The Vulnerable Architecture of Unmanned Aerial Systems: Mapping and Mitigating Cyberattack Threats

Gabriel Boulianne Gobeil and Liran Antebi

Unmanned aerial vehicles (UAVs), frequently referred to as drones, have become an essential and dominant tool of advanced military forces, especially those engaged in counterinsurgency, where they are used mostly for intelligence, surveillance, and reconnaissance (ISR) missions as well as for different kinds of operations involving targeted strikes. As the usage of unmanned systems for military purposes increases, so does their vulnerability to cyberattacks, the result of their growing dependence on computer-based systems. The article maps the different kinds of plausible cyberattacks targeting UAV systems, assesses their odds, and offers some guidelines for a recommended policy for the users of those systems.

Keywords: Cyberattacks, cybersecurity, military technology, unmanned aerial vehicles (UAVs)

Gabriel Boulianne Gobeil is a B.C.L./LL.B. Candidate at the Faculty of Law, McGill University. He has an MA in Security and Diplomacy from Tel Aviv University and an MA in Political Science from the University of Ottawa. Dr. Liran Antebi is a research fellow at the INSS, a lecturer in the academia and a member of IPRAW (The International Panel on the Regulation of Autonomous Weapons).The authors would like to thank Mr. Niv David for helpful comments on an earlier draft of this article.

Introduction

The role played by unmanned aerial vehicles (UAVs) in contemporary warfare has grown since they were first widely deployed in the early 1970s.[1] Primarily used by the US military, Daniel L. Byman even refers to them as Washington's "weapon of choice."[2] Their unmanned nature, enabling the projection of force without the need to send soldiers in physical harm's way, has rendered them quite appealing to other actors.[3] However, the feature that enables them to be operated from a distance potentially represents a double-edged sword, as it leaves the technology particularly vulnerable to cyber threats. Although the fact that UAVs are highly computerized and gives them the advantage of not requiring human operators in the cockpit, this characteristic also allows hackers to exploit UAV systems. This paper calls attention to these vulnerabilities; by being aware of the system's vulnerabilities, the UAV user is more likely to be prepared to prevent and protect against potential cyberattacks.

This paper begins by examining the various components involved in the broader operation of a UAV. By deconstructing the system, we can understand the UAV's vulnerability to potential cyber intrusion. Although hackers seek to gain access to the system itself, they do so by using at least one component as a point of entry into the larger system. The paper then highlights cyberattacks targeting UAV systems, which have either been recorded in the past or are technologically plausible. While some cyberattacks may be performed by individual hackers, more sophisticated attacks require advanced abilities and can only be performed by actors possessing greater resources, such as terrorist organizations, companies, or even states. Yet, as the article will show, even the least sophisticated cyberattacks can pose a serious risk to the user of UAVs. The paper concludes by offering policy recommendations to mitigate the threats stemming from these cyberattacks.

1 Ty McCormick, "Lethal Autonomy," *Foreign Policy* 204 (2013): 18–19.

2 Daniel L. Byman, "Why Drones Work: The Case for Washington's Weapon of Choice," Brookings Institution, June 17, 2013, accessed June 5, 2017, https://www.brookings.edu/articles/why-drones-work-the-case-for-washingtons-weapon-of-choice/.

3 See Sarah Kreps, *Drones: What Everyone Needs to Know* (Oxford: Oxford University Press, 2016), p. 60.

Research Questions and Structure of the Paper

The current literature on unmanned aerial vehicles (UAVs), which has burgeoned over the last five years, has investigated several important questions, especially related to the use of UAVs in targeted killing campaigns.[4] In particular, a significant portion of this literature has attempted to determine whether UAV strikes used to decimate terrorist organizations are strategically effective.[5] Additional work has examined whether the ways in which UAVs have been employed thus far comply with international legal and ethical standards, in an attempt to understand the various implications of the technology's different uses.[6]

Scholars, however, have not offered any extensive account of the limitations that are inherent to the technical architecture of UAVs, except for cursorily acknowledging that UAVs are susceptible to cyberattacks.[7] Thus, the main objective of this paper is to fill this void and, in doing so, contribute to bringing the academic literature on UAVs into conversation with current work in an emerging area of research in security studies, namely cybersecurity.

