2021 ASEE ANNUAL CONFERENCE
Virtual Meeting | July 26–29, 2021 | Pacific Daylight Time
Paper ID #32426

A Program for Managing Unmanned Aircraft Systems in Engineering Education

Col. Richard Melnyk, United States Military Academy

COL Rich Melnyk is an Army Aviator and Associate Professor in the Department of Civil and Mechanical Engineering at the United States Military Academy, West Point. He is also the Director of the Academic Flight program leading both the manned and unmanned aircraft programs. He has a PhD in Aerospace Engineering, a PE in Mechanical Engineering, an MBA in Technology Management and commanded a Battalion at Hunter Army Airfield, Savannah, Georgia.

A Program for Managing Unmanned Aircraft Systems in Engineering Education

ABSTRACT

Unmanned Aircraft Systems (UAS) are an increasingly important aspect of technology. As a result, they have become a very important tool in engineering education for a variety of disciplines. While many physical laboratories or training aids have regulatory and administrative requirements, the considerations related to UAS are multifaceted and include Federal Aviation Regulations, airspace requirements, and privacy considerations. Furthermore, UAS pose a physical hazard that must be taken into account to protect students, staff, faculty, and bystanders. Finally, some systems could potentially present a cybersecurity risk as evidenced by recent additions to the National Defense Authorization Act (NDAA). The purpose of this paper is to explain and document an academic flight program at the United States Military Academy that outlines the personnel structure associated with running the program, the procedures put in place to manage physical and regulatory risk, and the training and approval process associated with UAS operations.

Introduction

Unmanned Aircraft Systems (UAS) come in a variety of shapes and sizes and include both fixed and rotary-wing platforms. The system refers to the aerial vehicle, the controller, and the means to transmit data between the two. It is difficult to find a technology that has had such an explosive growth in the last ten years. In fact, the FAA predicts that the number of slightly larger UAS; those over 55 lbs, could exceed the number of general aviation aircraft by the mid-2030s. [1] It is important that academia stay ahead of any emerging technology to help develop innovative graduates and provide the appropriate knowledge and skills to succeed in industry. It is no surprise then that academic institutions, and STEM programs in particular, are incorporating UAS into their education. As with any technology, this can present both opportunities and challenges. This paper will outline the growth of the UAS industry and demonstrate the need for partnerships between academia and the industry. Then, it will discuss the safety, regulatory, and societal challenges associated with UAS usage. Finally, the paper will show several programs using UAS in education and demonstrate a structure and process for safely and effectively incorporating UAS into education. The focus of this paper is on post-secondary education, but the principles could be applied at other levels as well.

Literature Review

UAS have already experienced a tremendous amount of growth in the last two decades and will continue to do so in the near future, according to industry estimates. The FAA forecast from 2019 expected a doubling of the commercial fleet in five years by 2024. [2] It is important to

note that this refers to commercial systems, and not recreational use which indicates that there are financial implications for the economy. The same report shows that there were over 385,000 commercial UAS and over 162,000 remote pilot (Part 107) certifications at the end of the 2019 period. [2]

An article on UAS challenges states that there are several dozen countries with active UAS programs and that while military applications drove early development, the civil market is the fastest growth sector now. [3] The advocacy group Association of Unmanned Vehicle Systems International (AUVSI) predicted a market of more than $13 billion in the first three years of full UAS integration in the NAS. [4] Additionally, a Congressional Research report predicted an annual $14 billion industry by 2025. [5] Clearly, UAS have commercial as well military implications and will be important to world economies.

If unmanned aircraft are a clearly growing market and segment of technology, then it is important that academic institutions remain engaged in this space and help drive innovation. Graduates of leading institutions must be prepared to lead change in this dynamic and expanding area. In addition to providing students with vital tools, UAS present interesting opportunities for institutes of higher learning because of their interdisciplinary nature and complexity. The National Academies of Engineering encourage institutions to offer more interdisciplinary engineering education to better prepare students for the reality of the world they face in practice. [6], [7]

For example, an article by Chayoga describes an effort between the Naval Postgraduate School, the Defense Advanced Research Project Agency (DARPA) and the Georgia Tech Research Institute (GTRI) to better understand swarming UAVs. [8] The article describes the advantages of collaboration between the military, and academia to advance the state of unmanned swarming technology.

