Journal of Air Law and Commerce

Volume 84 | Issue 1 Article 2

2019

Preventing a Cyber-9/11: How Universal Jurisdiction Could Protect International Aviation in the Digital Age

Laura K. Ashdown
BYU Law, schmidtl@byulaw.net

PREVENTING A CYBER-9/11: HOW UNIVERSAL JURISDICTION COULD PROTECT INTERNATIONAL AVIATION IN THE DIGITAL AGE

LAURA K. ASHDOWN*

I. INTRODUCTION

MORE THAN EIGHT MILLION PEOPLE travel on commercial flights daily.[1] With the rise of modern aircraft and the development of affordable, low-cost airlines, more people are flying than ever before.[2] But cheaper tickets are not the only reason air travel is on the rise. Commercial airline passengers also take comfort in the fact that, statistically, they are safer flying on a jet than they are driving to the airport.[3] In fact, commercial flight remains the safest mode of transportation worldwide, with 2017 marking the safest year yet for commercial airline travel.[4]

---

* J.D. Candidate, Brigham Young University J. Reuben Clark Law School, 2019. The author would like to thank Professor Eric Talbot Jensen at BYU Law for his constant guidance and support, and for proofreading this Article on a trans-Atlantic flight. The author would also like to thank her husband and own commercial airline pilot—Jeff—for answering countless questions and providing valuable insight from an aviator's perpsective.

[1] *New Year's Day 2014 Marks 100 Years of Commercial Aviation*, INT'L AIR TRANSPORT ASS'N (Dec. 31, 2014), https://www.iata.org/pressroom/pr/Pages/2013-12-30-01.aspx [https://perma.cc/T9Q5-3XYZ].

[2] In 2017, a record breaking "4.1 billion passengers were carried by the aviation industry on scheduled" flights. *Continued Passenger Traffic Growth and Robust Air Cargo Demand in 2017*, INT'L CIV. AVIATION ORG. (Jan. 17, 2018), https://www.icao.int/Newsroom/Pages/Continued-passenger-traffic-growth-and-robust-air-cargo-demand-in-2017.aspx [https://perma.cc/2HWE-L4NU].

[3] "Every day, approximately 100,000 flights take to the sky and land without incident." *Safety*, INT'L AIR TRANSPORT ASS'N (2018), https://www.iata.org/whatwedo/safety/Pages/index.aspx [https://perma.cc/534P-MMF3]; Gillian Edevane, *'Am I Going Down?' App Tries to Help Anxious Flyers by Telling Them Odds of Plane Crash*, NEWSWEEK (Apr. 18, 2018), https://www.newsweek.com/what-are-odds-dying-plane-crash-app-892008 [https://perma.cc/74BN-K7QF].

[4] David Shepardson, *2017 Safest Year on Record for Commercial Passenger Air Travel: Groups*, REUTERS (Jan. 1, 2018), https://www.reuters.com/article/us-avia-

How did the aviation industry accomplish this record safe year? Years like 2017 happen because the aviation industry constantly evolves and learns from decades of trial and error.[5] Sadly, some of the most important safety lessons in aviation are learned the hard way.[6] Notably, the terrorist attacks of September 11, 2001 (9/11) shook the world and the aviation industry, resulting in stricter airport regulations as well as physical changes to commercial aircraft and cockpit doors.[7] But stronger cockpit doors and confiscated water bottles do not guarantee a flight's safety. The last line of defense for any flight's safety lies with the pilots operating and controlling the aircraft.[8]

Every day, the aviation industry relies on commercial pilots to be prepared to follow procedures, anticipate threats, and solve problems at a moment's notice, if need be.[9] Before any commercial flight takes off in America, the captain and first officer must review multiple checklists and conduct safety briefings.[10] During these safety briefings, the captain and first officer discuss any potential threats to the flight's safety, ranging from poor weather to an unruly passenger.[11] Because of the lessons learned on 9/11, pilots also lock the cockpit door before takeoff and follow strict procedures any time one of the pilots leaves to use the restroom.[12] While these pilots and commercial flight crew are arguably more prepared to stop a hijacker from physically

---

tion-safety/2017-safest-year-on-record-for-commercial-passenger-air-travel-groups-idUSKBN1EQ17L [https://perma.cc/PS74-ELS9].

[5] *See* Scott McCartney, *Why Flying Has Never Been Safer*, WALL ST. J. (Jan. 24, 2018), https://www.wsj.com/articles/why-flying-has-never-been-safer-1516804292 [https://perma.cc/Q48J-Z7BM].

[6] *Id.*

[7] After 9/11, aircraft manufacturers strengthened cockpit doors to withstand a grenade blast and lock more securely from the inside. *Who, What, Why: How are Cockpit Doors Locked?*, BBC MAG. MONITOR (Mar. 26, 2015), https://www.bbc.com/news/blogs-magazine-monitor-32070528 [https://perma.cc/S4S4-VDM6].

[8] Patrick Gontar et al., *Are Pilots Prepared for a Cyber-Attack? A Human Factors Approach to the Experimental Evaluation of Pilots' Behavior*, 69 J. AIR TRANSPORT MGMT. 26, 27 (2018).

[9] *See* Peter A. Bedell, *Career Pilot: Checklists and Discipline, It's a Checklist, Not a To-Do List*, AIRCRAFT OWNERS & PILOTS ASS'N (Dec. 1, 2016), https://www.aopa.org/news-and-media/all-news/2016/december/flight-training-magazine/career-pilot-checklist [https://perma.cc/WHF9-LBVL].

[10] *See* John Cox, *Ask the Captain: Standard Procedure for Starting a Flight*, USA TODAY (Aug. 19, 2018), https://www.usatoday.com/story/travel/columnist/cox/2018/08/19/standard-pilot-procedure-starting-flight/1009100002/ [https://perma.cc/KM3W-TPTE].

[11] *Id.*

[12] *Who, What, Why: How are Cockpit Doors Locked?*, *supra* note 7.

storming the cockpit, the same cannot be said for stopping a new and far more insidious kind of cockpit invasion. In the digital age of modern airliners, pilots, the aviation industry, and international lawmakers must now face the possibility of a cyberterrorist hacking and "hijacking" an aircraft cockpit remotely.

In recent decades, the international aviation community has started to transition away from relying on traditional air transport systems such as radar and ground-based air traffic control. With the development and adoption of digital communication systems and internet-connected aircraft, airlines worldwide may soon enjoy the advantages of wireless connectivity and more precise satellite monitoring. However, with these modern benefits also come the increased potential for malicious attacks from cyberhackers operating remotely in the shadows of cyberspace. Though current international aviation treaties like the Beijing Convention may outlaw cyber hijackings, the Convention and existing aviation law lack the enforcement power necessary to hold hacker-terrorists and their host nations accountable. Without accountability, there is little to deter cyberterrorists from exploiting aviation's technological vulnerabilities. In order to effectively address these new cyber threats and prevent a potential cyber 9/11, the International Civil Aviation Organization (ICAO) and the global community should consider adopting enforcement mechanisms such as universal jurisdiction to deter malicious cyber activities. Regardless of the deterrent mechanism, the global aviation industry as well as aviation lawmakers must implement stronger international standards and practices that hold malicious actors accountable for cyberattacks against the aviation industry. Ultimately, lawmakers, organizations, and private corporations must adapt and work together to meet the safety needs of an evolving world and aviation industry.

This Article proceeds in three parts. Part I discusses the rise of cyberattacks and the serious threat they pose to critical infrastructure systems. It then examines areas of cybersecurity vulnerabilities in the international aviation community and explains how advances in aviation infrastructure and technology bring not only benefits, but also new risks for aviation security. The first part also includes quotes and studies from the aviation industry demonstrating just how serious a concern cybersecurity poses to global aviation. It then concludes by highlighting some anecdotes of cyberattacks and hacks that are already occurring in the industry.

The second part begins by discussing the existing legal framework for international aviation. Part II identifies ICAO, the United Nations (U.N.) agency responsible for the creation of our international aviation framework, and then discusses the various international aviation conventions, treaties, and the changes made to the law as the aviation industry has evolved. The second part also examines other key players in the global aviation community, including organizations like the U.S. Federal Aviation Administration (FAA) and International Air Transport Association (IATA), as well as the influence of private corporations including Boeing and Airbus. This section will also examine steps aviation lawmakers and organizations are taking to address and counter rising cyber threats. The second part ends by concluding that, despite these efforts, the existing legal framework and organizations fail to sufficiently address and deter the cyber threats targeting the aviation community.

The third part begins by proposing that ICAO and the global aviation community should consider adopting universal jurisdiction as an enforcement mechanism to hold cyberterrorists and potential safe haven host nations accountable. This section will define universal jurisdiction and discuss its origin and rationale under customary international law. It will also discuss the history of universal jurisdiction's application in the context of piracy, as well as more recent applications for "heinous" crimes like genocide. The third part will also examine the controversy and limits of universal jurisdiction. To address and overcome these issues, it will then examine scholarly arguments made in favor of expanding universal jurisdiction to aircraft hijacking and cyberterrorism. This section will include the following arguments: (1) cyberterrorism and hijacking an aircraft are analogous to piracy and thus warrant the application of universal jurisdiction; and (2) the heinousness of a potential cyberattack on an aircraft justifies the expansion of universal jurisdiction.

This Article concludes by suggesting that international aviation lawmakers, organizations, and the world's nations consider expanding universal jurisdiction to apply to malicious cyber activities targeting the world's airlines and industry. Regardless of the enforcement mechanism, international aviation lawmakers, organizations, and the world's nations must implement stronger international standards that hold malicious actors accountable for cyberattacks against the aviation industry.

II. CYBERATTACKS AND CYBERSECURITY VULNERABILITIES IN THE INTERNATIONAL AVIATION COMMUNITY

A. What are Cyberattacks and How Do They Threaten Critical Infrastructure?

The U.S. National Academy of Sciences defines cyberattacks as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[13] Perpetrators of cyberattacks include cyberterrorists,[14] hacker groups or "hacktivists,"[15] state-sponsored actors,[16] ex-employees,[17] business competitors,[18] and even bored mischief-makers.[19] When it comes to cyberattacks, most individuals probably think of a hacker breaking into a financial institution's database and stealing valuable information like social security numbers or customer lists. However, while theft of information is arguably the most common crime perpetuated during a cyberattack, not all cyber actors are concerned with making a profit.[20] In recent years, various actors have also used malicious cyber activities to

---

[13] Nat'l Research Council of the Nat'l Acads., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities 1 (William A. Owens et al. eds., 2009).

[14] *See generally* John P. Carlin, *Inside the Hunt for the World's Most Dangerous Terrorist: How a British Hacker Joined ISIS's Top Ranks and Launched a Deadly Global Cyber Plot*, Politico (Nov. 21, 2018), https://www.politico.com/magazine/story/2018/11/21/junaid-hussain-most-dangerous-terrorist-cyber-hacking-222643 [https://perma.cc/B4LG-Y8EH].

[15] *See generally* Geneva Sands, *What to Know About the Worldwide Hacker Group 'Anonymous,'* ABC News (Mar. 19, 2016), https://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302 [https://perma.cc/P2W4-S4WB].

[16] *See generally* Edward McKinley, *China Pencil-Tip Spy Chip's Ultimate Market Risk: The Profits Built on Big Tech's Low-Cost Global Supply Chain*, CNBC (Oct. 5, 2018), https://www.cnbc.com/2018/10/05/chinas-cyber-spying-keeps-a-lot-of-us-tech-ceos-up-at-night.html [https://perma.cc/74LN-UTH2].

[17] *See generally* Salvador Rodriguez & Vibhuti Sharma, *Tesla Accuses Former Employee of Hacking and Transferring Data*, Reuters (June 20, 2018), https://www.reuters.com/article/us-tesla-ceo/tesla-accuses-former-employee-of-hacking-and-transferring-data-idUSKBN1JG2OV [https://perma.cc/E8FL-EAGA].

[18] *See generally* McKinley, *supra* note 16.

[19] *See generally* Andy Meek, *Google Engineer Was So Bored, He Hacked Google*, N.Y. Post (Sept. 4, 2018), https://nypost.com/2018/09/04/google-engineer-was-so-bored-he-hacked-google/ [https://perma.cc/54QM-85G8]; Stephen A. Wood et al., *Aviation and Cybersecurity: An Introduction to the Problem and the Developing Law*, 46 Brief 38, 38 (Summer 2017).

[20] *See* Wood et al., *supra* note 19.

embarrass and harass governments or companies,[21] provoke political or social change,[22] and even conduct terrorist activities.[23] No matter the purpose or crime, the internet enables criminals and other actors to further their agenda through remote cyberattacks by granting these cyber actors greater anonymity and a lower rate of detection.[24]

Even more concerning, a nation's critical infrastructure provides an easy target of attack for cyberterrorists hoping to intimidate or coerce a government or civilian population.[25] Critical infrastructure means "any system of high importance to the safety and operation" of a country.[26] As these critical systems have become more and more reliant on computer technology and the internet, they have also become more vulnerable to malicious cyber activities from opportunistic wrongdoers.[27] A nation's military defense systems, financial services sector, manufacturing industry, energy facilities, and transportation systems are all examples of critical infrastructure systems and services which, if destroyed or disrupted, could have a debilitating impact on a nation's health, safety, and security.[28] And while a cyberattack on any portion of a nation's critical infrastructure poses serious threats to a nation's well-being, a cyberattack on any nation's aviation industry could cause worldwide collateral damage.[29] As a globally connected industry responsible for 3.4% of the global GDP, a cyberattack on the international aviation

---

[21] Laura Jarrett & Evan Perez, *Justice Dept. Announces Charges Against North Korean Programmer for Sony Hack*, CNN (Sept. 6, 2018), https://www.cnn.com/2018/09/06/politics/doj-sony-hack-charges/index.html [https://perma.cc/69DR-59MY].

