The Undergraduate Research Journal

Volume 4 Article 8

7-12-2016

Cyber Warfare: International Security Intelligence

Marwan Sallam
The American University in Cairo AUC, sallam93@gmail.com

URJe –The Undergraduate Research Journal
No. 4 (2016)
https://urje.aucegypt.edu/

Essay

What threats may cyber warfare implicate on Unmanned Arial Vehicles (UAV)? Are those threats taken seriously by the US government?

Marwan Sallam

Student,
AUC School of Business

Abstract

This essay will investigate the cyber threats presented on UAVs, which are now the backbone of the US arsenal on the war on terror. In addition, it will assess whether the US government are taking serious measures to counter the threat that cyber warfare could implicate on their drone fleets. Finally, would suggest some policies prescription to combat that threat.

From the mountainous terrains of Afghanistan to the hustle and bustle in the streets of Baghdad, UAVs industry is greatly increasing due to their success and reliability demonstrated by the US and Israeli air forces. UAVs would deliver the precision strikes that one would require with minimum to no casualties on the attackers position, and if the UAV is down, no pilots are downed with it. Those are all reasonable factors that influence a governments decision into having a drone fleets at their disposal. But one tends to forget an important thing, is that because those

ISSN: 2356-8976

UAV are designed to be unmanned thus it is linked to the pilot, who is in a completely different place, by a software or in other words by cyber means. This simple fact as good and safe as it sounds that the pilot will be unharmed in course of a battle, is vulnerability, that now non-state actor, and states, and suspiciously state-sponsored "hackers" are taking advantage of. What we are now witnessing is the new age of asymmetric warfare; it is cyber warfare in its front lines. The main question that this essay addresses, are the politicians, manufacturers, and government tacking this new warfare, and threat on the UAVs, which could just be a start as a breach in the drone technology might be a wakeup call that the military establishment and infrastructure could be penetrated by cyber means, seriously enough? Are there being measures taken by the US government, in particular because they have the largest drone fleet that is deployed across the globe, more enemies which makes them more prone to attacks, to combat these new phenomena? This essay will investigate this issue, by comparing measures taken by other drone manufacturing states, for securing those drones by cyber means, and by looking at new technical innovations that could then help in making a policy prescription to secure the drones.

Back in the day cyber "attacks" were conducted though signals interception, radio transmission extraction or manipulation, today drones are ran by what seems to be a sophisticated method of delivery software system is not even the case these days in which this essay will demonstrate how these UAV are very vulnerable to cyber attacks. These cyber attacks are not specific meaning that it doesn't aim

Sallam: *Threats*

for destruction necessarily, but the evidence will show that the UAVs could be easily penetrated, by a virus or by a capable hacker who could acquire the UAV and transform its allegiance. Although there is no evidence which would support that a UAV has been infected by a virus or penetrated by a hacker and started killing it's owner like what we expect in our popular culture a "SkyNet" change of awareness issue or a machine revolution were we see the drones in the Terminator movies turn against the humans and starts killing them. This may not be the case today, but with the evidence at hand, and innovation, technology and very good cyber awareness, proper funding with a sense of purpose, whether guided or misguided, the sky is the only limit when coming to cyber activity versus modern day drones. It's very easy to use this asymmetric means of warfare and is less risky that the good old-fashioned guerilla warfare in which has to mobilize a large group of people who in most, if not all cases, have a state actor constantly supplying them whether with stinger missiles, AK-47s, Chinese Red Eagle anti-tank, Konkurs, it has a lot of hassle and involves a lot of countries, which in turn increase polarization. However, in the age of "cyber revolution" or the information age, we see many non-state actors are starting to adopt these new ways as an asymmetric means of warfare, as they are concealable, cheap a good cyber attack may vary its cost from 300$ to 50000$ maximum only, and with capable trained hands could be fatal to the victims key infrastructure. Though, this essay is only focusing on the attacks aimed at the military infrastructure, in specific drones and UAVs, because as it became obvious, its easier to destroy the drones cyber activity rather or

disabling their software is far more accurate and devastating than aiming and shooting a stinger missile at that drone. Which in this case, tactically speaking, since one could assume that the drone is transmitting back to base what it sees, could cause a retaliation of another drone in the same area. What we're seeing now is not just attacks on drones for the purposes of defense, in some cases drones when hacked and brought down are more valuable that a destroyed drone.

