

Aviation and Cyberspace

Convergence of Domains, Convergence of Threats

EMILIO IASIELLO

Introduction

Cyber threat is one of the most talked about dangers facing the international community because it's global in scope and impacts any public and private sector organization that touches the Internet. It is an environment that favors the criminal as there are few and ineffectual laws governing the activity that traverses interconnected networks, creating a functional, borderless domain. As such, the bad guys operate in a dark environment where their actions can hide in high volumes of Internet traffic. Malware creators build and sell their sophisticated and not so sophisticated creations in underground markets to actors of various skill levels to implement in a wide variety of hostile activities that include the perpetuation of cyber crime; politically or ideologically motivated hacktivist operations; or the surreptitious access into networks and theft of intellectual property and sensitive documents supporting industrial or nation state espionage. Reminiscent of the United States' "Wild West" of the late 1800s, there is no law enforcement presence or commonly accepted criminal legislation keeping malfeasants in check. As a result, foreign governments have acknowledged the importance of securing their own parts of this global network, some of which have drafted or are drafting national cyber security strategies to address this enigmatic and complicated threat. The United States in particular has taken aggressive initiatives in making cyber a military problem, outlining in its May 2011 *International Strategy for Cyberspace* that it "reserves the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law."¹ While a positive first step, the U.S. commercial landscape remains fragmented and tribal in terms of organizational cyber security, as evidenced in the 15 federally established, industry-specific Information Sharing and Analysis Centers (ISAC)² whose mission is to provide accurate and timely information and services to critical infrastructure stakeholder members. The Transportation ISAC (PT ISAC) in particular has a thankless job of trying to perform this function across all public transportation systems. As aircraft modernizes and adopts an inter-networked operations capability, aviation will be confronted with the hostile actors, equipment vulnerabilities, scripted malware, malicious activity, and security challenges associated with this new threat landscape. Instead of reacting to this complex and dynamic threat environment, aviation needs to proactively address cyber threats to stay ahead of the problem, or else risk playing catch up in an environment where the bad guys are hidden, and hostile activities occur in nano-seconds.

Aviation Cyber Incidents of Note

The aviation industry – and in particular, the air travel process – has had the unexpected luxury of not being targeted in visible and noteworthy attacks. While there have been well publicized incidents of suspected cyber espionage actors seeking to gain unauthorized access into aviation's industrial base, there has been no discernible similar reporting of hostile actors targeting *aircraft in motion*; that is, from runway to runway. Aviation needs to view this as a huge opportunity to address cyber security shortcomings in equipment, communications, or any point of

access that can be exploited by technically savvy actors. In 2011, there were several notable incidents of hostile actors directing their nefarious cyber operations against aviation interests. Most of these are suspected of being conducted by espionage actors as the majority of them focused on gaining unauthorized access to networks for the purposes of information collection consistent with espionage actor behavior. They did not exhibit a destructive intention typically observed in hacktivist activity (e.g., through distributed denial-of-service attacks, web defacements, etc.), nor did they implement e-mail spam campaigns and Trojanized emails to gain access and acquire personal identifiable information for monetization purposes as typically done by cyber criminals.

- **April 2011:** L-3 Communications was targeted by hackers using compromised SecurIDs, a two factor authentication system. L-3 was not clear if the attack was successful or not but the event was significant in that it was the first using SecurIDs to attempt to gain access to a network.³
- **May 2011:** Lockheed Martin was targeted in a cyber espionage campaign. Attackers apparently possessed the seeds–factory-encoded random keys–used by at least some of Lockheed’s SecurID hardware fobs, as well as serial numbers and the underlying algorithm used to secure the devices. The activity was detected early and no information was reported stolen or compromised.⁴
- **May 2011:** Northrop Grumman was targeted in a similar cyber espionage campaign attempt as Lockheed Martin. Attackers tried to gain access using compromised RSA Seeds. The activity was detected before any information could be stolen.⁵
- **October 2011:** A computer virus has infected the cockpits of America’s Predator and Reaper drones, logging pilots’ every keystroke as they remotely fly missions over Afghanistan and other warzones. Removal of the virus required multiple efforts indicating that the virus was resilient to mitigation.⁶
- **December 2011:** Iran claims to have exploited a known GPS vulnerability to trick the drone to land in Iran.⁷

As illustrated in the above examples, there has not been a real life example of a hostile actor attempting to impact an aircraft during the air travel process. However, if we look at the progression of the cyber threat environment, we see a dynamic landscape where the bad guys have steadily increased their capabilities and activities over a short amount of time. Malware in and of itself has changed dramatically. From 1988’s Morris Worm whose unintentional consequences caused denial of service attacks, to the 2010 discovery of Stuxnet whose design was to attack very specific industrial software and equipment demonstrates how quickly cyber weapons can achieve a sophisticated level of weaponization.