Another example is the robust UAS program at the University of Alaska, Fairbanks. This is one of ten locations designated by the FAA to spearhead specific technologies related to UAS, according to Hatfield, et.al.[1] The program is able to advance beyond visual line of sight technology, which is critical if UAS are eventually able to operate beyond a very small area near the operator or with multiple operators able to observe the air vehicle. In this role, the university is able to make contributions to UAS technology that will benefit society as a whole.

Finally, UAS have a tremendous capability to bring interdisciplinary, project-based learning to engineering programs. Authors from the University of Michigan describe projects that leverage UAS technology and incorporate elements of Aerospace education, and Robotics and cover topics ranging from structures, aerodynamics, propulsion, sensors, controls, software, processing, and design. [9] The advantage is that the systems are relatively affordable, scalable, and can be modified to support certain projects.

These are just a few examples of the use of UAS in academic programs. A paper in the Research of Higher Education Journal provides a list of programs offering a bachelor of science degree related to UAS. [10] The schools include Embry-Riddle Aeronautical University, Indiana State University, Indiana State University, Kansas State University – Polytechnic, Letourneau

University, Lewis University, Purdue University, and the University of North Dakota. Another article cited programs at Cochise College and Hinds Community College. [11] Clearly, this is a growing area of academia as these programs would not have existed 20 years ago.

Discussion

While there are certainly benefits of incorporating UAS into engineering education, the practice is not without significant challenges. President Obama originally directed the FAA to develop a plan for full integration of UAS into the National Airspace System (NAS) by 2015. [12] The goal was to treat UAS like their manned counterparts in terms of access and procedures in the NAS. However, as early as 2007 the FAA only allowed commercial users access to the NAS through a Certificate of Authorization (COA) system. [12] The process was lengthy in nature and was specific to a system, location, and activity so certainly did not allow for full freedom and access. Recent changes in the Federal Aviation Regulations, Part 107, allow for less restrictive access for educational users of systems less than 55 pounds. [13] However, the situation still falls well short of full and seamless integration.

In addition to the regulatory hurdles involved in UAS operations, current or potential educational users must also consider factors such as safety, privacy, and cybersecurity before implementing programs. For example, the previously cited article by Donato, et, al, highlights specific physical risks associated with UAS usage. [9] These include loss of control, cutting hazards from spinning rotors, and flyaway situations. Some of the physical hazards or as or less severe than other physical hazards associated with engineering education. For example, shops in many engineering programs feature large power tools such as mills or lathes. Others have chemical or electrical hazards. However, many of these hazards are in fixed locations that feature some level of supervision and are not new so have safety procedures in place. UAS, on the other hand, are often operated outdoors in remote locations. They are new to many programs so there may not be established safety procedures in place. More importantly, most staff and faculty did not have UAS programs during their education and training so are new to the safety protocols as well.

Beyond the immediate physical risk, UAS are more mobile than other applications so have the ability to affect a larger area. While many machines and pieces of lab equipment associated with engineering programs may pose a risk, that risk is contained to a specific lab space that can be tightly controlled. An air vehicle that loses data link and departs the intended flying area could cause harm to people or property across an entire campus or even beyond the limits of the academic institution. A vehicle that departs the area could also impact air traffic and other bystanders. As a result of these factors, developing physical safety procedures in any new or developing UAS educational program is critical.

Another unique concern posed by UAS in the public sector is that of privacy. While UAS do not necessarily have the ability to observe or conduct surveillance differently than manned aircraft, the fact that they can do so at a fraction of a cost and often with less overhead and without as much notice can be problematic. Institutes of higher learning are by nature public places, but students and the surrounding communities have some expectation of not being monitored and

surveilled at all times without their knowledge. [3] Ogan [11] highlights these privacy concerns with regards to the large amount of information UAS can collect and store on databases, potentially infringing on people's rights. In many instances, laws are not behind or insufficient to cover this new technology.

Beyond the concerns that UAS pose to the public, their use and employment can create hazards for the user in the form of cybersecurity threats. This is a real threat and was acknowledged in law under the National Defense Authorization Act for 2020. Under Section 848, the Department of Defense was prohibited from purchasing or operating unmanned systems with specific component manufactured in a specified country due to cybersecurity concerns. [14] These threats range from specific targeting or spoofing of the data link signal between the air vehicle and controller, the capture and use of the data extracted from the system, and cybersecurity threats embedded in the software used to control commercial-off-the-shelf UAS. [15] Although the NDAA is focused on military use of commercial systems, the threat to private and commercial users has also been documented. [16] In fact, smaller systems commonly in use by hobbyist, private, or educational users are perhaps more vulnerable to attacks since their size and weight often precludes the inclusion of encryption or defense measures. [17]