What we see here is the dawn of the cyber age, during the cold war, guerilla warfare strategy was considered the poor man's tactic of resisting the enemy and fighting the adversary, but now cyber warfare, in this case could be used by states less developed military to counter the US military hegemony based on attack their vulnerabilities, the problem is are the US taking serious measures? Are the other drone operating states also taking serious measures, because drones are heavily relied upon for security and field operations but are also very vulnerable what if the non-state actors or terrorist groups gain access to such cyber capabilities, terrorist organizations such as Al Qaeda are realizing this and taking advantage of this "breakthrough" and using it for themselves. This could reshape the battlefield tactics that are taking place on the ground, reducing the US tactical advantage that gave its boots on the ground the edge it has over the insurgents in Iraq and Afghanistan.

The most popular example that made the UAV vulnerabilities surface was when the Iranians capture Lockheed Martin's RQ-170 Sentinel UAV on

Sallam: *Threats*

December 4th 2011, by Iranian cyber warfare unit (Mick, 2009). The RQ-170 UAV and other military UAVs have the GPS as a backbone or core of their guidance system, in addition of an inertial navigation system (INS). According to INFOSEC Institute, the UAV was downed by a GPS "spoofing attack" which is basically sending to the drone's control system a fake coordinates which deceives the on board system which then makes it go to a place it is newly commanded. Spoofing is basically making the drone think it's going to its programmed designation while in fact the coordinates provided make it in reality go somewhere else (Mick, 2009). Drones get their orders from their local base, but are flown from another base through satellite transmission. Spoofing just intercepts this whole process and goes straight to the drone. Even though, this particular drone and military drones uses INS because it's known to have a healthy amount of errors and inaccuracies they have to have a GPS system and an air data computer to maintain the required navigation performance (Mick, 2009). This is how drones that have the GPS guidance system as a core is threatened, all they did was a radar jammer and deception system, and it's not that hard to accomplish according to University of Texas at Austin students even without the radar jamming and deception systems.

At Austin Texas, assistant professor Todd Humphrey along with some other 5 students have demonstrated how the UAV whether civilian or military (they proved their point on civilian drone though) is very vulnerable. Todd had demonstrated such in front of the Department of Homeland Security, that the process isn't complicated as the Iranians claim it is,

to show that they have a strong cyber warfare unit, but with a group of well aware students and not more than a thousand dollars could implicate around four million dollar damage, which is the price of one predator drone (Reuters, 2009). This only shows that drones do not have some proper cyber security mechanisms, and the drones in mid air are probably compromised. This was easy to conduct because the drones use an unencrypted GPS system and apparently with these two incidents it is not enough to convince DHS and DoD to commit or make a change or at least cut-back from the UAV use, since it is highly unlikely that they will change the GPS from the encrypted to unencrypted one. Imagine that non-state actors will shift all their efforts into cyber "air defense" to counter the UAVs attacking them. These are just simple starters of a more damaging storm coming further, let's say if those guys were either funded or well educated, for instance the Texas students we could give them the fact that they are US residents if not citizens so they are aware of the UAV systems used in the US and could therefore know how to access it and familiarize themselves to it, then later hack it.

On parallel incidents Wall Street Journal reported on rumors that Hezbollah might have also captured an Israeli drone using the same spoofing techniques. This is the probable explanation because there was not reports of anti-air fire, gun fire nor anything, that is according to the UN peacekeeping force in Lebanon reports, which speculates that Hezbollah may have found a cyber way to penetrate the drones, both sides had no comments (Reed, 2011) about this incident and was rapidly forgotten, however

Sallam: *Threats*

according to an anonymous Israeli source with IDF and military intelligence experience, the Israeli may have purposefully crashed the UAV into Lebanon so that Hezbollah wouldn't get this cyber victory. This could either suggest that Iran may have sold the technological cyber innovation applied on the RQ-170 incident and possibly handing it over to the none state-actor which in this case could be used in the future as means to increase their popularity as "guardians of the sky" and regain more influence on Lebanese internal politics, and with their involvement in Syria, this might increase their regional influence as well. The fact that this suggestion, Israel deliberately crashing the UAV, shows that the Israelis are aware that there is an imminent cyber threat facing their drones, which is not only a core in their air force, but also is the flagship of the Israeli military industry is at stake.

