahneman and Tversky, "Choices, Values, and Frames."

68. See, e.g., David R. Johnson and David R. Post, "Law and Borders: The Rise of Law in Cyberspace," *Stanford Law Review* 48 (1996): 1367.

The case for a multinational convention covering the entire range of threats is very strong. In the meantime, states should use the selective expansion approach to extend twenty-first century legal protections to civil aviation, a critical infrastructure that has all but defined the twentieth century.