

**This is a self-archived version of an original article. This version may differ from the original in pagination and typographic details.**

**Author(s):** Lehto, Martti

**Title:** Drones in cyber security environment

**Year:** 2019

**Version:** Published version

**Copyright:** © 2019 Cyberwatch Finland Oy

**Rights:** In Copyright

**Rights url:** <http://rightsstatements.org/page/InC/1.0/?language=en>

**Please cite the original version:**

Lehto, M. (2019). Drones in cyber security environment. Cyberwatch Magazine, 2019(4), 8-17.  
[https://issuu.com/cyberwatchfinland.fi/docs/cyberwatch\\_2019-4\\_eng](https://issuu.com/cyberwatchfinland.fi/docs/cyberwatch_2019-4_eng)



# Drones in cyber security

## ABSTRACT



Aerial unmanned vehicles (AUV) are currently used for a wide range of operations such as border surveillance, surveillance, reconnaissance, transport, aerial photography, traffic control, earth observation, communications, broadcasting and armed attacks. AUVs are presumed to be reliable, automated and autonomous machines, providing their services at any time and everywhere.

AUVs are extremely suitable for long missions that strain flight crews or put them in harm's way. Two advantages can be gained by eliminating the flight crew: 1) performance improves (range, endurance, increased payload and maneuverability, smaller physical size and lower observability) and; 2) the ability to take higher risks.

UAV/RPAS/drone cyber security has largely focused on exploitable vulnerabilities in either the communication channels or the hardware/software stack on the vehicle. Such attacks have focused on exploiting unencrypted communication over wireless media to implement eavesdropping, cross-layer attacks, signal jamming, denial of

service, and dropping Wi-Fi communication with ground control. Other attacks on drones involve GPS (Global Positioning System) spoofing attacks to fool the drone into moving to a different destination (possibly with the intention of hijacking the drone).

In the same time UAV or drone can be a cyber attack platform. Specially equipped drone can track signals based on Wi-Fi, radio frequency identification (RFID) and the Bluetooth and 802.15 specifications (PAN/WPAN communication). Combined with a GPS capability drone correlates signals to the location where they're detected. So, the drone spy not only on phones, tablets, and computers, but also, potentially, on pacemakers, fitness bracelets, smartcards, and other electronics. Additionally, drone can function as visual tracking platforms even without the use of beacons or GPS.

Swarms of small drones could soon become an important part of the modern military arsenal. The swarm idea inherently drives drones towards autonomy which allows many different kinetic and non-kinetic operations.



# Security environment

text: Prof. Martti Lehto  
University of Jyväskylä

## INTRODUCTION

➤ There is no one standard when it comes to the classification of unmanned aircraft system (UAS). Defense agencies have their own standard, and civilians have their own categories for UAS. UAVs can be roughly divided into fixed wings and rotary wings. Other classification argument is size, Maximum Gross Takeoff Weight (MGTW), range and endurance. For combat is two main groups: Unmanned Combat Aerial Vehicle (UCAV) and, Unmanned Combat Aerial Rotorcraft (UCAR). These can be categorized by performance and combat mission.

According U.S. DoD an UAS is a “system whose components include the necessary equipment, network, and personnel to control an unmanned aircraft.” UAV is the acronym of Unmanned Aerial Vehicle.

The International Civil Aviation Organization (ICAO) employs the acronym RPAS (Remotely Piloted Aircraft System). The definition associated is that these systems as “based on cutting-edge developments in aerospace technologies, offering advancements which are opening new and enhanced civil-commercial applications as well as improvements to the safety and efficiency of the entire civil aviation.”

French Directorate for Civil Aviation (DGAC) see commercial unmanned aerial vehicles as a drone. In a general way, in French speaking countries are mainly using this drone term. For many UAV is mostly used in a military context, so drone cover both civil and military purpose any type of aerial unmanned vehicle.

This article uses the term drone to cover the whole spectrum of aerial unmanned vehicle.