Model of a Small UAS (sUAS) Program

For educational institutions that choose to include UAS in their curriculum, it is vital that they develop a system to take advantage of the benefits UAS offer, while simultaneously mitigating the physical, social, and cybersecurity risks outlined above. The purpose of this next section is to provide an example of one such program as a proposed model. The proposed model from the United States Military Academy is by no means unique. For example, Rainier [18] outlines a UAS program in place at North Carolina State University. The program differentiates between hobby use, routine research, and more experimental use and places procedures in place for all three. The previously discussed article by Ogan also emphasizes the need for an education program at institutions that plan to employ UAS focused on topics such as safety, flight skills, and judgment. [11]

The program at the Academy was developed incrementally to address several challenges that various academic departments encountered during a period from roughly 2016-2017. Because the institution is both an academic and military one, it encountered several obstacles to UAS operations. Some were unique to the military status and will not be addressed in as much detail, but all of the obstacles could apply to any academic institution.

During the time period in question, there were four primary academic departments attempting to use sUAS for research, capstone projects, or to directly support classroom instruction. As obstacles to operations surfaced, each department had a representative attempting to navigate the various requirements. This was an inefficient approach that led to duplication and, in some cases, contradiction of effort. Therefore, the institution appointed a single person responsible for sUAS efforts. The institution already had a manned flight program for academic purposes, so it was logical to expand that person's responsibilities to include unmanned operations as well.

This individual became the Director, Academic Flight Program or DAFP. The DAFP has a flight background and was already a licensed pilot and remote pilot. In addition, the DAFP has an aeronautical engineering background so was able to understand both the regulatory as well as physical requirements associated with air vehicles and their design.

The next step was to establish procedures and a structure for training, approval, and operations of sUAS. The various stakeholders collaborated on a set of standard operating procedures (SOP). The stakeholders included interested academic departments, campus security, manned aircraft operators, cybersecurity experts, and airspace managers. This fairly extensive document established various roles and responsibilities, training requirements, developed the airworthiness process, established the format and elements of a sUAS test plan, outlined cybersecurity mitigation measures, and documented local flight procedures.

The SOP established several roles and an overall management structure, which is depicted in Figure 1. Among those was a Program Manager, Test Director, Officer in Charge, Flight Operator, and Safety Observer. The 2nd Aviation (2nd AVN) block represents an organization that operates rotary-wing helicopter on and around the campus so were stakeholders due to shared airspace requirements.

In addition to the SOP, the program established an aviation procedures guide or APG, that is a simple one-page document that test directors and operators use just before, during, and immediately after sUAS operations. It features important phone numbers, radio frequencies, operating areas, airspace rules, and emergency procedures for quick reference.

The Program Manager is typically the individual from the academic department that coordinates the sUAS usage for academic purposes. He or she can be a capstone project advisor, course director, research lead, or center director. The Test Director can also be the program manager, but is more focused on developing the actual test plan and ensuring that all of the requirements in the next section are met and that the operators and observers receive proper training. The Officer in Charge (OIC) is the on-site individual for the safe conduct of flight operations and testing. The operators are trained and employ the various sUAS associated with their academic operations and employ safety observers as necessary to ensure deconfliction with other traffic is maintained.

The Safety Review Board (SRB) is a group consisting of the appropriate stakeholders for each project, but is always chaired by the DAFP. It is convened whenever a program manager has a test proposal for review. The purpose of the board is to have an open discussion about the proposed test plan, airworthiness documents, and risk mitigation measures. All of the stakeholders can comment and make recommendations with the ultimate goal of ensuring a safe and effective test.

