CYBERTERRORISM: COMBATING THE AVIATION INDUSTRY'S VULNERABILITY TO CYBERATTACK

I. INTRODUCTION

"Warfare has always been an evolving concept."[1] Warfare continues to mold the international community, yet the leading forces behind this constantly evolving concept do not solely include "economic, social, or moral" implications; rather, the strongest force is the advancement of wartime technology.[2] For generations, state and non-state actors have researched and tested technological vulnerabilities either to counter or exploit weaknesses.[3] Today, our generation faces the malicious intent of international state and non-state actors that are willing to exploit advancing computer technologies.[4] President Barack Obama has emphasized that state and non-state actors are capable of compromising aviation security: "We know hackers steal people's identities and infiltrate private e-mail. . . . Now our enemies are also seeking the ability to sabotage . . . our air traffic control systems."[5]

---

1. Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY 603 (2011), *available at* http://digitalcommons.pepperdine.edu/cgi/viewcontent.cgi?article=1013&context=naalj (highlighting how historical warfare evolved into technologically efficient warfare).

2. *Id.* (setting foundation for evolving concept of warfare).

3. *Id.* (showing transformative means of warfare over period of generations).

4. *Id.* (suggesting revolutionary threat current and future generations face). *See* Danny Yadron, *Chinese Hacked U.S. Military Contractors, Senate Panel Says*, WALL ST. J., http://www.wsj.com/articles/chinese-hacked-u-s-military-contractors-senate-panel-says-1410968094 (last updated Sept. 18, 2014, 4:29 PM) (alleging hackers associated with China's government broke into "private transportation companies working for U.S. military"). In a declassified incident, "the People's Liberation Army stole flight details and encryption passwords for commercial airlines contracted by the U.S. Army . . . ." *Id. See also* Charlie Mitchell, *Cyberwar: Not If. Not When. Now.*, WASH. EXAMINER (Sept. 29, 2014) (noting "destructive capacity of nation-states and non-state actors is growing rapidly"). Non-state actors' destructive capacity is impacting the economy, according to Larry Clinton, Internet Security Alliance President and CEO. *Id.* Today, the international community is fully "dependent on cybersystems" that are constantly under cybercriminals' attacks. *Id.* Corporate intellectual property, national defense systems, personal data, and public utilities are all susceptible to cyberattack. *Id.*

5. President Barack Obama, State of the Union Address (Feb. 12, 2013).

This Note examines the threat that the international aviation community faces, concludes that a comprehensive legal framework directing attention to the aviation industry is necessary, and offers suggestions to prevent a "cyber Pearl Harbor" or another similar-to 9/11 terrorist event.[6] Part II highlights data security protection and cyberwarfare threats that have triggered critical concern for various industries, including business, government, and transportation; moreover, Part II discusses the emergence of the International Civil Aviation Organization (ICAO) and its role in the international community.[7] Part III evaluates aviation vulnerabilities, focusing on the unique and highly complex system encompassing the aircraft, air traffic management (ATM), and ground or satellite stations that feed data through this cycle; additionally, Part III highlights the strong influence that the United States' Federal Aviation Administration (FAA) has on the international aviation community.[8] Part IV argues that substantive cybersecurity measures

---

6. *See infra* Part IV.B (explaining cyber Pearl Harbor and pre-9/11 stage); *see also* Mitchell, *supra* note 4 (quoting Leon Panetta, former U.S. Secretary of Defense, as cautioning about "cyber Pearl Harbor [sic]"). For purposes of this Note, a cyber-Pearl Harbor and pre-9/11 stage refer to a period before a significant event occurs, i.e., a "Black Swan event." *See, e.g.*, Nassim Nicholas Taleb, *'The Black Swan: The Impact of the Highly Improbable'*, N.Y. TIMES (Apr. 22, 2007), http://www.nytimes.com/2007/04/22/book/chapters/0422-1st-tale.html?_r=0. The Black Swan theory provides that a particular event is an outlier, transmits significant consequences, and compels society to explain why the event occurred, whereby in hindsight, it was explainable and predictable. *Id.* A Black Swan event is one that is hardly predictable, yet has an extreme impact on society. *Id.* For example, the terrorist attacks of September 11, 2001, are a Black Swan event that had low predictability and caused a significant impact. *Id.* Had the terrorist attacks been predicted the day before, they might not have happened. *Id.* If terrorist attacks were of great concern, the U.S. government would have bolstered aviation security to prevent the terrorists' objectives. *Id.* Had the proper precautions been made before September 11, 2001, the horrific events might not have happened. *Id.* Similarly, a cybercrime attack against the aviation industry could lead to a future Black Swan event that has significant repercussions similar to the tragic events of 9/11 or Pearl Harbor where, had there been an inkling that such an event would occur, perhaps it would never have occurred. *Id.*

7. *See infra* Part II.A.1 (discussing international approach to data protection); *infra* Part II.B.1 (examining historical background to International Civil Aviation Organization (ICAO)).

8. *See infra* Part III.A.2-B (detailing civil aviation vulnerabilities concerning aircraft, air traffic management (ATM) system, and ground or satellite stations); *see also* Emilio Iasiello, *Getting Ahead of the Threat: Aviation and Cyber Security*, AEROSPACE AMERICA, July-Aug. 2013, at 22, 22-23, http://www.aerospaceamerica.org/Documents/AerospaceAmerica-PDFs-2013/July-August-2013/Viewpoint-Getting-Ahead-AA-Jul-Aug2013.pdf (evincing network vulnerabilities aviation industry faces).

must be implemented to counter the aviation network's vulnerabilities and to thwart state and non-state actors intending to disrupt global aviation security.[9] Part IV further provides that the ICAO's leadership is pivotal in implementing a cybersecurity taskforce to enhance international security, provide strategic relations, and offer recommendations to fight in the twenty-first century's cyberwarfare.[10] Finally, Part V emphasizes the necessity of a cybersecurity taskforce as innovative technologies are introduced into the aviation community, thereby increasing the risk of cyberattack.[11]

II. HISTORY

A. The Cyberthreat to Various Industries

1. Background on Cybercrime

A challenge exists in developing an appropriate lexicon for cyberterrorism, because a universal definition has not yet been adopted.[12] The term "terrorist" is used to identify "revolutionaries who seek to use terror systematically to further their views or to govern a particular area."[13] Terrorists have evolved with

---

9. *See infra* Part IV.A, B.1, B.3 (proffering implementations which international aviation community must enact before potential Black Swan event).

10. *See infra* Part IV.B.2 (analyzing ICAO's influence in aviation community and providing suggestions for ICAO in countering cyberwarfare).

11. *See infra* Part V (underscoring need for solutions to counter cybercrime against aviation industry).

12. *See* Jonalan Brickey, *Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace*, CTC SENTINEL, Aug. 2012, at 4, 4, https://www.ctc.usma.edu/v2/wp-content/uploads/2012/08/CTCSentinel-Vol5Iss8.pdf (covering how experts have not yet formed agreed-upon definition of cyberterrorism). Jonalan Brickey emphasizes "[t]hree [c]lusters of [c]yberterrorism": (1) enabling cyber militancy; (2) disruptive cybermilitancy; and (3) destructive cybermilitancy. *Id.* "Enabling cyber militancy [sic] . . . activities" play a key role in cyberattacks, including "recruiting, . . . radicalizing, financing, training, planning and communicating." *Id.* Actors participating in enabling cybermilitancy need not have religious motives; instead, "to fit in this category," actors must have political motives. *Id.* at 5. The second cluster of cyberterrorism is disruptive cybermilitancy. *Id.* This involves actors whose plans are to disrupt a Westernized, cyber-dependent lifestyle that relies on critical data infrastructure to support its medical, transportation, and financial organizations. *Id.* Finally, terrorists use destructive cybermilitancy to exploit and corrupt computer and information systems. *Id.* Critical systems, including transportation, financial, and healthcare systems, are particularly vulnerable to destructive cyberattack whereby terrorists intend to feed misinformation and create "confusion and loss of confidence." *Id.*

13. M.J. Warren, *Terrorism and the Internet*, *in* CYBER WARFARE AND CYBER TERRORISM 42, 42 (Lech J. Janczewski & Andrew M. Colarik eds., 2008) (defining terrorism).

the advancement of technology to adapt to cyberterrorism–a distinct type of terrorism that involves an immediate threat because of the international community's dependence on technology; although cyberterrorism might not be recognized to threaten our physical state, it can wreak havoc and chaos in various industries.[14] The Center for Strategic and International Studies (CSIS) has defined "cyberterrorism" as "the use of computer network tools to shut down critical national infrastructures . . . or to coerce or intimidate a government or civilian population."[15] Another interpretation of cyberterrorism involves the utilization of computers to cause significant bodily harm or death, or to incapacitate critical infrastructure that may jeopardize human lives.[16]

---

14. *See id.* (distinguishing cyberterrorism from terrorism). M.J. Warren explains that cyberterrorism would be a "physical systematic terror" if the specific cyberattack "causes a critical system to fail." *Id. See also* Brickey, *supra* note 12, at 6 (creating one example of plausible destructive cybermilitancy attack causing extensive damage to critical infrastructure). An example of an attack on critical infrastructure could involve "a key natural gas pipeline." *Id.* An electronic industrial control system controls such a pipeline and a pipeline is vulnerable to hacking, potentially leading to a dangerous "increase in pipeline pressure," causing a devastating explosion. *Id. See also* 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, 62-63 (providing definition of cyberterrorism). Cyberterrorism reflects terrorists' utilization of the Internet to sabotage computer systems, disrupt the international financial community, and engage in similar terrorist activities in the cyberspace realm. *Id.* at 62. Cyberterrorism is typically referred to as a terrorist event conducted on the Internet. *Id.* at 63. Cyberattacks against "the Estonian, U.S., and South Korean governments" generated the concern to counter cyberterrorism via government and international organizations. *Id.* at 64. Such international organizations include the North Atlantic Treaty Organization (NATO), the European Union, the Council of Europe, the Organization for Security and Cooperation in Europe (OSCE), and the United Nations. *Id.* These are just a few of the international groups attempting to counter cyberterrorism. *See id.* at 64-65.

15. William L. Tafoya, *Cyber Terror*, FBI L. ENFORCEMENT BULL. (Nov. 2011), (internal quotation marks omitted) *available at* http://leb.fbi.gov/2011/november/cyber-terror (expounding meaning of cyberterror). The energy, transportation, and government sectors are critical infrastructures. *Id.* According to author Barry Collin, cyberterror is "the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information." *Id.* (internal quotation marks omitted).

16. Aviv Cohen, *Cyberterrorism: Are We Legally Ready?*, 9 J. INT'L BUS. L. 1, 7 (2010), *available at* http://scholarlycommons.law.hofstra.edu/cgi/viewcontent.cgi?article=1111&context=jibl (citing to Shlomo Harnoy and Yossi Or of Sdema Group). "The Sdema Group is an integrated, homeland security solutions partnership helping to create secure environments around the world for governments and businesses to thrive." *About Sdema*, SDEMA GROUP, http://www.sdemagroup.com/About.aspx?a=

After 9/11, security experts and politicians have warned about the threat that cyberterrorists could "hack[ ] into government and private computer systems [to] crippl[e] the military, financial, and service sectors of advanced economies."[17] Cyberterrorists have utilized the Internet to demonstrate their power, intending to interfere with technological systems, i.e., computer and telecommunication services, to cause widespread disruption, and to cause the public to lose confidence in the government's ability to operate effectively.[18] The cyberterrorism threat is so severe that President Obama stated it as one of the biggest national security concerns and that the U.S. government has been preparing "for a possible doomsday scenario if hackers can successfully penetrate government and business computer systems . . . ."[19]

a. Cybercrime Against Businesses

Cybercrime is a rapidly developing international issue involving criminals who take advantage of the "convenience and anonymity of the Internet to commit a [broad] range of criminal

256 (last visited on Oct. 13, 2014) (summarizing background information on Sdema Group).

17. GABRIEL WEIMANN, Cyberterrorism: How Real Is the Threat? 1 (2004), *available at* http://www.usip.org/sites/default/files/sr119.pdf (indicating potential threat of cyberterrorism). After 9/11, "the political, business, and security" sectors highlighted cyberattacks as a potential threat. *Id.* Terrorists target these sectors, because of the ease of "anonymity, [the] potential to inflict massive damage, [the] psychological impact, and [the] media appeal." *Id.* Terrorists are aware that their success on the "war on terror" relies on their using "unconventional weapons, such as cyberterrorism." *Id.* at 2. "[D]espite . . . predictions of a cyber-generated doomsday, no single instance of real cyberterrorism has been recorded." *Id.* Since the most critical infrastructure in Western societies involves the interconnectedness of computers, the threat of cyberterrorism is disturbing. *Id.* Thus, the increasing reliance of society's use of computer systems has created an incentive for terrorists to approach targets that are vulnerable to cyberattack. *Id.*

18. Scott J. Shackelford, *Toward Cyberpeace: Managing Cyberattacks Through Polycentric Governance*, 62 AM. U. L. REV. 1273, 1301 (2013) (elucidating how terrorists utilize cyberspace and for what purpose).