Airport Incidents of Note

Airports have been the victims of suspected cyber malfeasance by actors. There are many potential digital entry points at an airport that can be targeted for disruption. Communications between the air traffic control and the aircraft, passenger boarding and check in services (which are accessible via the Internet), passenger processing systems, airport virtual private networks (used to secure Internet connections between an organization’s private network and a remote employee), and wireless networks are just some systems within an airport environment that can be targeted and exploited for nefarious purposes. Some recent incidents highlight the potential threat of hostile actors looking to gain unauthorized access into airports networks.

- **August 2012:** A Boston digital security firm uncovered malware hidden in the virtual private network (VPN) of a major non-U.S. international airport. The threat could have compromised everything from the employees’ personal information to the safety of passengers, said the firm. The attack used Citadel Trojan malware to read the screens of employees who logged in remotely to the airport’s VPN. ⁹
- **June 2012:** Infected game software was directed by a command server to attack South Korea’s Incheon International Airport in an effort to disrupt flight traffic via a DDoS attack. ¹⁰
- **June 2011:** Flights were affected at Indira Gandhi International Airport’s Terminal 3 when the common Use Passengers Processing System (CUPPS) failed and was down for almost 12 hours. Initial investigations showed use of “malicious code” from an unknown remote location led to CUPPS failure. ¹¹

Date	Source	Attack	Target	Vector
Apr 6 2011		L-3 Communications An E-mail, dated April 6, sent to 5000 employees of US Defense Contractor L-3 warns of an attack attempt made with compromised SecurIDs. It is not clear if the attack was successful (it was revealed half a month later). This is the first attack made with compromised RSA seeds. ⁷		Compromised SecurIDs
May 21 2011		Lockheed Martin This is the first known (and the only officially recognized so far) attack perpetrated with compromised SecurID Seeds targeting an U.S. Defense Contractor. The attack was detected before any sensitive information could be stolen. 100,000 accounts were locked as a precaution. ⁷		Compromised SecurIDs
May 26 2011		Northrop Grumman Third U.S. Defense Contractor attacked using compromised RSA seeds. Attack detected before any sensitive information could be stolen. Remote Access locked. ⁸		Compromised SecurIDs
Oct 8 2011	?	U.S. Military Drones Wired reports that a computer virus has infected Predator drones and Reaper drones, logging pilots’ keystroke during their fly missions over Afghanistan and other warzones. The virus was detected nearly two weeks ago at the Ground Control System (GCS) at Creech Air Force Base in Nevada and has not prevented drones from flying their missions, showing an unexpected strength so that multiple efforts were necessary to remove it from Creech’s computers. ⁷		Generic Malware via USB Stick
Dec 9 2011		Lockheed Martin RQ-170 Sentinel An RQ-170 Sentinel drone crash lands in Iran. After few days the Christian Science reports that Iran was able to capture the US RQ-170 drone exploiting a known GPS vulnerability, tricking the US drone to land in Iran. ¹⁰ Even if the solution of the mystery is much simpler. ¹¹		GPS Hack?

Figure 1: Chart of Notable Activity produced by Hackmageddon.com ⁸

In two of these instances, there was little insight into the individuals responsible for the attacks. In the South Korean incident, a man was arrested who was believed to have been purchased the gaming software from agents of North Korean intelligence. Whether witting or unwitting, these examples demonstrate the varied actor landscape that could be responsible for the perpetration of cyber attacks against airports.

Cyber Threat Actors – Who the Bad Guys Are

The anonymity of the Internet affords a long list of state and non-state actors the cloak of darkness from which to operate. Targeted and untargeted attacks originating from these sources have affected public and private sectors across the globe. While there is limited evidence of these actors targeting aviation through cyber means, the volume is subject to change based on the actors' intent, as well as their capabilities and resources required to conduct such attacks. Based on the evolution of hacking, all U.S. industry sectors have been the victim of nefarious actors at one time or another. Agriculture¹², Defense Industrial Base¹³, Energy¹⁴, Finance¹⁵, Government¹⁶, Healthcare,¹⁷ Military,¹⁸ and Water¹⁹ have faced hostile cyber activity from one or more of the below groups of threat actors.