It could be possible that this will be how future proxy wars will take place between the Chinese, American, and possibly Russians and Pakistanis, who also shown an increase in cyber activity (Bak, 2013), as it is a cheap and effective means to destroy and steal "intellectual property" of UAVs, it is popular that that's how the Chinese have built the Chengdu J-20 stealth fighter from the downed F-117 Nighthawk the only one shot down (Jennings, 2011). Would the Chinese known for their infamous cyber warfare unit be a part of these series of cyber attacks against specifically US UAV? It could be given that the Chinese are developing their own drone program it is a safe probability that they may have even aided the Iranians who would aid Hezbollah on the other had in return for the Chinese to get access over the

"downed" drones, as its cheaper to imitate a technology rather that start a new one from scratch. With Chinese economies of scale they could flood the drone market with their cheap UAVs and would also flood in this case the non-state actors, the anti-drones market.

To further emphasize how the UAVs are threatened by cyber attacks, Iraqi insurgents with what it may appear as a $26 dollars (MacAskill, 2009) have managed to tap into the video feeds of the drones making the insurgents have an intelligence advantage (BBC, 2009). This shows that there is a risk involving further investment on UAVs and continuous dependence on them.

A few days ago the US navy celebrated the launch of a bomber drone from an aircraft carrier, the mechanism of bombing is very simple, it has the same GPS coordinates stored in its software where it goes to bomb, then get back and lands in the aircraft carrier. This shows that GPS spoofing threats and drones being hacked aren't being taken seriously by the defense manufacturers, two years ago Iranians, Hezbollah, and insurgents managed to hack "recon" UAVs but with the advancement UAVs capabilities one must assume that there is also an advance in cyber weapons. Unfortunately, as we see with new drones being manufactured from the US haven't seen much change in policy, it has the same GPS system as core, which was shown to be compromised by the Iranians, non-state actors and even students, but ironically, they made new bombers completely automatic with that same core, wouldn't one fear that if this is hacked or spoofed it might bomb civilian

Sallam: *Threats*

targets? Or should this happen in order to grab the Department of Defense, and State attention?

With increasing dependencies on drones and robotics, the risk gets higher, previous incidents were proven limited to hacking for the purpose of acquisition of technology and intelligence gathering. However, we know that with the increase realization that cyber weapons were proved effective as asymmetric means of warfare, why would terrorist and none-state actors limit themselves into hacking into video feeds? There is no limit when it comes to ideas on what to do with another country's weapons so they'd get the blame, especially when it comes to civilian casualties. The US defense department must beware of the consequences and risks when coming behind future reliance on drones, because it wouldn't just be limited on leak of US technologies, but on innocent civilian lives, and when this happen there will be a larger uproar from the people in victimized countries.

On a military defensive level, countries reliance on drones may seem more cost effective, as they fly for much longer, don't require the same expenses of pilot training as pilots do. However, all that said too much reliance on a "drone fleet" may and will put a country in jeopardy, as James Pavitt said, "it's not a matter of if, it's a matter of when". The US defense department are putting too much then they should on an offensive weapon with no defense to it, while the Chinese, rogue agents, terrorists, and none state actors are investing on the counter-offensive, which is cyber offensive on those drones. On October 11th 2011, a US drone base was hacked and a virus was

planted to the drones cockpits in Nevada, the heart of the States, and wasn't reported (Shachtman, 2011). That virus is a "key logging" virus, which enables hackers to monitor the drones operations. The virus is yet unknown whether is continued contaminating the rest of the UAVs or no (Al Jazeera, 2011). This shows for one that the drones are very vulnerable to viruses too, meaning that they could get a virus and be grounded from flight, two it also shows that there aren't measures for cyber security regarding drones. What we're witnessing right now is the "when" happening maybe not on a Pearl Harbor scale but it is already happening, and each and every time it gets even more damaging, but also underrated attention. The reason behind these embarrassments or breaches being announced is plenty, but probably it may be due to the powerful influence of the military industrial complex over the department of defense. One must look at it from a CEO's perspective for a minute, a cost/profit analysis of this issue. The reluctance for cyber securing the drones might be because it will cost too much as opposed the profit it will make, so they just ignore it. Maybe, a project is underway however, it is classified so we wouldn't know it will only manifest by the number of future breaches we'll have to count, if there more then it's safe to assume that there is nothing being done about it. If not, then it is being taken seriously.