19. Charlie Gasparino, *Obama Said to Warn of Crippling Cyber Attack Potential*, FOX BUS. (Oct. 12, 2014), http://www.foxbusiness.com/economy-policy/2014/10/12/obama-said-to-warn-crippling-cyber-attack-potential/ (stating heightened concern of imminent cyberterrorism threat). President Barack Obama forecasted that a potential cyberterrorism event and concern of cyberterrorism will be a primary concern for his successor. *See id. See infra* Part II.B.2 (predicting occurrence of future tragic event similar to terrorist attacks of 9/11).

activities . . . ."[20] The International Criminal Police Organization (INTERPOL) divides cybercrime into two broad areas: (1) "attacks against computer hardware and software"; and (2) financial crimes.[21] In recent years, cybercriminals have developed

---

20. *Cybercrime*, ICPO-INTERPOL, http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (last visited Oct. 15, 2014) (characterizing cybercrime as "fast-growing area of crime" involving criminals who exploit ease "and anonymity of Internet"). The International Criminal Police Organization (INTERPOL) describes cybercrime as a nascent issue in the twenty-first century Internet world whereby cybercriminals participate in illegal activity that has no physical or virtual borders. *Id.* Cybercriminals take advantage of the "convenience and anonymity of the Internet" to participate in criminal activity. *Id. See also INTERPOL Chief Warns of 'Invisible' Threats to Personal and Economic Security*, ICPO-INTERPOL (Sept. 13, 2013), http://www.interpol.int/News-and-media/News/2013/PR111 (suggesting cybercrime, along with "increasing movement of people and goods," poses significant global safety threat). The head of INTERPOL warned that cybercrime poses a significant threat to global safety and security, because of "the ever-increasing movement of people and goods in both the real and virtual worlds." *Id.*

21. *Cybercrime*, *supra* note 20 (dividing cybercrime into two areas, although not intended as exhaustive list). Attacks against computer hardware and software include botnets, malware, and network intrusion. *The Threats*, ICPO-INTERPOL, http://www.interpol.int/Crime-areas/Cybercrime/The-threats/Malware,-bots,-botnets (last visited Jan. 17, 2016). Cybercriminals use "botnets" to send out "spam email messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud." Microsoft Safety & Security Center, *How to Better Protect Your PC from Botnets and Malware*, https://www.microsoft.com/security/pc-security/botnet.aspx (last visited Feb. 14, 2016) (demonstrating danger botnets pose). "Malware," short form for "malicious software," is undesired software that is installed onto a computer without consent. Robert Moir, *What Is Malware?*, MICROSOFT, https://technet.microsoft.com/en-us/library/dd632948.aspx (last visited Oct. 15, 2014) (educating general public about malware). Viruses, worms, and Trojan horses are common types of malware that cybercriminals utilize. *Id.* Financial crimes involve fraudulent transactions occurring online, and penetration and phishing of online financial services. *See Financial Crime*, ICPO-INTERPOL, http://www.interpol.int/Crime-areas/Financial-crime/Financial-crime (last visited Jan. 17, 2016) (listing financial crimes). Phishing is a kind of "identity theft" that uses email and fraudulent websites that are intended to steal personal data or information, especially financial information. *Online Safety*, ICPO-INTERPOL, http://www.interpol.int/Crime-areas/Cybercrime/Online-safety (last visited Jan. 17, 2016); *see also* Press Release, Darrell Foxworth, Federal Bureau of Investigation, FBI Warns Public that Cyber Criminals Continue to Use Spear-Phishing Attacks to Compromise Computer Networks (July 12, 2013), http://www.fbi.gov/sandiego/press-releases/2013/fbi-warns-public-that-cyber-criminals-continue-to-use-spear-phishing-attacks-to-compromise-computer-networks (alerting public about cybercriminals attempting "to access private computer networks"). Cybercriminals prefer spear-phishing attacks because they victimize members of an industry or organization that the cybercriminals wish to sabotage. *Id.* The Federal Bureau of Investigation (FBI) has warned the public about attacks whereby victims will open an email that will download malware and will compromise "victim[s'] usernames and passwords, bank account details, credit card numbers, and other personal information." *Id.* Cyberabuse is aimed against youngsters, particularly through "sexploitation." EUROPEAN FIN. COAL. AGAINST COMMERCIAL SEX-

sophisticated ways to attack computer hardware and software of businesses and financial institutions.[22] Financial institutions are prime targets for cybercriminals, because with minimal effort using a computer, malware can easily infiltrate into banks' internal computers.[23] Cybercriminals are increasingly becoming attracted to small businesses because they are generally more vulnerable than larger businesses.[24] As large enterprises increase

---

UAL EXPLOITATION OF CHILDREN ONLINE, COMMERCIAL SEXUAL EXPLOITATION OF CHILDREN ONLINE: A STRATEGIC ASSESSMENT 10 (2013), *available at* http://www.europeanfinancialcoalition.eu/private10/images/document/5.pdf. Children and young people conducting their social lives online expose themselves to a present-day trend involving sexualized behavior on a variety of online video or chat platforms. *Id.* (signaling current trend in sexploitation among children and young people who conduct their social lives online). Individuals interested in children employ "sextortion" techniques to coerce young people to provide indecent material. *Id.* Criminals enjoy the immediacy of the Internet through their using aggressive and coercive tactics to ensure victim compliance. *Id.* at 9-10.

22. The Economist, *Cyber-Criminals*, WORLD IN 2014 (2013), *available at* http://www.economist.com/news/21589042-cybercriminals?zid=291&ah=906e69ad01d2ee51960100b7fa502595 (emphasizing sophistication of cybercriminals). Cybercriminals have developed into a sophisticated group, finding ways to attack mobile-banking, smartphone operating systems, and cloud computing. *Id.*

23. *See* David E. Sanger & Nicole Perlroth, *Bank Hackers Steal Millions via Malware*, N.Y. TIMES, Feb. 14, 2015 (revealing hackers' ability to infiltrate banks through malware). In one case, malicious malware infiltrated several banks' computers and allowed hackers to observe employees' activities. *Id.* Malware transmits confidential information to the criminal group regarding the regular daily activities of the bank employees. *Id.* The involved cybercriminals successfully impersonated bank employees and were able to transfer millions of dollars from Russian, Japanese, U.S., Swiss, and Dutch banks into "dummy accounts" created in other foreign countries. *Id. See also* James Titcomb, *Could Your Bank Be the Next Victim of a Cyber Attack?*, TELEGRAPH (Oct. 19, 2014, 5:00 PM), http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/11170888/Could-your-bank-be-the-next-victim-of-a-cyber-attack.html (stating financial ease for cybercriminals in attacking banks). Attacking banks involves little expense for hackers and once they successfully attack one bank, subsequent attacks require minimal effort. *Id. See also Who Lies Behind the Latest Cyber Attacks on JPMorgan Chase?*, ECONOMIST (Aug. 28, 2014), http://www.economist.com/news/business-and-finance/21614181-who-lies-behind-latest-cyber-attacks-jp-morgan-chase-hacking-banks (addressing potential cybercriminals' motives in hacking into financial institutions). JPMorgan Chase was one bank institution that fell victim to cyberintrusion. *Id.* The involved cybercriminals' motive in siphoning mass data and hacking into bank customers' bank accounts was eventually revealed to be financial. Warwick Ashford, *Three Men Charged Over JP Morgan Hacking and Fraud*, COMPUTERWEEKLY.COM (Nov. 12, 2015), http://www.computerweekly.com/news/4500257262/Three-men-charged-over-JP-Morgan-hacking-and-fraud.

24. Ericka Chickowski, *Protect Your Small Business Against Cyber Attacks*, ENTREPRENEUR, May 14, 2010, http://www.entrepreneur.com/article/206656 (accentuating cyberthreat to small businesses). Smaller family-operated websites are unknowingly compromised while attacks secretly infect website viewers. *Id. See also* John Brandon, *Why Your Business Might Be a Perfect Target for Hackers*, INC., Dec.

and strengthen their cybersecurity infrastructure, less-secure small businesses become more desirable to cybercriminals intending to attack intellectual property, unprotected credit card numbers, or unsecured computers.[25]

b. Cybercrime Against Governments

International governments are particularly at risk of falling victim to cyberattacks.[26] Cybercriminals are striving to develop

---

2013-Jan. 2014, http://www.inc.com/magazine/201312/john-brandon/hackers-target-small-business.html (spelling out vulnerability of smaller companies because they lack strong online security). Smaller companies tend to have weaker security measures than larger companies. *Id.* Smaller companies engage in cloud services online that lack strong encryption technology. *Id.* Cyberattacks on small companies increased 300% in 2012 from 2011. *Id.*

25. Brandon, *supra* note 24 (articulating how smaller businesses remain more vulnerable than larger businesses to cyberhacking). Cybercriminals target smaller businesses because the risk of exposure is low. Robert Strohmeyer, *Hackers Put a Bull's-Eye on Small Business*, PCWORLD (Aug. 12, 2013, 3:30 AM), http://www.pcworld.com/article/2046300/hackers-put-a-bulls-eye-on-small-business.html (observing how small businesses become vulnerable to cyberattack). Small businesses are typically more vulnerable to larger businesses, because they lack sophisticated cybersecurity defenses, i.e., monitoring, audits, penetration testing, and warning systems, that the larger businesses typically have to alert them about a security breach. *Id.* Finding victims has gotten easy for criminals because the tools they use are cheap and easily acquired. *Id.* With minimal effort, hackers can use an app to explore "thousands of IP addresses" to find vulnerable computers. *Id.* Hackers can then plant viruses, such as spyware or software, and also emit "thousands of phishing emails" for the purpose of exposing computer users to malware that will leave them more vulnerable to cyberattack. *Id.* Moreover, "[a]ccording to the National Cyber Security Alliance, one in five small businesses falls victim to cybercrime . . . . And of those, about 60 percent go out of business within six months . . . ." *Id.* In other words, there is "a 20 percent chance" that a business may get hacked and if it does not have the proper means to recover, it risks dissolution. *Id.*

26. *See* KPMG Int'l, *Cyber Crime – A Growing Challenge for Governments*, ISSUES MONITOR, July 2011, at 1, *available at* https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf (setting forth cybercrime as increasing threat for governments); *see also* Damian Paletta, *White House Aims to Harden Cyberattack Defense*, WALL ST. J. (Jan. 11, 2015, 7:38 PM), http://www.wsj.com/articles/white-house-aims-to-harden-cyberattack-defense-1421023121 (reporting United States as "pushing for new laws and executive actions" strengthening defenses against cyberattacks). "[T]he number of cyber 'incidents' reported to the Department of Homeland Security rose from 105,931 in 2009 to 228,700 in 2013." *Id.* Suzanne Spaulding of the Department of Homeland Security said "that the Sony hack should galvanize industry and the government to focus on curbing such attacks. 'We need to continue to press the marketplace and within government to develop innovative approaches'. . . ." *Id.* Focus on cybersecurity increased following the hacking of Sony Pictures Entertainment, exposing the flaws in the communication between the U.S. government and the private sector. *See* Carol E. Lee, *Obama to Propose Cybersecurity Measures*, WALL ST. J., http://www.wsj.com/articles/obama-to-propose-cyber-

and strengthen techniques, focusing less on stealing financial information and more on spying and infiltrating government systems.[27] Cybercriminals have evolved their online arsenal to wreak havoc on government entities.[28] Richard Clarke, formerly a U.S. White House staff member who was head of cybersecurity and counter-terrorism, remarked, "that a full-scale cyber attack [sic] on a country's important infrastructure, such as military email systems, air traffic control systems, financial markets and utilities could have an unprecedented long-term effect."[29] For instance, the U.S., Canadian, Estonian, and Geor-

---

security-measures-1420912674 (last updated Jan. 10, 2015, 1:35 PM) (declaring "President . . . Obama will propose measures aimed at enhancing cybersecurity and addressing consumer issues"). President Obama's January 2015 visit with the National Cybersecurity and Communications Integration Center focused on how to effectively share critical information between private and government agencies. *Id.*

27. KPMG Int'l, *supra* note 26, at 1 (establishing transition of focus for cybercriminals); *see also* Peter Foster, *US Centcom Twitter Account 'Hacked by Islamic State'*, TELEGRAPH (Jan. 12, 2015, 8:02 PM), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11341057/US-military-twitter-account-hacked-by-Isil.html (preserving screenshots of tweets cyberhackers allegedly posted via U.S. Central Command's Twitter account); Roxana Tiron et al., *U.S. Military Twitter Account Hacked with Jihadist Messages*, BLOOMBERG (last updated Jan. 12, 2015, 6:03 PM), http://www.bloomberg.com/news/2015-01-12/u-s-military-twitter-account-hacked-with-jihadist-messages.html (announcing Islamic State purportedly hacked U.S. Central Command's YouTube and Twitter accounts). U.S. Central Command confirmed that hackers infiltrated its YouTube and Twitter accounts. Tiron et al., *supra*. A message that was posted to the Twitter account read, "American soldiers, we are coming, watch your back," and, "In the name of Allah the Most Gracious, the Most Merciful, the CyberCaliphate continues its CyberJihad." *Id.* Moreover, messages were posted on U.S. Central Command's YouTube site favoring the Islamic State. *See* Foster, *supra*. Central Command is responsible for covering the Middle East, including Afghanistan, Iraq, Syria, and Iran. Tiron et al., *supra*. It is leading the U.S. fight against Islamic State extremists. *Id.*

28. KPMG Int'l, *supra* note 26, at 8 (exposing how cybercriminals developed means to attack government entities).

29. *Id.* at 8 (introducing vulnerable infrastructures at risk in United States). *See also* Alice Lipowicz et al., *FAA Computer Failure Reflects Growing Burden on Systems,* THE BUS. OF FED. TECH. (Nov. 20, 2009), https://fcw.com/articles/2009/11/19/update-faa-software-hackers-delays.aspx (referring to air traffic control as target for cybercriminals); *British Armed Forces at Risk of Cyber Attack*, RT, http://rt.com/news/uk-military-cyber-attack-637/ (last modified Jan. 9, 2013, 17:58) (asserting U.K. economic, military, and industrial assets' risk of cyberattack). "The U[.]K[.] government refused to publicly blame the countries . . . most likely responsible for carrying out cyber attacks [sic]." *Id.* The U.K.'s "Security Community and GCHQ [Government Communications Headquarters] . . . . said, 'The greatest threat of electronic attack continues to be posed by state actors and of those, Russia and China are [suspected of carrying out] the majority of attacks. Their targets are in government as well as in industry." *Id.* (final alteration in original) (emphasis omitted). President Obama has emphasized the cyberthreat to the U.S. air traffic control system. *See* Corrin, *supra*;

gian governments have been targeted through cyberespionage.[30] This new domain of warfare through cyberspace just recently emerged in the twenty-first century whereby no land, sea, air, or space combat would apply and, therefore, governments have had to respond to cybercrime in unique defensive manners.[31]

---

see also Int'l Civil Aviation Org. [ICAO], *Twelfth Air Navigation Conference*, ¶¶ 1.2-2.3, ICAO doc. AN-Conf/12-WP/122 (Sept. 10. 2012), *available at* http://www.icao.int/Meetings/anconf12/WorkingPapers/ANConfWP122.1.1.ENonly.pdf (drawing attention to importance of cybersecurity for civil aviation). The ICAO has emphasized that cybersecurity is a high level impediment of the Global Air Navigation Plan. *Id.* at summary. *See also supra* note 23 and accompanying text (stressing financial threat to banking industry).