”

**This article uses the term drone to cover the whole spectrum of aerial unmanned vehicle.**





# 1. DRONE AND ITS SUBSYSTEMS



## 1.1 DRONE SUBSYSTEMS

Manned and unmanned aircraft of the same type generally have recognizably similar physical components. The main exceptions are the cockpit and environmental control system or life support systems. Drones carry often different type of payloads (such as a camera). Some of the drones can carry heavy payloads like weapons and other armaments. Drone-system may divide following five subsystems:

**1. THE HUMAN ELEMENT** consists of the drone pilot and the possible payload operator, if necessary. Drone personnel also include maintainers, mission commanders and intelligence analysts. At the ground station, drone is operated remotely by a team of two: a pilot and a sensor/payload operator. The pilot's primary function is flying the plane, while the sensor operator monitors the performance of the many different sensor systems utilized by the drone. Payload operator uses the possible armament of the drone. The increase in autonomy in drones reduces and changes the role of human in operations.

**2. THE CONTROL ELEMENT** handles multiple aspects of the mission, such as Command and Control (C2), mission planning, payload control and communications. It can be ground-based, sea-based or airborne. The portion of the Control Element where the drone pilot and the payload operator are physically located is referred to as the Ground Control Station (GCS). Here too, autonomy is reduced the human activity.

**3. DATA LINKS** include all means of communication among the drone, the Control Element and every relay station and network node in-between them. They are used for any means of data transfer. Data and Control link functions are:

- Uplink from the ground station or a satellite to send control data to the drone.
- Downlink from the drone to send data from the onboard sensors and telemetry system to the ground station.

**4. THE SUPPORT ELEMENT** includes all the prerequisite equipment to deploy, transport, maintain, launch and recover the drone and enable communications. These tasks are typically conducted by Launch and Recovery Units (LRU).

**5. THE PAYLOAD** includes sensors (camera, laser pointer, IR-camera etc.), communication equipment, weapons or cargo. They are carried either internally or externally by the drone.

## 1.2 DRONE AUTONOMY

The autonomy allows reducing the frequency at which the operators must interact with the drone supporting the implementation of more robust system solutions, where the role of the operators is to manage and supervise, through appropriate human machine interface, the command and control functions without direct interaction.

There are various ways to discuss autonomy in weapon systems. According Maj Thomas Payne USAF (2017) although precise definitions are critical for design and engineering purposes, understanding the debate about autonomy requires an acknowledgment of these differing uses of the term, typically centered on ethically relevant subprocesses of the system as a whole; targeting, goal-seeking, and the initiation of lethality.

According US DoD (2018) autonomy is defined as the ability of an entity to independently develop and select among different courses of action to achieve goals based on the entity's knowledge and understanding of the world, itself, and the situation. Autonomous systems are governed by broad rules that allow the system to deviate from the baseline. This contrasts with automated systems, which are governed by prescriptive rules that allow for no deviations. While early robots generally only exhibited automated capabilities, advances in Artificial Intelligence (AI) and Machine Learning (ML) technology allow systems with greater levels of autonomous capabilities to be developed. The future of unmanned systems will stretch across the broad spectrum of autonomy, from remote controlled and automated systems to near fully autonomous.

Autonomous categories are:

- **Human-in-the-loop:** In this mode, humans retain control of selected functions preventing actions by the AI without authorization; humans are integral to the system's control loop.
- **Human-on-the-loop:** The AI controls all aspects of its operations, but humans monitor the operations and can intervene when, and if, necessary.
- **Human-out-of-the-loop:** The AI-algorithms control all aspects of system operation without human guidance or intervention. The autonomous drone engages without direct human authorization or notification.

Autonomy results from delegation of a decision to an authorized entity to act within specific boundaries. An important distinction is that systems governed by prescriptive rules that permit no deviations are automated, but they are not autonomous. US Office of the Under Secretary of Defense (2016) addresses that to be autonomous, a system must have the capability to independently compose and select among different courses of action to accomplish goals based on its knowledge and understanding of the world, itself, and the situation.



