Designing for Security: A Cybersecurity Introduction for Aerospace Education

Karl Roush

Georgia Institute of Technology

Master's Division AIAA R2SC, April 05-09 2021

Goal and Structure

- Goal: serve as an introduction of topics, with the purpose of exposing the next generation of aerospace engineers to key areas where cybersecurity will prove essential.

- Structure:
  - Background
  - Area 1: Autonomous Navigation
  - Area 2: Communications
  - Area 3: Control Systems
  - Conclusion
  - Acknowledgements

Background

Background

Autonomous Navigation

Communications

Control Systems

Conclusion

Acknowledgements

What is Cybersecurity?

"Security in cyberspace (i.e., cybersecurity) is about technologies, processes, and policies that help to prevent and/or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor."

Computer Science and Telecommunications Board; National Research Council

Why care about Cybersecurity?

- **Digitalization**: Everything is moving towards digitalization
- **Sophisticated Methods:** dedicated groups with the goal of attacking systems
- **Widely Available Hacking tools:** many free and easy to use tools
- **Personal Security:** protecting your own data (files, photos, etc.)
- **Data Protection:** data breaches are common, personal details can be exposed
- **Legal Obligations:** companies must follow certain practices & disclosures

- Notable examples from this year:
  - Microsoft Exchange
  - Solar Winds

Key Stakeholders

- Many large technology companies have cybersecurity division or are solely devoted:
  - Google Project Zero
  - Microsoft
  - Cisco
  - FireEye
- Even entities not focused on technology have cybersecurity teams (e.g. universities)
- Governments ("nation state actors") have entire devoted agencies
  - Intelligence gathering (NSA, NRO, CIA, FBI)
  - CISA (Cybersecurity & Infrastructure Security Agency)

In an increasingly digital world, we are all stakeholders

Cybersecurity in Aerospace

- Within the Aerospace sector, the integration of communications, sensors, and data collection (often referred to as “Digital Enterprise” or “Digital Engineering”) is starting to become widespread
- As the number of systems grows, so does the attack surface

- Examples:
  - **2019:** Boeing 787 source code leak
  - **2020**: Operation North Star, attacks on F-22 production and projects, likely North Korea
  - **2020**: DEFCON satellite hacking event put on by the USAF

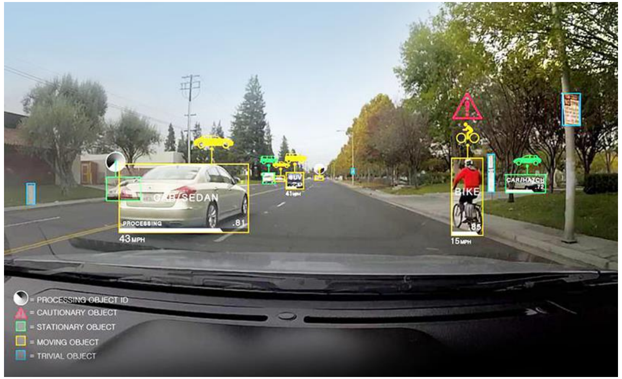
Autonomous Navigation

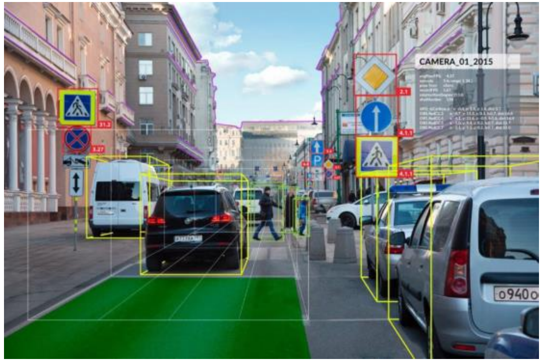
Background | Autonomous Navigation | Communications | Control Systems | Conclusion | Acknowledgements

What is Autonomous Navigation?

- Vehicle navigates with minimal or no human intervention.
- The most common instance of this is self-driving cars.
- Often these systems operate using cameras assisted by machine learning models to “understand” the environment and act accordingly.