30. KPMG Int'l, *supra* note 26, at 8-9 (naming several countries subject to cyberespionage). The document points out four occasions when the U.S. defense system was targeted between June 2008 and March 2011. *Id.* Canada was victimized through cyberattack in January 2011, when "two Canadian government departments" were left "without internet access for nearly two months." *Id.* at 8. "Estonia and Georgia witnessed [their own] Web War I" whereby in 2007, cybercriminals performed a DOS attack "which affected [Estonia's] government, media, and banking web servers." *Id.* at 9. In 2008 and 2009, Georgia experienced its own cyberattack "during its war with Russia" leaving President Mikheil Saakashvili to use a U.S.-based server that was effectively capable of countering the cyberattack. *Id. See also* Julie Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES, July 9, 2015 (considering vulnerability of U.S. government computer systems). Roughly 21.5 million people fell victim to a cyberattack where hackers successfully breached government computer systems to obtain Social Security numbers and even fingerprints. *Id.* The cyberattack victims were mostly those who had "a government background check" performed within last fifteen years. *Id.* The "attack[was] believed to originate in China" even though U.S. administration officers were unable to confirm the exact perpetrator. *Id.* The White House cybersecurity coordinator, Michael Daniel, stressed the importance of cybersecurity protection in the private and public sectors. *Id.*

31. KPMG Int'l, *supra* note 26, at 10 (explicating how governments counter cybercrime against themselves). The U.S. government has been safeguarding "its digital infrastructure, declaring it as a 'strategic national asset.'" *Id.* Moreover, "Iran, Israel, North Korea, and Russia [have been] creating and training 'cyber armies' [sic]" in the event of a catastrophic cyberattack. *Id.* at 10-11 (outlining how countries counter cybercrime). In March 2011, U.S. Senators introduced a bill allowing President Obama "to shut down the internet" in the United States if a cyberattack were to occur. *Id.* The proposed bill, however, was never enacted. *See S. 413 (112th): Cybersecurity and Internet Freedom Act of 2011*, GOVTRACK.US, https://www.govtrack.us/congress/bills/112/s413 (last visited Feb. 14, 2016) (acknowledging U.S. cybersecurity bill would shut down Internet never enacted into law); *see also* S. 413, 112th Cong. (2011), *available at* https://www.gpo.gov/fdsys/pkg/BILLS-112s413is/pdf/BILLS-112s413is.pdf. The U.K. government classifies cybercrime as "a tier 1 threat" so therefore "in 2008, the Police Central e-Crime Unit was" established to counter national cybercrime. KPMG Int'l, *supra* note 26, at 10. Even though "China has been regarded as the largest" hub of hackers, the country also falls victim to cyberattacks. *Id.* at 11. China received international support from "the [United Nations], the Association of Southeast Asian Nations and other international communities," such as the United

c. Cybercrime Against the Transportation Industry

Cybercriminals are members of a versatile group that is always searching for innovative ways to expose vulnerabilities.[32] A group of prominent security professionals and hackers has suggested that the automobile industry should improve its vehicle security.[33] As with the automobile industry, the railroad industry is another line of business that cybercriminals target.[34]

States. *Id.* Large-scale international organizations, such as Europol and NATO have provided platforms to enforce cybersecurity initiatives. *Id.* at 12. "In June, 2010, Europol, the E.U.'s law enforcement agency, created the European Union Cybercrime Task Force." *Id.* This task force is comprised of representatives who provide the E.U. member states "with investigative and analytical support on cyber crime [sic]." *Id. See also* Juliet Van Wagenen, *International Aviation Organizations Unite on Cyber Threats*, AVIONICS (Dec. 11, 2014), http://www.aviationtoday.com/av/rotocraft/International-Aviation-Organizations-Unite-Against-Cyber-Threats_83704.html#.Vq1VxmQrLZs (heralding unity among international aviation organizations to tackle cyberthreats). Five major international aviation organizations signed a new cybersecurity agreement to coordinate their actions: the International Civil Aviation Organization, the Civil Air Navigation Services Organisation, Airports Council International, the International Coordinating Council of Aerospace Industry Associations, and the International Air Transport Association. *Id. See also Cyber Action Team: Rapidly Responding to Major Computer Intrusions*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/about-us/investigate/cyber/cyber-action-team (last visited Oct. 5, 2015) [hereinafter *Cyber Action Team*] (specifying purpose of FBI's Cyber Action Team (CAT)). The FBI can respond to serious cyberbreaches by utilizing their CAT, which is comprised of cyberexperts who can be dispatched within forty-eight hours to anywhere in the world to assist in investigations. *Id.* In 2006, the FBI's Cyber Division established CAT to provide a fast response to cybercrime. *Id.* Upon investigating, CAT scrutinizes the hacker's "tools, techniques, and procedures" to identify the responsible group or person. *Id.*

32. *What Hackers & Cyber Criminals Are Eyeing for in 2014*, LAVASOFT (Jan. 6, 2014), http://www.lavasoft.com/mylavasoft/company/blog/what-hackers-cybercriminals-are-eyeing-for-in-2014 (predicting cybercriminals' behavior in 2014); *see also* Jose Pagliery & Evan Perez, *U.S. Intel Officials Warn Hacking Is Getting Worse,* CNN MONEY (Sept. 29, 2015, 2:27 PM), http://money.cnn.com/2015/09/29/technology/nsa-china-spying/ (underlining versatility of cyberattacks). James Clapper, director of national intelligence for the United States, has emphasized the cybersecurity problem that the United States faces is that cyberthreats are increasing in "frequency, scale, sophistication and severity of impact." *Id.*

33. *Hackers to Automakers: Protect Cars from Cyber Attacks*, NBC NEWS DIGITAL (Aug. 8, 2014, 4:54 PM), http://www.nbcnews.com/tech/security/hackers-automakers-protect-cars-cyberattacks-n176401 (contending automobile industry also at risk of cybercrime). Modern cars rely on minicomputers to manage, air conditioning, brakes, engines, navigation, and windshield wipers. *Id.* Cybersecurity experts predict that cybercriminals will exploit software and other technological vulnerabilities. *Id.*

34. Aliya Sternstein, *Hackers Manipulated Railway Computers, TSA Memo Says*, NEXTGOV (Jan. 23, 2012), http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498/ (relaying how railways at risk of cybercrime). In early December 2011, the Transportation Security Administration al-

Additionally, the maritime sector is particularly vulnerable to cyberattack–for instance, a cyberattack has the potential to "disrupt[ ] the navigation of large cruise" and cargo ships that "could . . . lead to horrific loss of life and significant property damage."[35] Much like the maritime sector, the airline industry faces a threat whereby ATM, airports, satellite communications, and airplanes are all vulnerable to cyberattack.[36]

---

leged that "[h]ackers, possibly from abroad, [attacked] a Northwest rail company's computers" effectively and "disrupted railway signals for two days." *Id.*

35. MARSH, THE RISK OF CYBER-ATTACK TO THE MARITIME SECTOR 3 (July 2014), *available at* http://france.marsh.com/Portals/29/Documents/Risk%20of%20cyber%20attack%20Maritime%20sector.pdf (evaluating concern for maritime sector as prime target for cyberattack); *see also* Judy Greenwald, *Marine Sector Faces Cyber Risks as Navigation Systems Shift to Digital World*, BUSINESS INSURANCE (May 11, 2014, 12:01 AM), http://www.businessinsurance.com/article/20140511/NEWS07/305119968/marine-sector-faces-cyber-risks-as-navigation-systems-shift-to (clarifying cyber-related vulnerabilities in maritime industry). "In October [2013, a] Tokyo-based cloud security firm[,] Trend Micro Inc.[,] said it discovered flaws in ships' mandated automated identification systems, installed in [about] 400,000 vessels," allowing cyber-attackers to sabotage vessel communications and to replicate non-existing vessels on radar maps. *Id.* Moreover, "researchers at Texas A&M University" manipulated the Global Positioning System (GPS) of a USD80 million yacht, thereby falsifying its location. *Id.* "Markus Wähler, [a] Munich-based marine consultant at Munich Reinsurance Co." explained that "cyber risks [sic] are a real threat . . . ." *Id.* (internal quotation marks omitted). "However, marine cyber risks [sic] are 'just kind of coming into the forefront now,' said Cmdr. Emil A. Muccin, an assistant professor at the U.S. Merchant Marine Academy in Kings Point, New York." *Id.* "The maritime industry's 'risk implications . . . are only now beginning to be understood,' said Ben Beeson, Washington-based vice president of cyber security and privacy at Lockton Cos. L.L.C." *Id.* The cyberthreat is "no longer . . . just about privacy and personal information," but also involves the risk of "physical damage and bodily injury arising." *Id.*

36. *See* Steve Nichols, *Boeing Warns Inflight Cyber Security Is a Growing Issue*, GET CONNECTED, http://www.getconnected.aero/2014/10/boeing-says-inflight-cyber-security-growing-issue/ (last modified Oct. 7, 2014) (recognizing high importance of vigilance for airlines about risk of cybersecurity attack). The chief engineer of cabin network systems for Boeing said at the 2014 Aircraft eEnablement (Connectivity and IFE) Conference that "[The airline industry] need[s] to be more vigilant. Don't be in denial and don't underestimate the problem, but the risk is real, so don't get overconfident." *Id.* (internal quotation marks omitted). The Federal Aviation Administration (FAA) announced that Boeing's new aircraft, the Boeing Dreamliner 787, could be at risk to cyberattack on-board its computer systems leading to catastrophic consequences. *See* Kim Zetter, *FAA: Boeing's New 787 May Be Vulnerable to Hacker Attack*, WIRED (Jan. 4, 2008, 12:00 PM), http://archive.wired.com/politics/security/news/2008/01/dreamliner_security (recognizing Boeing aircraft's interconnected network makes plane's control systems vulnerable to hackers). According to an FAA report, "the computer network in the [Boeing] Dreamliner [787]'s passenger compartment" that provides onboard Internet access "is connected to the plane's control, navigation[,] and communication systems." *Id. See also* Bart Jansen, *FAA Orders Boeing to Protect 737s from Computer Hackers*, USA TODAY (June 6, 2014, 3:40 PM), http://

B. Aviation Industry's Approach to Cybersecurity

1. The International Civil Aviation Organization

In December of 1944, the United States hosted the Convention on International Civil Aviation, known as the Chicago Convention, at which fifty-two nations met to create a plan for international cooperation in air navigation.[37] The Chicago Convention's purpose was to promote coordination among the international community to achieve uniform regulations and standards for the postwar era civil aviation.[38] The Chicago Convention led to the Provisional International Civil Aviation Organization and finally to the ICAO.[39]

The founding fathers of the ICAO set a forewarning that civil aviation may lead to abuse and threats and therefore, the ICAO was organized to promote coordination among nations for society's benefit.[40] Even before the ICAO's establishment,

---

www.usatoday.com/story/news/nation/2014/06/06/faa-boeing-737/10066247/ (recounting vulnerability of Boeing 737 to cyberattack). The FAA made an official report stating that the plane's technology may be exploited outside the aircraft, "making the [Boeing] 737 aircraft more vulnerable." *Id.*

37. *History*, INT'L CIV. AVIATION ORG., http://www.icao.int/secretariat/TechnicalCooperation/Pages/history.aspx [hereinafter *ICAO History*] (overviewing background to development of ICAO) (last visited Jan. 12, 2015); *see also About ICAO*, INT'L CIV. AVIATION ORG., http://www.icao.int/about-icao/Pages/default.aspx (last visited Oct. 9, 2014) (discussing ICAO and Convention on International Civil Aviation). The ICAO is a U.N. specialized agency that "works with the [Convention on International Civil Aviation's (Chicago Convention)]'s 191 Member States and" international aviation organizations establishing "Standards and Recommended Practices (SARPs)" for states to reference when forming their own national civil aviation regulations. *Id.*

38. *See ICAO History,* supra note 37 (noting purpose of Chicago Convention). Most importantly, "[t]he Chicago Conference laid the foundation for . . . rules and regulations regarding air navigation . . . which [brought] . . . safety in flight and [created the path for an international] common air navigation system . . . ." Douglas Marshall, *Unmanned Aerial Systems and International Civil Aviation Organization Regulations*, 85 N.D. L. REV. 693, 697-98 (2009).