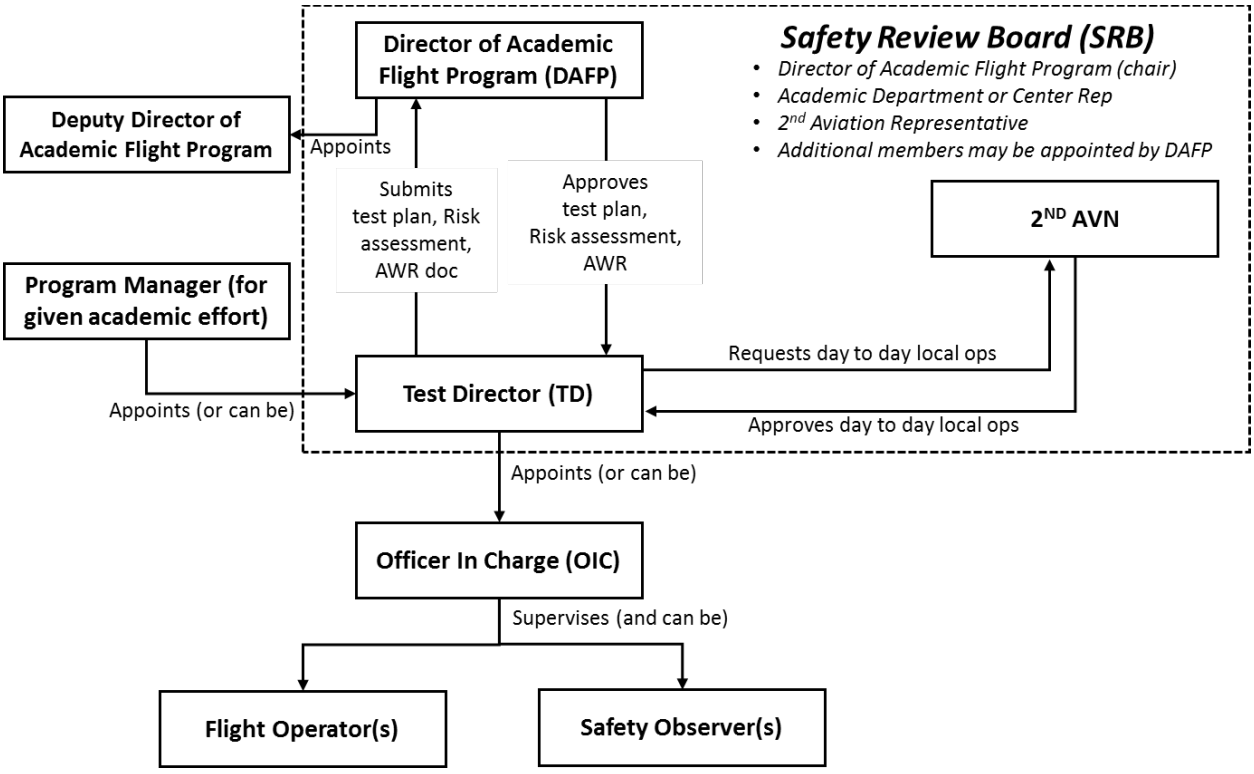

Figure 1: sUAS Approval System and Structure

The DAFP conducts and documents two training events annually, at a minimum. The first is focused on OICs, Flight Operators, and Safety Observers. This training covers safety procedures to include environmental impacts on UAS, proper observation and deconfliction, avoidance of personnel on the ground, and airspace rules. This training is similar in nature to the FAA training to obtain a remote pilot certificate. The institution does not require Part 107 licensure; however, due to it's military status. The other documented training is more procedural in nature for the Program Managers and Test Directors. This training covers the elements of the SOP, approval process, and risk mitigation strategies.

Airworthiness is a requirement on military organizations analogous to certification in the civilian community. It is a process to determine if the system is capable to operating safely under the expected flight conditions. The airworthiness approval document captures the physical characteristics of the air vehicle to include dimensions, weight, and performance. It also focuses on the data links and control modes to ensure proper redundancy and failsafe systems are in place. Once approved, the airworthiness release (AWR) is valid for two years and is a required document to operate in the NAS.

The test plan is a detailed document that covers several topics. First, it outlines the objectives of any flight tests. The plan also summarizes the system configuration and data communications architecture so does have some redundancy with the AWR. However, the test plan offers a much more detailed account of how the system will be employed, where it will operate, and details all of the measures put in place to ensure safety. These include geofences, observation plans, restricting access to the test site, and airspace deconfliction. In addition, the test plan covers the

required personnel and spectrum management. Finally, the test plan features a pre-accident plan with detailed steps to take in the event an incident occurs. An incident can range from loss of vehicle control, a flyaway situation, injury to test personnel or bystanders, or damage to property.

The cybersecurity risk mitigation strategies became an appendix to the original SOP, as cybersecurity concerns grew in importance. The measures put in place were primarily to prevent threats to the institution's network and loss or compromise of data or imagery. There are several measures outlined below.

First, any piece of information technology related to sUAS use remains off the local network and is considered a standalone device. This includes laptops, tablets, or phones that are used as controllers or to process data. This is done to prevent malware associated with the system software from affecting the institution's networks. If data must be moved to the network for analysis, it is first scanned with the appropriate software on a standalone system.