---

4 Often referred to as drones, UAVs are not actually unmanned, as a human operator controls them from a distance. Hence, a more accurate designation would be "remotely controlled aircrafts." However, given that this is not commonly used in the literature, this paper uses the more widely recognized term UAV.

5 Stephanie Carvin, "The Trouble with Targeted Killing," *Security Studies* 21 (2012); Matt Frankel, "The ABCs of HVT: Key Lessons from High Value Targeting Campaigns Against Insurgents and Terrorists," *Studies in Conflict and Terrorism* 34 (2011); Jenna Jordan, "Attacking the Leader, Missing the Mark: Why Terrorist Groups Survive Decapitation Strikes," *International Security* 38, no. 4 (2014); Avery Plaw, "Terminating Terror: The Legality, Ethics and Effectiveness of Targeting Terrorists," *Theoria: A Journal of Social and Political Theory* 114 (2007); Bryan C. Price, "Targeting Top Terrorists: How Leadership Decapitation Contributes to Counterterrorism," *International Security* 36, no. 4 (2012).

6 Grégoire Chamayou, *Théorie du drone* (Paris : La Fabrique éditions, 2013); John Krag and Sarah Krebs, *Drone Warfare* (Cambridge: Polity, 2014).

7 Kagu and Kreps, *Drone Warfare*, pp. 44–45; Kreps, *Drones*, p. 39; Peter W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin, 2009), p. 253; Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), pp. 314–315; Robert O. Work and Shawn Brimley, *20YY: Preparing for War in the Robotic Age* (Washington, DC: Center for a New American Security, 2014), p. 23, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_20YY_WorkBrimley.pdf.

As such, this paper is divided in three parts. The **first** section explains how UAVs and the larger system to which they are integral work. This discussion represents a necessary step to addressing the paper's main research question, which is posed in the **second** section**:** What are the vulnerabilities that stem from the way UAVs work? Having identified these vulnerabilities, the **third** part of the paper tackles another important question: How can the threats posed by these vulnerabilities be mitigated? In identifying the cyber vulnerabilities of UAVs, the broader objective of this paper is to understand how the architecture of the UAV's technology makes it susceptible to exploitation by diverse cyberattacks so that accessible policy recommendations can be offered to help reduce the cyber risks involved in using UAVs.

The scope of this paper is limited to UAVs classified by the US army as "Group 4" and "Group 5."[8] These two groups include UAVs that weigh above 1320 pounds and can fly at altitudes of *up to* 18000 feet for those in Group 4 and *above* 18000 feet for those in Group 5. UAVs such as the Predator, the Reaper, and the Global Hawk are all currently used by the US army and fall under these two categories, and therefore are the focus of this paper. Smaller UAVs, which require a direct line of sight and whose architecture is therefore distinct from those of Group 4 and 5, will not be discussed in this paper. This omission is not because UAVs of Groups 1 to 3 cannot be hacked. As opposed to UAVs of Groups 4 and 5 that are used strategically, UAVs from Groups 1 to 3 tend to fulfill tactical purposes, as is the case of the Raven, for instance. Thus, devoting resources to defend them against a wide range of cyberattacks likely would be ineffective in terms of cost because doing so could diminish the effectiveness of the UAVs, which stems from their being light, portable, relatively inexpensive, and not too sophisticated. In other words, by choosing to use a Raven, the user willingly opts for an UAV designed to provide certain tactical advantages that would be undermined by the addition of a complex defense mechanism.

Moreover, this paper focuses exclusively on UAVs from Groups 4 and 5 because, unlike their counterparts from Groups 1 to 3, they are highly computerized and made of even more sub-systems, rendering them particularly vulnerable to cyberattacks. UAVs classified as Groups 4 and 5 also bear higher risk given that they can be equipped with missiles and deployed for

8 United States Army, ""Eyes of the Army": U.S. Army Roadmap for Unmanned Aircraft Systems 2010-2035," (2010): 12.

targeted killing missions, unlike UAVs classified as Groups 1 to 3. Moreover, more advanced weapons platforms warrant special attention since their vulnerabilities can result in greater financial and security risk, when compared to the risk imposition of less advanced systems such as UAVs from Groups 1 to 3. The addition of defense mechanism to UAVs from Groups 4 to 5 will inevitably come at the price of reducing their effectiveness, such as when the encryption of a satellite datalink to secure the transmission of sensitive information concomitantly forces the user to spend more time decrypting that information; yet, these costs are outweighed by the advantages they bring to the overall security of the system.