39. *See ICAO History*, *supra* note 37 (giving broad history of ICAO). With "26 member states, the Provisional International Civil Aviation Organization . . . . functioned from 6 June 1945 until 4 April 1947." *Id.* The "ICAO became a specialized agency of the United Nations . . . ." *Id.*

40. Convention on International Civil Aviation preamble, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295. [hereinafter Chicago Convention] (making known preamble to convention agreement). The first paragraph of the Preamble provides: "WHEREAS the future development of international civil aviation can greatly help to create and preserve friendship and understanding among the nations and peoples of the world, yet its abuse can become a threat to the general security . . . ." *Id.* The founding fathers "created [the ICAO] to promote a safe and efficient development of [interna-

the Convention on International Civil Aviation concluded in its Preamble that governments settled on implementing certain standards to ensure the safety of civilian passengers and, as a whole, the civil aviation community.[41] After the ICAO's founding, it implemented a Technical Co-operation Programme designed to guide States, the private sector, and donors in issues dealing with ensuring a safe civil aviation community.[42] Today, the ICAO interacts with 191 Member States and global aviation organizations in creating international Standards and Recommended Practices (SARPs) that state actors refer to when formulating legally enforceable standards and regulations.[43]

---

tional] civil aviation." *ICAO History*, *supra* note 37 (telling of ICAO's awareness of potential abuse to international civil aviation). An "enduring aspect of the [ICAO]'s work [since its establishment has] been to [assist] States improve civil aviation in their country through projects [enacted] under ICAO's Technical Co-operation Programme." *Id.* The "ICAO's Technical Co-operation Programme [has] advis[ed] and assist[ed] States, donors, [and] the private sector . . . in . . . matters relating to the development of safe and secure civil aviation." *Id.* The preamble shows the foundational principles of the ICAO: "WHEREAS it is desirable to avoid friction and to promote that cooperation between nations and peoples upon which the peace of the world depends . . . ." Chicago Convention*, supra*; *see also ICAO History*, *supra* note 37 (abridging description of ICAO's Technical Co-operation Programme). The preamble reflects the priorities of ICAO in its purpose "to promote [a] safe and efficient development of civil aviation." *Id.* "[T]he Technical Co-operation Programme [is] a priority activity of . . . [the] ICAO['s] regulations, policies[,] and procedures." *ICAO History*, *supra*.

41. *See* Chicago Convention, *supra* note 40, at preamble (concluding purpose of ICAO). "THEREFORE, the undersigned governments having agreed on certain principles and arrangements in order that international civil aviation may be developed in a safe and orderly manner and that international air transport services may be established on the basis of equality of opportunity and operated soundly and economically . . . ." *Id.* Today, the ICAO is comprised of 191 member states. *See Member States.Multilingual*, INT'L CIV. AVIATION ORG., http://www.icao.int/MemberStates/Member%20States.Multilingual.pdf (last visited Jan. 31, 2016) (listing 191 member states of ICAO). United Nations created the ICAO as a specialized agency "to promote the safe and orderly development of international civil aviation ." *South Sudan Becomes 191st Member of ICAO*, SUDAN TRIB. (Nov. 12, 2011), http://www.sudantribune.com/spip.php?article40710 (going over background of ICAO). The ICAO establishes standards and regulations to promote safe, secure, efficient, and regular protections for the aviation community. *Id.*

42. *Supra* note 37 and accompanying text (presenting broad history of ICAO).

43. *About ICAO*, *supra* note 37 (providing number of ICAO members and ICAO goal); *see also SARPs - Standards and Recommended Practices*, INT'L CIV. AVIATION ORG., http://www.icao.int/safety/SafetyManagement/Pages/SARPs.aspx (last visited Apr. 18, 2015) (delving into detail regarding SARPs). SARPs are meant to help states manage aviation safety risks. *Id.* The safety management provisions provided in SARPs help to improve the performance of safety. *Id.* The safety management SARPs are found in the ICAO's Annexes. *Id. See also* Chicago Convention, *supra* note 40, at art. 37 (introducing SARPs). SARPs have been adopted to comply

2. *A Vulnerable Aviation Industry in Today's Cybercrime Environment*

Former U.S. Secretary of Defense Leon Panetta, argued that the United States must improve its cyberdefenses during the current pre-9/11 stage.[44] The terrorist attacks of September 11, 2001, which theorists categorize as a "Black Swan event," involved a devastating attack on the aviation industry that continues to reestablish itself from the tragedy.[45] Warning that another similar 9/11-event will occur in the near future does not necessarily mean that the aviation industry will be the prime target; rather, if a similar 9/11-type event were to occur in cyberspace, the aviation industry could likely be the target.[46] Cybersecurity is a nascent issue for the aviation industry because of its reliance on an interconnected network of electronic

---

with Article 37 of the Chicago Convention for states to collaborate in setting uniform procedures, regulations, and standards with regards to aircraft, airways, and personnel to ensure safe and efficient air transportation. *Id.* In particular, Article 37 provides that SARPs shall be adopted and amended to deal with "[a]ircraft in distress and investigation of accidents; and such other matters concerned with the safety, regularity, and efficiency of air navigation as may from time to time appear appropriate." *Id.* Article 37 could be grounded as the ICAO provision that sets the "international standards and recommended practices and procedures dealing with" cyberattacks against aircrafts. *See id.*

44. Pam Benson, *Panetta: Cyber Threat Is Pre 9/11 Moment*, CNN (Oct. 12, 2012, 3:00 AM), http://security.blogs.cnn.com/2012/10/12/panetta-cyber-threat-is-pre-911-mom-ent/ (evincing current times as pre-9/11 moment). Leon Panetta suggested that "failing to see . . . warning signs ahead of [a] devastating terrorist attack" is how the events of September 11, 2001, unfolded. *Id.* Panetta spoke of Shamoon, a cybervirus that "infected . . . computers of major energy firms in Saudi Arabia and Qatar" in the summer of 2012 and rendered the computers useless as an "attack on the Saudi state oil company ARAMCO" and a Qatar company, Ras Gas. *Id.* "[Leon] Panetta said [these] attacks were [likely] the most devastating to ever hit the private sector." *Id.*

45. HomelandSecurityMgmt, *RICHARD CLARKE at AIAA AVIATION 2013: What the Cyber Security Experience Can Mean for Aviation*, YouTube (Feb. 6, 2014), https://www.youtube.com/watch?v=mXCzVQRcMuM (addressing issues cybersecurity poses against various industries, including aviation). Richard Clarke referred to former U.S. Secretary of Defense, Leon Panetta, mentioning his warning that the international community is "at a pre-9/11 moment" for future cyberattack. *Id.* (quoting warning from Leon Panetta). The 9/11 terrorist attacks were "an attack on the aviation industry" and, therefore, the industry might be subject to future devastating attack. *Id. See also* Taleb, *supra* note 6 (breaking down details of Black Swan theory). A future cyberattack against the aviation community might lead to a Black Swan event that has a devastating, long-term global effect. *Id.* Had there been a forewarning just before the attack, perhaps it never would have happened. *Id.*

46. HomelandSecurityMgmt, *supra* note 45 (opining vulnerability of aviation industry in pre-9/11 era).

systems that is a critical component to everyday operations.[47] Today's cybersecurity threat against the aviation industry could involve a cyberterrorist group's malicious intent to steal information, compromise international governments' security, and achieve its own political goals.[48]

III. FACTS

A. Organizations and Infrastructure

1. Organizations Involved in the Aviation Industry

The ICAO is a group comprised of individual sovereign states, whereby its council adopts SARPs based on the Air Navigation Commission's recommendations.[49] The ICAO included an updated security framework in Annex 17 to help direct its Threat and Risk Working Group to assess cyberattack threats to the civil aviation community.[50] Another group, the European

47. CTR. FOR THE PROT. OF NAT'L INFRASTRUCTURE, CYBER SECURITY IN CIVIL AVIATION 4 (2012), *available at* http://www.cpni.gov.uk/documents/publications/2012/2012020-cyber_security_in_civil_aviation.pdf?epslanguage=en-gb [hereinafter UK CYBER SECURITY IN CIVIL AVIATION] (reviewing cybersecurity situation today in civil aviation industry).

48. AM. INST. OF AERONAUTICS & ASTRONAUTICS, THE CONNECTIVITY CHALLENGE: PROTECTING CRITICAL ASSETS IN A NETWORKED WORLD–A FRAMEWORK FOR AVIATION CYBERSECURITY, at introduction (2013), *available at* http://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf (elucidating cyberthreat to aviation industry). *See generally* Frank Palmay, *Cyber-Risk–The Electronic Ebola of the 21st Century*, MCMILLAN INS. BULL. (2014), *available at* http://www.mcmillan.ca/Files/176820_Cyber-Risk.pdf (explaining current widespread issue of cybersecurity threat and offering suggestions to counter cybercrime).

49. *Supra* note 37 (providing background information on ICAO and its members); *Air Navigation Commission*, INT'L CIV. AVIATION ORG., http://www.icao.int/about-icao/Pages/Air-Navigation-Commission.aspx (last visited Oct. 19, 2014) (relating what Air Navigation Commission does). The Air Navigation commission analyzes and recommends Standards and Recommended Practices and Procedures (SARPs) for Air Navigation Services to the ICAO Council to ensure a safe and efficient international civil aviation community. *Id. See also* UK CYBER SECURITY IN CIVIL AVIATION, *supra* at note 47, at 7 (saying how SARPS covers safety, "operation of aircraft, aerodromes, air traffic services, accident investigation"). The ICAO addresses cybersecurity as it works with "SARP[s] for Air Traffic Network (ATN) security." *Id.* at 8. *See also Progress in Cyber Security in ATM*, EUR. ORG. FOR SAFETY AIR NAVIGATION (Dec. 17, 2013), https://www.eurocontrol.int/news/progress-cyber-security-atm (addressing ICAO Threat and Risk Working Group tackling cybersecurity issues). The ICAO's work will form the foundation for a current global risk context statement and updates of the ICAO's Annex 17 (Security) in addressing cybersecurity concerns. *Id.*

50. *See Progress in Cyber Security in ATM*, *supra* note 49 (announcing amendment of ICAO's Annex 17 to include information security dimension); *see also The*

Civil Aviation Conference (ECAC), seeks to harmonize civil aviation policies with its member states and promote policy matters.[51] EUROCONTROL is a European organization that manages the European ATM network's day-to-day operations.[52] EUROCONTROL's Security Team is an advisory body whose mission is to improve the handling of threats and risks to "ATM security and the security of air navigation" in Europe.[53] An-

---

ICAO Council, INT'L CIVIL AVIATION ORG., http://www.icao.int/about-icao/pages/council.aspx (last visited Feb. 15, 2016) (explaining ICAO Council's Annexes). The ICAO Council through its Standards and Recommended Practices are assimilated as "Annexes" to the Convention on International Civil Aviation. *See generally* Int'l Civil Aviation Org. [ICAO], *Outcomes of the Twenty-Fourth Meeting of the Aviation Security (AVSEC) Panel*, ICAO Doc. AVSEC/FAL/RG/3 — IP/03 (June 5, 2013), *available at* http://www.icao.int/SAM/Documents/AVSEC-FAL-RG3/AVSECFALRG3-IP03-AVSECP24.pdf (recommending practices to prepare for cyberattacks). The ICAO noted that a new recommended practice provides for states to create regular training concerning cyberattacks, because of evidence that suggests cybercriminals targeting "aircraft and aviation infrastructure." *Id.* at § 2.1.

51. *We Need to Talk About Cybersecurity*, AIRPORT BUS. (June 26, 2014), http://www-.airport-business.com/2014/06/need-talk-cyber-security/ (summarizing how "European Civil Aviation Conference (ECAC) has a Study Group on Cyber Threats [sic]"). The ECAC Study Group overlooks the developments in cybersecurity and cyberthreat that the ICAO makes on "reducing cyber-attacks on critical aviation information systems." *Id.* ECAC Study Group supports the mandate on "cyber-threats [sic] to aviation." *Id.* (supporting ECAC Study Group in writing material on cybersecurity for member states).

52. UK CYBER SECURITY IN CIVIL AVIATION, *supra* note 47, at 8 (calling European Organisation for Safety of Air Navigation (EUROCONTROL) major contributor in defining future ATM systems). ATM involves a three-pronged definition. *What Is Air Traffic Management?*, EUR. ORG. FOR SAFETY AIR NAVIGATION, https://www.eurocontrol.int/articles/what-air-traffic-management (last visited. Apr. 18, 2015) (designating definition for ATM). First, ATM involves ensuring safe air traffic control. *Id.* Air traffic control (ATC) involves the process of aircrafts landing, commuting, and taking off. *Id.* ATC centers assist aircraft navigation in various classes of airspace surrounding airports. *Id.* Second, ATM involves proper air traffic flow management. *Id.* Pilots using ATC for navigation file flight plans and send them to air traffic controllers. *Id.* Filed flight plans are computed and analyzed. *Id.* As a safety precaution, air traffic controllers hesitate to overwhelm themselves with managing too many flights at once. *Id.* Controllers use sophisticated computers to calculate a future location of a specific aircraft to ensure "controllers in that airspace can safely" manage the flight. *Id.* If the calculation predicts an overwhelming number of flights that a controller cannot reasonably handle, the aircraft will remain at the airport until the airspace is less congested and it is safe to fly. *Id.* Third, Aeronautical Information Services are responsible for compiling and distributing critical information to airspace users. *Id.* Aeronautical Information Services include information relating to administrative, navigation, safety, and technical issues for the purpose of ensuring safe and efficient air navigation. *Id.*

53. UK CYBER SECURITY IN CIVIL AVIATION, *supra* note 47, at 9 (describing Security Team and its goals).

other organization, the FAA, is a United States Department of Transportation Agency that "has the authority to regulate and oversee all aspects of civil aviation in the [United States]."[54]

2. Aviation's Critical Infrastructure

International aviation organizations work with key infrastructure providers to develop information security and cyber-protection standards.[55] Two of the airline industry's most significant assets that require enhanced security are: (1) Communications, Navigation, and Surveillance (CNS); and (2) ATM.[56] The design and production of aircraft systems are another area that requires crucial security measures.[57] Moreover,

---

54. *Id.* (summing up role of FAA). The FAA "considers . . . new aircraft 'architectures and network configurations'" that are potentially vulnerable to intentional or unintentional interference with critical flight data and systems that ensure a safe flying environment. *Id.* Moreover, the FAA has issued special conditions to protect aircraft systems and data networks from interference with either "wired or wireless electronic connections" that aircrafts rely on. *Id.* (internal quotation marks omitted).