- **Hactivists:** Hactivists are politically or ideologically motivated hackers who conduct hostile and sometimes destructive activity in support of a cause or belief. Groups like Anonymous engage in operations against targets to punish a perceived transgression or draw attention to a situation. Typical hactivist behavior involved conducting distributed denial-of-service attacks (DDoS), which floods a web site's server with so much traffic it renders the site inoperable; web page defacements, which is a form of electronic graffiti to send messages; doxing, which is a process where people's personal information (e.g., home address, phone numbers, personal identifiable information, etc.) are stolen and posted on the Internet. Hactivists have repeatedly demonstrated their willingness to conduct offensive cyber operations against enterprises they feel deserve to be made an example. If an airline should fall in a hactivist group's crosshairs, it is expected that hostile cyber activity at the very least would target airline webpages.
- **Hackers:** Hackers break into networks for the thrill of the challenge, or bragging rights in the hacker community, among other reasons. They are differentiated from hactivists in that their motivations are not politically or ideologically based. While gaining access to a network or computer used to require a level of skill that separated experienced hackers from newbies, hackers can now download attack scripts and protocols from the Internet to launch against targets.²⁰ What's more, these attack tools have grown increasingly sophisticated while also becoming easier to use, negating the need of an individual to be advanced to launch attacks. Hacking sites feature free tools, tutorials, and a plethora of experienced hackers to serve as mentors for those less experienced.
- **Nation State Actors:** Nation state actors typically use cyber espionage to collect sensitive information and intellectual property information from their targets. However, depending on the intent of nation state actors, gaining unauthorized access into target networks can be leveraged to reconnoiter and map out the network in order to gain intelligence in support of a later attack. This is considered the cyber equivalent of "intelligence preparation of the battlefield."
- **Terrorist Groups:** While terrorists and terrorist organizations prefer kinetic strikes against targets, there is growing body of information of terrorist use of the cyber domain. Primarily, terrorist use cyberspace to recruit, disseminate propaganda, incitement, radicalization, financing, training, planning, and research.²¹ However certain terrorist leaders at times have encouraged radical Islamists to use the Internet for more operational purposes. In 2004, Imam Samudra, the individual responsible for engineering the 2002 Bali night club bombings, published a memoir detailing the use of committing cyber crime against U.S. interests to bankrupt the country.²²
- After the death of Osama Bin Laden in 2012, an Al-Qaeda video promoted electronic jihad against the United States.²³

- **Insiders:** A witting or unwitting insider can provide hostile actors direct access to networks and systems they want to target for disruption, destruction, or manipulation. According to a study primary sources of computer crimes. ²⁴ Insiders constitute any individual who has direct or indirect access to a targeted computer or network.

Future Malware Threats and Aviation

Cyber threats to critical infrastructure networks continue to evolve as the global landscape becomes more networked. Essentially, the more complex and advanced a network becomes, the more technical glitches and vulnerabilities it contains, and the more difficult it becomes to manage from a security perspective. The aviation industry is moving toward a more networked environment to improve all facets of air travel, from an aircraft on the ground to take off to air flight. The U.S. Federal Aviation Authority estimates that by 2020, the majority of global civilian aircraft will have implemented the Automatic Dependant Surveillance Broadcast (ADS-B) an advanced surveillance technology, which will be replacing radar as the primary means of tracking aircraft. During all aspects of travel, information will flow through this networked environment from ground stations to air traffic control to the plane in flight. While this technology will not be able to be accessed directly via the Internet, two high impact anecdotes reveals how savvy actors have developed cyber tools to successfully penetrate and impact systems not readily accessible via the Internet but form its own network.