[22] Jason Murdock, *Anonymous vs. Qanon: Hackers Pledge to Take Down Pro-Trump Conspiracy*, NEWSWEEK (Aug. 6, 2018), https://www.newsweek.com/anonymous-hacking-collective-threatens-qanon-conspiracy-theorists-1058062 [https://perma.cc/JMS2-CYLX].

[23] Carlin, *supra* note 14.

[24] Nicholas W. Cade, *An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Code*, 37 BROOK. J. INT'L L. 1139, 1146–47 (2012).

[25] Kim Zetter, *Hacker Lexicon: What Counts as a Nation's Critical Infrastructure?*, WIRED (Feb. 16, 2016), https://www.wired.com/2016/02/hacker-lexicon-what-counts-as-a-nations-critical-infrastructure/ [https://perma.cc/U2CN-EARS].

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Hackable at Any Height: Cybersecurity in the Aviation Industry*, LONDON CYBERSECURITY SOLUTIONS 1, 5 (Apr. 2015), https://static1.squarespace.com/static/56d0212027d4bded627db544/t/56e00f379f7266ed7f057f97/1457524543915/LCS_Report_April.pdfpg [https://perma.cc/YQS6-NSCA].

industry would lead to a devastating impact on the global economy.[30]

B. Rising Threat of Cyberattacks in the Aviation Industry

Cyberattacks against the aviation industry are on the rise. Just in the year 2018 alone, one airline reported defending itself from "hundreds of thousands of [cyber] attacks" against its systems.[31] According to a survey conducted by PricewaterhouseCoopers in 2015, "85 percent of airline CEOs view cybersecurity as a significant risk."[32] But executive officers of airlines are not the only ones worried about cyber threats. In recent years, national aviation regulators and international aviation experts have acknowledged serious cyber threats facing aviation due to the industry's "reliance on an interconnected network of electronic systems that [are] a critical component to everyday operations."[33] The American Institute of Aeronautics and Astronautics noted that "[a]s one of the most complex and integrated systems of information and communications technology (ICT) in the world, the global aviation system is a potential target for a large-scale cyber attack."[34]

1. Areas of Vulnerability

How exactly is the aviation industry at risk for a large-scale cyberattack? Over the past two decades, the aviation industry's ICT has become increasingly complex and interconnected.[35]

---

[30] *Id.* at 4–5.

[31] Mark Holmes, *How WestJet Dealt With 'Hundreds of Thousands' of Cyber Attacks*, Avionics Int'l (Sept. 7, 2018), https://www.aviationtoday.com/2018/09/07/westjet-dealt-hundreds-thousands-cyber-attacks/ [https://perma.cc/M6CH-MLAQ].

[32] *Aviation Perspectives 2016 Special Report Series: Cybersecurity and the Airline Industry*, PricewaterhouseCoopers 1, 1 (2016), https://www.pwc.com/us/en/industrial-products/publications/assets/pwc-airline-industry-perspectives-cybersecurity.pdf [https://perma.cc/9NEN-4JWV].

[33] Andrew V. Schmidt, *Cyberterrorism: Combatting the Aviation Industry's Vulnerability to Cyberattack*, 39 Suffolk Transnat'l L. Rev. 169, 183–84 (2016).

[34] *The Connectivity Challenge: Protecting Critical Assets in a Networked World: A Framework for Aviation Cybersecurity*, Am. Inst. Aeronautics & Astronautics, at *Executive Summary* (Aug. 2013), https://www.aiaa.org/uploadedfiles/issues_and_advocacy/aiaa-cyber-framework-final.pdf [https://perma.cc/F5M7-FUZG].

[35] Roberto Sabatini, Presentation of the First Cyber Security Workshop at RMIT University, *Cyber Security in the Aviation Context* 1, 3 (Nov. 1, 2016), *available at* https://www.researchgate.net/publication/312191777_Cyber_Security_in_the_Aviation_Context [https://perma.cc/GL7D-6S4Y].

Historically, the aviation industry relied on ground-based radar systems to manage air traffic.[36] However, as air travel has continued to increase each year, traditional radar air traffic control (ATC) systems have struggled to efficiently manage air traffic while meeting increased demands.[37] To resolve radar's inefficiencies, aviation agencies worldwide are beginning to implement ATC systems that rely heavily on cyberspace and other Internet Protocol (IP) technologies to communicate.[38] One of the ATC systems that the FAA created to manage air traffic more efficiently is known as the Next Generation Air Transportation System (NextGen).[39]

NextGen is a GPS-based navigation system that will enable planes to "fly closer, descend straighter, and approach airports from multiple angles."[40] For example, traditional radar ATC systems only update every twelve seconds, requiring air traffic towers to space planes a minimum of twenty-four seconds apart to avoid any possible mid-air collisions.[41] In contrast, NextGen's GPS system can report a plane's location several times per second, allowing air traffic towers at airports to reduce required intervals between planes and allow for more efficient use of crowded air space.[42] Additionally, NextGen's GPS system would allow ATC towers to accurately locate an aircraft flying outside the range of radar towers.[43]

While NextGen and other IP-based ATC systems would allow ATC towers to more accurately locate aircraft and avoid air traffic "gridlock," IP-based ATC systems could also make the avia-

---

[36] Jennifer Ann Urban, *Not Your Granddaddy's Aviation Industry: The Need to Implement Cybersecurity Standards and Best Practices Within the International Aviation Industry*, 27 ALB. L.J. SCI. & TECH. 62, 71 (2017).

[37] *See generally Hackable at Any Height*, *supra* note 29, at 10.

[38] *Id.* at 9.

[39] Schmidt, *supra* note 33, at 188–89. The European Union created its own analogous advanced IP-based ATC system known as "SESAR." *About: History*, SESAR, https://www.sesarju.eu/discover.sear/history [https://perma.cc/WN5Q-939H].

[40] *Hackable at Any Height*, *supra* note 29, at 11.

[41] *Id.*

[42] *Id.* at 11–12; *see infra* Figure 1.

[43] NextGen's ability to locate aircraft outside the range of radar could potentially help prevent another aircraft from disappearing like Malaysian Flight MH370. Roger Howard, '*NextGen' Tracking Would Mean No Plane Could Disappear. So Why Aren't We Using It?*, NEWSWEEK (Mar. 21, 2014), https://www.newsweek.com/nextgen-tracking-would-mean-no-plane-could-disappear-so-why-arent-we-using-it-232393 [https://perma.cc/FY2Q-ANKG].

tion industry vulnerable to malicious cyberattacks.[44] Because NextGen relies on the internet to function, it is vulnerable to hacking by cyber actors who could potentially disrupt air traffic management by implanting a virus, malware, or other disruptive programs within the NextGen system.[45] Additionally, because NextGen relies on GPS to accurately locate an aircraft's location, malicious cyber actors could potentially jam these GPS signals or even send pilots false location data, creating a serious safety risk for commercial pilots and their passengers.[46]

Experts and even the U.S. government recognize these risks and have criticized the FAA for failing to adequately address these cybersecurity concerns.[47] In 2015, the U.S. Government Accountability Office (GAO) evaluated the FAA's efforts to address cybersecurity risks associated with the FAA's decision to transition from radar ATC to NextGen's IP-based systems.[48] In its report, the GAO identified three main areas of cybersecurity concern, stating that the FAA needed to: "(1) protect[ ] . . . (ATC) information systems, (2) protect[ ] aircraft avionics used to operate and guide aircraft, and (3) clarify[ ] cybersecurity roles and responsibilities among multiple FAA offices."[49] The GAO admonished the FAA to address these issues before implementing NextGen.[50]

Air traffic management systems are not the only areas of aviation infrastructure where the industry has become more dependent on the internet. Modern commercial aircraft have also become more reliant on computers and IP-based systems.[51] For example, the information systems used on modern aircraft include: (1) the cockpit avionic systems that pilots use to navigate the plane; and (2) the in-flight entertainment (IFE) systems that airline passengers use to amuse themselves.[52] The IFE systems

---

[44] *Hackable at Any Height*, *supra* note 29, at 11.

[45] *Id.*

[46] *Id.*

[47] *See* U.S. Gov't. Accountability Office, GAO-15-370, Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to NextGen 2 (2015), https://www.gao.gov/assets/670/669627.pdf [https://perma.cc/WTJ4-8F5G] [hereinafter Air Traffic Control] (looking at how the FAA has addressed cybersecurity challenges).

[48] *Id.* at "What GAO Found."

[49] *Id.*

[50] *Id.*

[51] *Id.* at 18.

[52] *Id.* Note that this is a highly simplified explanation. For more detailed explanations, see Sabatini, *supra* note 35. *See also infra* Figure 2.

on today's major airliners offer commercial passengers the ability to watch a variety of films, browse television channels, and even connect to wireless internet (wi-fi) while in-flight.[53] On newer aircraft, both the avionic systems and IFE systems are interconnected, meaning access to one system could potentially provide access to the other.[54] While in-flight wi-fi provides a welcome relief for passengers anxious to finish term papers or meet work deadlines, the convenience of modern IFE systems may also "potentially provide unauthorized remote access to aircraft avionics systems."[55] Cybersecurity experts caution that "[i]nternet connectivity in the cabin should be considered a direct link between the aircraft and the outside world, which includes potential malicious actors."[56] Even an innocent passenger could threaten an aircraft's safety if, for example, the passenger unintentionally accesses a website infected with a virus or malware while using the in-flight wi-fi.[57] Once a virus or malware infects a passenger's device, experts warn that a hacker could potentially use the compromised devise to access the aircraft's "IP-connected onboard information system" and potentially even the plane's avionics.[58]

To prevent unauthorized access to a flight's avionics, airlines rely on firewalls to separate the IFE and passenger wi-fi from avionic systems in the cockpit.[59] However, according to cybersecurity experts, the GAO, and even the FAA, these firewalls are easily circumvented, meaning a passenger on-board or even a remote cyber actor could potentially access the cockpit avionics systems.[60] While reviewing the aviation industry's cybersecurity measures, one security consultant even reported that he discovered a backdoor that could allow him access to one of the most important pieces of satellite communication equipment on an aircraft.[61]

---

[53] Urban, *supra* note 36, at 76.

[54] AIR TRAFFIC CONTROL, *supra* note 47, at "What GAO Found." For example, both the Boeing 787 Dreamliner and Airbus's A350 and A380 have advanced cockpit systems that are also connected to the main cabin IFE systems. *Id.* at 20.

[55] *Id.* at "What GAO Found."

[56] *Id.* at 19.

[57] *Id.*

[58] *Id.*

[59] *Id.* at 18.

[60] *Id.*

[61] Thomas Brewster, *This Guy Hacked Hundreds of Planes from the Ground*, FORBES (Aug. 9, 2018), https://www.forbes.com/sites/thomasbrewster/2018/08/09/

Even more alarming, a pilot's own electronic devices, whether personal or work related, could also provide malicious cyber actors with unauthorized access to an aircraft's avionics.[62] During any flight, pilots must reference various resources such as navigation charts, checklists, and aircraft manuals.[63] Historically, these manuals and other references were only available in paper form, requiring airlines to print these materials in heavy binders and then store these binders in the cockpit for pilot reference.[64] To reduce paper clutter in the already cramped cockpits, airlines now provide most of these materials to pilots in digital form on electronic tablets referred to as "electronic flight bags" (EFBs).[65] Many airlines give their pilots a light-weight tablet, such as an iPad or Microsoft Surface, to carry on-board the aircraft and access throughout the flight as needed.[66]

While EFBs are primarily used for pilots to reference necessary materials during a flight, airlines also use these tablets to provide their pilots with recurrent and on-going training modules.[67] Additionally, some airlines allow their pilots to take these tablets home so pilots can use them for training or their own personal entertainment.[68] Much like innocent passengers who may stumble upon a virus-infected website during a flight, airline pilots could also potentially and unwittingly expose a flight to a cyberattack if these pilots do not exercise caution while using their EFBs for personal entertainment at home or elsewhere.[69]

---

this-guy-hacked-hundreds-of-planes-from-the-ground/#4ae6969d46f2 [https://perma.cc/EL2G-925R].

[62] Peter Cooper, *Aviation Cybersecurity: Finding Lift, Minimizing Drag*, ATLANTIC COUNCIL 1, 31 (2017), http://www.atlanticcouncil.org/images/Aviation_Cybersecurity_web_1107.pdf [https://perma.cc/83Z3-4ZZH].

[63] *See generally* David Allen, *Technology/Product Development Electronic Flight Bag*, AEROMAGAZINE BOEING, July 2003, at 16–27, *available at* http://www.boeing.com/commercial/aeromagazine/aero_23/EFB.pdf [https://perma.cc/DXG8-NQAN].

[64] *Aviation Perspectives 2016 Special Report Series*, *supra* note 32, at 3.

[65] *Id.*

[66] *See* Malcolm Owen, *Delta Allegedly Switching Flight Crew Hardware from Surface to Ipad in Early 2018*, APPLEINSIDER (Oct. 20, 2017), https://appleinsider.com/articles/17/10/20/delta-allegedly-switching-flight-crew-hardware-from-surface-to-ipad-in-early-2018 [https://perma.cc/M4YE-W5WY].

[67] *See* Barbara G. Kanki & Thomas L. Seamster, *Optimizing EFB Through Training, Standards, and Best Practices*, 2007 INT'L SYMP. ON AVIATION PSYCH. 315 (2007), https://corescholar.libraries.wright.edu/cgi/viewcontent.cgi?article=1055&context=isap_2007 [https://perma.cc/QG34-KKWH].

[68] *Id.* at 316.

[69] *See* Cooper, *supra* note 62, at 31.