55. AM. INST. OF AERONAUTICS & ASTRONAUTICS, *supra* note 48, at executive summary (designating organizations critical to establishment of cyberstandards for aviation systems). Organizations such as "[t]he National Institute of Standards and Technology, the Federal Information Processing Standards (FIPS), the International Organization for Standardization (ISO), and the Information Systems Audit and the Control Association (ISACA) Control OBjectives [sic] for Information and related Technology (COBIT)" developed standards for aviation industry to follow. *Id.* Moreover, "[s]ecurity . . . groups such as the Computer Security Incident Response Team (CSIRT) and the Computer Emergency Response Team (CERT)" have responded to breaches in security. *Id.* The Center for Education and Research in Information Assurance and Security has made "[m]ajor efforts in . . . research and education" on various industries that can apply to aviation. *Id.* Information technology standards provide the airline industry with a strong framework conducive to developing higher standards. *Id.* at establishing a cybersecurity framework for aviation.

56. *Id.* (sketching aviation infrastructure). The communications, navigation, and surveillance (CNS)/ATM system is complex, because "hundreds of service providers . . . may be government owned, privately owned, or a hybrid of" both. *Id.* Furthermore, the CNS/ATM system is becoming "a network-centric operations environment" and therefore, "becoming more dependent on cyber and digital technology." *Id.* The CNS/ATM system faces new threats and risks such that it must emphasize security in the overall infrastructure cycle. *Id. See also Communication, Navigation and Surveillance*, EUR. ORG. FOR SAFETY AIR NAVIGATION, http://www.eurocontrol.int/dossiers/communications-navigation-and-surveillance (last visited Oct. 19, 2014) (observing broadly importance of CNS). Communications, navigation and surveillance are essential technological systems for global air traffic control, because CNS "facilitate[s] the process of establishing where the aircraft is and when and how it plans to arrive at its destination." *Id.*

57. AM. INST. OF AERONAUTICS & ASTRONAUTICS, *supra* note 48, at establishing a cybersecurity framework for aviation (introducing aircraft system design and production as key to critical infrastructure). An aircraft is composed of millions of parts

airline operations are a paramount component because an airline carrier holds the responsibility of updating its aircraft information technology components as a security measure.[58]

Additional key components to the aviation's infrastructure involve ground services such as: flight reservations; ticketing; cargo and baggage handling; and airport and aircraft maintenance.[59] Airport infrastructure also involves critical functions that the air transportation system relies on including "[s]ecurity, power, fueling systems, and aircraft servicing."[60] Finally, the American Institute of Aeronautics and Astronautics emphasizes the importance of the aviation supply chain because its interconnected global system signifies one of the most complex and relied upon networks in the world.[61]

---

and "it is critical that manufacturers ensure that the design process . . . address[es] the evolving nature of cyber threats [sic]." *Id.* The NIST, the Radio Technical Commission for Aeronautics, and the European Organisation for Civil Aviation Equipment are institutions known to create standards and guidance information for the aviation industry's use. *Id.* These organizations are part of the necessary driving force for the certification of "the safety and functionality of the design and operation, and are developed in public forums by aviation stakeholders." *Id.*

58. *See id.* (holding airline's operations play critical role to cyberprotection on its aircrafts). During flight operations, airline must "be in [a] position to control all data flow [to and from] the aircraft." *Id.* Additionally, "the airline [must] agree with the aircraft manufacturer about" preventative measures through maintenance and operations designed to thwart cyberincidents. *Id.* "The aircraft developer must provide ongoing support and [inform airlines of] potential aircraft threats or design vulnerabilities." *Id.* *See* Nichols, *supra* note 36 (implying aircraft-manufacturer Boeing may have cybervulnerabilities). "[T]he entire aviation ecosphere," which "involves multiple software providers, airlines, [and] airports" is at an enormous cybersecurity risk. *Id.* (internal quotation marks omitted).

59. AM. INST. OF AERONAUTICS & ASTRONAUTICS, *supra* note 48, at establishing a cybersecurity framework for aviation (including ground services as key to infrastructure safety). The American Institute of Aeronautics and Astronautics highlights ground services as an issue for the aviation industry to address because it "may influence the public's decision to fly, not just the ability of an adversary to [inhibit] flight." *See id.* (advocating establishment of cybermeasures for aviation industry).

60. *Id.* (indicating airport infrastructure requires development of new safety standards).

61. *See id.* (displaying intricacies of highly complex supply chain of aviation industry). The "information-intensive supply chain" involves: "(1) interrelated global transportation safety and security standards; (2) international alliances between carriers; (3) original equipment manufacturers (OEMs) cross-supplying and sourcing from common entities; (4) outsourcing operations and maintenance; and (5) seamless handoff of [ATC] between sectors." *Id.*

International aviation agencies depend heavily on the sufficiency and reliability of their air traffic control (ATC) systems.[62] The FAA relies on over one hundred ATC systems to manage and track flights worldwide.[63] The interconnectedness of ATC systems is essential to carrying out ATC operations and depends

---

62. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-221, INFORMATION SECURITY: FAA NEEDS TO ADDRESS WEAKNESSES IN AIR TRAFFIC CONTROL SYSTEMS 5 (2015), *available at* http://gao.gov/assets/670/668169.pdf [hereinafter US GAO INFORMATION SECURITY] (noticing FAA's mission to properly rely on ATC systems). The FAA and other international aviation agencies rely on an interconnected system involving "air traffic control systems, . . . computer hardware, software, and communications equipment." *See id.* The FAA air traffic controllers' roles and responsibilities involve ensuring secure and efficient air travel for millions of passengers per day. *Roles and Responsibilities of Air Traffic Control Facilities*, FED. AVIATION ADMIN., https://www.faa.gov/jobs/career_fields/aviation_careers/atc_roles/ (last modified Mar. 10, 2014) (illuminating duties of FAA air traffic controllers). The air traffic control workforce involves the operation of several different facilities, including "air traffic control towers, terminal radar approach control centers, and en route control centers." *Id.* Air traffic control tower controllers manage incoming and outgoing traffic from an airport. *Id.* The tower controllers provide pilots with pre-flight and flight instructions, air traffic clearance, and general guidance from their own observations. *Id.* Moreover, tower controllers instruct separation between incoming and outgoing aircraft and transfer aircraft control to other air traffic controllers when planes enter and exit their airspace. *Id.* When aircrafts are "about 20 to 50 miles from [an] airport," terminal radar approach controllers assist them as they approach its facility before transferring pilots over to en route center controllers. *Id.* Finally, en route center controllers direct aircraft traveling above 17,000 feet to their destination by providing route instructions, advice, and clearances. *Id.* Air traffic control "clearance" means an authorization that ATC makes to keep safe distance between traveling aircraft and to instruct pilots to fly complying with specific conditions when traveling within a particular airspace. FED. AVIATION ADMIN., U.S. DEP'T OF TRANSP., AERONAUTICAL INFORMATION MANUAL: OFFICIAL GUIDE TO BASIC FLIGHT INFORMATION AND ATC PROCEDURES § 4-4-1-a (2014), *available at* http://www.faa.gov/air_traffic/publications/media/aim_basic_4-03-14.pdf (supplying definition of clearance). If ATC issues a clearance, it is the pilot-in-command's responsibility to follow the rules and regulations to ensure aircraft safety. *Id.* § 4-4-1-b. The FAA acts as a global industry leader that establishes high standards for other international aviation agencies to follow. *See FAA Strategic Initiatives: The Strategic Imperative*, FED. AVIATION. ADMIN., at 1, https://www.faa.gov/about/plans_reports/media/FAA_Strategic_Initiatives_Summary.pdf (last visited Mar. 16, 2015) (highlighting FAA's global influence).

63. US GAO INFORMATION SECURITY, *supra* note 62, at 5 (covering various aspects of interconnectedness of air traffic control systems). The complex and automated systems involve a wide range of data processing "including radar, weather, flight plans, surveillance, navigation/landing guidance, traffic management, air-to-ground communication, voice, network management" and information about airspace restrictions. *Id.* Critical to the ATC's interconnectedness are the ATC tower controllers, terminal radar approach controllers, and the en route center controllers. *See Roles and Responsibilities of Air Traffic Control*, *supra* note 62 (identifying vital ATC players).

heavily on Internet Protocol (IP) networking technologies for purposes of communication.[64] The FAA's newly modernized ATC system is known as the Next Generation Air Transportation System (NextGen).[65] One of NextGen's purposes is to advance air travel and limit security weaknesses that could place aviation operations in jeopardy.[66]

---

64. US GAO INFORMATION SECURITY, *supra* note 62, at 6. An Internet Protocol (IP) address is "[t]he address of a connected device in an IP network (TCP/IP network). Every desktop and laptop computer, server, scanner, printer, modem, router, smartphone[,] and tablet is assigned an IP address, and every IP packet traversing an IP network contains a source IP address and a destination IP address." *Definition of: IP Address*, PCMAG, http://www.pcmag.com/encyclopedia/term/45349/ip-address (last visited Mar. 16, 2015) (specifying definition for IP address).

65. US GAO INFORMATION SECURITY, *supra* note 62, at 6 (identifying Next Generation Air Transportation System (NextGen)). NextGen is the foundation to the aviation industry's future. *See id.* The modernization of air transportation includes "the acquisition of newly integrated systems (both software and hardware) . . . to transform the current air transportation system" from ground-based radar into "satellite-based surveillance and navigation operations." *Id.* NextGen is intended to improve "the efficiency and capacity of the air transportation system while maintaining" safe air travel. *Id.* NextGen is an upgrade from World War II-era technology to satellite-based technology. Thom Patterson, *Help on the Way for Air Traffic Jams*, CNN (Mar. 7, 2011, 12:41 PM), http://www.cnn.com/2011/TRAVEL/03/04/nextgen.consumers/; *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 1 (2015), http://www.gao.gov/assets/670/669627.pdf [hereinafter US GAO AIR TRAFFIC CONTROL] (condensing explanation of NextGen). *See generally What is NextGen?*, FED. AVIATION ADMIN., http://www.faa.gov/nextgen/ (last modified Oct. 19, 2015) (depicting what NextGen does). For over the past ten years, the FAA has been in the process of transforming its ATC system. US GAO AIR TRAFFIC CONTROL, *supra*. Since 2004, ATC modernization efforts involved improving digital communication between pilots and air traffic controllers, and between satellites and navigation. *Id.* Since NextGen depends predominately on interconnected information systems, digital communications, and GPS technologies, it is more vulnerable to breaches in cybersecurity. *Id.* at 1-2.

66. US GAO INFORMATION SECURITY, *supra* note 62, at 6 (recapitulating purpose and concern of NextGen). *But see* US GAO AIR TRAFFIC CONTROL, *supra* note 65, at 12 (offering issues FAA must confront in its transition to NextGen). NextGen's new information systems connect with other information systems using IP networking. *Id.* If one system is compromised, then damage can expand to other systems connected to the IP network. *Id.* The FAA reports that roughly "36 percent of the ATC systems . . . are connected using IP" networking and by 2020, it is predicted to expand to "50 to 60 percent." *Id.* at 13. According to experts, the increased connectivity to IP-connected systems has also raised the potential for a cyberbreach. *Id.*

a. Air Traffic Control Systems Critical to Air Traffic Control Management

The FAA's Telecommunications Infrastructure (FTI) is the framework for NextGen's telecommunications system in providing strong telecommunication services for the National Airspace System (NAS).[67] FTI's purpose is "to reduce costs, improve bandwidth, and offer improved information security services" so that the aviation industry can attain an industry-wide method to information security.[68] Another system critical to ATC is the Surveillance and Broadcast Service System (SBSS) that acts as a surveillance tool for the aviation community.[69] SBSS furnishes the Automatic Dependent Surveillance-Broadcast service that utilizes Global Positioning System technology to determine and share precise aircraft location information, and streams critical flight information to the cockpits.[70]

---

67. US GAO INFORMATION SECURITY, *supra* note 62, at 6-7 (providing "five key [ATC] systems" paramount to ATC functions). FAA's Telecommunications Infrastructure (FTI) replaces the agency's outdated networks to provide advanced telecom services for the U.S. aviation industry. *Id.*

68. *Id.* at 6 (detailing FAA's Telecommunications Infrastructure (FTI) functions). FTI is the FAA's main telecommunication service for NextGen. *Id. FAA Telecommunications Infrastructure (FTI)*, FED. AVIATION ADMIN., https://www.faa.gov/air_traffic/technology/fti/ (last modified Dec. 3, 2015) (affirming role of FTI as supporting framework for NextGen). FTI replaces FAA's older networks to provide telecom services and improved bandwidth and security for over "5,000 facilities and 30,000 circuits in the National Airspace System [(NAS)]." *Id.*

69. US GAO INFORMATION SECURITY, *supra* note 62, at 6 (showing importance of Surveillance and Broadcast Service System (SBSS) to U.S. aviation industry). The SBSS "includes radio stations, control stations, and network connections that enable the [Surveillance and Broadcast Services] to operate." FED. AVIATION ADMIN., U.S. DEP'T OF TRANSP., ORDER 8200.45, AUTOMATIC DEPENDENT SURVEILLANCE-BROADCAST (ADS-B) FLIGHT INSPECTION 4 (2014), http://www.faa.gov/documentLibrary/media/Order/8200_45_ADS-B.pdf (laying out functions and benefits of SBSS). The SBSS supports four different services: "[1] Automatic Dependent Surveillance – Broadcast (ADS-B), [2] ADS-Rebroadcast (ADS-R), [3] Traffic Information Services - Broadcast (TIS-B), and [4] Flight Information Services – Broadcast (FIS-B)." *Id.* at 4.