As another layer of safety, any imagery devices are kept covered and off when not in use. When in use, part of the test plan is to ensure that any places or activities that are captured in imagery are not sensitive in nature. Operators also make every attempt to avoid capturing imagery of facial areas, particularly for bystanders. These techniques are used to avoid any sensitive imagery or imagery of people from being uploaded to servers in a third-party location where it could be exploited.

Cybersecurity is not the only security consideration. UAS can be used to conduct unauthorized physical attacks or surveillance and could be a threat to the institution. As a result, part of the APG is for the test director to alert the security office on the installation prior to any sUAS operations. This communication includes the times, locations, and operating parameters of any academic sUAS. This plan is logged into the security record so any reports of sUAS usage that does not match the academic proposals can be investigated and dealt with accordingly.

Another tool the program uses is a formal risk assessment. This table helps the test director identify, assess, and control various hazards associated with the sUAS project. An example of one portion of the form is below in Figure 2. This tool is primarily focused on physical risk and requires the test director to identify, assess, and mitigate each hazard posed by UAS operations. Since none of the sUAS operations are an absolute necessity, all residual risk must be mitigated to a Low level.

5. SUBTASK	6. HAZARDS	7. INITIAL RISK LEVEL	8. CONTROLS	9. RESIDUAL RISK LEVEL	10. HOW TO IMPLEMENT	11. HOW TO SUPERVISE (WHO)	12. WAS CONTROL EFFEC-TIVE?
sUAS Flight Test	Mid-Air Collision with Non-Participating Aircraft	L	(1) Fly SUAS in controlled airspace (restricted or NOTAM'd COA); (2) Operating protocols to ensure aircraft remains in approved area. (3) Cease test if non-participant approaches.	L	(1) Restricted Airspace or COA, (2) Loss of Link + visual or Loss of Link + Loss of GPS + Geofence.	(1) TD coordinates airspace, (2) OIC briefs boundaries (3) Operator Preflight, (4) all visual SA	
sUAS Flight Test	sUAS Impacts Civilian Personnel / Property	M	(1) Operations limited to controlled areas (range, installation, etc...), (2) Operating protocols to ensure aircraft remains in approved area. (3) Position monitored real-time. (4) Safety monitors.	L	(1) Controlled area away from civilians, (2) Failsafe protocols. (3) Visual track. (4) safety monitor	(1) TD coordinates area (2) OIC briefs boundaries (3) Operator Preflight, (4) all visual SA	

Figure 2: Risk Assessment Matrix

Conclusions

The program outlined above has been in effect for approximately four years with successful outcomes. Each year, anywhere from seven to twelve distinct projects occur that engage students from up to six different academic departments. The institution has conducted sUAS operations in Alaska, Arizona, Georgia, Virginia, and New York with no incidents or accidents.

While the military nature of the institution creates some aspects not applicable to other academic entities, there are a lot of components that other programs could leverage. First, it has been essential to have one individual designated as the primary coordinator and approval authority for sUAS operations. This individual should have an aviation background to better understand airspace, weather, and the regulatory environment. At a minimum, the coordinator should be a remote pilot but it is better if the person is a certified pilot. This person should also have experience operating sUAS and an engineering or STEM background is helpful.

In addition, organizing a working group or sUAS committee is helpful as well. All of the sUAS users can bring their experience, equipment, and knowledge to the group and help prevent mishaps due to lack of training or knowledge. This group can form the safety review board that help the director review test plans and mitigate risk. The group members also learn from previous test plans and can share equipment-specific information and expertise.

A training program that is periodic, standardized, and documented is vital. Using the FAA training for remote pilot certification under Part 107 is very helpful, especially if the institution has a certified flight instructor (CFI) that can sign off on the training. However, this training is minimal and should be augmented with more detailed local procedures and safety considerations.

Having a set of standardized operating procedures streamlines operations and prevents confusion. In addition, the APG provides an easy to use format for operators during the actual conduct of testing. This practice can be incorporated at any institution for ease of operation and to ensure that any mishaps are quickly contained and addressed.

Another recommendation that the program is beginning to implement is to standardize the sUAS fleet across the institution to the extent possible. While there are many different sUAS systems, the users found that 2-3 multi-copters and 1-2 fixed-wing platforms could perform most of the

required testing and research. Standardizing the fleet simplifies purchases, training, and the sustainment of these systems.