## 2. DRONE'S MILITARY AND CIVILIAN OPERATIONS



### 2.1 MILITARY OPERATIONS

The development of unmanned aerial vehicles is intensifying as technology becomes cheaper. Drones can be used in a flexible manner in different tasks such as intelligence, surveillance, target acquisition, and recognition missions, in strikes against surface targets, over-the-horizon relaying of information, Electronic Warfare (EW), Combat Search and Rescue (CSAR), Chemical, Biological, Radiological and Nuclear Warfare (CBRN), logistic replenishments and Counter Improvised Explosive Devices (C-IED) in a favorable environment or in areas where the risk level is elevated.

Drones are presumed to provide their services at any time, be reliable, automated and autonomous. Based on these presumptions, governmental and military leaders expect drones to improve national security through surveillance or combat missions. To fulfill their missions, drones need to collect and process data. Therefore, drones may store a wide range of information from troop movements to environmental data and strategic operations. The amount and kind of information enclosed make drones an extremely interesting target for espionage and endangers drones of theft, manipulation and attacks.

Various types of air domination systems are being considered to enable a military force to dominate an area from the air for extended periods and deny enemy movements and maneuvering. The unmanned combat aircraft can be divided into two categories according to their operating model: loitering or swarming.

In USA current systems under consideration are standard weaponized drones or small expendable loitering weapons, fitted with imaging sensors, such as the Low-Cost Autonomous Attack System (LOCAAS). Operating in swarms of "intelligent munitions" weapons, the LOCAAS can autonomously search for and destroy critical targets while aiming over a wide combat area.

A loitering weaponized drone (also known as a suicide drone or kamikaze drone) is a weapon system category in which the weaponized drone or munitions loiters around the target area for some time, searches for targets, and attacks once a target is located. Loitering systems enable faster reaction times against concealed or hidden targets that emerge for short periods without placing high-value platforms close to the target area and allow more selective targeting as the actual attack mission can be aborted.

### 2.2 CIVILIAN OPERATIONS

Various UAVs are increasingly being used for various civilian purposes, such as government missions (law enforcement, border security, coastguard), firefighting, surveillance of oil and gas industry infrastructure and electricity grids/ distribution networks, traffic control, disaster management, agriculture, forestry and fisheries, earth observation and remote sensing and communications and broadcasting. In 2016, PwC estimated the value added of the drone economy at \$ 127 billion. According SESAR (Single European Sky ATM Research) the growing drone marketplace shows significant potential, with European demand suggestive of a valuation in excess of EUR 10 billion annually, in nominal terms, by 2035 and over EUR 15 billion annually by 2050.

The development of the civil drone industry is dependent on the ability of drones to operate in various areas of the airspace, especially at very low levels. In aggregate, some 7 million consumer leisure drones are expected to be operating across Europe and a fleet of 400 000 is expected to be used for commercial and government missions in 2050.

Critical infrastructure (CI) includes large variety elements from nuclear reactors, chemical facilities, water systems, logistics and airports to healthcare and communications, and now drones are growing a very important part in this critical infrastructure environment. They have numerous tasks in critical infrastructure maintenance and protection. Human work is reduced, and tasks can be performed cost-effectively.

At the same time CI must deal with the new and emerging threat of drones. The most headline-grabbing risks tend to be those of physical and electronic attacks. For example, drones could carry explosives into a nuclear power plant or get close enough to execute cyber-attacks, causing disruptions or even mechanical failures or even stealing sensitive data. The low-cost, global proliferation and capabilities of drones weighing less than 20 pounds make them worthy of specific focus. Future adversaries could use these small systems to play havoc with critical infrastructure both in the air and on the ground, necessitating new actions to defend CI assets. Today several small UASs have payload capacity, extended range, and the ability to be GPS- or pilot-guided to locations with great precision.



### 3. DRONE SWARMING

➤ Drones are currently in widespread use around the world, but the ability to employ a swarm of these systems to operate collaboratively to achieve a common goal will be of great benefit to national defence. A swarm could support lower operating costs, greater system efficiency as well as increased resilience in many areas.