70. *See* FED. AVIATION ADMIN., *supra* note 69, at 4, 6 (expressing details of ADS-B service). The ADS-B service is part of NextGen's transformative programs that replaced radar with satellite-based services. *See id.* at 5. "ADS-B is a surveillance service" that assists with traffic flow management. *Id.* at 4 (commentating on ADS-B service). While ADS-B helps control air traffic flow, "the SBSS receives, processes, and validates position reports broadcast from properly equipped aircraft and [transmits] this information to . . . ATC . . . automation systems at designated Service Delivery Points (SDPs)." *Id.* The automated system helps ATC with safety alerting functions that warn about minimum safe altitudes and traffic conflicts. *Id.* Moreover, the SBSS provides system updates to automated platforms so that the

To ensure safe and efficient air travel, the NextGen system offers En Route Automation Modernization and En Route Communications Gateway.[71] The Traffic Flow Management-Infrastructure provides support to air traffic controllers when there is a high volume of aircraft.[72] All of the above mentioned systems comprise the structure of the NAS computing system and work to ensure safe flight passageway for aircraft from take-off to landing.[73]

B. Aviation Industry's Focus on Cybersecurity

1. ICAO's Take on Cybersecurity

The ICAO's Twelfth Air Navigation Conference identified cybersecurity as a serious concern to implementing the Global Air Navigation Plan.[74] The ICAO noted the importance of approaching cybersecurity because civil aviation organizations have increased their reliance on electronic systems for key components, i.e., day-to-day operations and critical safety functions.[75] The current development and broad spectrum of new

---

FAA Automation Specials can certify "data, status, and traffic information" for ATC use. *Id.*

71. *See* US GAO INFORMATION SECURITY, *supra* note 62, at 7 (pointing out advanced technologies NextGen offers to aircrafts). En Route Automation Modernization (ERAM) replaces an older system developed over forty years ago. *Id.* The next generation air traffic control involves "a satellite-based system of [ATM]" as opposed to the old ground-based system of ATC. *See id.* at 6, 7. ERAM is intended to improve automatic navigation. *Id.* at 6. "En Route Communications Gateway (ECG) is a communications system that receives" critical flight data from aircrafts, including flight plan information and weather updates, and transmits to other automatic systems like ERAM. *Id.*

72. *Id.* at 7 (familiarizing readers with Traffic Flow Management-Infrastructure (TFM-I)). TFM-I transmits and receives data about "planned and active flights," and forecasts the demand of flying aircraft to traffic management personnel, and "provides automation support for traffic management" to reduce congestion. *Id.*

73. US GAO AIR TRAFFIC CONTROL, *supra* note 65, fig.1 at 5 (illustrating NAS compatibility with NextGen technologies). NextGen is expected to provide a number of benefits. *Id.* For example, NextGen is expected to reduce workload by providing digital communication, increasing terminal capacity between aircraft and ground traffic management, providing weather information for flight operations, connecting 4-D trajectories to ensure efficient routing, and improving the spacing of airborne and on-the-ground aircraft. *Id.*

74. *See Twelfth Air Navigation Conference*, *supra* note 29, at summary (emphasizing importance of approaching cybersecurity for aviation industry).

75. *See id.* ¶ 1.2 (encapsulating ICAO's reasons for cybersecurity approach). Cybersecurity encompasses protecting "electronic systems from malicious electronic attack" and the procedural means of dealing with the consequences of such attacks. *Id. See* AM. INST. OF AERONAUTICS & ASTRONAUTICS, *supra* note 48, at the need for

information technologies increases the risk of cyberattack.[76] The ICAO has estimated that over the next two decades, "US[D]120 billion will be spent on transform[ing the] air transportation systems."[77]

2. Vulnerabilities in the Aviation Sector

The Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation categorizes cybercrime as an offense against international civil aviation.[78] Cybersecurity breaches and vulnerabilities against the aviation industry have and will continue to emerge.[79] A demonstration exposed ATC

---

a cybersecurity framework for aviation (suggesting aviation's reputation as one of world's safest modes of transportation requires heightened industry cybersecurity measures). "Aviation is considered . . . [an] efficient, safe, and resilient system . . . ." *Id.* Therefore, the need for a cybersecurity framework is critical to maintaining public confidence in the aviation industry. *Id. See also* Matt Thurber, *Security Expert Raises Issues of Satcom Vulnerabilities*, AIN ONLINE (Oct. 4, 2014, 3:55 AM), http://www.ainonline.com/aviation-news/aviation-international-news/2014-10-04/security-expert-raises-issues-satcom-vulnerabilities (evincing possible vulnerability to electronic systems "may allow hackers to gain access to aircraft systems"). Cybersecurity on an aircraft's computer network "is something that the airframe manufacturers take very seriously," because they are responsible for its design and protection. *Id.* (internal quotation marks omitted).

76. *See Twelfth Air Navigation Conference*, *supra* note 29, ¶ 1.3 (imparting awareness of how cyberattacks increase as new technology develops). The ICAO has explained that there are four factors responsible for increasing vulnerability to cybersecurity: (1) "increased reliance on a small" range of widely-used software, e.g., Ethernet (AFDX) IPv6 protocols, Linux, and Windows; (2) reliance on frequently-used small-range software leads to widespread understanding of such technologies, whereby computer specialists identify weaknesses and vulnerabilities; (3) interconnectedness of systems and leads to a domino effect in security lapses; and (4) greater impact from system failures as reliance increases. *Id.*

77. *Id.* ¶ 1.5 (predicting investment in transforming air transportation systems). This transformation will involve modernized ATM operations intended to improve the safety and efficiency of the air transportation systems. *Id.*

78. *See* ICAO, *Administrative Package for Ratification of or Accession to the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation*, at 1 (Sept. 10, 2010), *available at* http://www.icao.int/secretariat/legal/Administrative%20Packages/Beijing_Convention_EN.pdf (noting how convention intends to criminalizes illegal acts against civil aircraft). The Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (the Beijing Convention) emphasizes that any person who makes a threat to engage in an offense may be held criminally accountable if the particular threat is credible. *Id.* Furthermore, the purpose of the Beijing Convention is "to modernize the legal framework for aviation security." *Id.* at 2. Preventative measures such as criminalizing preparatory acts that constitute "emerging threats against civil aviation." *Id.*

79. *See Twelfth Air Navigation Conference*, *supra* note 29, ¶ 2.1-2.2 (discussing four significant examples of cybersecurity events within aviation sector).

systems' weaknesses at the 2012 Black Hat hacking conference.[80] Even airport terminals face cybersecurity risks: in June 2011, software engineers were accused of sabotaging a new airport's terminal program code.[81] Onboard an aircraft, the electronic flight bag is vulnerable to hacking as it communicates critical data via external networks.[82] Global positioning systems used for navigation, position, and timing services run the risk of cyberattack because cyberhackers can easily infiltrate and sabotage their signals.[83]

---

80. *Hacker Shows Air Traffic Control Danger with 'Ghost Planes'*, HUFFINGTON POST, http://www.huffingtonpost.com/2012/07/27/hacker-shows-air-traffic-_n_1711343.html (last updated Sept. 26, 2012) (reporting demonstrated vulnerability of ATC systems at conference). At the July 2012 Black Hat hacking conference, Andrei Costin demonstrated that he could use "[USD]2000 worth of store-bought electronics" to convince the FAA that "a non-existent plane was" on final approach to land at an airport. *Id.* Airports commonly use ATC systems that are unable to verify a message's source and can only identify an existing aircraft visually or by conducting a lengthy cross-check. *Id.* Manipulating ATC systems and inserting fake aircraft involves minimal effort for the cybercriminal. *See* John Foley, *FAA's New Flight Control System Has Security Holes: Researcher*, INFO. WK. DARK READING (July 26, 2012, 12:41 PM), http://www.darkreading.com/risk-management/faas-new-flight-control-system-has-security-holes-researcher/d/d-id/1105520? (conveying how easy to add fake planes on ATC radars). The cyberintruder can craft the infiltrated data to fit his own needs in carrying out a malicious plan. *Id.* The Black Hat conference is one of the world's most notable and prominent hacking conferences. *See generally* Michael Gregg, *How to Speak 'Hacker'*, HUFFINGTON POST, http://www.huffingtonpost.com/michael-gregg/how-to-speak-hacker_b_1690465.html (last updated Sept. 22, 2012) (chronicling history of Black Hat conference). The Black Hat conference invites the most sophisticated "hackers from around the world to display the latest cyberthreats to" anything computer related. *Id.*

81. *Twelfth Air Navigation Conference*, *supra* note 29, ¶ 2.1.b, at 3 (commenting on incident disrupting airport terminal's program code). Check-in services failed "and 50 flights were delayed, causing" a domino effect of delay. *Id.*

82. *Id.* ¶ 2.1.c, at 3 (recounting electronic flight bags' (EFBs) vulnerability to hacking). An EFB is a software and data service that provides pilots operational performance calculations, charts, documents, and taxi maps. *See* David Allen, *Electronic Flight Bag: Real-Time Information Across an Airline's Enterprise*, AERO, Quarter 2, 2008, at 22-23, http://www.boeing.com/commercial/aeromagazine/articles/qtr_2_08/AERO_Q208.pdf (describing benefits of EFBs). *But see* Phil Muncaster, *Airlines Failing on Cybersecurity Says New Research*, INFOSECURITY (Oct. 8, 2014), http://www.infosecurity-magazine.com/news/airlines-failing-on-cyber-security/ (discerning vulnerabilities of EFBs). Cybercriminals have the potential to hack into EFBs. *Id.* EFBs are tablets that "pilots typically use in the cockpit to calculate and display . . . fuel, GPS coordinates[,] and real-time satellite weather feeds." *Id.*

83. *Twelfth Air Navigation Conference*, *supra* note 29, ¶ 2.1.d, at 3 (stressing vulnerability of global positioning systems aircraft rely on); *see also* Thurber, *supra* note 75 (discussing security vulnerabilities in satellite communication).

While the U.S. aviation community has made advancements to protect its ATC systems from cyber-based threats, technological vulnerabilities remain and threaten the industry's ability to guarantee a safe and efficient national airspace system.[84] Particularly since January 2015, a U.S. Government Accountability Office report announced that the FAA has not fully addressed cybersecurity issues that could make aviation technological systems susceptible to hackers.[85] For example, the FAA did not ensure that controls would be implemented to appropriately identify and grant access to authorized NAS system users.[86] Moreover, the FAA failed to ensure that sensitive data is sufficiently encrypted.[87] Finally, the FAA failed to identify

---

84. *See* US GAO INFORMATION SECURITY, *supra* note 62, at 1 (warning about and providing background on aviation vulnerabilities to cyber-based threats). Effective ATC depends on interconnected systems and networks that provide critical data between aircraft flight crews and air traffic controllers, allowing them to achieve safe and efficient air travel. *Id.*

85. Aaron Cooper, *Report: Air Traffic Control System Vulnerable to Cyberattack*, CNN, http://www.cnn.com/2015/03/02/politics/cyberattack-faa-air-traffic-control-hacking/ (last updated Mar. 2, 2015, 2:54 PM) (referring to U.S. Government Accountability Office (GAO)'s report about FAA's cybersecurity vulnerabilities). A GAO report found that there are problems with the FAA's approach to cybersecurity. *Id.* The GAO determined that the FAA has addressed some cybersecurity issues, however, it has not yet fully addressed vulnerabilities to critical computer systems that malicious hackers intend to compromise. *Id. See also* US GAO AIR TRAFFIC CONTROL, *supra* note 65, at 11-12, 20 (reacting to FAA's failure to assure cybersecurity for aircrafts' avionics system). Historically, an aircraft's avionics system was not considered susceptible to a cyberbreach. *See id.* at 18. Today, an aircraft's IP-connectivity creates the risk that unauthorized users might access and infiltrate an airplane's avionics systems. *Id.*

86. US GAO INFORMATION SECURITY, *supra* note 62, at 14 (criticizing FAA's inability to ensure proper identification and authentication of NAS systems). The FAA must properly manage information systems so that unauthorized users do not gain access to privileged systems. *See id.* Although the FAA policy requires strong passwords with, at minimum, "eight alphanumeric characters[,] . . . at least one upper- and one lower-case letter, . . . numbers and special characters, and" specific expiration dates. *Id.* at 14-15. Moreover, the FAA failed to constantly ensure identification and authentication measures to comply with security guidelines. *Id.* at 15. "[C]ertain servers and applications [that support] NAS systems did not" have complex passwords. *Id.* To conclude, the FAA has increased its vulnerability to unauthorized users who may have malicious intentions. *See id.*

87. *Id.* at 16 (reproving FAA for lacking ideal protection of computer systems). The failure to properly encrypt sensitive data left the FAA vulnerable to attackers with malicious intentions. *See id.* Encryption involves cryptographic controls that protect the "confidentiality of data and computer systems by" making data indiscernible "to unauthorized users and" protecting transmitted and stored data. *Id.* Cryptography involves the utilization of mathematical functions, specifically algo-

security weaknesses in a timely manner.[88] What the FAA has recognized, however, is that extensive updates to its information-security are necessary to ensure the cybersecurity of its newly "interconnected IP-based ATC system": NextGen.[89]

Hugo Teso (Teso), a security researcher for the German information technology consultancy N.Runs, presented a scenario in which cybercriminals may have the capability to compromise a protocol used to send data to commercial aircraft.[90] Teso focused on the Aircraft Communications Addressing and Report System (ACARS) for three years–during this time, he reverse engineered the flight navigation software responsible for receiving ACARS signals and sent his own commands to the flight computer system.[91] The researcher developed an Android application that allows a user to redirect a virtual plane using a

---

rithms and bits also known as "keys," to protect a message so that only authorized users with the proper security code can access the data. *Id.*

88. *Id.* at 23-24 (denouncing FAA's inability to properly identify vulnerabilities in timely fashion). Although the FAA addressed some security issues, it failed to consistently remedy actions according to its own established deadlines. *Id.* at 24. According to FAA officials, one reason that the FAA did not meet deadlines was because of insufficient resources and funding. *Id.*