As of now, all we know is that this issue has caught congress's attention (Sperry, 2012), and is under debate. However, as this essay discovered, there seems to be a "drone lobbying" group, which basically undermines those threats, saying that the average person cannot hack nor plant a virus on the

Sallam: *Threats*

drones. Should governments wait till the "average" person hack those drones (Pruvis, 2012) to take action? Or should we assume that one day the average "adversary" is an average person who cannot hack a drone? That argument of theirs is redundant it simply shows that they're only concerned on their sales, not security. It is very ironic that the lobby even makes such statements; even if they're true the enemy is recruiting experts in this cyber business and the insurgents if they are not trained they will get the training they'll need to become the "above average" in order to grab those lobbyists' attention. However, Department of Homeland Security (DHS) seems disinterested, as it failed to attend the hearing in July 2012, in addition to its unwillingness to accept the task of regulating the drones with the Federal Aviation Administration. Bearing in mind, that currently domestic forces such as DHS, and police forces use unencrypted GPS system which is at risk, because the "unencrypted" one that the US military claims to use, Iranians don't attest to that, is also compromised, the Iranians took over the RQ-170. For the reason that using "unencrypted" GPS system for domestic use would cost too much, can DHS, which its sole purpose is to secure the homeland is reluctant to pay such cost, does that mean that their willing to risk people's lives because of greed or is the cost of life, privacy, and the way of life now has a price tag to it? Isn't that contradicting their primary objective? But that seems like the military industrial complex is speaking from the cost/profit point of view, because as long as DHS is concerned cost should bother them as long as it will make their life easier. So that third party may be influencing the

DHS into not taking serious measures regarding drone cyber security.

There are several measures to combat this threat facing the drones that drone operating governments, if they aren't willing to cut-back, could do to avoid future setbacks. For instance, instead of using unencrypted GPS system that could be spoofed easily by a bunch of Texas students, or by the sky scanner application or cheap software that could be downloaded from the internet is one, they could use encrypted ones, the same way the Chinese do it. That way it will at least secure domestic drones, from hacking as it is harder to bring a radar jammer inland without being noticed is something.

There should be a formal cyber security division to protect against hackers, and cyber attacks, such as viruses. The same way the Chinese are appearing to have a cyber unit why not all governments especially the US (since it's the one being under constant attack) have one on its own? At least as defensive means, for the drones there is a cyber unit that its main goal isn't just limited to prevention of hacking, but protection of the intelligence is has, because when speaking domestically, drones may be used as means to breach civilian privacy also. Or reshaping, reinforcing the DoD's Host Based Security System to meet contemporary standards, in order to include UAVs among the "threatened" units that should be protected.

Apparently, the defense advanced research projects agency (Darpa) is currently looking for different measures for protecting the drones. One of them is

Sallam: *Threats*

by simply hiring other hackers to advice on what to do. Hackers who now work for Darpa are being used to design a new program that would decrease the drone's dependency on the Internet, by creating an Internet without the anonymity part, is a popular suggestion (Ackerman, S. , 2011a). Also, considered creating a second secure network of the network to replace the current network and work in parallel with other networks (Ackerman, S. , 2011a), basically as complicated as it sounds will give the hacker a hard time hacking into the drones. However, most of Darpa's focus is on securing the military network as a whole not the drones in particular which means that there are no guarantees. What seems to be specific project for the drones will be, still a concept, Crowd Sourced Formal Verification (CSFV) a means to control who is going in and out of the systems (Ackerman, 2011b).

Even though, those measures may sound and seem powerful measures, but the reliance of Darpa to outsourced hackers is a risky task itself, especially when looking at Edward Snowden's case what guarantees we have that there wouldn't be a leak. Moreover it shows that the methods to counter these threats are the cheap and fast way only looking for short term and not long term, we don't see a training program or a cyber education in countries except China. Which means that this threat is not taken as seriously as it should from the departments concerned but the measures taken is to contain the media effect and please the crowd.