- Potential Attacks:
  1. Adversarial objects- e.g., printing a logo that looks like a stop sign
  2. Environmental modification- e.g., modifying a sign via stickers or graffiti

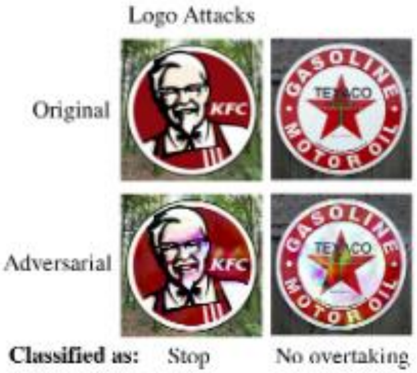


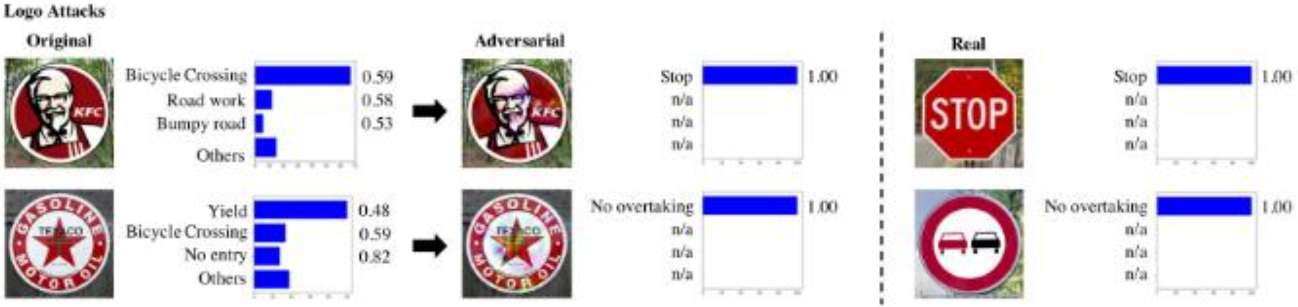


Adversarial Objects

- Modifying the object at an interpretation level.
- Causes misclassification

- Aerospace application:
  - Entry, descent, and landing (EDL) systems support computer assistance.
  - An adversary could modify runway indicators, throwing off the landing.

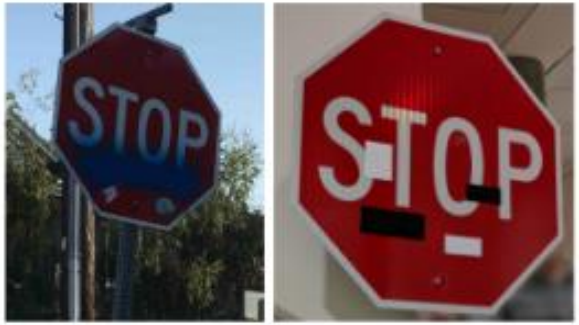




Environmental Modification

- Modifying the object at a physical level
- Causes misclassification or ignores the object
- Simpler due to minimal setup and knowledge of target system

- Aerospace application:
  - Entry, descent, and landing (EDL) systems support computer assistance.
  - An adversary could modify runway indicators, throwing off the landing.



Mitigation and Counters

- Attacks are limited to physical modifications, their effects are less so when compared to direct attacks, e.g., hijacking the navigation system itself.
- Attacks are exploiting the visual aspect of autonomous navigation systems.
- Engineers should not only seek to protect that specific avenue of attack, but also consider integrating a wider range of sensors into their design (i.e., sensor fusion).
- Every additional sensor and integration adds further risk, so additional exploration and consideration is encouraged.