Zachary Kallenborn (2018) from US National Defense University defines drone swarm technology as the ability of drones to autonomously make decisions based on shared information. This has the potential to revolutionize the dynamics of conflict. In fact, swarms will have significant applications to almost every area of national and homeland security. Swarms of drones could search the oceans for adversary submarines. Drones could disperse over large areas to identify and eliminate hostile surface-to-air missiles and other air defenses. Drone swarms could potentially even serve as novel missile defenses, blocking incoming hypersonic missiles. On the homeland security front, security swarms equipped with chemical, biological, radiological, and nuclear (CBRN) detectors, facial recognition, anti-drone weapons, and other capabilities offer defenses against a range of threats.

McMullan (2019) argues that swarming drones come in different shapes and sizes. The DARPA, for example, has been working on a program dubbed Gremlins; micro-drones the size and shape of missiles, designed to be dropped from planes and perform reconnaissance over vast areas. On the

other side of the spectrum is the larger XQ-58 Valkyrie drone, measuring almost 9m in length. It has been called a 'loyal wingman' for a human pilot - able to carry precision-guided bombs and surveillance equipment. It recently completed its first successful test flight, although the eventual aim is for it to work in a group alongside a manned fighter jet. In either case, the biggest advantage of a 'swarm' is the ability of machines to work together in numbers.

Finland's MoD (2015) addresses that in some cases, drones can carry out missions better and cheaper than manned aircraft. The widespread proliferation of Micro Air Vehicles (MAV) which are difficult to detect is on the cusp of becoming extremely challenging for air defences. Even the smallest drones are suitable for intelligence and PGM target designation. Moreover, they can double as weapons, even inside buildings. The most radical concepts focus on replacing the intelligence-targeting-fire chain; they aim at achieving a rapid weapons effect with the coordinated use of swarming unmanned aerial vehicles. This requires sufficient survivability and cost-effectiveness from drones in order to saturate the defence.

Haberl and Huemer (2019) described in their conference paper the drone swarm attack. In 2018 the Russian Ministry of Defence announced that 13 drones, which had been fitted with small bombs managed to attack Russian bases in Syria. Such drones, which are intended to explode on impact need to be modified in order to carry explosives and it is easy to imagine how 3D-printing could come in handy in this regard, especially since drones are capable of evading missile warning systems without any additionally needed infrastructure or equipment.

”

**In some cases, drones can carry out missions better and cheaper than manned aircraft.**



## 4. CYBER THREATS AGAINST DRONES



### 4.1 CYBER VULNERABILITIES

According Hartmann and Steup (2013) drones are highly dependent on wireless systems and therefore can face considerable cybersecurity risk. Drone security has largely focused on exploitable vulnerabilities in either the communication channels or the hardware/software stack on the drone. Such attacks have focused on exploiting unencrypted communication over wireless media to implement eavesdropping, cross-layer attacks, signal jamming, denial of service, and dropping Wi-Fi communication with ground control, to name a few. Other attacks on drones involve GPS spoofing attacks to fool the drone into moving to a different destination (possibly with the intention of hijacking the drone).

Hartmann and Steup continue that the vulnerability may impose a threat to the systems security. Interestingly, attackers searching for targets go the same way as system architects designing a secure system. An attacker is searching for a system vulnerability imposing a high threat, implying a high risk. A system architect is trying to eliminate vulnerabilities imposing high threats and hardens the system through the integration of coping mechanisms. To heighten the systems security, it is essential that the system designer finds vulnerabilities before attackers do.

### 4.2 CYBER-ATTACK VECTORS

US Joint Air Power Competence Centre analysis (JAPCC) categorizes the cyber-threats against the drone according to the attacker's intention:

- **Intelligence.** Attackers could intercept and monitor the unencrypted data or information the drone transmits to the ground in order to derive intelligence.
- **Disruption** of the drone. Intentional modification of computer systems by use of malicious code, e.g. viruses, trojans, or worms taking advantage of familiar weaknesses of commercial operating systems.
- **Takeover** of the drone by taking over communication layouts and exploiting the systems bugs, or by way of 'smart entry' into the GCS and its computer systems or drones' avionics.