- **Stuxnet:** Discovered in 2010, Stuxnet is a computer worm designed to attack Siemens control systems. It was likely introduced into the closed network by a USB key. ²⁵The malware was designed to only Siemens supervisory control and data acquisition (SCADA) systems that were configured to control and monitor specific industrial processes. ²⁶ This was the first instance of a cyber weapon targeting a specific type of system and successfully impacting its operations. This worm successfully damaged as many as 1,000 centrifuges.
- **OPERATION BUCKSHOT YANKEE:** In 2008, the U.S. Department of Defense suffered a significant compromise of its classified military computer networks. It began when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control ²⁷

Just because aviation industry has not suffered a substantial cyber attack such as a DDoS, or an incident like those described above, it does not mean it cannot happen, and it should not presume that because operational networks are not connected to the Internet, that these systems are protected from malware. Disruptive or destructive malware acts (e.g., Stuxnet, or the 2012 Shammooon malware that swept through 30,000 computers on Saudi Aramco's network, wiping the hard drives clean.) are just one avenue available for hostile actors. As aviation adopts the highly networked ADS-B ²⁸ technology, several information sources will be fed to the ADS-B to include but are not limited to:

- **Traffic:** A pilot would be able to access information on air traffic to include altitude, heading, speed, and distance to aircraft.
- **Weather:** Aircraft equipped with UAT ADS-B In technology will be able to receive weather reports, and weather radar through flight information service-broadcast (FIS-B).
- **Terrain:** ADS-B In technology, broadcasts a terrain overlay for pilots to view in the cockpit.

- **Flight Information:** Not to be confused with FIS-B, traffic information service-broadcast (TIS-B) transmits readable flight information.²⁹
- Any misrepresentation or purposeful manipulation of critical flight information can achieve equally damaging results as any other cyber attack. However, in this case, data manipulation can be the catalyst for causing physical damage to the aircraft and directly impacts passenger safety.

Conclusion

The aviation industry continues to make strides toward creating an e-enabled environment that successfully interconnects the multi-faceted components of the aviation landscape. The overhaul of the National Airspace System will make travel more convenient and dependable, facilitating information sharing at unprecedented levels to better inform operators and increase efficiency while maintaining a high level of safety. However the technology involved in implementing a seamless communication process provides a myriad of opportunities for hostile actors to exploit. Although aviation has successfully evaded the attention of hostile cyber actors, this may steadily be changing particularly as networked environments draw the interest of actors that see aviation as a viable target – nation state actors can target aviation to maintain access for future considerations; cyber criminals can target aviation to steal sensitive data or blackmail airline operations for monetization purposes; and hackers can target aviation to punish perceived transgressions or to draw attention to their political and/or ideological causes. The one constant amidst these actors is that they are dynamic, able to adapt quickly to their operating environments. If aviation has not been targeted to the extent other industries have, it's because these actors have not yet recognized how targeting aviation can further their respective objectives, not that they are unable. Aviation is at a unique position because it has the opportunity to plan for these threats prior to them becoming too overwhelming and expensive to fix. To wait to address them because they are not yet a problem will be the equivalent of closing the barn door after the horse has bolted. □

Notes

1. The White House, International Strategy for Cyberspace; May 2011; accessed at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
2. National Council of ISACs home page accessed at: <http://www.isaccouncil.org/memberisacs.html>.
3. William Jackson, "Another Major Defense Contractor Hacked, RSA Tokens Likely Involved," Government Computer News, June 1, 2011, accessed at: <http://gcn.com/Articles/2011/06/01/Defense-contractors-L3-Lockheed-hacked.aspx?p=1>
4. Matthew J. Schwartz, "Lockheed Martin Suffers Major Cyberattack," Information Week, May 31, 2011, accessed at: <http://www.informationweek.com/government/security/lockheed-martin-suffers-massive-cyberatt/229700151>
5. Jeremy Kaplan, "Northrop Grumman May Have Been Hit With a Cyberattack," Fox News, June 1, 2011, accessed at: <http://www.foxnews.com/tech/2011/05/31/northrop-grumman-hit-cyber-attack-source-says/>
6. Noah Shachtman, "Computer Virus Hits U.S. Drone Fleet," Wired Magazine, October 7, 2011, accessed at: <http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/>
7. Scott Peterson, "Iran Hijacked US Drone, Says Iran Engineer," Christian Science Monitor, December 15, 2011, accessed at: <http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video>
8. Hackmageddon.com, accessed at: <http://hackmageddon.com/?s=aviation>.
9. Michael Dolgow, "Cyberwars Reach a New Frontier: The Airport," Bloomberg Businessweek, August 15, 2012, accessed at: <http://www.businessweek.com/printer/articles/67128-cyberwars-reach-a-new-frontier-the-airport>.
10. Jeff Goldman, "South Korean Man Arrested Over Airport Cyber Attacks," ESecurity Planet, June 5, 2012, accessed at: <http://www.esecurityplanet.com/print/network-security/south-korean-man-arrested-over-airport-cyber-attacks.html>
11. Manan Kakkar, "CBI Believes Cyber Attack Led to IGI Airport's Technical Problems in June," ZdNet, September 25, 2011, accessed at: <http://www.zdnet.com/blog/india/cbi-believes-cyber-attack-led-to-igi-airports-technical-problems-in-june/710>