In the technological interactivity of war, the advent of UAVs has offered important advantages. One obvious benefit is removing soldiers from the physical battlefield. Additionally, their technological complexity relies on computer networks—often referred to as "unmanned aerial systems"[9]—rendering their reproduction technically burdensome.[10] As relatively sophisticated technologies, UAVs necessitate substantial resources and knowledge to build and operate. Furthermore, their airborne platform, flying at relatively high altitudes, makes them more difficult to attack via kinetic means, and thus demand more advanced capabilities to take them down. For these reasons, actors seeking to attack them are likely to look for alternatives in the cyber world. Cyberattacks present a likely substitute for kinetic attacks because the architecture of UAVs—that is, their reliance on computer networks—makes them inherently vulnerable to hackers seeking to exploit the technology's limitations. Therefore, it becomes important for the user of UAVs to understand how the technology can be exploited so that the threats that arise can ultimately be mitigated. These interactions between users and hackers of UAVs deserve special attention—both within national security and academic circles—a task to which this paper is devoted.

Three Central Components of the UAV System: How UAVs Work?

UAVs are part of a complex system that consists of several interconnected and integrated elements, all of which are needed for the UAV to conduct an intelligence, surveillance, and reconnaissance (ISR) mission, or to locate

9 Kagu and Kreps, *Drone Warfare*, pp. 49–50.

10 Kreps, *Drones*, p. 63.

and hit its target. Although this system contains several parts, this paper focuses exclusively on the following three components: (1) a military base or a command and control center from where the operator controls the UAV; (2) a satellite that connects the UAV to the command and control center; and (3) the UAV or aircraft itself.[11] These components are based on the US Air Force Road Map, which regards Predators and Reapers as more than individual aircrafts, and as complete "systems" in and of themselves.[12]

Another ground base, called a launch-and-recovery station, is also essential for the UAV to take off and land before and after missions. Such stations, which may also be an aircraft carrier from where the UAV is refueled and stored when not in operation, are also a part of the system. They are not discussed here, however, because they are less likely to be targeted by *cyber*attacks as opposed to *kinetic* attacks.

Moreover, each part of the UAV system contains smaller technologies that may be subject to cyberattacks. For instance, the command and control center is equipped with several communication technologies that enable communication with the UAV, each of which can be individually targeted by hackers. As is briefly addressed below, missiles or payloads carried by UAVs can also be the object of cyberattacks. That said, the countless ways in which the myriad parts within the whole system can be hacked is beyond this paper's scope. Conceiving of UAV systems as being made of the abovementioned three components is therefore sufficient to enable the reader to identify the main points of entry into the UAV in the event of a cyberattack.

---

11 See United States Air Force, "MQ-9 Reaper." Refer to Image 1 for a visual representation of the three parts of the system. For other useful graphical representations of this system, see *Eye in the Sky*, directed by Gavin Hood (Toronto: Entertainment One, 2015); Derek Gregory, "From a View to a Kill: Drones and Late Modern War," *Theory, Culture and Society* 28, no. 7–8 (2011): 197; Ian G. R. Shaw, "The Rise of the Predator Empire: Tracing the History of U.S. Drones," *Understanding Empire*, 2014, accessed December 30, 2016, https://understandingempire.wordpress.com/2-0-a-brief-history-of-u-s-drones/.

12 United States Air Force, "MQ-1B Predator," 2015, accessed December 31, 2016, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104469/mq-1b-predator.aspx; United States Air Force, "MQ-9 Reaper," 2015, accessed December 31, 2016, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104470/mq-9-reaper.aspx.

Component 1: The command and control center

The first component of the system—**the command and control center**—is where pilots and operators control and supervise the system from a distance, on the ground. Although a command and control center located in the United States, for example, might reduce the exposure of the crew to physical harm, it is likely to be the target of cyberattacks. Command and control centers are equipped with numerous computers and other technologies, and they are essential for the operation of the UAVs but also vulnerable to external and internal cyber intrusion.