Communications

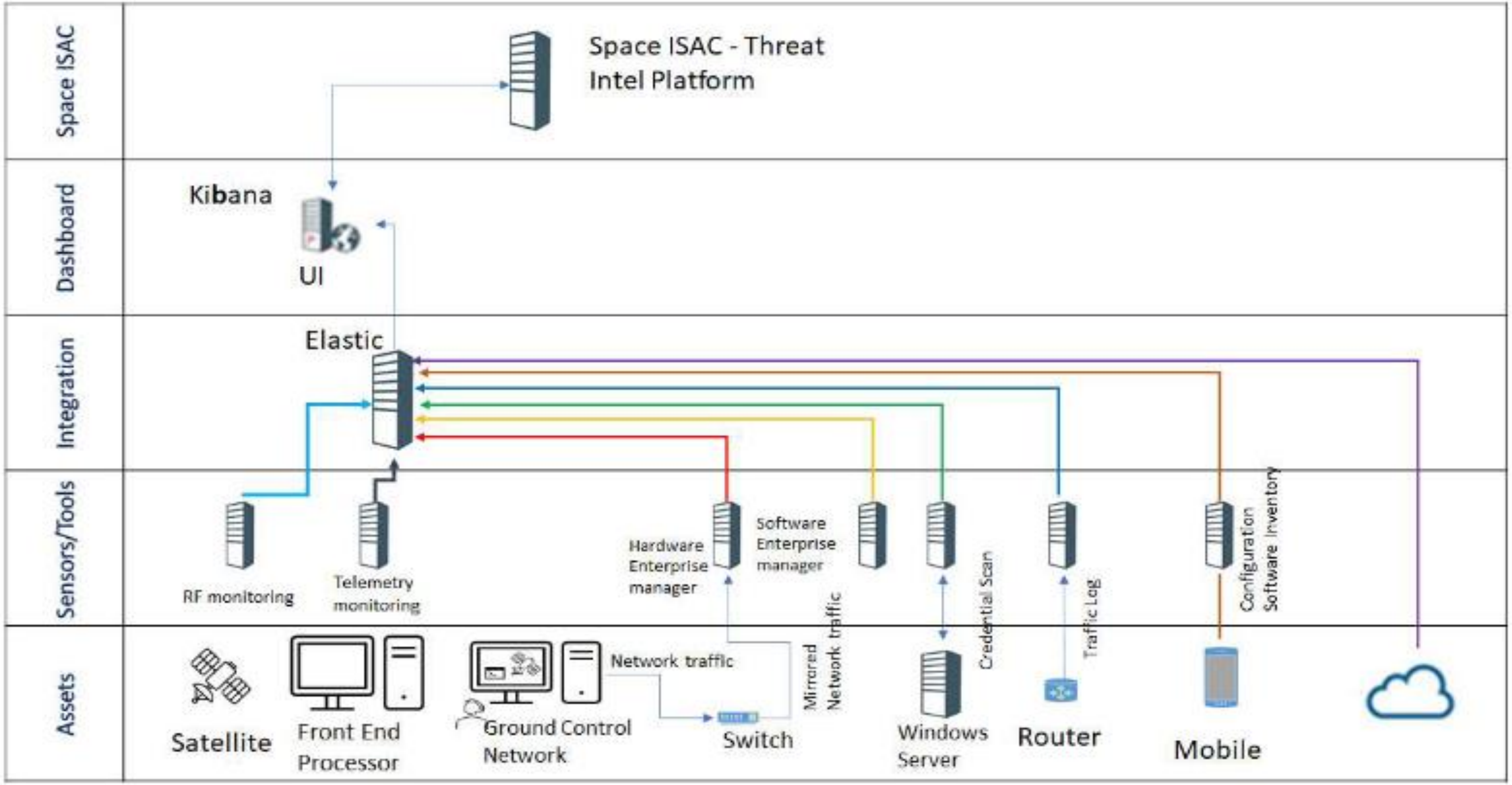
Background → Autonomous Navigation → Communications → Control Systems → Conclusion → Acknowledgements

Defining Communications

- ➢ Communications are a critical component of any interconnected system.
- ➢ The simplest definition of such is simply the process of relaying information from one place to another

- ➢ Potential Attacks:
  1. Eavesdropping
  2. Man in the middle (MITM)
  3. Distributed Denial of Service (DDoS)

Defining Communications



Eavesdropping

- Data integrity of the information transmitted between components requires:
  - Confidentiality
  - Availability
  - Completeness

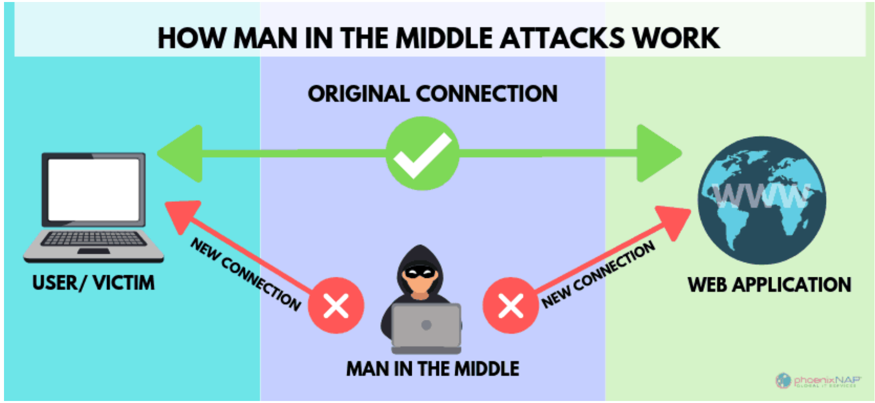
- Eavesdropping= unauthorized interception or sniffing of a conversation, communication, or data transmission

- Aerospace application:
  - Consider a fighter aircraft transmitting target coordinates
  - Should that communication be intercepted, it could have disastrous consequences

Man in the middle (MITM)

- Extension of eavesdropping
- Attacker sits between the communicating parties.
- Can see all sides of the conversation.