To ensure that EFBs do not pose a cyber threat to aviation safety, before allowing any airline to issue its pilots an EFB tablet, national regulators like the FAA require airlines to implement firewalls and conduct recurring virus scans on EFB software.[70] Additionally, many airlines continually train their pilots to refrain from allowing family members or friends to use their EFB tablets.[71] However, aviation cybersecurity experts believe these security measures may fail to adequately protect EFBs from a cyberattack.[72] Firewalls can be easily breached and experts note that the diversity of tablets and the complexity of devices "may make it harder to demonstrate assurance and deliver reliability."[73]

Fortunately, as of fall 2018, these threats remain mostly hypothetical and there are no credible reports of a cyberattack causing a commercial aircraft to crash.[74] Though sensationalized news sources have attempted to attribute various aircraft crashes or disappearances to the handiwork of malicious cyber actors,[75] there has yet to be any reliable reports that cyberattacks on aircraft or the aviation industry have caused any deaths or serious injuries.[76] Currently, the possibility of a hacker remotely hi-

---

[70] FED. AVIATION ADMIN., AC NO. 120-76D, AUTHORIZATION FOR USE OF ELECTRONIC FLIGHT BAGS 1, 21 (2017), *available at* https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_120-76D.pdf [https://perma.cc/7HZB-KN6F].

[71] *See id.* at 22.

[72] Cooper, *supra* note 62, at 31.

[73] *Id.*

[74] Gontar et al., *supra* note 8, at 26.

[75] Leslie Meredith, *Malware Implicated in Fatal Spanair Plane Crash*, NBC NEWS (Aug. 20, 2010), http://www.nbcnews.com/id/38790670/ns/technology_and_science-security/t/malware-implicated-fatal-spanair-plane-crash/#.XAdT-C3Mx8d [https://perma.cc/B9LT-VXKN]; Ed Bott, *Fact Check: Malware Did Not Bring Down a Passenger Jet*, ZD NET (Aug. 24, 2010), https://www.zdnet.com/article/fact-check-malware-did-not-bring-down-a-passenger-jet/ [https://perma.cc/Y79W-NMXZ]; Ruth Brown, *Mystery of MH370 Only Grows After Final Report Into Disappearance*, N.Y. POST (July 31, 2018), https://nypost.com/2018/07/31/mystery-of-mh370-only-grows-after-final-report-into-disappearance/ [https://perma.cc/E2TW-TCJV].

[76] During a September 2018 hearing before the House Committee on Homeland Security, one panelist noted that he has yet to see a credible report that shows it is possible for a hacker to hijack a plane remotely, but also acknowledged that "[w]e do not know what we do not know." *Understanding Cybersecurity Threats to America's Aviation Sector: Hearing Before the H. Comm. on Homeland Sec.*, 115th Cong. (2018), (testimony of Jeffrey L. Troy, Executive Director, Aviation Information Sharing Analysis, Inc.) [hereinafter *Hearing*], *available at* https://docs.house.gov/meetings/HM/HM08/20180906/108646/HHRG-115-HM08-Wstate-TroyJ-20180906.pdf [https://perma.cc/AX8V-J6AG].

jacking a commercial aircraft remains highly unlikely.[77] However, industry experts and regulators acknowledge that these kinds of cyberattacks are theoretically possible[78] and the aviation industry remains an attractive target for malicious cyber actors.[79] Experts warn that as these malicious actors continue to wage cyberattacks against the industry, they will also use more and more sophisticated methods of hacking in their attempts to infiltrate aviation systems.[80] Some cyber experts even estimate that it is only a "matter of time before a cybersecurity breach on an airline occurs."[81]

2. Anecdotes

Though no casualties have occurred, there are reported incidents of cyberattacks against the aviation industry and these attacks continue to increase each year.[82] Some hackers and cyber experts even allege that they have already been able to successfully hack a commercial aircraft.[83]

In the fall of 2017, a U.S. Department of Homeland Security (DHS) report surfaced alleging that a DHS-led research team had been able to remotely hack into the systems of a commercial Boeing 757 jet.[84] According to this report, the DHS research team allegedly hacked the jet during a 2016 test while the plane

---

[77] *See id.*

[78] Matthew Hoye & Rene Marsh, *GAO: Newer Aircraft Vulnerable to Hacking*, CNN (Apr. 14, 2015), https://www.cnn.com/2015/04/14/politics/gao-newer-aircraft-vulnerable-to-hacking/ [https://perma.cc/TPQ8-6368].

[79] During a September 2018 U.S. Department of Homeland Security (DHS) Committee hearing, Chairman Katko stated that malicious actors are "constantly trying to probe how to get into our systems and attack our airlines." *Understanding Cybersecurity Threats to America's Aviation Sector*, YOUTUBE (Sept. 8, 2018 at 24:10), https://www.youtube.com/watch?v=6FUI6EDk6as&feature=youtu.be [https://perma.cc/59BK-PV8M].

[80] *See* Holmes, *supra* note 31.

[81] Kris Van Cleave, *DHS Experts Warn it's a "Matter of Time" Before Hackers Hit Commercial Airliners*, CBS NEWS (June 12, 2018), https://www.cbsnews.com/news/cybersecurity-dhs-experts-warn-its-a-matter-of-time-before-commercial-airliners-get-hacked/ [https://perma.cc/K5NG-8TKM].

[82] *See* Holmes, *supra* note 31.

[83] Brewster, *supra* note 61.

[84] *See* Peggy Hollinger, *Can Your Flight Be Hacked?*, FIN. TIMES (Oct. 16, 2018), https://www.ft.com/content/2e416eca-4e3d-11e8-ac41-759eee1efb74 [https://perma.cc/H5B7-UGTW]; Dep't of Homeland Sec., ACT R & D Risk Summary and Report, *available at* https://www.documentcloud.org/documents/4495659-DHS-Document-Release-on-Aviation-Cybersecurity.html [https://perma.cc/T3VV-PC4M].

was sitting on the ramp outside the Atlantic City Airport.[85] While the authenticity and truthfulness of this report remain uncertain, members of the United States Congressional Committee on Homeland Security referred to the report during a September 2018 hearing as evidence of the need to enhance aviation cybersecurity.[86]

In a separate 2015 incident, a security researcher allegedly hacked a United Airlines plane by connecting his laptop to a Seat Electronic Box (SEB) under his passenger seat during his flight.[87] The researcher claimed that he was able to access the plane's avionics through the SEB and briefly commandeer the plane by issuing a climb command.[88] After publishing a tweet in which he boasted that he was considering playing with the plane's avionics,[89] United Airlines contacted the U.S. Federal Bureau of Investigation (FBI) and federal agents seized the researcher and his laptop upon landing.[90] The researcher also claimed that he had accessed in-flight networks at least fifteen times during various flights, but claimed that he did so to raise cybersecurity awareness.[91] Despite his claims, it remains uncertain whether or not the researcher actually caused the United plane to climb, and manufacturers like Boeing have attempted to discredit the researcher's hacking claim as impossible.[92]

While the idea that a hacker could remotely hijack a commercial jet is certainly alarming, cyberattacks against the aviation industry often take subtler forms. As of 2018, the majority of the reported cyberattacks in aviation have involved other areas of aviation infrastructure, such as airline websites, airline

---

[85] Hollinger, *supra* note 84; ACT R & D Risk Summary and Report, *supra* note 84.

[86] *Understanding Cybersecurity Threats to America's Aviation Sector*, *supra* note 79, at 20:09, 27:36.

[87] Kim Zetter, *Is It Possible For Passengers to Hack Commercial Aircraft?*, WIRED (May 26, 2015), https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/ [https://perma.cc/MY5S-9BAR].

[88] *Id.*

[89] *Id.*; *see infra* Figure 3.

[90] Zetter, *supra* note 87.

[91] Jose Pagliery, *Fearing United Plane Was Hacked, FBI Pulls Security Expert Off Flight*, CNN (Apr. 17, 2015), https://money.cnn.com/2015/04/17/technology/security/fbi-plane-hack/index.html [https://perma.cc/5HUH-KZDG].

[92] Evan Perez, *FBI: Hacker Claimed to Have Taken Over Flight's Engine Controls*, CNN (May 18, 2015), https://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/index.html [https://perma.cc/6T46-74V8].

databases, and airport websites.[93] While these attacks may not pose as direct a threat to human life or commercial flight safety, these attacks cause significant financial loss and lead to serious disruptions of international commerce and travel.[94] Additionally, cyberattacks on aviation infrastructure—like an airline or airport website—cause serious reputational damage and security experts warn that these attacks could harm the flying public's perception by creating unnecessary fear that commercial aviation is insecure and unsafe.[95]

For example, less than a year after the mysterious disappearance of Malaysia Airlines Flight MH370,[96] Malaysia Airlines suffered another reputational blow when a group known as "Lizard Squad – Official Cyber Caliphate" hacked Malaysia Airline's website and re-directed visitors to a page with a picture of a lizard wearing a top hat and text reading "404 – Plane Not Found."[97] The page also included a tab stating, "ISIS will prevail."[98]

Along with causing an airline reputational harm, cyberattacks on an airline's website can interfere with an airline's ability to sell tickets and serve its customers.[99] Today, many commercial airlines rely on internet sales and webpages to carry out their

---

[93] *See Hearing*, *supra* note 76 (statement of Christopher Porter, Chief Intelligence Strategist, Fireeye, Inc.).

[94] *Hackable at Any Height*, *supra* note 29, at 5.

[95] *Hearing*, *supra* note 76 (statement of Christopher Porter).

[96] Flight MH370 remains one of aviation's biggest mysteries. *See* Sinead Baker, *The Mystery of MH370 Remains 5 Years Later—Here are All the Theories, Dead Ends, and Unanswered Questions from the Most Bizarre Airline Disaster of the Century*, BUS. INSIDER (July 28, 2018), https://www.businessinsider.com/mh370-theories-dead-ends-unanswered-questions-ahead-of-major-new-report-2018-7 [https://perma.cc/A8UY-5U33]. As of 2018, only small portions of the plane have been recovered. All 239 of MH370's passengers and crew are presumed dead. *Id.* None of their remains have been found. *Id.*; Yantoultra Ngui & Gaurav Raghuvanshi, *Malaysia Airlines Flight 370 Reports Leaves Families in Dark Four Years On*, WALL ST. J. (July 30, 2018), https://www.wsj.com/articles/malaysia-airlines-flight-370-report-leaves-families-in-dark-four-years-on-1532955801 [https://perma.cc/5F9B-RYJB].

[97] Terrence McCoy, *Lizard Squad Hacks Malaysia Airlines, Claiming Link to Islamic State*, WASH. POST (Jan. 26, 2016), https://www.washingtonpost.com/news/morning-mix/wp/2015/01/26/lizard-squad-hacks-malaysia-airlines-claiming-link-to-islamic-state/?noredirect=on&utm_term=.a7b35d661030 [https://perma.cc/33LK-9F45]; *see infra* Figure 4.

[98] Clement Tan, *Malaysia Airlines Websites Hacked With ISIS Attack Claim*, BLOOMBERG (Jan. 25, 2015), https://www.bloomberg.com/news/articles/2015-01-26/malaysia-air-website-hacked-with-phrase-isis-will-prevail-.

[99] *Hackable at Any Height*, *supra* note 29, at 14.

businesses, creating a digital "Achilles heel."[100] This cyber-dependence provides terrorists and other cyber-political groups with easy targets to attack. For example, the conflict between Israel and Palestine is now being waged in cyberspace as well as in the Middle East.[101] Pro-Palestinian hackers have continuously targeted the website of Israel's national airline, El Al, as well as other areas of Israeli cyber-infrastructure.[102] In 2012, Pro-Palestinian hackers successfully brought down El Al's website, making the airline unable to process new reservations.[103]

Along with attacking airlines, malicious cyber actors have also targeted airports and their websites.[104] During a 2015 cyberattack, hackers defaced the website of a Tasmanian airport by replacing the website with pro-radical Islamic messages, such as "I am Muslim & I love jihad/I love ISIS."[105] While the attack did not impact the safety of any of the airport's flights or operations, the attack exemplifies the way in which alleged cyberterrorists attempt to disrupt the aviation industry and damage the public's faith in flight safety.

These examples demonstrate how malicious cyberattacks impact all sectors of the aviation industry and how these attacks are not restricted to a single nation or corporation. When a cyberattack causes a disruption at any major airport worldwide—whether it is Hartsfield-Jackson in Atlanta, Heathrow in London, or Dubai International Airport in the United Arab Emirates—the global aviation community continues to feel the impact for days afterwards.[106] While cybersecurity measures by one nation's regulatory body may help to mitigate damage and even deter cyberattacks in one nation, these anecdotes illustrate that avia-

---

[100] *Id.*

[101] Aviel Magnezi, *Cyber War: El Al, Stock Exchange Sites Down*, YNET NEWS (Jan. 16, 2012), https://www.ynetnews.com/articles/0,7340,L-4176132,00.html [https://perma.cc/UPB4-VGSX].

[102] Erik Kain, *Cyber Attacks Take Down Two Israeli Websites – Is Cyber Warfare the Next Front in the Middle East Conflict?*, FORBES (Jan. 16, 2012), https://www.forbes.com/sites/erikkain/2012/01/16/cyber-attacks-take-down-two-israeli-websites-is-cyber-warfare-the-next-front-in-the-middle-east-conflict/#19cdddcc5b5a [https://perma.cc/D2HD-CZ36].

[103] *Id.*; *see infra* Figure 5.

[104] *Hackable at Any Height*, *supra* note 29, at 16.

[105] *Hobart Airport Website Hacked with 'Pro-Islamic Militant Messages,'* ABC NEWS (Apr. 12, 2015), https://www.abc.net.au/news/2015-04-12/hobart-aiport-website-hacked-with-pro-islamic-militant-messages/6386936 [https://perma.cc/BT5W-478M]; *see infra* Figure 6.

[106] *Hackable at Any Height*, *supra* note 29, at 14.

tion cybersecurity is ultimately a global problem that warrants a global solution.