Harry Wingo (2018) reminds us that events such as the loss of a RQ-170 Sentinel to Iranian military forces on 4th December 2011 or the "keylogging" virus that infected an U.S. UAV fleet at Creech Air Force Base in Nevada in September 2011 show that the efforts of the past to identify risks and harden drones are insufficient. This causing concern over the potential compromise of highly sensitive surveillance capabilities. This incident sparked much research directed towards the hardware and software

security of unmanned vehicle systems. Also, the Predator UAV video stream was hijacked in 2009. Islamic militants used cheap, off-the-shelf equipment to stream video feeds from a UAV.

Next the cyber-attacks against the drone subsystems are described based JAPCC analysis.

### 1. HUMAN ELEMENT AND SUPPORT ELEMENT

Attacking personnel rather than the drone may be a favorable option for an adversary. Depending on the mission, drone personnel may be working at different locations. So, an adversary may execute the special operations against drone personnel group, which is usually very small in size

### 2. CONTROL ELEMENT

The Control Element consists of physical infrastructure (external hardware), computer systems (internal hardware) and non-physical software. All may be subject to different types of attack. The physical hardware may be attacked by kinetic weapons while the software may be a target of the non-kinetic attack. The Control Element's computer systems often include Commercial-off-the-Shelf (COTS) components. Identifying the multiple layers of contractors, subcontractors and suppliers contributing to the design or fabrication of a specific chip is difficult; tracing all the contributors for a complete integrated circuit is even more difficult. This widely dispersed supply chain may provide an adversary with opportunities to manipulate or compromised those components or penetrate the distribution chain with counterfeit products. The software components necessary to operate a drone are not limited to the GCS, but also include the drone, satellites and ground stations if applicable, as well as support systems for logistics, maintenance or Processing, Exploitation and Dissemination (PED). This variety provides an adversary with a broad spectrum of possible entry points into the drone system.

Kim Allan et. al states that **hardware attacks** can occur whenever an attacker has direct access to any of the drone autopilot components. An attacker can then corrupt the data stored on-board the autopilot or install extra components that can corrupt the data flow. These types of attacks can be carried out during the maintenance and storage of the drone or during the manufacturing and delivery. An attacker can link directly to the drone autopilot and damage it or reprogram it if he has the means or replace or add components which will give him control over the drone and/or the tactical data collected. Hardware attacks can affect the survivability of the drone, compromise control of the drone, and compromise the tactical data collected by the drone.





**NETWORK ATTACK** is most effective if there is regular access to it over time. This can provide the adversary with high quality intelligence that allows the surreptitious installation of malware for future use. Such an electronic backdoor is virtually undetectable by existing defensive technologies. It requires long term maintenance and preservation because of the continuous update process of the defensive systems designed to uncover malicious elements or activity.

**SOFTWARE CORRUPTION.** Military networks are usually separated from the public internet. This is done to provide the first line of physical or logical defence and protect them from unauthorized remote access. Drone are one of many nodes in the entire network centric environment and countermeasures providing cyber-security are usually applied using a comprehensive approach. Current security software suites offer a variety of methods to counter cyber-attacks. They typically include antivirus, configuration change detection, device control, intrusion detection and prevention, firewall and rogue system detection modules. Many of these modules are COTS applications integrated into the military security system. Simple changes to a malicious program's footprint can reduce its detection even for heuristic search algorithms because they can only defend against threats already known to the software, either by its signature or behavior.

### 3. DATA LINK

Data links connect drone with the GCS and enable the operators to remotely control the drone and receive transmissions. Possible EW targets for the adversary include the GCS, drone, satellites and satellite ground segments. From the enemy's perspective, the satellite's receiving antenna and the drones GPS antenna appear to be the most promising targets for EW engagements. Regarding the exploitation of transmitted drone signals, multiple discoveries of pirated drone video feeds have proven that

militant groups have adapted their tactics and have regularly intercepted Full-Motion Video (FMV) feeds. Shortly after these security issues were revealed, encryption of FMV streams was designated as a high priority. However, even today, not all currently fielded drone can transmit encrypted video feeds.