Component 2: The satellite

Unlike smaller UAVs, which depend on a radio signal to be maneuvered and typically remain in the operator's direct line of sight, the UAVs classified by the US army as Groups 4 and 5 depend on **satellites**—the second component of the system—that act as an intermediary between the UAVs themselves and their operators. These satellites facilitate the transmission of images and data captured by the cameras and sensors installed on the UAVs, from the aircraft to the command and control center; and likewise, vice-versa, transmitting commands from the base back to the UAVs. The satellite is a crucial part of the system because it provides the UAV and its operator with the precise geographical position of the aircraft, facilitating the UAV to locate its target. Moreover, as Ian G. R. Shaw notes, the use of satellites to connect UAVs to their operators is precisely what allows for the significant increase in the distance between these two parts of the broader system.[13] In fact, he explains that prior to the use of satellites, UAVs had a short command and control datalink that would have made it impossible to operate a UAV in the Middle East from a base located in the United States, as is now the case with Predators, Reapers, and Global Hawk.

In short, the satellite performs two key functions for the UAV: it is the integral part of its GPS navigation, and it acts as the main communication channel for all data exchange between the aircraft and the human operators. Because it relays such crucial information, the datalink that passes through the satellite represents a strategic target for any hacker seeking to disturb or disrupt any UAV operations (These real eventualities are discussed in more details in the next section of the paper).

13 Shaw, "The Rise."

Component 3: The aircraft (UAV)

The third component of the system is the UAV—the **aircraft** itself. As previously mentioned, one of the main incentives behind the deployment of UAVs is removing pilots from physical harm when operating in various war theaters. For this reason, UAVs can be operated in a space that is thousands of miles away from the location of their operators. However, by not being in the cockpit, operators are forced to trust the data they receive from the UAV transmissions. UAVs are therefore equipped with both aperture and infrared cameras that enable operators to direct them and monitor the terrain below them even in harsh meteorological conditions.[14] In other words, these cameras act as the operator's eyes, gathering information and subsequently projecting this information through images on computer screens in front of their operators who rely on the continuous and live optic feed before them to maneuver the UAV. The high resolution of the cameras with which UAVs are equipped and the fact that the images are being live-streamed creates a situation potentially vulnerable to exploitation. For instance, the Gorgon Stare and ARGUS systems respectively consist of twelve and ninety-two high resolution cameras that can be installed on UAVs to upgrade their less sophisticated standard camera.[15] Given that the very high quantity of images captured by the Gorgon Stare or ARGUS can overwhelm the operator tasked to monitor them, it could be nearly impossible for the operator to know if the UAV has been targeted by a cyberattack, underscoring the system's vulnerability.

Mapping the Different Plausible Cyberattacks on UAV Systems

Since UAVs are technologically complex machines, perhaps the "easiest" way for an adversary to attack UAVs is not to emulate them but rather to exploit the weaknesses within their architecture. Moreover, the United States has is deploying its UAVs in the last two decades primarily against non-state actors such as terrorists mostly in situations of "air superiority." Given this competitive advantage, the actors seeking to attack UAVs will

14 Ibid.

15 See Noah Shachtman, "Air Force to Unleash 'Gorgon Stare' on Squirting Insurgents," *Wired*, February 19, 2009, accessed December 30, 2016, https://www.wired.com/2009/02/gorgon-stare/.

find doing so via kinetic means more difficult than if they too possessed sophisticated weaponry. Consequently, a likely alternative for non-state actors is to exploit its architecture, which can sometimes be done with very limited resources (table 1 lists the different kinds of plausible cyberattacks targeting a UAV system).

While fully commandeering a UAV—as sea pirates would upon successfully boarding a vessel—represents a cyberattack that requires a high degree of sophistication, gaining *some* "access" to UAVs is relatively uncomplicated given their reliance on computer networks. The most vulnerable component of the unmanned aerial system is the satellite connection between the aircrafts and the command and control center with which they are in contact. In fact, the aircrafts and communication datalink can be accessed—and indeed exploited—by hackers who strive to steal valuable intelligence. For instance, the US military documented several cases of insurgents who accessed the video feed of Predators.[16]

16 Siobhan Gorman, Yoshi J. Dreazen, and August Cole, "Insurgents Hack U.S. Drones: $26 Software Is Used to Breach Key Weapons in Iraq; Iranian Backing Suspected," *Wall Street Journal*, December 17, 2009, accessed January 1, 2017, http://www.wsj.com/articles/SB126102247889095011.