III. EXISTING AVIATION LEGAL FRAMEWORK

A. Sources of International Aviation Law

In order to determine a cybersecurity solution for international aviation, it is important to first understand existing international aviation law, its framework, and how it developed. Though Orville Wright made manned flight a reality in 1903, international aviation law did not fully develop until international flight and commercial passenger aviation became realities during the World War II.[107] During World War II, innovations such as the development of radar, jet engines, pressurized cabins, and lighter metals made international air travel by plane a possibility.[108] These innovations ushered in a new era of civilian air travel between nations, creating the need for international aviation agreements and laws.[109] Though some international aviation laws existed before World War II, this existing framework was highly inefficient because it consisted of a "patchwork of hundreds of individual agreements between countries."[110] As the end of World War II approached, the international community recognized the need for a uniform legal framework in aviation.[111]

1. Chicago Convention and the Creation of ICAO

In 1944, delegates from fifty-two countries held a conference in Chicago, Illinois, to discuss developments in international aviation.[112] During this conference, delegates from each country signed a treaty which became known as the Chicago Convention on International Aviation.[113] The Chicago Convention replaced the patchwork aviation agreements between countries and created a global legal framework that would allow for "interna-

---

[107] Dawna L. Rhoades, *Who Governs International Aviation? in* Ethical Issues in Aviation 43, 41–47 (Elizabeth A. Hoppe ed., 2011).

[108] *Id.*

[109] *Id.*

[110] Michael W. Pearson & Daniel S. Riley, Foundations of Aviation Law 308 (2015).

[111] *Id.*

[112] *Id.*

[113] Convention on International Civil Aviation, *opened for signature*, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295 (effective Apr. 4, 1947) [hereinafter Chicago Convention].

tional commercial aviation to flourish."[114] The Convention recognized the right of every member nation to maintain its sovereign airspace, regulate air travel within the nation's own borders, and encouraged member states to adopt uniform air regulations created by international aviation regulators.[115] Additionally, a 1998 Amendment to the Chicago Convention prohibits the use of weapons by member states against any civilian aircraft.[116]

The Chicago Convention also created ICAO to develop a uniform system of international aviation regulations.[117] Today, ICAO is a body of the U.N. and is the international administrative agency that specializes in aviation regulation worldwide.[118] All nations involved in international aviation are members of ICAO.[119]

ICAO consists of three branches—the Assembly, the Secretariat, and the Council.[120] The ICAO Assembly contains representatives from ICAO member states and meets every three years to review the agency's work, decide on policies, approve a budget, approve amendments to the Chicago Convention, and select which member states will participate in ICAO's rulemaking body.[121] The ICAO Secretariat implements the Assembly's policy and contains various committees or bureaus of expertise.[122] The ICAO Council is the rulemaking body that establishes standards and recommended practices (SARPs) for international air travel that are "considered necessary for the safety or regularity of international air navigation."[123] Before establishing SARPs, the ICAO Council receives technical expertise and advice from various ICAO Committees.[124] The ICAO Council then votes whether to approve a proposed SARP.[125] If two-thirds of the

---

[114] PEARSON & RILEY, *supra* note 110, at 308.

[115] *Id.* at 309.

[116] Schmidt, *supra* note 33, at 196.

[117] *Id.* at 197.

[118] *ICAO and the United Nations*, INT'L CIVIL AVIATION ORG., https://www.icao.int/about-icao/History/Pages/icao-and-the-united-nations.aspx [https://perma.cc/Y7P2-NAZR].

[119] Rhoades, *supra* note 107, at 43.

[120] PEARSON & RILEY, *supra* note 110, at 309.

[121] *Id.*

[122] *Id.*

[123] *Id.* at 309–10.

[124] *Id.* at 309.

[125] *Id.* at 310.

ICAO Council approve the SARP, it becomes incorporated into the Chicago Convention as an Annex.[126]

Annexes to the Chicago Convention are guidelines that govern different areas of international aviation.[127] The Annexes provide ICAO member states with aviation SARPs that regulate issues such as airworthiness of aircraft, pilot training and licensing, and environmental protection.[128] Annexes do not have the power of law and ICAO has no legal authority to enforce the Annexes.[129] However, ICAO member states are expected to comply with the Annexes and implement these standards when promulgating their own national aviation regulations.[130] If an ICAO member state does not wish to comply with an Annex Standard, the member state must notify ICAO of its intentions and file an exception with ICAO.[131] However, if an ICAO member state refuses to comply with an Annex Recommended Practice, the member state is not obligated to notify ICAO or file an exception.[132] Currently there are eighteen Annexes to the Chicago Convention.[133] Annex 17 establishes ICAO's civil aviation security program and requires each member state to protect against unlawful interference with civil aviation.[134]

2. Tokyo Convention

Though the Chicago Convention, its Annexes, and ICAO all provide the global aviation community with a uniform legal framework, during the 1960s and 70s, the global aviation community recognized the need to enact additional treaties that could combat international aviation crimes such as hijacking and terrorism.[135] In 1963, ICAO members signed the Convention on Offences and Certain Other Acts Committed on Board

---

126 *Id.*

127 *Id.* at 312.

128 *Id.*

129 *Id.* at 311–12.

130 *Id.* at 312.

131 *Id.*

132 *Id.*

133 *Id.*

134 Chicago Convention, *supra* note 113, at Annex 17.

135 Samuel M. Witten, *Introductory Note to the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation and the Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft*, 50 I.L.M. 141, 141 (2011).

Aircraft (Tokyo Convention)[136] in Tokyo, Japan.[137] The treaty marked the first international effort to "assert formal international control over the criminal acts of hijackers."[138] Specifically, the treaty prohibited acts that jeopardize the safety of commercial aircraft or passengers while the aircraft is in flight.[139] The Tokyo Convention also vested the aircraft commander (typically the captain) with the authority to restrain persons jeopardizing the flight's safety and then deliver these individuals to state authorities in the territory where the aircraft lands.[140] The Tokyo Convention granted jurisdiction and prosecutorial power of any treaty violations to the state of aircraft registry.[141] In addition to establishing the powers of the aircraft commander and the duties of states involved, the Tokyo Convention also adopted the expression "unlawful seizure of aircraft" to denote "aircraft hijacking" or the "wrongful exercise of control of an aircraft."[142]

Though the Tokyo Convention granted prosecutorial jurisdiction to the nation where the aircraft was registered, the treaty greatly limited the ability of other nations to claim jurisdiction over a Tokyo Convention violation.[143] For nations other than the nation of aircraft registry, the Tokyo Convention only allowed states that were affected by the on-board offense in some manner to claim prosecutorial jurisdiction.[144] If a violation of the treaty occurred while an aircraft was cruising above a state's territory, the state that claimed this sovereign airspace could not exercise jurisdiction over the hijacker or offender without demonstrating some territorial impact.[145]

Along with failing to grant a member state jurisdiction over offenses carried out above its own sovereign airspace, the Tokyo Convention also failed "to create a definitive obligation on be-

---

[136] Convention on Offenses and Certain Other Acts Committed on Board Aircraft, Sept. 14, 1963, 20 U.S.T. 2941, 704 U.N.T.S. 219 [hereinafter Tokyo Convention].

[137] Michael S. Simons, *A Review of Issues Concerned with Aerial Hijacking and Terrorism: Implications for Australia's Security and the Sydney 2000 Olympics*, 63 J. AIR L. & COM. 731, 740 (1998).

[138] *Id.* at 741.

[139] *Id.* at 742.

[140] LORI FISLER DAMROSCH & SEAN D. MURPHY, INTERNATIONAL LAW CASES AND MATERIALS 776 (6th ed. 2014).

[141] Simons, *supra* note 137, at 742.

[142] *Id.*

[143] DAMROSCH & MURPHY, *supra* note 140, at 776.

[144] Paul S. Dempsey, *Aerial Piracy and Terrorism: Unilateral and Multilateral Responses to Aircraft Hijacking*, 2 CONN. J. INT'L L. 427, 432 & n.26 (1987).

[145] *Id.*

half of its signatories actually to prosecute or extradite" a hijacker offender.[146] Additionally, the Tokyo Convention also failed to declare hijacking an international crime.[147] Consequently, the Tokyo Convention was criticized for its lack of enforcement power as well as its failure to deter aircraft hijackings.[148] Despite these criticisms, the Tokyo Convention was the first step in the right direction for the international aviation community and ICAO members attempting to grapple with the new crimes of aircraft hijacking.[149]

3. Hague Convention

To compensate for the failures of the Tokyo Convention, ICAO member representatives signed another treaty in 1971—the Convention for the Suppression of Unlawful Seizure of Aircraft (Hague Convention).[150] Using the Tokyo Convention as its foundation, the signers of the Hague Convention took a definitive stance on aircraft hijacking by declaring the hijacking of an aircraft an international crime.[151] The Convention criminalized the conduct of aircraft hijackings and established severe punishments for the unlawful seizure of an aircraft in flight.[152]

The Hague Convention expanded prosecutorial jurisdiction to include: "the state of registration of the aircraft, the state in which the aircraft land[ed] with the offender on board, and the state of the principal place of business or permanent residence of the lessee of the aircraft."[153] Unlike its predecessor, the Hague Convention created mandatory extradition requirements for the states that signed the treaty.[154] If the state that apprehended a hijacker failed to extradite the alleged offender to a state that could establish prosecutorial jurisdiction, the Hague Convention required the state holding custody of the offender to begin prosecuting the offender, even if the custodial state was not impacted by the offense.[155] This obligation to either extra-

---

146 *Id.*

147 *Id.* at 434.

148 *Id.* at 433–34.

149 *Id.* at 444–45.

150 Convention for the Suppression of Unlawful Seizure of Aircraft, Dec. 16, 1970, 22 U.S.T. 1641, 860 U.N.T.S. 105 [hereinafter Hague Convention].

151 Dempsey, *supra* note 144, at 435.

152 *Id.* at 435–36.

153 *Id.* at 435.

154 *Id.*

155 Hague Convention, *supra* note 150, art. 7.

dite or prosecute became known as the "Hague Formula"[156] and has been repeated in subsequent international aviation conventions as well as conventions related to war crimes and other universally condemned acts.[157]

While the Hague Convention was a marked improvement from its predecessor, the Hague Convention also suffered from its own weaknesses. Specifically, the Convention failed to criminalize acts of aircraft sabotage that fell short of a physical hijacking or seizure of the aircraft.[158]

4. Montreal Convention and 1988 Supplement

To criminalize acts of aircraft sabotage that failed to qualify as criminal acts under the Hague Convention, ICAO member representatives signed the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Montreal Convention) in 1971.[159] The Montreal Convention was a response to a rise in bombings and sabotage of aircraft that were not addressed in earlier aviation treaties.[160] Specifically, the Montreal Convention criminalized acts of violence onboard aircraft, destruction of aircraft, as well as acts that damage aircraft or render the aircraft incapable of flying.[161] The Montreal Convention made it illegal to bring substances onboard an aircraft that damaged the aircraft and also outlawed any acts that caused serious damage to air navigation facilities.[162] The Montreal Convention adopted the same "extradite or prosecute" formula of the Hague Convention, creating the possibility that several states could exercise jurisdiction over violators of the Montreal Convention in the event that one state was unwilling or unable to prosecute.[163]

However, the Montreal Convention limited itself to criminalizing violent acts that targeted physical aircraft.[164] In the 1980s, the international aviation community realized that the Montreal

---

156 It is also known as "aut dedere aut judicare." Int'l Law Comm'n, *Rep. on the Work of Its Sixty-Sixth Session*, U.N. Doc A/69/10, at 139, 145 (2014).

157 Witten, *supra* note 135, at 141.

158 Dempsey, *supra* note 144, at 436.

159 Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, Sept. 23, 1971, 24 U.S.T. 564, 974 U.N.T.S. 177 [hereinafter Montreal Convention].

160 Dempsey, *supra* note 144, at 436–37.

161 Montreal Convention, *supra* note 159, art. 1.

162 *Id.* art. 1.

163 DAMROSCH & MURPHY, *supra* note 140, at 777.

164 Witten, *supra* note 135, at 141.

Convention needed to be strengthened to address other kinds of attacks against civil aviation—specifically terrorist attacks targeting international airports.[165] In 1985, terrorists attacked both the Rome and Vienna Airports.[166] To expand the Montreal Convention to extend beyond aircraft and protect international airports, ICAO members supplemented the Montreal Convention by creating the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation in 1988 Protocol.[167] The Protocol criminalized violent, dangerous, or damaging acts at airports and declared these acts a violation of international law.[168]

5. Beijing Convention

The 9/11 attacks marked a watershed moment for ICAO and the aviation industry when terrorists hijacked American aircraft and then used these aircraft as weapons of terror. Though previous ICAO conventions addressed and criminalized the hijacking of aircraft, the 9/11 attacks highlighted weaknesses in the existing international aviation conventions.[169] In response to the 9/11 attacks, ICAO and its member nations began a nine-year process to strengthen and modernize existing aviation conventions like the Hague Convention and Montreal Convention.[170] After nine years of negotiating, the Beijing Convention was concluded on September 10, 2010, and as of July 1, 2018, the treaty is now in force.[171]

The Beijing Convention prohibits the use of aircraft as weapons.[172] The Beijing Convention also expands the scope of hijacking offenses to include acts that further the hijacking both

---

165 *Id.*

166 *Id.*

167 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Feb. 24, 1988, 1589 U.N.T.S. 474 [hereinafter Montreal Protocol].

168 *Id.* art. II.

169 Witten, *supra* note 135, at 141.

170 *Id.*

171 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, Sept. 10, 2010, 50 I.L.M. 144 [hereinafter Beijing Convention]; Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft, Sept. 10, 2010, 50 I.L.M. 153 [hereinafter Beijing Protocol]. Note: because both the Beijing Protocol and Beijing Convention work together in unison, this Article will simply refer to both of them as one single unit and reference them as "the Beijing Convention."

172 Beijing Convention, *supra* note 171, art. 1, ¶ 1(f).

before and after the flight.[173] The Beijing Convention acknowledges advances in technology and cyberspace and criminalizes seizures of aircraft achieved "by any technological means."[174] Along with criminalizing the use of civil aircraft as weapons, the Beijing Convention also criminalizes the release of any biological, chemical, or nuclear weapons or related material on a flight.[175] Additionally, the Beijing Convention prohibits the use of dangerous materials to attack aircraft or ground facilities and prohibits hijacking or attacks on air navigation facilities by technological means or coercion.[176] ICAO has clarified that the Beijing Convention also criminalizes cyberattacks on air navigation facilities.[177] By expanding the prohibitions of previous aviation conventions and criminalizing the use of aircraft, nuclear materials, and technology as weapons, the Beijing Convention has helped bring international aviation law into the twenty-first century.