Data links connect the drone with the GCS, enabling operators to remotely control the drone and receive transmissions. Data links can be established either by radio for LOS communications or satellites and network nodes for BLOS communications. The radio transmissions may be subject to attack by EW whereas the network nodes may be attacked by means of cyber warfare. Disrupting drone data links by taking out the originators of the transmissions, i.e. the GCS, drone and satellite, or by acquiring access to any of these components by means of cyber-attack is also a viable option for an adversary.


According Kim Allan et. al (2012) **wireless attacks** can occur if an attacker uses the wireless communication channels to alter data on-board the drone autopilot. The worst-case scenario for this attack is if an attacker can break the encryption of the communication channel. Once this occurs, an attacker can gain full control of the drone if the communication protocol is known. Another possibility is an attack such as a buffer overflow that corrupts some data onboard or initiates some event. The most significant danger of wireless attacks is the fact that an attacker can carry out the attacks from afar while the drone is being operated.

**Sensor spoofing attacks** are directed towards on-board sensors that depend on the outside environment. Examples of such sensors are the GPS receivers, vision, radar, sonar, lidar, and IR sensors. An attacker can send false data through the GPS channels, or blind any of the vision sensors. The drone pilot relies heavily on sensor data for Guidance and Navigation, so corrupted sensor data can be very dangerous, Kim Allan et. al. argues.





## 5. DRONE CYBER SECURITY

 The best way to mitigate a threat is to avoid it; this is also true for the cyber-domain. According to JAPCC analysis suppressing cyber-threats may require pre-emptive infiltration of enemy systems with insertion of malicious code. If necessary, the adversary's cyber-weapon may then be terminated before it can impose a cyber-threat to friendly systems. Hence, pre-emptive cyber-attacks should be considered as an option to suppress enemy cyber-capabilities.

Focus to the human personnel is crucial, JAPCC argues. To prevent corruption, adversary recruitment or blackmail attempts, drone personnel should receive mandatory training to raise the awareness of those issues. Keeping the identities of drone personnel classified could also help to deter those activities. In addition, computer system access policies (both for software and hardware) should be as restrictive as necessary to defend against intrusion attempts or exploitation of human carelessness.

Security software suites and computer system access policies can only provide the foundation for drone computer system protection. JAPCC proposed that personnel with regular access to drone computer systems may be exploited by an adversary to circumvent protective measures, either unwittingly or unwillingly. To minimize the risk of corruption, adversary recruitment or blackmail attempts, regular training that raises the awareness of those issues should be compulsory for drone personnel. Keeping identities of drone personnel classified could also help to avert those types of activities.

Aviation data will be used by drone operations to plan flights. To prevent the possibility of intentional corruption of the data safeguards must be assured. Drone have already inadvertently been infected with malicious software through the careless use of USB memory sticks. According JAPCC in order to minimize the risk of drone computer systems being compromised by viruses, Trojan Horses and other malicious code, security techniques and policies must be improved. Security software suites must use the most current updates to cope with rapidly evolving cyber-threats. Computer system access policies, not only on the software site but also on the hardware site, should be as restrictive as necessary to

defend off intrusion attempts or exploitation of carelessness.

Cyber-security is an extremely fast and adaptive environment. Simple changes to a malicious program's footprint can reduce its detection even for heuristic search algorithms. JAPCC has informed that drone computer systems have already been infected with malicious software. This is most likely due to the prolific use of discs and removable drives. Once discovered, it took several years to disinfect the compromised systems. Eventually, the human factor turned out to be the weakest link for gaining access to even highly secured and physically separated networks.

The supply chain for microelectronics is extremely diffuse, complex and globally dispersed. This makes it difficult to verify the trust and authenticity of the electronic equipment used in the drone. According JAPCC deliberate modification of the product assembly and delivery could provide an adversary with capabilities to completely sidestep any software-based security countermeasures. For example, extraction of encryption keys by carefully modifying the involved integrated circuits has already been demonstrated.