89. *See* US GAO AIR TRAFFIC CONTROL, *supra* note 65, at 40 (responding to FAA's response to cybersecurity measures regarding NextGen). Although the FAA has recognized the need to advance its cybersecurity platform, experts have expressed concern that it has not adequately ensured the protection of aircrafts' avionics systems. *Id.* The avionics systems of an aircraft enable communication between the aircraft and air traffic control. *Id.* Moreover, an aircraft's avionics system includes "flight and in-flight entertainment." *Id.* at 18. Experts argue that the IP-networking onboard an aircraft is likely vulnerable to unauthorized users because the protection of these software components are easily penetrable and could lead to access of the cockpit avionics systems. *Id.* Firewalls are a security measure designed to protect cockpit avionics systems from unauthorized users connected to the in-flight entertainment services in the cabin. *Id.*

90. Andy Greenberg, *Researcher Says He's Found Hackable Flaws in Airplanes' Navigation Systems (Update: The FAA Disagrees)*, FORBES (Apr. 10, 2013, 7:02 PM) http://www.forbes.com/sites/andygreenberg/2013/04/10/researcher-says-hes-found-hackable-flaws-in-airplanes-navigation-systems/ (publicizing what security researcher purported about hacking into navigation of plane). Hugo Teso (Teso) told a crowd at the Hack In The Box security convention in Amsterdam that radio signals can be sent to aircraft, causing them to follow arbitrary commands such as modifying direction, speed, and altitude. *Id.* "Teso focused on a . . . protocol called Aircraft Communications Addressing and Report System, (ACARS)," a data exchange system that provides data such as weather, airline schedules, and flight management system changes. *Id.*

91. *Id.* (introducing ACARS as vulnerable system lacking any kind of security measure). Teso said that ACARS lacks the sophisticated authentication features to thwart "spoofed commands" and is therefore vulnerable to cyberattack on the aircraft. *Id.*

map application on a Samsung Galaxy smartphone.[92] The simplicity of infiltrating a network and gaining control of an aircraft through the use of a smartphone indicates the current vulnerability of a cyberattack.[93]

C. International Aviation Law

1. The Convention on International Civil Aviation

Cybercrime operations targeting civil aviation violate numerous international aviation laws.[94] The Convention on International Civil Aviation, also known as the Chicago Convention, is the fundamental international law that governs civil aviation.[95] The Convention established the ICAO, which is an organization that provides rules of airspace, aircraft registration, and safety.[96] The Convention follows eighteen annexes that provide the SARPs that the ICAO regularly amends.[97] Annex 17 establishes the foundation of the ICAO's security program and strives to protect its facilities against malicious interruptions.[98]

---

92. *Id.* (revealing ease of compromising aircraft communication systems through use of smartphone).

93. *See id.* (demonstrating smartphone application system may sabotage navigation of airplane). *But see* David Gilbert, *Aircraft Hack Using Smartphone Does Not Pose Security Threat Says FAA*, INT'L BUS. TIMES (Apr. 12, 2013, 10:50 AM), http://www.ibtimes.co.uk-/andoird-aircraft-hack-pose-security-risk-faa-456417 (balancing out Teso's claim of exploiting aircraft vulnerabilities via smartphone with FAA's denial hacking could actually occur).

94. *See* Arie. J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 166 (2009) (overviewing how cybercrime implicates international aviation laws). Operations such as obstructing "an air traffic control tower, [altering] a flight's passenger list, or manipulating a no-fly list" may result in the delay or cancellation of flights. *Id.*

95. *See* Chicago Convention, *supra* note 40, at preamble (putting forth preamble to Convention on International Civil Aviation).

96. Schaap, *supra* note 94, at 166-67 (summarizing responsibility of Convention on International Civil Aviation).

97. *The ICAO Council*, *supra* note 50 (introducing ICAO's annexes).

98. Schaap, *supra* note 94, at 167 (specifying Annex 17). The ICAO formulated SARPs for international civil aviation. *See Annex 17*, INT'L CIV. AVIATION ORG., http://www.icao.int/Security/SFP/Pages/Annex17.aspx (last visited Oct 20, 2014). These SARPs are encompassed in nineteen technical annexes to the Convention on International Civil Aviation. *Id.* The ICAO took measures to prevent and suppress unlawful acts that would interfere with civil aviation. *Id.* Thus, the ICAO Council first adopted SARPs in March 1974, and designated them as Annex 17. *Id. See also* ICAO, *Annexes 1 to 18*, at Annex 17, http://www.icao.int/Documents/annexes_booklet.pdf (last visited Oct. 20, 2014) (detailing Annex 17 of ICAO). Annex 17 is titled the "Security - Safeguarding International Civil Aviation against Acts of Unlawful Interference." *Id.*

A 1998 Chicago Convention Amendment prohibits weapons from being used against civil aircraft.[99] A state, whose obligation under the Chicago Convention is to defend against any prohibited interference with civil aviation, may intercept cyberwarfare operations against civil aviation.[100] Additionally, if a cyberattack is made against an aircraft, the operation is a violation of the 1998 Amendment's requirement against using weapons to attack an operating civil aircraft.[101]

2. The Montreal Convention

The Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation is known as the Montreal Convention of 1971 (the Montreal Convention).[102] The Mon-

---

99. Schaap, *supra* note 94, at 167 (taking note of Chicago Convention's prohibition of weapons against aircraft). Article 3 bis(a) of this Amendment states, "the contracting States recognize that every State must refrain from resorting to the use of weapons against civil aircraft in flight . . . ." *Id.* (ellipsis in original) (internal quotation marks omitted)

100. *Id.* (making point cyberattack violates Chicago Convention). The Chicago Convention is unique because "it specifically acknowledges that a state may lawfully disregard its obligations under the Convention in times of war or national emergency." *Id.* at 168. Moreover, this national emergency exception may provide flexibility in cyberwarfare operations. *See id.* at 169.

101. *Id.* at 167 (inferring possible application of Article 3bis). Article 3bis of this Amendment prohibits states from using weapons against civil aircraft in flight. *Id.* A cyberattack is likely to be viewed as a "weapon" against civil aircraft, therefore violating international law. *See id.*

102. *See generally* Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, Sept. 23, 1971, 974 U.N.T.S. 1975, *available at* https://treaties.un.org/doc/Publication/UNTS/Volume%20974/volume-974-I-14118-English.pdf [hereinafter Montreal Convention] (containing text to Convention). Article 1 stipulates that one commits an offense under the Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (the Montreal Convention) by intentionally and unlawfully doing or attempting to do one of these acts:

> (a) performs an act of violence against a person on board an aircraft in flight if that act is likely to endanger the safety of that aircraft; or
> (b) destroys an aircraft in service or causes damages to such an aircraft which renders it incapable of flight or which is likely to endanger its safety in flight; or
> (c) places or causes to be placed on an aircraft in service, by any means whatsoever, a device or substance which is likely to destroy that aircraft, or to cause damage to it which renders it incapable of flight, or to cause damage to it which is likely to endanger its safety in flight; or
> (d) destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight; or

treal Convention may apply to prohibit unlawful operation of an aircraft that would render it incapable of flying.[103] The Montreal Convention may also prohibit interference with air navigation facilities because it would interrupt ATC communications and air navigation, thereby endangering the safety of in-flight aircraft.[104] Finally, "this Convention may prohibit cyber warfare [sic] operations from" infiltrating and sabotaging communication that would endanger an operating aircraft.[105]

After the Montreal Convention, the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (the Protocol) expanded the legal framework to include unlawful violent acts that occur at airports.[106] Article II of the Protocol provides:

> [A]ny person commits an offense if he unlawfully and intentionally, using any device, substance, or weapon "performs an act of violence against a person at an airport serving international civil aviation which causes or is likely to cause serious injury or death" or "destroys or seriously damages the facilities of an airport serving international civil aviation or aircraft not in service located thereon or disrupts the services of the airport, if such an act endangers or is likely to endanger safety at that airport."[107]

The Protocol may protect international airports from illegal cyberactivity involving a hacker's infiltration of their computer

---

> (e) communicates information which he knows to be false, thereby endangering the safety of an aircraft in flight.

Id. at art. 1.

103. Schaap, *supra* note 94, at 168 (pointing to cyberinterference occurring onboard aircraft might not qualify as impermissible under the Montreal Convention).

104. *Id.* at 169. *See also* Montreal Convention, *supra* note 102, at art. 1 (focusing on prohibition against maliciously targeting in-flight aircraft).

105. Schaap, *supra* note 94, at 169 (concluding Convention may prohibit thwarting communication systems onboard aircraft).

106. *Id.* (concentrating on extended legal framework of the Montreal Convention). The Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (the Protocol) seeks to "encompass unlawful acts of violence committed at airports serving international civil aviation, even" if it does not "endanger the safety of" in-flight aircraft. *Id.*

107. *Id.* at 169 (internal footnote omitted) (quoting Convention for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation art. II, Sept. 23, 1971, 1589 U.N.T.S. 1990, *available at* https://treaties.un.org/doc/Publication/UNTS/Volume%201589/volume-1589-I-14118-English.pdf) (offering Article II of the Protocol). The Protocol could potentially protect international civil airports from cybercriminals. *Id.*

network systems, revision of a passenger manifest list, or even placement of a person on a no-fly list.[108]

IV. Analysis

A. An Increase in Today's Cybercrime Climate

1. Vulnerable Businesses

As cybercrime threats among international businesses increase, criminals continue to take advantage of opportunities to use the convenience and secrecy of the Internet to commit their crimes.[109] According to the United States Department of Homeland Security, the number of cyberattacks rose "from 105,931 in 2009 to 228,700 in 2013."[110] Small businesses in particular are vulnerable to cybercrime because they represent easier access and low risk of cybercriminal exposure.[111] At the same time, cybercrime poses a significant threat to medium- and large-sized businesses because the tools cybercriminals use to infiltrate data systems are inexpensive and readily available.[112] Today, it is vital for businesses of all sizes to be aware of increasing cybercrime and establish preventive measures so that they can avoid disaster that will likely compromise their business processes.[113] "According to the National Cyber Security Alliance, one in five

---

108. *Id.* (considering how the Protocol may or may not prohibit cyberwarfare activity in airports). For cybercrime to be unlawful under the Protocol, it "would have to endanger the safety of those at the airport." *Id.*

109. *See INTERPOL Chief Warns of 'Invisible' Threats to Personal and Economic Security*, *supra* note 20 (suggesting cybercriminals seize advantages of performing crime via Internet).

110. Paletta, *supra* note 26 (reporting significant increase in cybercrime within past five years).

111. *See* Brandon, *supra* note 24 (cautioning small businesses vulnerable to cybercrime); Strohmeyer, *supra* note 25 (maintaining small businesses more vulnerable to cyberattack than large businesses). "Symantec's . . . annual Internet Security Threat Report found that companies with fewer than 250 employees constituted . . . 31 percent of targeted attacks in 2012," a rise from 18 percent in 2011. Strohmeyer, *supra*. Smaller companies are easy to attack because they lack the heightened cybersecurity measures that larger companies have. Brandon, *supra*; *see also* Strohmeyer, *supra*.

112. *See* Strohmeyer, *supra* note 25 (pushing for recognition of ease of cybercrime against businesses); *see also* Titcomb, *supra* note 23 (emphasizing minimal effort for cybercriminals to compromise bank security). Once a cybercriminal has hacked one bank, subsequent hacking becomes easier. Titcomb, *supra*.

113. *See* Strohmeyer, *supra* note 25 (accentuating destruction of business as result of cybercrime).

small businesses fall victim to cybercrime" and of those, about 60% dissolve within six months as a result.[114]

2. Governments' Attempt to Counter Cybercrime

Along with businesses, governments face increasing threats of cybercrime.[115] Cyberwar and espionage against governments has recently intensified.[116] As cyberwar emerges, legal authorities and governments are left to determine the necessary actions that must be made after an attack and they must also discern measures that could prevent future cyberattacks.[117] In addition to attacking governments, cyberhackers also target global summits.[118] In December 2010, cyberhackers penetrated the French Finance Ministry's computers, stealing confidential information about the February 2011 G20 Summit.[119] In effect, attacks like

---

114. *Id.* Small businesses that are hacked have greater than 50% chance of going out of business within six months than those that do not get hacked. *See id.* A problem is that small business owners fail to prioritize cybersecurity because they do not think that it is an issue. *Id.* Business owners assume it is an impossibility that hackers would target their business rather than several million others, without realizing that cyberattacks are mostly automated and target vulnerable systems. *Id.*

115. KPMG Int'l, *supra* note 26, at 8 (indicating governments face increasing cybercrime threats over past few years). Governments, including the United States, are developing laws to counter cyberattack. *Id.* at 10-11. *See also* Tiron et al., *supra* note 27 (showing Islamic State extremists purportedly hacked into U.S. Central Command's Twitter and YouTube accounts). Hackers posted the following message to the U.S. Central Command's Twitter account: "'While the US [sic] and its satellites kill our brothers in Syria, Iraq and Afghanistan we broke into your networks and personal devices and know everything about you' . . . ." Foster, *supra* note 27.

116. *See* KPMG Int'l, *supra* note 26, at 8 (directing attention to increasing cybercrime against government entities). Throughout the past few years, cybercrime has evolved to using online weapons and attacking government entities. *Id. See supra* note 30 and accompanying text (discussing cyberattacks against several nations' governments).