Other measures would be, decentralizing the drone system, meaning it doesn't have to get the orders

from one single base but the drones become more autonomous yet with more direct control in the same time. Most of the hacking occurs to the fact that the drone gets the order from the base, if the base is penetrated or the drone gets order from what it's convinced is the "base" then it gets easier to hack. However, if drones are more decentralized and independent like piloted aircraft in which each and every drone had its unique unencrypted GPS system and cyber security mechanism then it would be safer to have. It would cost more, but would risk less. Also, creating new software, like the Mac software that makes it immune from most viruses and cyber attacks, unlike Microsoft which may sound not an innovative idea but practical.

To conclude, cyber warfare is a major threat not only to a state's infrastructure, but also to its military capacity. Today cyber weapons are used as cheap asymmetric means to counter established armies such as the USA. That being said, the measures and attacks that have taken place against UAVs in the recent years haven't rallied the attention that it deserves in order to pressure policy makers, and defense department heads to cyberly secure the UAVs, before terrorists, and rogue agents may use this vulnerability to their advantage. Unfortunately, it seems that the US and governments operating drone, need a sort of cyber pearl harbor against their drone fleet in order to appreciate the need for cyber security when it comes to UAV alike the other pillars of the state. Cyber war is by nature discreet, making us unaware with what is currently happening and only relying on what is exposed to us, maybe there are serious classified measures taking place for

Sallam: *Threats*

future drone projects, but we wouldn't know what we know though is that there is a vulnerability that is being exploited and if kept that way without proper attention terrorist would use this in the future to their ends.

Bibliography

Ackerman, S. (2011a). Darpa looks to protect drones from hack attacks. *Wired*. Retrieved from https://www.wired.com/2011/11/darpa-cybersecurity-drones/

Ackerman, S. (2011b). Darpa begs hackers: Secure our networks, end 'season of darkness'. *Wired*.http://www.wired.com/dangerroom/2011/11/darpa-hackers-cybersecurity.

Al Jazeera, (2011). US drones infected by key logging virus: The infection could allow hackers to access intelligence gathered by the unmanned aerial vehicles. *Al Jazeera*. http://www.aljazeera.com/news/americas/2011/10/20111110816388104988.html

Bak, Ch. (2013). *Cyber warfare and cyber terrorism*. Unpublished manuscript, Christ's College, University of Cambridge.

BBC (2009, December 17). Iraq insurgents 'hack into video feeds from US drones. *BBC*. http://news.bbc.co.uk/1/hi/world/middle_east/8419147.stm

Jennings, Ch. (2011, March 13). Did China develop its deadly stealth fighter using parts from a downed U.S. bomber?" *Mail Online*. http://www.dailymail.co.uk/home/moslive/article-1365330/Did-China-develop-deadly-

stealth-fighter-using-parts-downed-U-S-bomber.html

MacAskill, E. (2009, December 17). US Drones hacked by Iraqi insurgents. *The Guardian*. http://www.guardian.co.uk/world/2009/dec/17/skygrabber-american-drones-hacked

Mick, J. (2009, December 15). Iran: Yes, we hacked the U.S.'s drone, and here's how we did it. *Daily Tech*. http://www.dailytech.com/Iran+Yes+We+Hacked+the+USs+Drone+and+Heres+How+We+Did+It/article23533.htm

Paganini, P. (2013). Hacking drones: Overview of the main threats. *InfoSec Institute Resources.* http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/

Pruvis, C. (2012, July 19). Drone lobbying group says the average person couldn't hack a UAV. *Security Management*. https://sm.asisonline.org/migration/Pages/drone-lobbying-group-says-average-person-couldn_E2_80_99t-hack-a-uav-0010089.aspx

Reed, J. (2011, December 7). The downed RQ-170 and hezbollah. *DefenceTech*. http://defensetech.org/2011/12/07/the-downed-rq-170-and-hezbollah/

Reuters (2012, June 21). Texas college hacks drone in front of DHS. *Reuters*. https://www.rt.com/usa/texas-1000-us-government-906/

Shachtman, N. (2011, Novermber 10). Get hacked, don't tell: Drone base didn't report virus. *Wired*.

http://www.wired.com/dangerroom/2011/10/drone-virus-kept-quiet/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+WiredDangerRoom+%28Blog+-+Danger+Room%29

Sperry, T. (2012). Drones vulnerable to being hacked, Congress told. *CNN Security Clearance*. http://security.blogs.cnn.com/2012/07/19/aerial-drones-vulnerable-to-being-hacked-congress-told/