Improvement of drone Command, Control, Communications, and Computer (C4) security must be comprehensive and should encompass the physical components required for drone communication, the computer systems (to include their software packages), the electromagnetic spectrum they operate in, and any personnel with access to the drone. Any of them may be subject to different types of attack and require different efforts to protect them. JAPCC addresses that the financial benefits of incorporating COTS computer hardware should be thoroughly balanced against the inherently superior security of proprietary systems. If COTS systems are preferred, trustworthy supply chains for these hardware components and their sub-components must be ensured. Also, capable, trustworthy and updated security software suites are essential in defending computer networks. Cutting off potential entry points into the drone, e.g. network bridges or removable devices, would further improve cyber security.

Use of the electromagnetic spectrum is required for all drone operations. Ground based links are used for controlling the vehicle, monitoring, and air traffic communications. These links are subject, to varying degrees, vulnerable to jamming, spoofing, and interference. JAPCC suggested that to prevent this from happening, a system of high-integrity, secure data links between the aircraft, the ground control stations, and air traffic facilities will be a fundamental requirement in approving drone operation. Future drone development should focus on reducing radio communications dependency by introducing new means of data transmissions and increasing drone automation.



## 6. DRONE AS A CYBER-ATTACK PLATFORM

➤ Dan Goodin (2014) described in his article how a drone that can steal the contents of smartphone is developed. Dubbed Snoopy drone can track not only Wi-Fi, but also signals based on radio frequency identification (RFID) and the Bluetooth IEEE 802.15 specifications (Personal Area Network (PAN), Wireless Personal Area Networks (WPAN) communication). Combined with a GPS that correlates signals to the location where they're detected, the capabilities let Snoopy spy not only on phones, tablets, and computers, but also, potentially, on pacemakers, fitness bracelets, smartcards, and other electronics. Plus, the geographically aware Snoopy can also be mounted on a low-cost aerial drone so it can locate and maintain radio contact even when subjects are on a morning run or situated in a high-rise building, a country inn, or some other out-of-the way location.

Dan continued saying that when mobile devices try to connect to the Internet, they look for networks they've accessed in the past. So Snoopy the drone can send back a signal pretending to be networks you've connected to in the past and so the smartphone believes being in trusted Wi-Fi network. When the phones connect to the drone, Snoopy will intercept everything they send and receive. Thus, is possible collect metadata, or the device IDs and network names, intercept usernames, passwords and credit card information. Installing the new cyber intelligence technolo-

gy on drones creates a powerful threat because drones are mobile and often out of sight for pedestrians, enabling them to follow people undetected. When we use different wireless devices and systems, we produce ourselves "digital terrestrial footprint." Based on this footprint, us can be followed, located and attacker has access to our messaging.

In an interview with Pritchard Stephen (2019), Tony Reeves former officer in the UK's Royal Air Force said that "There are plenty of reports to be found of individuals or organizations building or modifying drones to carry RF-based payloads including Wi-Fi tracking, capture and access capabilities – predominantly using Raspberry Pi and Wifi Pineapple devices, but also 2/3/4G network devices. Bluetooth sniffing is also possible. Putting a Wi-Fi access point on top of a building, or inside its perimeter, could allow hackers to listen in to data traffic. Drone operators could also drop a sophisticated microphone into a restricted area for eavesdropping, if technicians can overcome issues of power, weight and range."



**Putting a Wi-Fi access point on top of a building, or inside its perimeter, could allow hackers to listen in to data traffic.**



## CONCLUSION

➤ Security and cyber resilience are a priority area of development to mitigate the risk that drones could be subjected to malicious or accidental takeovers of datalinks leading to accidents, theft or deliberate use of the aircraft to damage infrastructure or hurt civilians. Security requirements of the drone, ground control station, data link infrastructure and even the data must be a fundamental consideration in system design – security by design principle. In addition to being vulnerable to security breaches, drones are also a security threat.