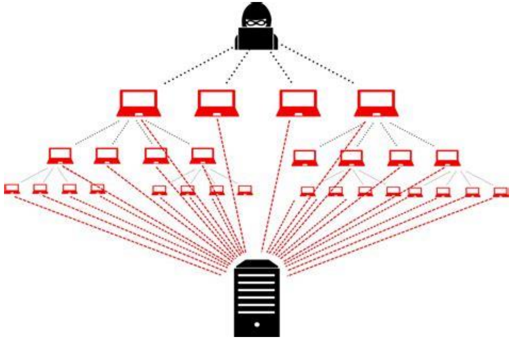
- Aerospace application
  - Consider the same fight jet example
  - MITM could prove even worse as the attacker could feed parties incorrect information or simply block communications.

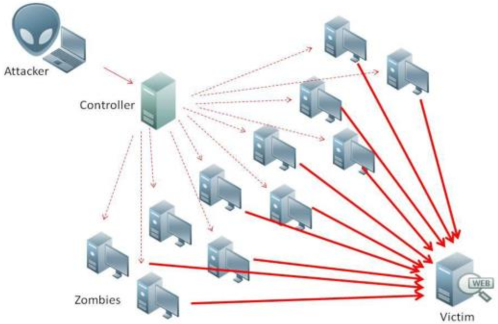


Distributed Denial of Service (DDoS)

- Blocks service using a distributed network. The purpose of the attack is to degrade or block the availability of services to users.
- Botnets (a large number of often hacked devices, united for a single purpose) are commonly used to conduct DDoS attacks against networks and services

- Aerospace application:
  - Flight scheduling software gets DDoS'd and air traffic controllers are no longer able to coordinate flights.
  - Communication itself gets knocked offline





Mitigation and Counters

- Eavesdropping and MITM
  - Rely on obtaining access to the communications.
  - Best defense is to secure the network.
  - Usage of virtual private networks (VPNs), monitoring network traffic, and extensive filtering.

- In contrast, DDoS attacks are harder to counter and are much more prevalent.
  - February 2021: over 100 financial services were targeted by DDoS attacks conducted by a single threat actor
  - The best counter to this kind of attack is to leverage services provided by Content Delivery Networks (CDNs) or specific filtering services like Cloudflare.

- Attacks against communications systems and protocols are the most common simply due to the sheer number of them.
- Given the interconnectivity of aerospace systems, it is paramount that engineers consider how to secure those communications when designing them

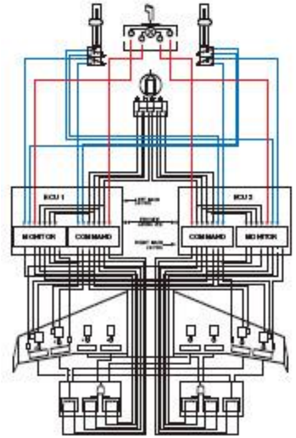
Control Systems

Background | Autonomous Navigation | Communications | **Control Systems** | Conclusion | Acknowledgements

What are Control Systems?

- Control systems broadly refer to systems related to regulating the behavior of the parent system.
- As an example, the flaps on an airplane are part of the control system.
- Often there is an overlap between control systems and communications systems, with the latter conveying information to the former.