The Beijing Convention adopts the "extradite or prosecute" formula of the Hague Convention, but also expands jurisdiction to allow states to claim jurisdiction over a treaty violation if the offense is committed by the state's national or a victim of the offense is a state's national.[178] Additionally, the Beijing Convention also allows a legal entity, such as a corporation, to be held criminally liable if a nation's domestic law allows.[179]

While the Beijing Convention criminalizes malicious cyberattacks against civil aviation, as of September 2018, only thirty-four of the 192 ICAO member states have signed the Beijing Convention and only sixteen states have ratified it.[180] Despite the ICAO

---

[173] Witten, *supra* note 135, at 142.

[174] Beijing Protocol, *supra* note 171, art. II, ¶ 1.

[175] Witten, *supra* note 135, at 142; Beijing Convention, *supra* note 171, art. 1, ¶ 1(g).

[176] Beijing Convention, *supra* note 171, art. 1, ¶ 1(d).

[177] *Declaration on Cybersecurity in Civil Aviation*, INT'L CIVIL AVIATION ORG. (Apr. 6, 2017), https://www.icao.int/Meetings/CYBER2017/Documents/Draft%20Dubai%20DECLARATION%20ON%20CYBERSECURITY%20IN%20CIVIL%20AVIATION_10%20March%202017.pdf [https://perma.cc/MEM6-UX3A]; JAMES JORDAN, EMERGING THREATS IN A CHANGING WORLD: BEIJING CONVENTION ON AVIATION SECURITY TO ENTER INTO FORCE ON 1 JULY 2018 2 (June 2018), http://www.hfw.com/downloads/BRIEFING-Emerging-threats-in-a-changing-world-Beijing-Convention-on-aviation-security-to-enter-into-force-on-1-July-2018.pdf [https://perma.cc/4L5T-KE6N].

[178] JORDAN, *supra* note 177, at 2.

[179] *Id.*

[180] *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation Done at Beijing on 10 September 2010, List of Signatories*, INT'L CIVIL AVIA-

Assembly urging all ICAO member states to ratify the Beijing Convention in a 2016 Resolution, it remains uncertain whether all ICAO members will actually make themselves parties to the new treaty.[181]

6. Other Sources of International Aviation Law

While ICAO is responsible for actually implementing international aviation regulations, much of the international aviation community is also influenced by nongovernmental organizations, as well as corporations like Boeing or Airbus.[182] For example, along with establishing ICAO, the Chicago Convention also led to the creation of the IATA to work as an international "trade association" composed of various airlines.[183] Since its formation in 1945, IATA and its member airlines have worked to promote safety in civil aviation and set industry standards such as carry-on baggage allowance, ticketing procedures, and rate agreements.[184] IATA plays an important role in allowing members of the global aviation community to set aviation standards without having to wait for ICAO member states to negotiate or sign another treaty.[185]

Additionally, states' domestic aviation regulatory bodies also influence international aviation and regulations.[186] For example, the U.S. Department of Transportation (DOT) is the "agency responsible for negotiating and enforcing most international aviation treaties and agreements."[187] The FAA, the administration responsible for regulating American aviation, is a part of the DOT.[188] Today, the DOT plays a significant role in the global aviation economy.[189] Foreign airlines often enter into code-sharing agreements to allow each other to sell tickets for

---

TION ORG., https://www.icao.int/secretariat/legal/List%20of%20Parties/Beijing_Conv_EN.pdf [https://perma.cc/JZ3A-WMM6].

181 *Beijing Convention to Enter into Force on 1 July 2018*, INT'L CIVIL AVIATION ORG., https://www.icao.int/Newsroom/Pages/Beijing-Convention-to-enter-into-force-on-1-July-2018.aspx [https://perma.cc/43SW-535B].

182 Urban, *supra* note 36, at 70.

183 Rhoades, *supra* note 107, at 44.

184 *Id.*; *Early Days*, INT'L AIR TRANSPORT ASS'N, https://www.iata.org/about/Pages/history-early-days.aspx [https://perma.cc/75J4-3828].

185 Rhoades, *supra* note 107, at 44.

186 PEARSON & RILEY, *supra* note 110, at 322.

187 *Id.*

188 *See, e.g.*, *id.* at 323.

189 *Id.* at 322–23.

other airlines.[190] Because the DOT must first approve these code-sharing agreements between U.S. and foreign airlines, the DOT wields serious economic power over the international aviation industry.[191]

Aircraft manufacturer corporations also exercise a large influence on the international aviation community. For example, the two largest commercial aircraft manufacturers in the world include Airbus and Boeing.[192] The American Boeing Company and European company Airbus SE each own "roughly 50% of the global commercial airliner market."[193] Because Boeing and Airbus manufacture the majority of the aircraft used in international commercial aviation, both companies must also comply with nations' domestic aviation regulatory agencies as well as international agencies like ICAO.[194] Because these companies compete to produce the most sought after aircraft for airlines, Airbus and Boeing constantly try to innovate and make their planes more technologically advanced and efficient.[195] However, as these manufacturers rush to add new features to their aircraft, production teams may fail to notice cyber loopholes or other cyber insecurities of these features.[196] As mentioned previously, these manufacturers do not always address cyber issues until after a nation's aviation regulatory agency (like the FAA in the United States) discovers the issue and then demands that the companies implement safeguards.[197]

---

[190] *Id.* at 322.

[191] *See, e.g.*, *id.* at 322–23.

[192] Benjamin Zhang, *How Airbus Became Boeing's Greatest Rival*, BUS. INSIDER (Sept. 8, 2018), https://www.businessinsider.com/airbus-history-boeing-rivalry-2018-4.

[193] *Id.*

[194] *See Technology Standards*, INT'L CIVIL AVIATION ORG., https://www.icao.int/environmental-protection/Pages/technology-standards.aspx [https://perma.cc/N8HG-YMG8]; *Production Certificate*, FED. AVIATION ADMIN., https://www.faa.gov/aircraft/air_cert/production_approvals/prod_cert/ [https://perma.cc/6M36-75ZM].

[195] Zhang, *supra* note 192.

[196] *See, e.g.*, Ashlee Kieler, *GAO Report Finds Airplanes With WiFi Connections May Be Vulnerable to Cyber Attacks*, CONSUMERIST (Apr. 15, 2015), https://consumerist.com/2015/04/15/gao-report-finds-airplanes-with-wifi-connections-may-be-vulnerable-to-cyber-attacks/ [https://perma.cc/3MNV-5RME].

[197] *Id.* Though not caused by cyberattacks, tragic and fatal back-to-back crashes of the Boeing 737 MAX and its subsequent grounding demonstrate how hasty innovation and inadequate instruction by aircraft manufacturers can and does result in serious safety issues and vulnerabilities for commercial avation. Robert Wall & Merrill Sherman, *The Multiple Problems, and Potential Fixes, With the Boeing*

B. Are International Aviation Lawmakers and Organizations Addressing Cyber Threats?

As cyberattacks have become more prevalent in the past two decades, cybersecurity awareness has also increased among governments, corporations, and civilian populations.[198] Thanks to this increased awareness, international aviation lawmakers, organizations, corporations, and domestic regulators have all taken steps to address new cyber threats to aviation in recent years.[199]

For example, in 2013, the ICAO Council modified Annex 17 of the Chicago Convention, which addresses security.[200] Annex 17 now includes a Recommended Practice, urging each ICAO member state to "develop measures in order to protect information and communication technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation."[201] However, because the change is only a Recommended Practice, ICAO member states are not required to comply with the suggestion or even notify ICAO if the state intends not to comply.[202] Along with modifying Annex 17, ICAO members recently created Resolution A39-19—Addressing Cybersecurity in Civil Aviation.[203] The Resolution "sets out the actions to be undertaken by States . . . to counter cyber threats to civil aviation through a cross-cutting, horizontal and collaborative approach."[204] However, like all ICAO Resolutions, A39-19 is just a guidance document and is not binding upon ICAO member states.[205]

---

737 MAX, Wall St. J. (Aug. 19, 2019), https://www.wsj.com/articles/fixing-the-problems-with-boeings-737-max-11566224866 [https://perma.cc/Y738-DF5K].

198 Laurence Bradford, *What You Need to Know About Cybersecurity in 2018*, Forbes (Mar. 30, 2018), https://www.forbes.com/sites/laurencebradford/2018/03/30/why-people-should-learn-about-cybersecurity-in-2018/#3e6c4cf45d00 [https://perma.cc/PJM6-EH87].

199 Hannah Davies, *Airlines Look to Invest in Cyber Security*, MRO-Network (July 5, 2016), https://www.mro-network.com/emerging-technology/airlines-look-invest-cyber-security [https://perma.cc/7SUD-3FU3].

200 Urban, *supra* note 36, at 84.

201 *Id.*

202 Pearson & Riley, *supra* note 110, at 312.

203 *Civil Aviation Cybersecurity Information Repository*, Int'l Civil Aviation Org., https://www.icao.int/cybersecurity/Pages/default.aspx [https://perma.cc/R8G2-QFTJ].

204 *Id.*

205 *See* Alejandro Piera, *The Challenge of Finding a Legal Vehicle to Enforce Compliance with a Global Aviation Emissions Scheme*, GreenAir Online (Nov. 19, 2014), http://www.greenaironline.com/news.php?viewStory=2007 [https://perma.cc/YKL7-P3M2].

During the 39th Session, ICAO also established the Secretariat Study Group on Cybersecurity (SSGC) to focus on cyber issues related to air navigation systems, airworthiness, and aerodromes.[206] SSGC reviews existing cybersecurity SARPs and works to promote cybersecurity awareness throughout the global aviation community.[207] While these efforts demonstrate that ICAO takes aviation cybersecurity issues seriously, some scholars have criticized ICAO's efforts for not being "thorough or concrete enough" and some critics claim that many of these measures have not been implemented "quickly enough to garner support" or effectively address aviation cybersecurity issues.[208]

In 2017, ICAO took additional steps to promote aviation cybersecurity by formalizing the Declaration on Cybersecurity in Civil Aviation.[209] While not binding, the Declaration set out cybersecurity goals and policies for ICAO member states.[210] In particular, the Declaration established that it is the responsibility of ICAO member states to help mitigate the risks posed by cyber threats to civil aviation and that each state needs to take action against cyber actors targeting the aviation industry.[211] The Declaration also claims that cyberattacks on civil aviation must be considered an offense against the international aviation community.[212]

Domestic regulatory agencies like the FAA have also made efforts to increase cybersecurity measures at the domestic level.[213] For example, the FAA has met with members of the airline industry like Boeing and Airbus to discuss security measures on aircraft and find ways to increase aircraft cybersecurity.[214] The

---

[206] *Civil Aviation Cybersecurity Information Repository*, *supra* note 203.

[207] *Id.*

[208] Urban, *supra* note 36, at 84.

[209] *Declaration on Cybersecurity in Civil Aviation*, *supra* note 177.

[210] *Id.*

[211] *Id.*

[212] *Id.*

[213] Aliya Sternstein, *FAA Working on New Guidelines for Hack-Proof Planes*, NEXTGOV (Mar. 4, 2016), https://www.nextgov.com/cybersecurity/2016/03/faa-has-started-shaping-cybersecurity-regulations/126449/ [https://perma.cc/BM9U-RJT6].

[214] Jonathan Vanian, *How the FAA and Airline Industry Hope to Protect Planes From Hackers*, FORTUNE (June 29, 2015), http://fortune.com/2015/06/29/faa-airlines-planes-hacked/ [https://perma.cc/6RUQ-7M7X].

FAA also created a Cyber-Security Steering Committee to address and respond to cyber concerns in commercial aviation.[215]

Aviation manufacturers like Boeing and Airbus have also made efforts to enhance cybersecurity on commercial aircraft. In 2012, Boeing implemented additional security measures on its Boeing 777 jet to prevent onboard hacking of critical computer systems.[216] Additionally, Boeing started a friendly hacker program to improve the cybersecurity of its new aircraft, the 787 Dreamliner.[217] As part of the program, Boeing pays friendly hackers to find ways to break into the Dreamliner's onboard software and then inform Boeing of security holes so it can implement additional cybersecurity measures.[218] Boeing's European competitor, Airbus, has also invested heavily in cybersecurity research and development for its commercial aircraft.[219] In 2017, Airbus teamed up with an international information technology company, SITA, to launch the first aviation Security Operation's Center (SOC).[220] Airbus's SOC works to mitigate cyber risks in civil aviation by responding to cyberattacks and then sharing this information with the aviation industry.[221]

C. Is Existing Aviation Law Sufficient to Address and Deter Cyber Threats to Aviation?

While these examples demonstrate that the aviation industry is taking steps in the right direction to address cybersecurity issues, there are still no uniform international cybersecurity standards that bind the aviation industry or nations.[222] And while the Beijing Convention implicitly outlaws malicious cyberattacks

---

[215] Fed. Aviation Admin., FY 2018 ANG-NextGen Business Plan 2 (2018) https://www.faa.gov/about/plans_reports/media/2018/ang_business_plan.pdf [https://perma.cc/ZC6R-JJ9P].

[216] Boeing, Co., FAA Special Conditions No. 25-503-SC, 2013 WL 6047130 (Nov. 18, 2013).

[217] Vanian, *supra* note 214.

[218] *Id.*

[219] *Cybersecurity: How to Protect Europe From a Growing Threat*, Airbus, https://www.airbus.com/public-affairs/brussels/our-topics/defence/cybersecurity.html [https://perma.cc/6XCY-98B2].