JAPCC argues that the challenge of incorporating security measures into unmanned systems is like that of manned systems, however there are C2 requirements which are unique to unmanned systems and expand their overall requirement for security. The added complexity of these systems and the new technologies they often employ increases the opportunity for adversaries to discover and exploit zero-day vulnerabilities, which may rapidly and severely compromise unmanned systems in new or unexpected ways. This system complexity along with the wide range of capabilities that these systems will be expected to perform will increase the number of attack surfaces for adversaries to exploit. Additionally, it will be challenging to ensure that the underlying architectures of unmanned systems consistently remain in a properly patched and

configured state to eliminate any known cyber vulnerabilities. Cyber is made more challenging by the rapid advancement in the capabilities and design of unmanned systems, which makes fully testing the security of each new iteration extremely difficult. The network needs to be able to handle adding new systems without that affecting the security, availability, throughput, or reliability. Cyber-security teams need to develop new techniques to monitor drones, and to keep confidential information safe.

US DoD (2018) addressed that unmanned systems may be at an even greater risk of cyberattack than traditional systems, due to their autonomy and potential operations in communication and/or GPS-denied environments. This risk is further exacerbated due to the lethal capabilities that some of these systems possess. As a result, cyber expertise and technology must be fully integrated from the onset in the development of unmanned systems architectures. These systems must also be designed with flexibility and the ability to add updates as new cyberattack vectors are identified, and new capabilities are incorporated. For unmanned systems to effectively operate, they must maintain high level cyber security of sensitive information. If adversaries can exploit cyber vulnerabilities in an unmanned system to corrupt any subsystems drones, the result could be a paralysis of the critical infrastructure and vital functions of the society.



### Main references

- > DoD (2018). Unmanned Systems Integrated Roadmap 2017–2042, 28 Aug. 2018
- > Goodin D. (2014). Meet Snoopy: The DIY drone that tracks your devices just about anywhere, 26 March 2014
- > Haberl F. & Huemer F. (2019). The Terrorist/Jihadi use of 3D-Printing Technologies: Operational Realities, Technical Capabilities, Intentions and the Risk of Psychological Operations, in proceedings of the ICCWS 2019, 28 February – 1 March 2019, Stellenbosch, South-Africa
- > Hartmann K. and Steup C. (2013). The vulnerability of UAVs to cyber-attacks – an approach to the risk assessment, in proceedings of the 5th International Conference on Cyber Conflict.
- > JAPCC. (2014). Remotely Piloted Aircraft Systems in Contested Environments A Vulnerability Analysis, September 2014
- > Kallenborn Z. (2018). The era of the drone swarm is coming, and we need to be ready for it, Modern War Institute at West Point, October 25, 2018
- > Kim A., Wampler B., Goppert J., Hwang I., Aldridge H. (2012). Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles, Infotech@ Aerospace
- > McMullan T. (2019). How swarming drones will change warfare, BBC News, March 16, 2019
- > MoD. (2015). Preliminary Assessment for Replacing the Capabilities of the Hornet Fleet Final Report, 8.6.2015
- > Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (2016). Report of the Defense Science Board Summer Study on Autonomy, Washington, D.C., June 2016
- > Papireddy T. (2015). Tracking and Monitoring Unmanned Aircraft Systems Activities with Crowd-Based Mobile Apps, University of Nevada, USA, 1 May 2015
- > Payne T. (2017). Lethal Autonomy What It Tells Us About Modern Warfare, Air & Space Power Journal, Winter 2017
- > Pritchard S. (2019). Drones are Quickly Becoming a Cybersecurity Nightmare, Threatpost, 22 March 2019
- > SESAR. (2016). European Drones – Outlook Study –Unlocking the value for Europe, November 2016
- > Wingo H. (2018). Beyond the Loop: Can Cyber-Secure, Autonomous Micro-UAVs Stop Active Shooters? in proceedings of the 13th International Conference on Cyber Warfare and Security ICCWS 2018, 8 – 9 March 2018