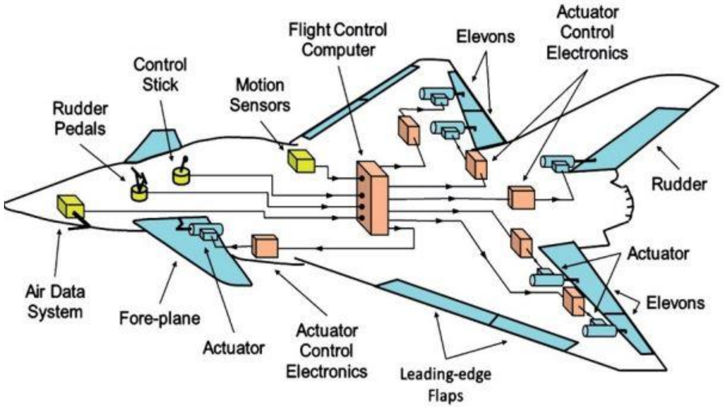
- Potential attacks:
  1. Sensor modification
  2. Fake command data



Sensor Modification

- Exactly what it says: modifying the output of a sensor.

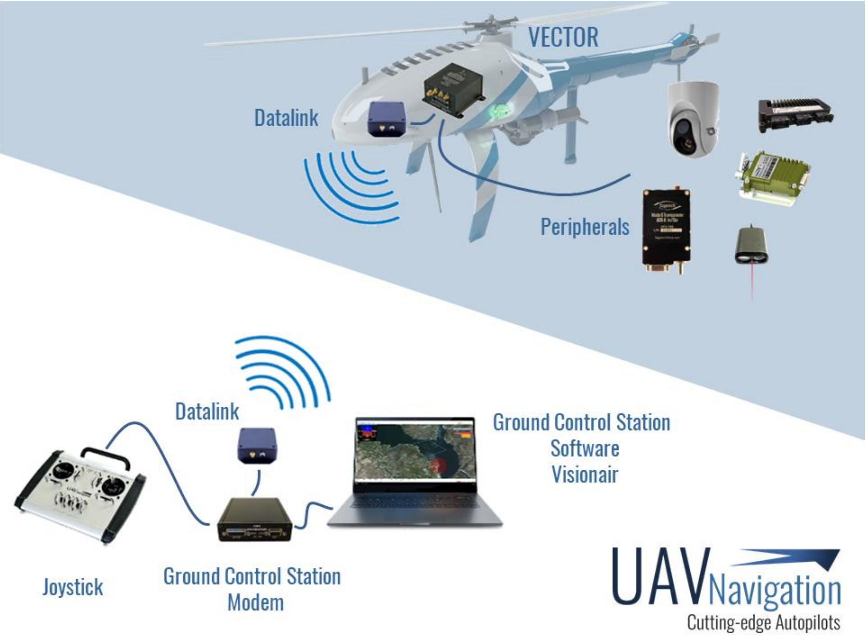
- Aerospace application:
  - Consider an attacker that has control over the angle of attack sensor
  - Attacker could change the sensor to say the aircraft was at an angle of 15 degrees instead of the actual angle of -15 degrees
  - Plane pitches down instead of up
  - This is bad



Fake Command Data

- Instead of the operator’s commands, the attacker inputs their own commands (similar to a MITM attack).

- Aerospace application
  - Consider the case of a commercial quadcopter.
  - The attacker commands the drone to fly forward into the tree, crashing the aircraft
  - Could be even more hazardous around airport



Mitigation and Counters

- Attacks against control systems often involve the attacker gaining access to a system,
- Best counter is to protect said systems,
- Example defenses:
  - Firewalls
  - Restricting system access
  - Additional authentication

- However, assuming an attacker manages to gain control of a control system, there are two main techniques to reduce their effects:
  - Sandboxing- systems are separated from each other
  - Redundancy- information is cross checked with additional sources

Conclusion

Background | Autonomous Navigation | Communications | Control Systems | **Conclusion** | Acknowledgements

What’s Next?

- Cybersecurity is a fast-growing field
  - US Bureau of Labor Statistics predicting a 39% growth between 2019 and 2029 (much higher than the average of 4%)

- Much of the focus in the aerospace sector is on porting existing standards, recommendations, and practices from other fields to aerospace applications
- ***The best way to protect a system is to consider the cybersecurity aspects early in the design phase***

- Aerospace engineers should be exposed to these concepts early on in their career as they learn to implement development processes.

What's Next?

"Publicly available information and policy actions to date have been insufficient to motivate an adequate sense of urgency and ownership of cybersecurity problems afflicting the United States as a nation."

Computer Science and Telecommunications Board; National Research Council

Acknowledgements

Background

Autonomous Navigation

Communications

Control Systems

Conclusion

Acknowledgements

Acknowledgements

The author would like to thank the fellow students Ian Marks and Mollie Johnson for helping proofread the paper, effectively translating incoherent thoughts into concise, human readable concepts.