Each institution will have to weigh the cybersecurity risks outlined above when developing a plan to address them. As a military organization, the risks were deemed to have greater consequences, so the mitigation plan is fairly conservative. However, civilian counterparts may find these procedures cumbersome and not worth the potential risks. A recent interagency report on sUAS security recommends several steps that were also outlined in this paper. These include developing security procedures in advance, educating the community on use and threats of sUAS, and involving law enforcement in the process as well. [19]

Summary

Overall, the United States Military Academy maintains a robust, safe, and growing sUAS program. The use of these systems to support various STEM projects and research is vital for the academic growth of the faculty and students. However, the benefits of using these systems must be balanced with a methodical and deliberate risk mitigation program.

Works Cited

[1] M. Hatfield, C. Cahill, P. Webley, J. Garron, and R. Beltran, "Integration of Unmanned Aircraft Systems into the National Airspace System-Efforts by the University of Alaska to support the FAA/NASA UAS Traffic Management Program," *Remote Sens.*, vol. 12, no. 19, 2020, doi: 10.3390/RS12193112.

[2] Federal Aviation Administration, "FAA Aerospace Forecasts Fiscal Years 2020-2040," 2020.

[3] R. L. Finn and D. Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications," *Comput. Law Secur. Rev.*, vol. 28, no. 2, pp. 184–194, 2012, doi: 10.1016/j.clsr.2012.01.005.

[4] Association of Unmanned Vehicle Systems Internation, "The Economic Impact of Unmanned Aircraft Systems Integration in the United States," 2013.

[5] B. Canis, "Unmanned Aircraft Systems (UAS): Commercial Outlook for a New Industry," 2015.

[6] Natrional Academy of Engineering, "Educating the Engineer of 2020: Adapting Engineering Education to the New Century," National Academies Press, 2020. doi: 10.17226/11338.

[7] National Academy of Engineering, *Educating Engineers: Preparing 21st Century Leaders in the Context of New Modes of Learning*. Teh National Academies Press, 2013.

[8] J. Chagoya, "Calhoun: The NPS Institutional Archive NPS, Academic Partners Take to the Skies in First-Ever UAV Swarm Dogfight." Accessed: Oct. 21, 2020. [Online]. Available: http://hdl.handle.net/10945/51935.

[9] P. F. A. Di Donato, P. E. Gaskell, and E. M. Atkins, "Small Unmanned Aircraft Systems for Project-Based Engineering Education," 2017, doi: 10.2514/6.2017-1377.

[10] C. T. Kendall and R. C. Rhett Yates, "Assessment of unmanned aerial systems programs in collegiate aviation." Accessed: Oct. 21, 2020. [Online]. Available: http://www.aabri.com/copyright.html.

[11] R. T. Ogan, "Educating the next generation engineers for Unmanned Aircraft Systems applications and challenges," *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2015-June, no. June, pp. 1–7, 2015, doi: 10.1109/SECON.2015.7132931.

[12] A. C. Watts, V. G. Ambrosia, and E. A. Hinkley, "Unmanned aircraft systems in remote sensing and scientific research: Classification and considerations of use," *Remote Sens.*, vol. 4, no. 6, pp. 1671–1692, 2012, doi: 10.3390/rs4061671.

[13] Federal Aviation Administration, "Unmanned Aircraft Systems - Educational Users." https://www.faa.gov/uas/educational_users/ (accessed Nov. 17, 2020).

[14] 116 U.S. Congress, *National Defense Authorization Act for Fiscal Year 2020 Public Law 116–92*. 2019, pp. 1–1120.

[15] K. Best *et al.*, *How to Analyze the Cyber Threat from Drones: Background, Analysis*

Frameworks, and Analysis Tools. 2020.

[16] J. Valente and A. A. Cardenas, “Understanding security threats in consumer drones through the lens of the discovery quadcopter family,” *IoT S P 2017 - Proc. 2017 Work. Internet Things Secur. Privacy, co-located with CCS 2017*, no. Ii, pp. 31–36, 2017, doi: 10.1145/3139937.3139943.

[17] C. G. Leela Krishna and R. Murphy, “A review on cybersecurity vulnerabilities for unmanned aerial vehicles,” *Auvsi Xponential 2018*, pp. 0–5, 2018.

[18] D. Rainer, “Code corner,” *Chem. Heal. Saf.*, vol. 12, no. 4, pp. 39–40, 2005, doi: 10.1016/j.chs.2005.05.008.

[19] Interagency Security Committee, “Protecting Against The Threat of Unmanned Aircraft Systems,” 2020.