117. KPMG Int'l, *supra* note 26, at 8-11 (declaring "glimpses of cyber war [sic]" underscore importance of formulating preventative measures and posthoc protocol). Rosemary Scully, the Global Head of Justice and Security at KPMG, has stressed the importance of addressing what steps to take after an attack so that governments can be one step ahead of cybercriminals. *Id.*

118. *Id.* at 9 (classifying states along with global summits as prime targets for cybercriminals). In March 2011, hackers targeted the E.U. headquarters' computer network before a summit concerning current affairs and economic reforms. *Id.*

119. *Id.* (addressing issue of when hackers compromised French Finance Ministry's data before G20 Summit). The criminals hijacked control of an estimated 150 computers and accessed sensitive information concerning the upcoming G20 Summit. *Id.*

these have resulted in an increased focus on international crackdown on cybercrime.[120]

In January 2011, two U.S. Senators proposed a measure to counter cybercrime "granting President Obama the authority to shut down the Internet in the event of a cyberattack."[121] A bill that would grant a U.S. President to shutdown the Internet is an extreme reaction; a less extreme alternative would involve the Federal Bureau of Investigation's leading a coordinated investigation to locate the source of the hacking.[122] A beneficial approach for the aviation industry and international governments would be to reference the U.K.'s Police Central e-Crime Unit that works with both law enforcement and private specialists.[123] A critical component to countering cybercrime requires collaboration among international communities.[124] China, for instance, collaborates with the Association of Southeast Asian Nations, the United Nations, and other international governments and

120. *See id.* at 10-11 (explaining several countries' approach to countering cybercrime). *See also supra* note 31 and accompanying text (reviewing various governments' cyberdefense measures).

121. KPMG Int'l, *supra* note 26, at 10 (observing extreme proposal to counter cyberattack). Although Senators proposed this bill in 2011, Congress has declined to enact it. *S. 413 (112th): Cybersecurity and Internet Freedom Act of 2011*, *supra* note 31 (pointing out bill failed). The proposal of this bill received heavy criticism because "many organizations . . . believe[d] it may give the government more power and control over the internet." KPMG Int'l, *supra*.

122. *See* KPMG Int'l, *supra* note 26, at 10 (encapsulating how FBI counters cybercrime). The FBI established a separate entity to investigate cybercrime. *Id.* In an incident that occurred in October 2010, the FBI arrested over ninety people who allegedly engaged in cybercrime against U.S. computer networks with the intent of stealing USD70 million. *Id. See also Cyber Action Team*, *supra* note 31 (articulating what FBI's fast-reacting cyber team does). Upon the report of a cybersecurity breach, the CAT team will investigate using "tools, techniques, and procedures" to identify the hacker. *Id.*

123. *See* KPMG Int'l, *supra* note 26, at 10-11 (acquainting readers with United Kingdom's Police Central e-Crime Unit for countering national cybercrime). "According to a UK [sic] government spokesman, 'The government is determined to build an effective law enforcement response to the cyber crime [sic] threat, building upon the existing expertise within SOCA (national police unit responsible for pro-active operations against serious and organized crime) and the Met Police Central e-Crime Unit.'" *Id.* at 11. Furthermore, the United Kingdom coordinated with Poland to protect information "while planning for Euro2012 [soccer] championships and the London 2012 Olympics." *Id.*

124. *See id.* (highlighting China's approach to countering cybercrime). "In 2009, nearly 200 Chinese government websites" fell victim to cyberattack and the country subsequently "incorporated computer crimes into its criminal law legislation." *Id.*

communities to counter cybercrime.[125] Collaborating with organizations is beneficial to the international community–for example, large international organizations, such as Europol and the North Atlantic Treaty Organization (NATO), attempt to counter cybercrime through a coordinated effort.[126]

3. Transportation Industry's Approach to Cybercrime

Cybercriminals continue to find new and innovative ways to hack into vulnerable computers to steal confidential information.[127] Cybercriminals intend to attack critical infrastructures, such as the transportation industry, to meet their tactical and calculated objectives.[128] The railroad, maritime, and aviation industries face a high risk of cyberattack, because their complex computer systems make it nearly unfeasible to eliminate every weakness.[129] Once hackers manage to gain access to computer systems, they can "easily create user accounts, delete existing accounts, reformat hard drives, scramble stored data," and shutdown systems.[130] This could have a devastating effect on the aviation industry's newly developed NextGen system.[131]

---

125. *Id.* (demonstrating China's collaboration with international actors to counter cybercrime). China has realized the importance of cooperating with other state actors in an attempt to counter its own cybercrime attacks. *Id.* "In 2003, China signed the ASEAN-China Coordination Framework for Network and Information Security Emergency Responses . . . ." *Id.* Additionally, the United States has provided China with support to fight against cybercrime. *Id.* Between 2009 and 2010, the United States assisted China in thirteen significant cybercrime cases. *Id.*

126. *See id.* at 12 (providing examples of international organizations working together to build solid cybersecurity framework). Such a coordinated effort will provide for faster reactions and response after a cybersecurity breach. *See id.* "At the [NATO] summit in November 2010, the EU [sic], NATO, and the US [sic], approved plans . . . to tackle cyber crime [sic] in member states" so that an E.U. cybercrime center can coordinate among member states and "facilitate communication between rapid response teams and law enforcement authorities." *Id.*

127. *What Hackers & Cyber Criminals Are Eyeing for in 2014*, *supra* note 32 (portraying cybercriminals' goal to hack using innovative approaches); *see also* Pagliery & Perez, *supra* note 32 (recognizing limitless possibilities of cyberattack).

128. Iasiello, *supra* note 8, at 24 (arguing critical infrastructures become targets for cybercriminals).

129. *See* WEIMANN, *supra* note 17, at 6 (drawing attention to vulnerability of key infrastructures). The extensive amount of targets that cybercriminals seek to infiltrate include, but are not limited to, "governments, individuals, public utilities, [and] private airlines." *Id.*

130. *Id.* (enumerating repercussions of hacking). *See also* Sternstein, *supra* note 34 (warning railroad industry at risk of cyberattack).

131. *See supra* Part III.A.2 (delving into complexities of aviation infrastructure). NextGen is a complex, intricate network that could be subject to cyberattack. *See*

B. Aviation Industry's Need for a Solid Cybersecurity Framework

1. Currently Living in Pre-9/11 Stage

The aviation community is currently living in a pre-9/11 time period.[132] The cyberhacking threat against the aviation community is real.[133] Aviation continues to be a prime target for terrorists and cybercriminals because of its potential to massively damage significant public infrastructure.[134] The aviation industry now has the chance to prepare for a cyberattack that has not yet significantly impacted its operations.[135] Given that technology has become more advanced since 9/11, proper security considerations must be developed to tackle a cybersecurity threat before it is too late.[136] One consistency in the cyberdomain is that all of today's intricate technologies have been or will fall victim to cyberattack; the key to achieving an advanced cybersecurity framework requires the potential victim to outsmart the cybercriminal.[137]

The problem is that the FAA and other international aviation agencies have not fully instituted responsibilities and duties for information security related to the NAS systems.[138] The aviation industry must implement preventative measures as a

---

supra notes 65, 85,86 and accompanying text (revealing FAA's NextGen system and issues GAO reports noted with FAA security practices).

132. *Supra* note 44 and accompanying text (imparting importance for aviation industry to establish precautionary measures against cyberattack).

133. Iasiello, *supra* note 8, at 25 (focusing on aviation industry as involving public's confidence in integrity of its network and systems). As a critical component to a country's infrastructure, the aviation industry is key to economic success. *See id.* The international aviation community will remain a cyberterrorist's prime target because of the potential to place human lives at risk and cause financial disruption. *Id.*

134. *Id.* (punctuating importance of imminent cyberthreat against aviation industry).

135. *Id.* (stressing opportunity for aviation industry to prevent another 9/11 event from occurring). After the terrorist attacks on September 11, 2001, the aviation industry regained confidence after it implemented higher security measures. *Id.*

136. *Id.* (opining preventive measures needed to ensure proper response to future cyberattacks). *See* US GAO AIR TRAFFIC CONTROL, *supra* note 65, at 12 (underscoring vulnerabilities of FAA's new ATC networking technologies).

137. Iasiello, *supra* note 8, at 25 (detailing importance of remaining ahead of cybercriminals in their desire to target aviation industry).

138. *See* US GAO INFORMATION SECURITY, *supra* note 62, at 28 (noticing shortcoming FAA must counter).

means to successfully combat future cyberattacks.[139] Specifically, an aviation agency must have strategic procedures for information security, that is, identify its goals and objectives related to its aim to strengthen its computer systems against exposure.[140]

2. Cooperation Among Governments and International Organizations Are Necessary to Combat Aviation Cybercrime

For the aviation industry to successfully counter future cybercrime, guidance and leadership from international organizations and governments is necessary.[141] Five major international organizations announced that they would form a cybersecurity agreement to combat cybercrime against the aviation industry.[142] The participating organizations are: the ICAO; the Civil Air Navigation Services Organization; the International Air Transport Association; Airports Council International; and the International Coordinating Council of Aerospace Industry Associates.[143] Such an agreement would synchronize actions and responses in the common fight against any type of cyberattack.[144] A great benefit of international aviation organizations collaborating to combat cybercrime is that members be-

---

139. *See* Cooper, *supra* note 85 (suggesting recommendations to aviation industry to properly combat cyberthreats). The GAO recommended that the industry should increase training, learn to identify and fix problems, "strengthen[ ] protocols for access control, increas[e] organizational planning, and" maintain proper records to monitor data traffic and detect unauthorized access. *Id.* Moreover, the vulnerabilities lie among the interconnected aviation system, particularly with the newly developed NextGen system for the FAA. *See* US GAO AIR TRAFFIC CONTROL, *supra* note 65, at 6 (defining NextGen System). The NextGen system is particularly vulnerable to cyberattack because it is a newly developed system comprised of reliance on software and hardware as well as reliance on satellites for surveillance and navigation purposes. US GAO INFORMATION SECURITY, *supra* note 62, at 6.

140. US GAO INFORMATION SECURITY, *supra* note 62, at 27 (indicating agencies should focus on goals and objectives to counter cybercrime).

141. *See* UK CYBER SECURITY IN CIVIL AVIATION, *supra* note 47, at 5-6 (commenting on need for international organizations to guide aviation industry in right direction). International groups such as the ICAO, FAA, EU, and ECAC are critical to providing solid foundation to protect the aviation industry against cyberattack. *Id.* at 5.

142. *See* Van Wagenen, *supra* note 31 (recounting how five international organizations agreed upon new cybersecurity agreement to coordinate actions).

143. *Id.* (listing aviation organizations involved in cybercrime agreement).

144. *See id.* (implying agreement among international aviation organizations acts as step in right direction to combat cybercrime).

come more aware of threats and develop preventative measures in response to cyberattacks.[145]

3. International Aviation Response to Cyberattack

The risk of a cyberattack has increased dramatically over the last few years.[146] For the aviation industry to successfully combat cybercrime, it must establish a fast detection and response to impending threats.[147] Additionally, an important approach to countering cybercrime is to recognize all key vulnerabilities because the more networked and interconnected an enterprise, the greater the chance of sabotage to any built-in weaknesses.[148] In the event of a cybercrime attack, it is imperative that the response considers not only matters within the aviation industry but also the industry's customers and regulators.[149] The reason to have a comprehensive framework to respond to a cyberattack incident is that the public has strong confidence in the aviation industry; moreover, the aviation industry now has a chance to prepare for a threat that has not yet severely impacted its operations.[150] Finally, the recovery plan after a cyberattack cannot only focus on the rehabilitation process but must also look to the airline company and industry's reputation with its customers, regulators, and the public.[151]

---

145. *See id.* (saying some benefits of international organizations collaborating together against cybercrime). Such an international agreement encourages considerable cooperation from all government levels and industry stakeholders to develop adequate cybersecurity policies. *Id.*

146. *See* Paletta, *supra* note 26 (conveying insight to increasing cyberattacks over years).

147. *See* Palmay, *supra* note 48, at 3-4 (offering suggestions on how to counter cyberattacks).

148. *Id.* at 2-3 (intimating how to identify cyberweaknesses of company or industry intending to protect). The weakest link "become[s] the source of attack." *Id.* at 2. *See* Iasiello, *supra* note 8, at 23 (communicating more sophisticated and intricate systems prone to cyberattack). Built-in weaknesses include "[a]ircraft-to-ground, aircraft-to-aircraft, and in-aircraft access points [which] can all be exploited." *Id.* Additionally, "communications between aircraft and air traffic controllers [continue to be] unencrypted and unsecured," leaving a gateway open for malicious hackers to disrupt air transportation. *Id.*

149. *See* Palmay, *supra* note 48, at 2-3 (telling of important point when responding to cyberbreach).

150. *See* AM. INST. OF AERONAUTICS & ASTRONAUTICS, *supra* note 48, at conclusions (noting strong confidence in aviation industry to combat and protect public).

151. *See* Palmay, *supra* note 48, at 3-4 (explaining importance of recovery after cyberattack).

V. Conclusion

Today, the world faces cybercriminals' malicious intentions in desiring to take advantage of the convenience and anonymity of the Internet to commit criminal activities.[152] Various industries are vulnerable to cybercrime, particularly the aviation industry.[153] The aviation industry has been subject to terrorist attacks before and that is why the international community must set precautions to successfully combat an unprecedented cyberattack.[154] As the aviation industry advances with its modernized ATC systems and aircraft, knowledge of computer system vulnerabilities emerges.[155] Therefore, the future of ensuring the safety of the international aviation community lies in how it establishes preventative measures and, more importantly, how it recovers from a devastating cyberattack.[156]

Andrew V. Schmidt

---

152. *See supra* Part II.A.1.a (covering cybercrime attacks on businesses); *supra* Part II.A.1.b (focusing on cybercrime attacks on governments); *supra* Part II.A.1.c (discussing cybercrime against transportation industry).

153. *See supra* Part II.B.2 (admitting cyber vulnerability aviation industry faces).

154. *See supra* Part III.B.2 (emphasizing aviation industry as prime target for cyberattack).

155. *See supra* Part III.B.2 (showing FAA's lack of preparedness to ensure proper security measures in countering cyberattack).

156. *See supra* Part IV.B.2 (declaring cooperation among international community necessary to prepare against cyberattack); *supra* Part IV.B.3 (reasoning how aviation industry should respond to cyberattack).