Table 1: Cyberattacks targeting UAV systems and required abilities to conduct them[17]

Type of cyberattack	Attacked component / UAV type	Actors possessing the minimum required ability[17]	Historical examples	Likely defense options
Access video feed	Satellite datalink; ISR and armed	Individuals	Insurgents against Predators United States and United Kingdom against Israel	Encrypt datalink
Access video feed and DoS attack	Satellite datalink; ISR and armed	Individuals or terrorist organizations	None recorded to date	Encrypt datalink
Access video feed and swap RCA's video	Satellite datalink; ISR and armed	Corporations	None recorded to date	Encrypt datalink
GPS spoofing	Satellite datalink; ISR and armed	States	Allegedly, Iran against RQ-170 Sentinel	Cryptography, signal-distortion detection, and/ or direction-of-arrival sensing
Hack computers controlling RCAs	Command and control center	States	Key logger virus at Creech Air Force Base	Air-gap command a control center; restrict use of removable drives; restrict use of outer technologies (e.g., smartphones or private laptops near or inside the command and control center)

17 This category includes four types of actors. In increasing order based on the resources available to them in carrying out cyberattacks, they are individuals, terrorist organizations, corporations, and states. The reader should note that this category represents an estimated *minimum* threshold; that is, a cyberattack that can be performed by an individual will also be available to terrorist organizations, corporations, and states as they tend to possess more resources than individuals. However, a cyberattack that can be performed by a state will not be accessible to individuals, terrorist organizations, and corporations, which have fewer resources.

Peter W. Singer and Allan Friedman explain that "to pull this trick," the insurgent hackers used nothing more than a laptop computer and "Skygrabber"—Russian-made software that cost $25.95 and was easily available on the web.[18] Skygrabber allowed them to intercept and exploit unencrypted satellite datalinks between UAVs and command and control centers, obtaining hours of video which they then shared with fellow insurgents.[19] Considering that it costs this modest sum to hack a UAV's datalink but millions to safeguard it, Singer and Friedman ask "[whether] the cybersecurity world favor[s] the weak or the strong?"[20] This type of cyberattack may be among the least sophisticated but most worrisome attack to military users. Seeing what the enemy sees can provide the hacker with critical intelligence. For example, by accessing the video feed of the UAV, the hacker can learn about the user's intelligence-gathering capabilities, including the nature and identities of targets as well as ISR practices and routines. Seeing what one's enemy (or friend) sees does not enable one to determine the thinking or strategizing that takes place behind what is seen; however, it certainly helps to anticipate what the user's next move might be and it allows the hacker to stay a step ahead of the user, which can prove decisive on the battlefield.

Another, more sophisticated instance of UAV cameras being accessed surreptitiously was recorded by *The Intercept*. According to Cora Currier and Henrik Moltke, several Israeli UAVs—including the Hermes and Herons—have been hacked by American and British intelligence agencies.[21] As they explain, the United States' National Security Agency (NSA) and the United Kingdom's Government Communications Headquarters (GCHQ) established a base in Cyprus from where the two countries intercepted the signal of Israeli UAVs and successfully collected video footage, which they used to monitor Israel's activities in Gaza and the West Bank. Currier and Moltke add that this joint secret program, named "Anarchist," allowed the Americans and the British to track the flight path of Israeli UAVs. The

18 Singer and Friedman, *Cybersecurity*, 260–261.

19 Gorman et al., "Insurgents Hack."

20 Singer and Friedman, *Cybersecurity*, 260.

21 Cora Currier and Henrik Moltke, "Spies in the Sky: Israeli Drone Feeds Hacked by British and American Intelligence," *The Intercept*, January 29, 2016, accessed May 25, 2017, https://theintercept.com/2016/01/28/israeli-drone-feeds-hacked-by-british-and-american-intelligence/.

ability to track Israeli UAVs suggests that the United States and the United Kingdom likely could identify both the location of the Israeli launch-and-recovery station, as well as the command and control center.