[220] SITA, Airbus: CyberSecurity Aviation SOC 3 (2017), https://airbus-cybersecurity.com/resource/sita-airbus-cybersecuritys-aviation-soc/ [https://perma.cc/CRF5-9JWV]; *The Industry's First Dedicated Aviation Security Operations Center (SOC)*, YouTube (Aug. 28, 2017), https://www.youtube.com/watch?v=wTij6NoHZWw [https://perma.cc/XZ7A-WBTG].

[221] SITA, *supra* note 220, at 3.

[222] *Understanding Cybersecurity Threats to America's Aviation Sector*, *supra* note 79.

against aircraft or air-navigational facilities, the Convention lacks the enforcement power necessary to hold malicious cyber actors and their host nations accountable. Without accountability, there is little to deter cyberterrorists from exploiting aviation's technological vulnerabilities.

For example, though the Beijing Convention and previous aviation treaties require state parties to extradite or prosecute an alleged cyber-hijacker, ICAO has little, if any, power to punish a member state for refusing to comply with this requirement.[223] Currently, if a member state fails to comply with the Beijing prosecution or extradition requirements, the only penalties that ICAO can impose on the non-compliant state is to strip that member nation of its voting power in the ICAO Council and Assembly.[224]

A nation that is a party to the Beijing Convention might refuse to comply with the extradition or prosecution requirement for various reasons: the alleged criminal may be one of the state's nationals that the state wishes to protect; the state may believe there is inadequate evidence to establish a prima facie case that the accused actually committed the offense; the state may not trust that the nation requesting extradition will be able to carry out a fair trial; or even worse—the state may have sponsored the attack itself.[225] For states complicit in an aviation cyberattack, the consequences of ICAO penalties may be outweighed by the potential political or financial benefits of a cyberattack on another nation's aircraft or aviation facilities.

Unfortunately, these issues are not just hypothetical. History has shown that states do not always comply with their aviation treaty obligations.[226] For example, in 1988, terrorists planted a bomb on a Pan American World Airways plane scheduled to fly from London to New York.[227] The bomb exploded over Lockerbie, Scotland, destroying the plane and killing all 243 passen-

---

[223] *ICAO: Frequently Asked Questions*, INT'L CIVIL AVIATION ORG., https://www.icao.int/about-icao/FAQ/Pages/icao-frequently-asked-questions-faq-2.aspx [https://perma.cc/N2C6-TMCB].

[224] *Id.*

[225] CRIMINAL LAW SECTION, COMMONWEALTH SECRETARIAT, IMPLEMENTATION KITS FOR THE INTERNATIONAL COUNTER-TERRORISM CONVENTIONS 8 (2003) [hereinafter IMPLEMENTATION KITS], https://www.unodc.org/pdf/crime/terrorism/Commonwealth_Chapter_1.pdf [https://perma.cc/2X2V-7276].

[226] Sarah Mazzochi, *The Age of Impunity: Using the Duty to Extradite or Prosecute and Universal Jurisdiction to End Impunity for Acts of Terrorism Once and For All*, 32 N. ILL. U. L. REV. 75, 96 (2011).

[227] *Id.* at 78.

gers and eleven crew members on board.[228] Fiery debris from the plane also killed eleven people when it fell to the ground in Lockerbie, Scotland.[229]

After three years, and testimonies from more than 15,000 witnesses, two Libyan nationals were indicted for the bombing.[230] When authorities from the United States and the United Kingdom requested that the Libyan government extradite the two alleged bombers, the Libyan government refused.[231] In its defense, the Libyan government argued that the Montreal Convention authorized Libya to prosecute its own nationals and that it was not required to extradite the alleged bombers if Libya handled the matter in its own domestic courts.[232] However, allowing Libya to exercise jurisdiction over the matter raised serious concerns due to evidence that Libya's leader, Muammar al-Gaddafi, likely sponsored the bombing himself.[233] Despite Libya's assertion that it would exercise its own prosecutorial jurisdiction over the alleged bombers, Libya failed to prosecute the two alleged bombers or discipline them at all for fifteen years.[234] It took until 2003 for the Libyan government to finally accept responsibility for the Lockerbie bombing and also agree to compensate families of the victims.[235]

Just as the Lockerbie bombers evaded prosecution for fifteen years due to Libya's refusal to extradite or prosecute, cyberterrorists could also remain unaccountable for a cyberterrorist attack or hijacking of a civilian aircraft if a host nation fails to comply with its treaty obligations. For a cyberterrorist attack on aviation, this risk is heightened even more due to the remote nature of cyberattacks.[236] For example, with events like the Lockberbie bombings or the 9/11 hijackings, terrorists are ei-

---

[228] *Id.*

[229] *Pan Am Flight 103 Explodes Over Lockerbie, Scotland*, HISTORY.COM (Nov. 13, 2009), https://www.history.com/this-day-in-history/pan-am-flight-103-explodes-over-lockerbie-scotland [https://perma.cc/D8AU-HGUF].

[230] Mazzochi, *supra* note 226, at 78.

[231] *Id.* at 96.

[232] *Id.*

[233] *Id.*

[234] *Id.*

[235] In 2003, Gaddafi admitted Libya's accountability for the act but denied giving the order personally. *Colonel Gaddafi 'Ordered Lockerbie Bombing,'* BBC NEWS (Feb. 23, 2011), https://www.bbc.com/news/uk-scotland-south-scotland-12552587 [https://perma.cc/77L3-W9TA].

[236] *See, e.g.*, Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, SCI. AM. (June 11, 2011), https://www.scientificamerican.com/article/tracking-cyber-hackers/ [https://perma.cc/VB3K-MHKQ].

ther physically present during the attack or they physically plant an explosive, making it much easier to trace these attacks using physical evidence or eyewitness accounts.[237] However, a remote cyberattack can be much more difficult to trace. Tools like the Onion Router can mask a hacker's true location, making it much more difficult to trace an attack back to the correct host nation.[238]

Additionally, if a victim nation lacks the technological means to provide evidence that the perpetrator committed the crime while acting remotely in a different host nation, the victim nation would likely struggle to present adequate evidence during an international tribunal.[239] A host nation of a cyberterrorist might argue that the victim nation has not shown adequate proof that their national perpetrated the cyberattack. Additionally, even if a victim nation can successfully demonstrate that another state's nationals were responsible for a deadly cyberattack, the host nation might still legally refuse to extradite its nationals by insisting on prosecuting the alleged criminals in its own domestic courts. Like the Lockerbie bombings, this could result in the host nation failing to ever actually prosecute the alleged terrorists.

If the Beijing Convention lacks adequate enforcement mechanisms to hold party-nations accountable for their binding treaty agreements, then the international aviation community is even more powerless to hold non-party nations or their nationals accountable for an aviation cyberattack. Under customary international law, states have no duty to surrender individuals accused of committing offenses in a foreign state's territory.[240] Before a state can demand a second nation to extradite one of its nationals, there must be some existing extradition agreement between

---

[237] *See, e.g.*, Elizabeth F. Loftus, *Eyewitness Testimony in the Lockerbie Bombing Case*, 21 MEMORY & THE LAW: CASE STUDIES 584 (Feb. 25, 2013), https://www.tandfonline.com/action/captchaChallenge?redirectUri=%2Fdoi%2Fabs%2F10.1080%2F09658211.2013.774417 [https://perma.cc/A9Z4-HSFJ]; Eve Conant, *Terror: The Remains of 9/11 Hijackers*, NEWSWEEK (Jan. 2, 2009), https://www.newsweek.com/terror-remains-911-hijackers-78327 [https://perma.cc/E9K4-A8YF].

[238] Bruce Schneier, *Why Proving the Source of a Cyberattack Is So Damn Difficult*, CNN (Jan. 6, 2017), https://www.cnn.com/2017/01/05/opinions/proving-source-of-dnc-hacks-difficult-opinion-schneier/index.html [https://perma.cc/56EQ-KE2M].

[239] *See generally Evidence Matters in ICC Trials*, INT'L BAR ASS'N (Aug. 9, 2016), *available at* https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=b9b8dc23-6616-41ba-8ef2-3d209398bdbd [https://perma.cc/E8T6-VME4].

[240] IMPLEMENTATION KITS, *supra* note 225, at 8.

the two nations or a treaty, like the Beijing Convention, that provides grounds for extradition.[241] However, if a nation hosting a "cyber hijacker" or actor is not a party to the Beijing Convention and also has no extradition arrangement with the victim nation, the host nation may legally refuse to hand over the remote hijacker for prosecution, leaving these hacker-hijackers unaccountable and at large.[242]

While it took more than fifteen years to bring the Lockerbie bombers to justice, a similar miscarriage of justice could likely be prevented if the global community adopted universal jurisdiction to apply to a malicious cyber-hijacking of a civilian aircraft. Universal jurisdiction could help overcome the issues that could arise if a treaty party refuses to comply with its extradition or prosecution obligations. Additionally, universal jurisdiction could also hold states accountable even if they are not parties to the Beijing Convention or they have no extradition treaties. For example, if a cyber-Lockerbie incident occurred and a responsible host nation refused to extradite its nationals to the victim state, a third-party state that has no relation to the terrorist attack could issue an extradition request under universal jurisdiction and on behalf of the victim state. If this third-party state has adequate financial sway or influence over the nation hosting the cybercriminals, it could incentivize the host nation to extradite its nationals. Allowing a third-party state to request extradition of a cybercriminal could also "provide a more neutral ground for prosecuting terrorists" because the third-party state may have less bias since it is neither the victim state nor the host state of the perpetrator.[243]

By adopting universal jurisdiction to apply to malicious cyberattacks targeting the civil aviation community, aviation lawmakers and the global community could better hold cybercriminals accountable for their crimes and thus help secure "international peace and security."[244] ICAO and the aviation global community should consider adopting universal jurisdiction as an enforcement mechanism to hold cyberterrorists and potential safe haven host nations accountable. However, such a solution is not without its controversies. The next section will discuss the history of universal jurisdiction, its controversies, and then

---

[241] *Id.*

[242] *See id.*

[243] Mazzochi, *supra* note 226, at 100.

[244] *Id.*

propose some arguments in favor of expanding universal jurisdiction.

IV. UNIVERSAL JURISDICTION

A. What is Universal Jurisdiction?

While not uniformly defined, universal jurisdiction is generally understood as the principle that allows any nation to exercise jurisdiction and prosecute alleged international criminals for acts committed outside that state's territory, regardless of whether or not the prosecuting nation has any connection with the offense.[245] Other scholars define universal jurisdiction as the "principle that certain crimes are so heinous, and so universally recognized and abhorred, that a state is entitled or even obliged to undertake legal proceedings without regard to where the crime was committed or the nationality of the perpetrators or the victims."[246]

Universal jurisdiction stems largely from customary international law—the set of rules or norms that impacts every state and obligates all nations.[247] While universal jurisdiction is not accepted for most international crimes, nations commonly apply universal jurisdiction to combat piracy on the high seas.[248] In the seventeenth century, any nation could try and execute pirates caught on the high seas, regardless of the nationality of the vessel the pirate chose to attack or the original nationality of the pirates.[249] Universal jurisdiction played an important role in helping the international community deter and prosecute piracy, because traditional theories of jurisdiction often failed to hold pirates accountable for their acts.[250]

---

[245] Kenneth C. Randall, 98 Am. J. Int'l L. 627 (2004) (reviewing Luc Reydams, Universal Jurisdiction: International and Municipal Legal Perspectives (2003)).

[246] Stephen Macedo, *Introduction*, *in* Universal Jurisdiction: National Courts and the Prosecution of Serious Crimes Under International Law 1, 4 (Stephen Macedo ed., 2004).

[247] Thomas Buergenthal & Sean D. Murphy, Public International Law in a Nutshell 27 (5th ed. 2013).

[248] *Id.* at 334.

[249] Eugene Kontorovich, *The Piracy Analogy: Modern Universal Jurisdiction's Hollow Foundation*, 45 Harv. Int'l L.J. 183, 190 (2004). Note that this Article will discuss the rationale for applying universal jurisdiction to piracy in more detail in the sections to follow.

[250] Mitsue Inazumi, Universal Jurisdiction in Modern International Law: Expansion of National Jurisdiction for Prosecuting Serious Crimes Under International Law 50–51 (2005).

Before a state can prosecute an individual, it requires jurisdiction to prescribe, meaning it must have the authority to "make its substantive laws applicable to particular persons and circumstances."[251] This prescriptive jurisdiction must be based on at least one of the following grounds: (1) the perpetrator committed the crime within the nation's territory (the Territoriality Principle);[252] (2) the crime was committed by one of the state's nationals (the Nationality Principle);[253] (3) the crime was committed outside of the state's territory, but one of the state's nationals was injured by the crime (the Passive Personality Principle);[254] or (4) the crime was committed outside the state's territory, but the crime threatens the state's security (the Protective Principle).[255] With piracy and other crimes committed on the high seas, nations cannot claim jurisdiction based on the territorial principle because the high seas are considered to be part of the shared "global commons" and fall outside any nation's territory.[256] Consequently, a state can only claim jurisdiction over a crime committed on the high seas if the crime involves the state's citizens (whether as the criminal or the victim) or the crime involves one of the state's vessels.[257]

However, piracy often complicated traditional theories of jurisdiction, because pirates typically claimed to be unaffiliated with any nation.[258] While a nation could claim jurisdiction on behalf of piratical acts against its citizens or vessels, not all states enjoyed the enforcement power necessary to effectively prosecute the pirates.[259] Without effective prosecution, pirates on the high seas would continue undeterred with their piratical acts.[260] Because all nations valued the safety of the high seas as a shared global commons, the global community made an exception to

---

[251] RESTATEMENT (THIRD) OF THE LAW OF FOREIGN RELATIONS OF THE UNITED STATES pt. IV, intro. note (AM. LAW INST. 1987).

[252] BUERGENTHAL & MURPHY, *supra* note 247, at 249.

[253] *Id.* at 251.

[254] *Id.* at 254.

[255] *Id.* at 256.

[256] Kontorovich, *supra* note 249, at 190.

[257] Kenneth C. Randall, *Universal Jurisdiction Under International Law*, 66 TEX. L. REV. 785, 793 (1988).