The author would also like to thank fellow GreyHat club members for their continued efforts in educating university students about cybersecurity using applied problem-solving sessions and real-world examples.

References

1. Yusuf Ogun Kargin, Ashley A. Barnes, O D. Uysal, Olivia J. Pinon-Fischer, Michael G. Balchanos, Dimitri N. Mavris, Melissa Hughes, Jason LaJeunesse, Alexander Karl, and John F. Matlik. "Digital Enterprise Across the Lifecycle," AIAA 2021-0240. AIAA Scitech 2021 Forum. January 2021. doi.org/10.2514/6.2021-0240
2. Sheema Mirchandani and Sam Adhikari. "Aerospace cybersecurity threat vector assessment," AIAA 2020-4116. ASCEND 2020. November 2020. doi.org/10.2514/6.2020-4116
3. HackersOnBoard. (2019, October 5). Black Hat USA 2018 - Last Call for SATCOM Security [Video]. YouTube. https://www.youtube.com/watch?v=CvlCt6a17ho
4. Gregory Falco. "The Vacuum of Space Cyber Security," AIAA 2018-5275. 2018 AIAA SPACE and Astronautics Forum and Exposition. September 2018. doi.org/10.2514/6.2018-5275
5. Jeremy L. Pecharich, Kendra Cook, Wesley Walker, Michel D. Ingham, Kymie Tan and Stephen Watson. "Cyber Risk Management Process for Space Missions," AIAA 2020-4114. ASCEND 2020. November 2020. doi.org/10.2514/6.2020-4114
6. Krishna Sampigethaya. "Aircraft Cyber Security Risk Assessment: Bringing Air Traffic Control and Cyber-Physical Security to the Forefront," AIAA 2019-0061. AIAA Scitech 2019 Forum. January 2019. doi.org/10.2514/6.2019-0061
7. Thomas Llanso and Dallas Pearson. "Achieving Space Mission Resilience to Cyber Attack: Architectural Implications," AIAA 2016-5604. AIAA SPACE 2016. September 2016. doi.org/10.2514/6.2016-5604
8. Information Internetworks Degree Program. College of Computing, Georgia Institute of Technology (2021). Retrieved 18 February 2021, from https://www.cc.gatech.edu/information-internetworks
9. Sitawarin, C., Bhagoji, A. N., Mosenia, A., Chiang, M., & Mittal, P. (2018). Darts: Deceiving autonomous cars with toxic signs. arXiv preprint arXiv:1802.06430.

References

10. Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., ... & Song, D. (2018). Robust physical-world attacks on deep learning visual classification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 1625-1634). DOI: 10.1109/CVPR.2018.00175
11. Theresa Suloway, Scott Kordella and Samuel S. Visner . "An attack-centric viewpoint of the exploitation of commercial space and the steps that need to be taken by space operators to mitigate each stage of a cyber-attack," AIAA 2020-4015. ASCEND 2020. November 2020. doi.org/10.2514/6.2020-4015
12. Kenneth Freeman and Steve Garcia. "A Survey of Cyber Threats and Security Controls Analysis for Urban Air Mobility Environments," AIAA 2021-0660. AIAA Scitech 2021 Forum. January 2021. doi.org/10.2514/6.2021-0660
13. Fs-Isac. (2021, February 09). More than 100 financial services firms hit with ddos extortion attacks. Retrieved February 18, 2021, from https://www.fsisac.com/newsroom/globalleaders
14. Kevin Yang, Jeremy Price, Robert H. Klenke and Matthew Leccadito. "Implementation of a Hierarchical Embedded Cyber Attack Detection system for sUAS Flight Control Systems," AIAA 2021-0038. AIAA Scitech 2021 Forum. January 2021. doi.org/10.2514/6.2021-0038
15. Information Security Analysts. (2021). Retrieved 18 February 2021, from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
16. AEROSPACE CYBERSECURITY AND SAFETY. (2021). Retrieved 18 February 2021, from https://www.aiaa.org/docs/default-source/uploadedfiles/issues-and-advocacy/key-issues/aerospace-cybersecurity-and-safety.pdf?sfvrsn=818c1784_0
17. CYBER THREATS TO THE AEROSPACE AND DEFENSE INDUSTRIES. (2021). Retrieved 18 February 2021, from https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-aerospace.pdf

AMERICAN INSTITUTE OF
AERONAUTICS AND ASTRONAUTICS