The fact that insurgents or states can access the camera of a UAV and see what the UAV sees indeed is a vulnerability, as explained above; however, the ramifications would be far more significant if the hacker gains access not only to the camera but also to the UAV controls. For instance, a mere denial of service (DoS) attack could lead the operator to lose sight of a target for just long enough to allow the target to escape. Depending on the moment at which it is performed (e.g., immediately before taking off or landing of the UAV), such an attack could also result in the crash of the UAV, for a "blind" operator may be unable to avoid nearby obstacles. Insurgents would have a strong incentive to conduct a DoS attack when seeking to escape a UAV hovering above them. The longer the duration of the DoS attack, the more time insurgents would have to leave the area over which the UAV is loitering.

A cyberattack that targets the datalinks connection may corrupt the video feed to lead operators astray. This scenario has been depicted in many films where an individual or an organization hacks into a computer system and into surveillance cameras connected to the system and plays a different footage (sometimes a looping of the sites) with nothing abnormal happening so that those monitoring the cameras will not know that they are being fooled. A parallel can be made between UAVs and this typical movie scenario because UAV cameras are the only medium through which the operator can see what is happening. Thus, if a hacker manages to hack into a UAV's camera—as the above Skygrabber demonstrates—and sends back a looped video influencing the operator to think that the UAV is hovering over a desert, the operator may not realize that they are not actually looking at what the UAV is really seeing. In sum, misdirection could compromise missions and beyond that.

Satellite datalinks make the UAV system's architecture vulnerable for another important reason, namely because they are the channel through which GPS data is passed from the UAV to the command and control center. In so-called "spoofing" attacks, which are similar to the abovementioned movie scenario, the hacker could hack into the GPS transmission and mislead the UAV and its operator into believing that it is somewhere that it is not. A notable instance of this kind of cyberattack took place in 2011 when

Iran allegedly spoofed the GPS of a stealth RQ-170 Sentinel.[22] In fact, Iran claimed that it hacked into the GPS of one of the American UAVs, co-opting it into switching on its auto-pilot mode and then sending it different GPS coordinates that ultimately led it to land in Iran.[23]

Although many specialists have raised doubts about Iran's ability to pull off this type of hack,[24] GPS expert Richard Langley maintains that "it's theoretically possible to take control of a drone by jamming the P(Y) code and forcing a GPS receiver to use the *unencrypted* [original emphasis], more easily spoof able C/A code to to [sic] get its directions from navigational satellites."[25] The "coarse acquisition" or C/A code represents the signal used by all GPS to transmit information to satellites. C/A codes are unencrypted and therefore easier to decode. The "precise" or P code is simply a more powerful and more accurate version of the C/A code and fulfills the same function. The "(Y)" is added after the P to denote that the precise code is encrypted, with an encrypted signal being more secured than an unencrypted one.

While the hacker could not necessarily decrypt the GPS data transmitted under the P(Y) code, due to its encryption, the hacker could overwhelm its signal and compel it to switch to the C/A code, which is not encrypted. Once on the C/A code, the now unencrypted data emitted by the GPS could be intercepted, as with the Skygrabber-based attack mentioned above. Thus, while there is a chance that Iran did not actually hack into the RQ-170 Sentinel in 2011, the possibility of other actors doing so does exist—provided they possess sufficient technological know-how. Given their degree of sophistication, the ability to carry out spoofing attacks is likely held by only a handful of a *state* actors.[26]

---

22 Adam Rawnsley, "Iran's Alleged Drone Hack: Tough, but Possible," *Wired*, December 16, 2011, accessed January 2, 2017, https://www.wired.com/2011/12/iran-drone-hack-gps/.

23 Ibid.

24 See David Axe, "Nah, Iran Probably Didn't Hack CIA's Stealth Drone," *Wired*, April 24, 2012, accessed January 2, 2017, https://www.wired.com/2012/04/iran-drone-hack/; Rawnsley, "Iran's Alleged."

25 Rawnsley, "Iran's Alleged."

26 Mark L. Psiaki and Todd E. Humphreys, "Protecting GPS from Spoofers is Critical to the Future of Navigation," *IEEE Spectrum*, July 29, 2016, accessed July 30, 2017, http://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation.