[258] *Draft Convention and Comment on Piracy*, 26 AM. J. INT'L L. 739, 825 (Supp. 1932).

[259] *See* Cade, *supra* note 24, at 1158–59.

[260] *See id.*

the typical jurisdiction rules and allowed any state to exercise jurisdiction and prosecute pirates.[261]

For the most part, piracy remains one of the only crimes most nations agree warrants the application of universal jurisdiction.[262] However, during the twentieth century and after the end of World War II, the world community began to apply universal jurisdiction to particularly "heinous" crimes that were globally condemned, including genocide and other crimes against humanity.[263] In light of the Nazi atrocities committed during the Holocaust, the international legal community asserted that genocide is so universally condemned that it should enjoy the status of *jus cogens* in international law.[264] *Jus cogens* refers to rules of international law that are so universally accepted, that no state may derogate from or refuse to abide by these norms.[265] The concept of *jus cogens* became much more accepted for heinous crimes in response to war atrocities during World War II.[266] However, aside from the expansion of universal jurisdiction during the Nuremberg trials and a few other notable examples, many nations consider universal jurisdiction highly controversial and refuse to expand universal jurisdiction to apply to other international crimes or even universally condemned acts.[267]

Aside from the notable exceptions,[268] nations resist applying universal jurisdiction to crimes other than piracy because exercising universal jurisdiction encroaches on the sovereignty of other states.[269] Additionally, many nations and legal scholars view universal jurisdiction as a potential slippery slope that could easily lead to abuse and could involve courts in highly po-

---

[261] *See id.*

[262] *See id.* at 1159–60.

[263] *Id.*

[264] Mazzochi, *supra* note 226, at 94.

[265] *Id.*

[266] *Id.*

[267] M. Cherif Bassiouni, *Universal Jurisdiction for International Crimes: Historical Perspectives and Contemporary Practice*, 42 VA. J. INT'L L. 81, 115–34 (2001).

[268] Universal jurisdiction was invoked to extradite the former Chilean head of state, General Augusto Pinochet. Naomi Roht-Arriaza, *The Pinochet Precedent and Universal Jurisdiction*, 35 NEW ENG. L. REV. 311, 311 (2001). Additionally, universal jurisdiction enabled Israel to convict Nazi war criminal Adolf Eichmann for his crimes during the Holocaust. Kenneth Roth, *The Case for Universal Jurisdiction*, 80:5 FOREIGN AFFAIRS 150 (Sept./Oct. 2001), *available at* http://www.foreignaffairs.com/articles/57245/kenneth-roth/the-case-for-universal-jurisdiction [https://perma.cc/K48A-UT7V].

[269] Cade, *supra* note 24, at 1158.

litical cases for which judges have no familiarity or precedent.[270] While these concerns are valid, the purpose of this Article is to suggest a limited application of universal jurisdiction to cases involving cyber hacking or hijacking of commercial aircraft.[271] To support this contention and address the concerns surrounding universal jurisdiction, the following section will examine other scholarly arguments made in favor of expanding universal jurisdiction to aircraft hijacking and cyberterrorism.

B. Scholarly Arguments for Applying Universal Jurisdiction

When arguing in favor of applying universal jurisdiction to certain international crimes, scholars often take two approaches: (1) analogizing the specific crime to piracy and then arguing that the analogous crime also warrants the application of universal jurisdiction; or (2) arguing that the "heinousness" of the crime is severe enough that it would warrant the application of universal jurisdiction under *jus cogens*.[272] This section will examine both of these arguments.

1. Piracy Analogies

Because this Article addresses the threats of cyber hacking or hijacking of commercial aircraft and other critical areas of aviation infrastructure, this section will focus on piracy analogies made by scholars in the context of aircraft hijacking as well as cyberterrorism.

a. Aircraft Hijacking

Scholars have argued that universal jurisdiction should apply to aircraft hijacking because it equates to "aerial piracy" and can be analogized to piracy on the high seas.[273] Additionally, scholars argue that such an expansion of jurisdiction would allow the world community to prosecute hijackers while also providing a

---

[270] *See* Michael Kirby, *Universal Jurisdiction and Judicial Reluctance: A New "Fourteen Points"*, *in* Universal Jurisdiction: National Courts and the Prosecution of Serious Crimes Under International Law 240, 240–57 (2001).

[271] Anything more than that is beyond the scope of this Article.

[272] *See generally* Peter M. Jacobson, *From Piracy on the High Seas to Piracy in the High Skies: A Study of Aircraft Hijacking*, 5 Cornell Int'l L.J. 161 (1972); Cade, *supra* note 24.

[273] Jacobson, *supra* note 272, at 161.

significant deterrence mechanism against the menace of aircraft hijacking.[274]

Just as ships in the seventeenth century traveled on the shared global commons of the high seas, modern-day aircraft travel through the global commons of airspace when cruising above international waters.[275] During the seventeenth century, the global community shared an interest in ensuring the safety of the high seas because international commerce depended on ships to carry goods and people to and from various nations.[276] To preserve international commerce and the global commons, all nations could apprehend and prosecute pirates that threatened the safety of the high seas.[277] That same rationale also justifies expanding universal jurisdiction to protect international airspace in the twenty-first century.[278] Today, the global community values the safety of international airspace just as much, if not more so, than the safety of the high seas.[279] Air cargo currently "represents more than 35% of global trade by value."[280] Because air travel enables much of our modern global commerce, just a single disruption in the aviation community can cause major global economic damage.[281] For example, when a volcano erupted in Iceland in 2010, the ash that spread from the eruption caused serious flight restrictions worldwide, leading to a $4.7 billion impact on the global GDP.[282] Accordingly, because the global community relies on air-freight and cargo to supply the world with goods, food, and medical care, the "case for granting universal jurisdiction over hijacking is today as compelling as the case for granting similar jurisdiction over piracy on the high seas."[283]

However, critics of applying universal jurisdiction to aircraft hijacking may argue that aviation treaties already supply enough jurisdictional grounds to multiple nations and that the ability of multiple nations to claim jurisdiction increases the likelihood

---

[274] *Id.*

[275] *Id.* at 165.

[276] Cade, *supra* note 24, at 1159.

[277] *Id.*

[278] Jacobson, *supra* note 272, at 165.

[279] *Hackable at Any Height*, *supra* note 29, at 5.

[280] Int'l Air Transport Ass'n, IATA Cargo Strategy 3 (Feb. 2018), https://www.iata.org/whatwedo/cargo/Documents/cargo-strategy.pdf [https://perma.cc/X2QZ-2KWU].

[281] *Hackable at Any Height*, *supra* note 29, at 5.

[282] *Id.*

[283] Jacobson, *supra* note 272, at 175.

that at least one nation will be able to effectively prosecute and deter an aircraft hijacker. While the state of registry of the aircraft and an attack above a nation's sovereign territory provide multiple bases for jurisdiction, the same obstacles that prevented victim nations from prosecuting pirates back in the seventeenth century can also prevent a nation in our current age from successfully prosecuting a cyber-hijacker operating remotely. For example, during the seventeenth century, some nations lacked the naval forces or manpower necessary to successfully apprehend pirates and then prosecute them.[284] However, the global community resolved this issue by allowing any other nation to step in and use its own naval force or ships to arrest and then prosecute pirates.[285] In our current age, a nation may lack the technological means to trace a cyber-hijacker to the alleged perpetrator's host nation.[286] While a friendly neighbor nation could help the victim nation by using its technology to identify the cyber-hijacker's location, current treaties only allow the victim nation or any nation with custody of the hijacker to extradite or prosecute the alleged criminal.[287] A friendly neighbor nation that has the technology needed to trace the cyber-hijacker might also have more influence or sway over nations harboring a cyberterrorist. Additionally, the nation with the technological capabilities to trace the cyber-hijacker is also arguably more prepared to put on evidence during a prosecution. Applying universal jurisdiction to allow any nation to prosecute or request extradition of a cyber-hijacker would enable these friendly nations to hold cyber-hijackers accountable and reduce the likelihood that cyberterrorists will remain undeterred. While some may argue that the victim nation is more entitled to claim prosecutorial jurisdiction over a cybercriminal, victim nations may prefer for friendly nations to prosecute on behalf of the victim nation. This is especially likely if the victim nation knows that the friendly nation has more influence over other nations as well as the technological evidence needed to successfully prosecute the cyber-hijacker.

---

[284] *See* Cade, *supra* note 24, at 1159.

[285] *Id.*

[286] Alison DeNisco Rayome, *UN Report: 50% of Countries Have No Cybersecurity Strategy in Place*, TECHREPUBLIC (July 6, 2017), https://www.techrepublic.com/article/un-report-50-of-countries-have-no-cybersecurity-strategy-in-place/ [https://perma.cc/9KPN-PTUA]; Cade, *supra* note 24, at 1150.

[287] JORDAN, *supra* note 177, at 2.

Allowing universal jurisdiction to apply against cyber-hijackers could also prove helpful in the event that the nation hosting the cyber-hijacker is unable to prosecute or extradite because it is in "a state of war or internal turmoil."[288] Even if a host nation of a cyber-hijacker wishes to bring the alleged cybercriminal to justice, it may not always be capable of doing so and universal jurisdiction could allow another nation to initiate prosecution instead.[289] For example, after the Bosnian genocide occurred in the former Yugoslavia, Austria asserted universal jurisdiction over an alleged defendant for complicity in the genocidal acts.[290] Though Bosnia was arguably the state most entitled to claim prosecutorial jurisdiction over the acts, the Bosnian government and judicial system was unable to take any judicial action due to "its then-ongoing internal conflict."[291] Thus, even though Austria could not claim any prescriptive jurisdiction based on territoriality or another principle, it successfully claimed jurisdiction over the defendant using universal jurisdiction.[292] Though not an example of universal jurisdiction for piracy or hijacking, the same principles can apply if a nation is unable to prosecute a cyber-hijacker because of internal turmoil or conflict. The Austrian example demonstrates how universal jurisdiction enables the global community to keep international criminals accountable and also deter wrongful actors.

However, critics of universal jurisdiction would likely argue that aircraft hijacking and piracy are not perfectly analogous. For example, the United Nations Convention of the Law of the Sea (UNCLOS) defines piracy as any act of illegal violence or detention on a private ship or aircraft but requires that this act be committed for "private ends."[293] If a hijacker's motivation stems primarily from political or religious motives rather than personal or financial reasons, the hijacking does not satisfy the "private ends" definition requirement of piracy.[294] However, scholars acknowledge that modern-day pirates on the high seas are typically "terrorists and hijackers who act for political rea-

---

[288] Anthony J. Colangelo, *The New Universal Jurisdiction: In Absentia Signaling Over Clearly Defined Crimes*, 36 GEO. J. INT'L L. 537, 552 (2005).

[289] *Id.*

[290] *Id.* at 553.

[291] *Id.*

[292] *Id.*

[293] United Nations Convention on the Law of the Sea, art. 101, *opened for signature* Dec. 10, 1982, 1833 U.N.T.S. 397.

[294] Jacobson, *supra* note 272, at 168.

sons"[295] and that the "private ends" requirement should be modified to reflect contemporary needs and realities.[296]

Additionally, critics would likely argue that piracy is limited to acts of violence over or on the high seas, so aircraft hijacking cannot qualify as "piracy" if the hijacking occurs while the plane is flying over a nation's territory.[297] While UNCLOS does restrict piracy to acts occurring over the high seas, scholars acknowledge that the law of piracy is blurry and the definition of piracy has been inconsistent throughout history.[298] Rather than restricting universal jurisdiction from applying to aircraft hijacking because of piracy's "doctrinal controversies," scholars suggest that an aviation convention granting limited universal jurisdiction in respect to hijacking could help deter additional aircraft hijackings.[299]

b. Cyberterrorism

When arguing that universal jurisdiction should expand to apply to cyberterrorist acts, scholars have noted that the "borderless and transnational nature of the Internet and cyberterrorism complicates the [traditional] application of territorial jurisdiction" to international crimes.[300] While a cyberterrorist must access the internet from a discrete location somewhere in the world, tools like the Onion Router can mask the cyberterrorist's true location, making it difficult to trace the cyberterrorist to the correct nation.[301] Additionally, even if a cyberterrorist is successfully traced to his or her location in a country, as previously noted, it could be difficult to prosecute that cyberterrorist if the host nation is either unwilling or unable to extradite or prosecute the cyberterrorist domestically.

---

[295] Randall, *supra* note 257, at 797. For example, in 1985, Palestinian terrorists hijacked the cruise ship *Achille Lauro* in the Mediterranean Sea. *Achille Lauro Hijacking Ends*, HISTORY.COM (Nov. 29, 2009), https://www.history.com/this-day-in-history/achille-lauro-hijacking-ends [https://perma.cc/V52Q-EMYD]. The armed hijackers held the ship hostage and demanded that Israel release fifty Palestinian militants imprisoned in Israel. *Id.*

[296] Randall, *supra* note 257, at 797; Jacobson, *supra* note 272, at 173.

[297] Randall, *supra* note 257, at 797; Jacobson, *supra* note 272, at 171.

[298] Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 108 (2010).

[299] Jacobson, *supra* note 272, at 175.

[300] Gable, *supra* note 298, at 65–66.

[301] Scheiner, *supra* note 238.