12. Eduard Kovacs, "US Department of Agriculture Sites Hacked in Protest Againsts Mohammed Movie," NewsSoftpedia, September 21, 2012, accessed at: <http://news.softpedia.com/news/US-Department-of-Agriculture-Sites-Hacked-in-Protest-Against-Mohammed-Movie-293926.shtml>.
13. Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace," October 2011, accessed at: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf
14. Ellen Nakashima, "U.S. Said to Be Target of Massive Cyber Espionage Campaign," Washington Post, February 10, 2013, accessed at:
15. Matthew J. Schwartz, "Bank Attackers Restart Operation Ababil DDoS Disruptions," Information Week, March 6, 2013, accessed at: <http://www.informationweek.com/security/attacks/bank-attackers-restart-operation-ababil/240150175>
16. Bryan Krekel, "Capabilities of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," US China Economic and Security Review Commission, October 2009, accessed at: http://www.dodea.edu/Offices/Safety/upload/14_china_spy.pdf
17. RSA, "Cybercrime and the Healthcare Industry," 2010, accessed at: http://www.rsa.com/products/consumer/whitepapers/11030_CYBHC_WP_0710.pdf
18. Bob Orr, "Pentagon Expands Cyber Defense Amid Daily Attacks," CBS News, February 6, 2013, accessed at: http://www.cbsnews.com/8301-18563_162-57568079/pentagon-expands-cyber-defense-amid-daily-attacks/
19. Ellen Nakashima, "Foreign Hackers Target U.S. Water Plant in Apparent Malicious Attack," Washington Post, November 18, 2011, accessed at: http://www.washingtonpost.com/blogs/checkpoint-washington/post/foreign-hackers-broke-into-illinois-water-plant-control-system-industry-expert-says/2011/11/18/gIQAgmTZYN_blog.html.
20. Government Accountability Office, "Cybersecurity: Threats Impacting the Nation," GAO-12-666T, April 24, 2012, accessed at: <http://www.gao.gov/assets/600/590367.pdf>.
21. United Nations Office on Drugs and Crime, "The Use of the Internet for Terrorist Purposes," 2012, accessed at: http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
22. Alan Sipress, "An Indonesian's Prison Memoir Takes Holy War into Cyberspace," Washington Post, December 14, 2004, accessed at: <http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html>
23. Jack Cloherty, "Virtual Terrorism: Al-Qaeda Video Calls for Electronic Jihad," ABC News, May 22, 2012, available at: <http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875>.
24. Government Accountability Office, "Cybersecurity: Threats Impacting the Nation," GAO-12-666T, April 24, 2012, accessed at: <http://www.gao.gov/assets/600/590367.pdf>
25. Robert McMillan, "Siemens Stuxnet Hits Industrial Systems," Computer World, September 14, 2010, accessed at: http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142
26. Nicholas Falliere, "Stuxnet Introduces First Root Kit for Industrial Control Systems," Symantec, August 19, 2010, accessed at: <http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices>
27. William J. Lynn, "Defending a New Domain," Foreign Affairs, September/October 2010, accessed at: <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>
28. Reuters, "Saudi Aramco Says Hackers Too Aim at Its Production," New York Times, December 9, 2012, accessed at: http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0
29. Federal Aviation Administration, "ADS-B Frequently Asked Questions," accessed at: <http://www.faa.gov/next-gen/implementation/programs/adsb/faq/>



Emilio Iasiello is the Chief Threat Analyst at iSIGHT Partners, a global cyber intelligence firm, supporting federal and commercial entities to manage cyber risks, understand their threat environment, and help prioritize their investments against those threats impacting their business or mission. He has worked in cyber threat analysis since 2002 both as a government contractor and a government civilian with the Department of State and the Department of Defense, respectively. Emilio has written papers on the development of a new cyber threat analytic methodology, and on the IT Supply Chain.