At the time of writing, "cryptography," "signal-distortion detection" and "direction-of-arrival sensing" are the three defense mechanisms that are able to mitigate GPS spoofing attacks.[27] Relying on the experimental data they obtained by detecting spoofing attacks against the navigating GPS of a super yacht, Mark L. Psiaki and Todd E. Humphreys note that these complex defense mechanisms may not be sufficient to protect against a spoofing attack if used individually, yet they increase the likelihood of a successful defense when deployed conjointly.[28] That being said, some of these mechanisms may not be suited to the RQ-170 Sentinel or other stealth UAVs. This is because the addition of some defense systems to the UAV could undermine its "stealthiness" unless the system is equipped with the same stealth technology as the aircraft itself. If it is not stealthy, the added defense would be detectable by enemy radars, thereby defeating the main purpose of the stealth UAV.

In addition, considering that the RQ-170 Sentinel is one of the United States' most secret and technologically advanced UAVs at the time of writing, these theoretical eventualities further underscore the architectural vulnerability of the country's UAVs.[29] As mentioned above, Predators and Reapers may still not be using encrypted datalinks, unlike the Sentinel, which makes them even more susceptible to GPS spoofing attacks. Beyond the strategic value of seeing what their enemy sees, hackers would have an incentive to conduct such attacks when a UAV is hovering near an area they consider of importance. The incentive would be even stronger with armed UAVs if the hacker believes that by being inactive, the UAV would strike a militant hideout that the hacker is trying to protect. In such a case, a mere DoS attack might not be sufficient because, unlike militants who can try to flee when being chased by an UAV, physical infrastructure—such as a hideout or training camp—might not be easily and rapidly relocated, if at all.

While satellite datalinks connecting UAVs to command and control centers are vulnerable elements of the UAV system's architecture, the command and control centers are also susceptible to cyberattacks given that they operate exclusively over computer networks. That they are protected by air gaps

27 Ibid.

28 Ibid.

29 While the US Air Force (2009) website features a fact sheet page for the RQ-170 Sentinel, no technical data regarding the aircraft's capabilities and key features is publicly available, in contrast to the MQ-1B Predator and MQ-9 Reaper.

has not prevented malware from infecting these networks, as evidenced by the presence of a key logger virus that infiltrated the military computer systems at Creech Air Force Base in 2011.[30] A private network is said to be protected by an air gap when it is disconnected from the surrounding public networks. This is done to ensure that the network is secured and cannot be accessed through any of the nearby public networks. In other words, the air gap isolates the private network (i.e., the network used at the command and control center) so that the hacker will only be able to hack into the network via physical access to the computers connected to that private network, thereby making it more challenging for the network to be compromised. Publicly available information on the specific virus that targeted Creech Air Force Base has not been released, which makes it difficult to determine exactly how it affected the computer network at the base; however, it is believed that the virus reached the network via removable drives that were inserted by the UAV operators themselves and since then are no longer used by the US military.[31]

This event demonstrates the vulnerability of the human factor.[32] That is, even though their bodies may no longer be present on the battlefield, operators remain at risk of being used by hackers to gain unauthorized access to the system. This can have a wide range of operational implications. A simple infection of the network by a virus could disseminate classified data gathered by UAVs to malicious actors. A more sophisticated malware attack could send unofficial commands to UAVs while it tells the monitors in front of the operators that everything is happening the way it should, somewhat in the manner of the "Stuxnet worm" that struck Iranian uranium enrichment

30 See Noah Shachtman, "Exclusive: Computer Virus Hits U.S. Drone Fleet," *Wired*, October 11, 2011, accessed January 2, 2017, https://www.wired.com/2011/10/virus-hits-drone-fleet/.

31 Ibid.

32 While attacks based on the human factor may prima facie appear less sophisticated as they do not involve technologically advanced knowledge, their potential effects should not be understated. In fact, the highly-mediatized ransomware WannaCry—reportedly reaching "tens of thousands" of computers in no less than "74 countries" on May 12, 2017 alone—exploited a vulnerability within Microsoft Windows for which a security update had been available since March 14, 2017 (see Microsoft 2017); yet the people sitting in front of those infected computers had failed to install it.

facilities in 2009.[33] While the cyber component of these types of attack need not be elaborate, they remain quite sophisticated overall because they first require physical access to the command and control center, a step that might prove cumbersome given the high level of physical security surrounding these sites.