To overcome these limitations, scholars argue that universal jurisdiction is the most effective way to deter would-be cyberterrorists from attacking critical infrastructure systems.[302] Universal jurisdiction would allow victim nations to overcome the practical challenges of locating and then prosecuting cyberterrorists because it would allow any other nation to also request that the host nation extradite the cyberterrorist. Additionally, a different nation could initiate its own prosecution of the cyberterrorist if it successfully gains custody of the cyberterrorist. Applying universal jurisdiction to allow all nations to arrest and prosecute cyberterrorists could potentially strip cybercriminals of "data" safe havens.[303] Without universal jurisdiction, an attacked state may be forced to potentially wait for a cyberterrorist to either voluntarily enter the attacked country or for a friendly country to extradite the cyberterrorist to the attacked state before the victim nation can attempt to prosecute the cyberterrorist.[304]

However, convenience and deterrence may not prove enough for the global community to accept an additional application of universal jurisdiction for cyberterrorism. To overcome this resistance, scholars also argue that cyberterrorism is analogous to piracy on the high seas, a crime for which the world has traditionally allowed any nation to prosecute.[305] Scholars note that cyberterrorism is often conducted by hackers who act individually or within hacking groups.[306] Typically, these hackers act without state consent.[307] Similar to pirates on the high seas, cyberterrorists are often unaffiliated with any nation and refuse to abide by the laws of any nation or even society.[308] Because these cyberterrorists refuse to abide by the laws of nations and their cyber activities can seriously threaten any nation's critical infrastructure, universal jurisdiction should be applied to encourage all nations to apprehend and prosecute cyberterrorists.

For example, terrorist organizations like Al Qaeda or ISIS have started to use cyberspace to expand their influence in recent years.[309] These terrorist groups resemble pirates who have

---

[302] Gable, *supra* note 298, at 57.

[303] Cade, *supra* note 24, at 1155.

[304] Gable, *supra* note 298, at 108.

[305] *Id.* at 105.

[306] *Id.* at 110–11.

[307] *Id.*

[308] *Id.*

[309] Mike Rogers, *How ISIS Uses the Internet to Recruit New Members (Hint: It Involves Kittens)*, N.Y. DAILY NEWS (Sept. 6, 2017), https://www.nydailynews.com/

"opted out of the 'law of society'" by potentially targeting the entire world and abandoning their allegiance to any state.[310] While it is uncertain whether Al Qaeda or ISIS have sophisticated hacking skills, it is very possible that these terrorist organizations might try to employ cyberhackers to conduct cyberterrorist attacks for them.[311] If ISIS partnered with a cyberhacker group, they could attempt to conduct a cyber-9/11 or cyber-Lockerbie incident. To help deter hackers from participating in such an event, universal jurisdiction should be expanded to apply to terrorists and cyberhackers that take part in terrorist activities.

2. Examining the "Heinousness" of the Act

The second, and more difficult, argument for applying universal jurisdiction to an international crime involves persuading the international community that the crime committed is so heinous that it is on par with other crimes that have qualified for universal jurisdiction—for example, genocide and other crimes against humanity.[312] However, the meaning of the term heinous is defined in vague terms, such as a crime "shocking to the conscience," making it challenging to determine which crimes qualify for universal jurisdiction.[313]

Because it is difficult to determine which crimes qualify as "heinous" and should be afforded the status of *jus cogens* under international law, the amount of crimes that qualify for universal jurisdiction have been restricted.[314] However, a cyber-hijacking act could very likely qualify as heinous. Aircraft hijacking poses a grave threat to all nations and the events of 9/11 were largely condemned by the global community.[315] In the context of cyberterrorist acts, scholars argue that extreme acts of terrorism that are of such a scale that entire financial or national security

---

news/national/isis-internet-recruit-members-hint-kittens-article-1.3473890 [https://perma.cc/M3ZC-HR9E].

[310] Anthony J. Colangelo, *Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law*, 48 HARV. INT'L L.J. 121, 145 (2007).

[311] Carlin, *supra* note 14.

[312] Cade, *supra* note 24, at 1166; Kontorovich, *supra* note 249, at 205–06.

[313] Cade, *supra* note 24, at 1166; Kontorovich, *supra* note 249, at 206.

[314] *See, e.g.*, Colangelo, *The New Universal Jurisdiction*, *supra* note 288, at 603.

[315] Press Release, Security Council, Security Council Condemns, 'In Strongest Terms,' Terrorist Attacks on United States, U.N. Press Release SC/7143 (Sept. 12, 2001), https://www.un.org/press/en/2001/SC7143.doc.htm [https://perma.cc/K4UQ-AWGD].

systems may be dismantled may meet this standard.[316] Accordingly, if acts of cyberterrorism or hijacking aircraft qualify as "heinous" and "shocking to the conscience," the combination of these two crimes during a cyber-9/11 or cyber-Lockerbie incident would very likely meet the heinous standard and subsequently qualify for universal jurisdiction.

While a cyber-9/11 or Lockerbie would likely qualify as "heinous" and aircraft hijacking is almost universally condemned, crimes such as aircraft hijacking have not yet reached an accepted status under customary law to be governed by universal jurisdiction.[317] Additionally, malicious cyber activities targeting areas of aviation infrastructure that do not explicitly hijack the airplane's avionics or cockpit controls may prove more subtle and difficult to trace, especially if the cyberattack does not result in a crash, injuries, or death.[318] These subtler cyberattacks on the aviation industry may fall short of the "conscience-shocking" heinous standard and consequently fail to justify the use of universal jurisdiction.[319]

However, as previously noted, subtle cyberattacks on the aviation industry still lead to huge financial losses and potentially devastating impacts on the global economy.[320] A cyberterrorist would not need to necessarily hack and hijack an airplane to have a deadly impact.[321] Though more attenuated, a smaller cyberattack that disrupts flight operations can still have deadly consequences if it prevents a plane from delivering valuable medical supplies or food to dependent nations or individuals.[322] For example, certain remote portions of Alaska do not have highways or roads that connect the towns to the rest of the state, forcing citizens of these remote areas to rely on air-freight to deliver food, medical supplies, and to transport citizens to and from these regions.[323] If airlines are unable to operate and deliver to these remote areas, populations could be forced to uproot or face extinction. While these examples are extreme, they

---

316 Gable, *supra* note 298, at 118.

317 Bassiouni, *supra* note 267, at 115–34.

318 Cade, *supra* note 24, at 1166; Kontorovich, *supra* note 249, at 206–07.

319 Cade, *supra* note 24, at 1166; Kontorovich, *supra* note 249, at 206–07.

320 *Hackable at Any Height*, *supra* note 29, at 5.

321 *Id.*

322 *Id.*

323 Jad Mouawad, *Alaska Airlines Powers Through Tough Winter Conditions, Turbulent Industry*, SEATTLE TIMES (Mar. 3, 2013), https://www.seattletimes.com/life/travel/alaska-airlines-powers-through-tough-winter-conditions-turbulent-industry/ [https://perma.cc/7SYA-4HKX].

demonstrate how much the global community depends on aviation. If considered in the aggregate, the destabilizing impact of smaller cyberattacks could still lead to heinous results that might warrant the application of universal jurisdiction.

Extending universal jurisdiction to apply to malicious cyberattacks on the aviation industry could provide the global community with a greater ability to prosecute cyberterrorists and send a message that cyberterrorists will be held accountable in the event of a cyber-Lockerbie or 9/11. Just as the international legal community took a stand against genocide after World War II, the international community today should also take a stand against cyberterrorists by applying universal jurisdiction to hold these terrorists accountable. While many nations bear valid concerns about potential universal jurisdiction abuses, the global aviation community's concern with protecting the international skies and the well-being of the global population must take precedent over these controversies. If the global community is unwilling to adopt universal jurisdiction for cyberattacks on the aviation industry, then the global community must also bear the responsibility for a potential cyber catastrophe in aviation. Ultimately, the global aviation industry as well as aviation lawmakers must implement some type of standard or best practice to strengthen cybersecurity in aviation.

V. CONCLUSION

Malicious cyber actors will continue to take advantage of technological vulnerabilities in the aviation industry. No matter their motivation or purpose, cyber actors will continue to wage sophisticated cyberattacks against the aviation industry while enjoying the anonymity and convenience of the internet. Aviation lawmakers and organizations, and the world's nations must implement international standards that deter cyberattacks and hold cyber actors accountable for their actions. Specifically, international aviation lawmakers should consider expanding universal jurisdiction to apply to malicious cyber activities targeting the world's airlines and industry. Regardless of the deterrent mechanism, the global aviation industry as well as aviation lawmakers must adapt and strengthen international cybersecurity standards and practices.

APPENDIX

FIGURE 1: NextGen System[324]

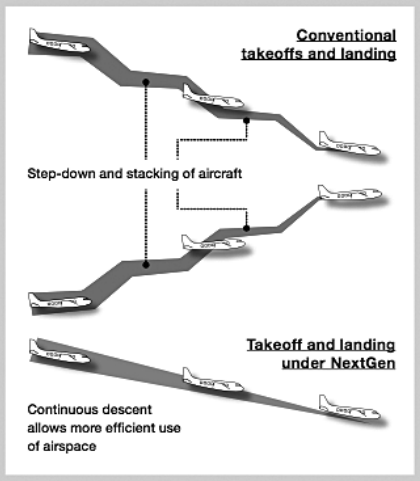


Figure 1: **Continuous descent under NextGen, compared with traditional take-off and landing**

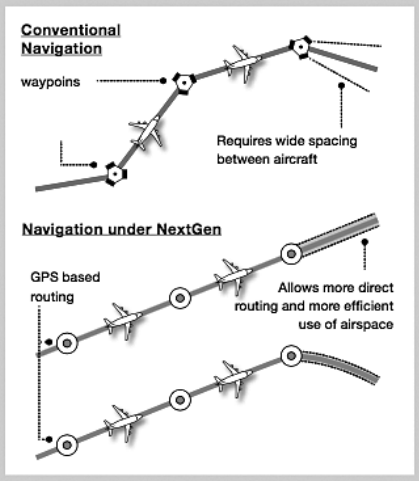
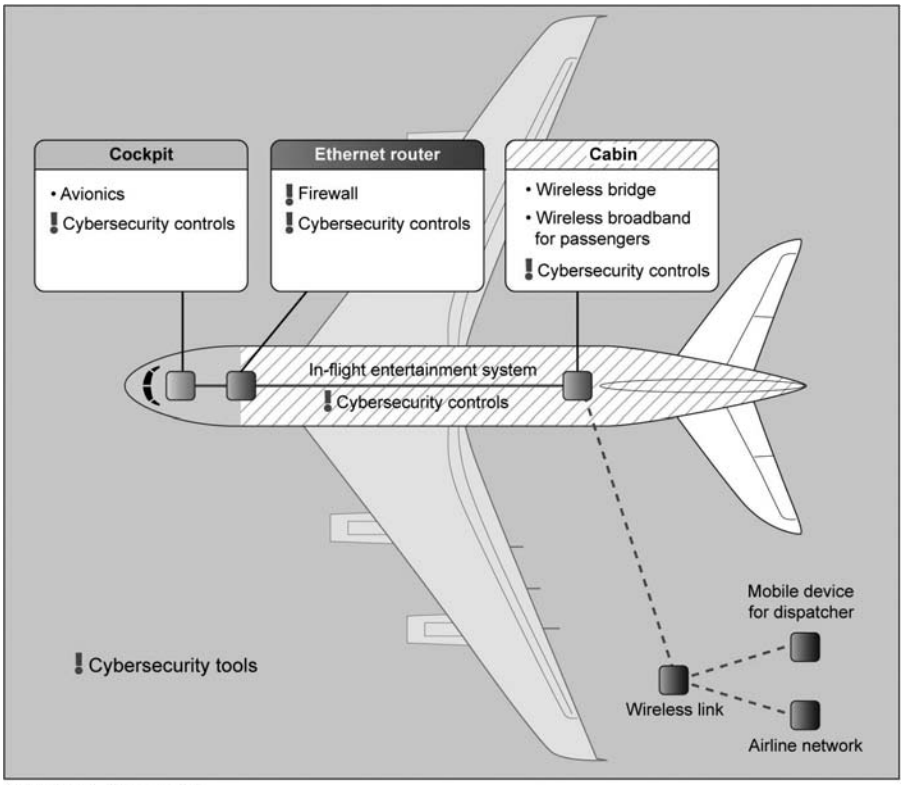


Figure 2: **Navigation under NextGen versus traditional radar-based navigation**

[324] *Hackable at Any Height*, *supra* note 29, at 12, figs. 1 & 2.

FIGURE 2: IP Networks on Modern Aircraft[325]



Source: GAO. | GAO-15-370

[325] AIR TRAFFIC CONTROL, *supra* note 47, at 19, fig. 4.

FIGURE 3: United Hacker Tweet[326]

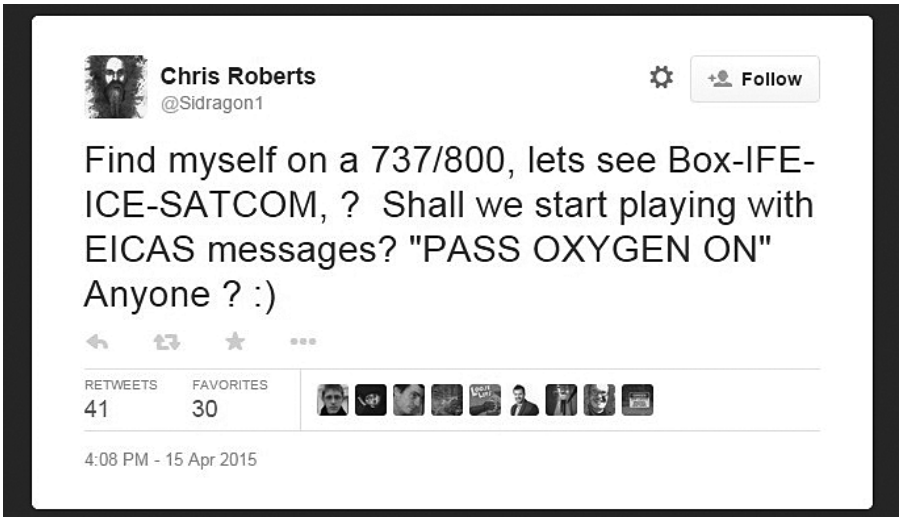


FIGURE 4: Malaysia Website Hack[327]

[326] Pagliery, *supra* note 91.
[327] *Hackable at Any Height*, *supra* note 29, at 16, fig. 5.

FIGURE 5: El Al Website[328]

FIGURE 6: Hobart Airport Hack[329]

[328] *Id.* at 17, fig. 6.
[329] *Id.* at 14, fig. 3.