Although attacks targeting the command and control center are comparatively more difficult to carry out, as explained above, hackers have significant incentives in launching them given the strategic value of successful attacks. For instance, by implanting highly sophisticated malware into the command and control center, the hacker could create a kinetic effect on the UAV by issuing malware commanding an armed UAV to fire its missiles at the wrong targets. Moreover, the malware could cause the UAV's missiles, which contain small computers that are also subject to cyberattacks, to be dysfunctional or even detonate while still on the UAV, thus destroying the aircraft. Given that they often lack the ability to conduct air-to-ground attacks, terrorist organizations would have an incentive to conduct cyberattacks that would enable them to gain some control over a UAV's payload, which they could use as if it were their own. The cyberattack possibilities here are endless and cannot be addressed comprehensively. Yet, stressing their plausibility should be sufficient to alert the reader (as well as UAVs users) of their potential threats.

Regardless of which type of attack is pursued, hackers have an incentive to design malware that will take a long time before being noticed so that they can exploit the system as long as possible. In fact, a Department of Defense official puts it this way: "For a sophisticated adversary, it's to his advantage to keep your network up and running. He can learn what you know. He can cause confusion, delay your response times—and shape your actions."[34] And since UAVs have gained such an important position at the center of the US military's arsenal, the "prize" for hacking them becomes even more valuable, perhaps even more than shooting them down from the sky. In other

33 See Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014, accessed January 2, 2017, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

34 Quoted in Nathan Hodge and Noah Shachtman, "Insurgents Intercept Drone Video in King-Size Security Breach (Updated, with Video)," *Wired*, December 17, 2009, accessed January 2, 2017, https://www.wired.com/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/.

words, the more powerful and effective the weapon is, the more coveted it will become for actors hoping to gain operational advantage.

Conclusions and Policy Recommendations

UAVs are now at the center stage of many of the major world powers' counterterrorism campaigns, including the United States, Israel, and the United Kingdom. Referencing a 2014 Rand Corporation assessment, Kreps notes that "China, India, Iran, Russia, Taiwan, Turkey, [and] the United Arab Emirates" are currently developing their own UAVs.[35] She goes on, saying that "the world is becoming awash with drones and the indications are that these are not only here to stay, but to spread."[36] The subject of UAVs is therefore becoming very important and relevant for all states using them for military purposes.

As UAV systems become entrenched within the militaries, the cyber threats posed to those systems have also become more frequent and from various types of adversaries, as this paper has highlighted; yet, as was explained above, not all adversaries are able to carry out all kinds of plausible cyberattacks on UAVs. An important part of mitigating these threats begins with an awareness of their existence, which is the aim that this paper sought; simply being aware of a vulnerability is not enough, however, and additional steps must be conducted in order to alleviate the potential damage that the cyberattacks can engender for the user of UAV systems.

The following three recommendations should be regarded as critical next steps toward addressing the cyber vulnerabilities of UAVs and should ultimately increase their defense system:

1. Users should begin by **assessing the vulnerability** of their systems. This assessment should be based on both the system's architecture—which includes the command and control center, the satellite, and the aircraft—as well as the capabilities of the adversaries or others that have incentives to hack the system.
2. The user of UAVs should create technological back-up solutions than would alert or **indicate that the system has been accessed** by an unauthorized actor and is therefore compromised. In the absence of such an alarm system, the operator cannot detect that a cyberattack has

35 Kreps, *Drones*, p. 60.

36 Ibid., p. 160.

taken place or is in the process of being carried out and is less likely to be able to defend against it.

3. More efforts should be made to **encrypt datalinks that transmit information** from one part of the system to another. The user should also devise other protection methods—especially on armed systems—even if they are employed in arenas where the threat is estimated to be lower, as the least sophisticated cyberattacks can still damage the system.

In conclusion, these recommendations undoubtedly come at a cost to the system—both financially and in terms of the system's relative effectiveness. For instance, while encrypted datalinks are more secured, encryption inescapably lengthens the decoding process. However, the potential damage that a successful cyberattack on the UAV system could produce likely outweighs the costs. Awareness is key; a realistic assessment of the system's vulnerabilities that does not underestimate the potential damage of a simple cyberattack by an individual, a terrorist organization, or even a state represents an essential first step toward setting up cost-effective defensive measures for UAVs.