**CHAPTER**

**4**

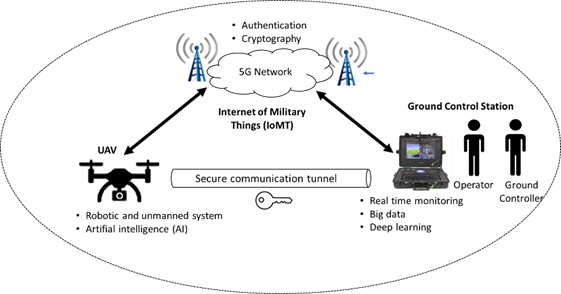
**UNMANNED WEAPON SYSTEM: CYBERSECURITY EMPOWERMENT FOR FUTURE WARFARE**

*Mohamad Tarmini bin Mohamad Openg and Anazida Zainal*

# INTRODUCTION

Modern warfare combines advanced integrated virtual reality (VR) and mixed reality (MR) systems with artificial intelligence (AI). Reality can be projected from virtual data. As a first step, the suggested mixed reality technology would be combined with all available sensors, such as air and surface surveillance radar, GPS, AIS, satellite image, IoT, camera sensor, etc. The system will be shared as a Common Operating Picture (COP) and integrated with inventory military assets like tanks, battleships, aircraft, and UAVs.

The global military uses various weapons. Legacy high-value weapons systems being employed alongside modern ones for decades to come. Modern weapons have hundreds of thousands of billion-transistor chips. This makes them complex systems. Military strategy has always relied on the virtual and autonomous environment, but the fast-changing world of global military operations requires it more. The Unmanned Weapon System (UWS) deploys to low-human-interaction operational regions to acquire and rapidly distribute ISR data. Today, UWS may be produced and upgraded by AI with mass production and cheaper cost than legacy systems. UWS will be designed and manufactured economically while preserving high-precision performance systems for enormous military buildup. This ultimate upgrade of this future UWS system can be employed as a platform for genuine military operations instead of limited legacy high-value weapon assets used for decades. UWS will patrol, analyse, identify, and dissuade targets. UWS can reduce soldier casualties in dangerous situations. UWS lets soldiers explore previously inaccessible battlefields. The suggested UWS structure is presented in Figure 4.1.



**Figure 4.1** Structure of the Proposed UWS

UWS is a lethal UAV developed as a weapon. Drones are avionic aircraft without a pilot that can be controlled from a distance or by themselves using software-controlled flight paths. GPS devices, and sensors. Compact and medium-sized combat UAVs are effective tactical weapons, but they have limitations. Here are the benefits: UAVs can rapidly give the most valuable combat operational data digitally. They watch a battlefield using high-resolution optics, data linkages, radars, and laser-guidance systems from the sky. Lingering at high altitudes over a target for hours, days, or weeks is a UAV's advantage. UAVs conduct ISR without adversary notice in remote and unreachable places, making them excellent instruments.

The only problem with UAV is that it needs good weather a lot (Standardization, 2018). The weather could get in the way of plans to expand UAV operations. When it comes to testing and tolerance standards for weather, UAVs are not as good as aircraft. ANSI (2018) said that being able to handle bad weather is a need and a high priority for technical and performance requirements for drones. Guidelines rarely talk about how weather affects the performance and safety of UAV flights (Roseman, 2019). Weather can affect a UAV's features. It is hard to know where, when, and how bad weather will affect drone operations, but most unmanned aerial vehicles (UAVs) shouldn't fly. For local drone operations, researchers have made a list of the weather resources and tools that are available and set up a risk-based framework based on weather forecasts, the number of people, the number of buildings, and the specifications of the drone. (Roseman, 2019).

The objectives of the UWS development are to:

* Use the latest technology to automate the operating system for the unmanned weapon system.
* Use AI to make weapon systems work better.
* Improve speed, accuracy, persistence, and coordination on the battlefield and in operation areas.
* Reduce the use of people and resources.
* Make important decisions by using command and control.
* Strengthening military operations can help protect national sovereignty.

Hence, the suggested UWS will add a deterrent so that threats can be denied and attacked when forced. Three ideas from UWS:

* Detect: Detect hazards by optimizing ISR. To maximize detection, military, and government radar sensors and UWS operations will be gathered.
* Ident: Identified risks using ISR tracking and information delivery networks. Commanders will use AI to process and analyze data.
* Deter; Prevent barriers by always having UWS in the area of operations and coordinating a joint surface intervention in deep focus areas. Threats will be shot or killed if necessary.

The unmanned weapon system will be protected by anti-drone jammers. Drones may be used in the future to keep an eye on the UWS because of the identified risks. To stop this from happening, all suspected drones will be jammed before they are taken in. The UWS system will use AI to process all inputs, especially photos and videos. For example, weapon detection can tell if a threat is armed and what kind of weapon it has. The people on the ground will know what to expect from the warriors. Vehicle movement detection is another way to figure out what the threat is. The economy and national safety will be affected by the use of UWS. Keeping borders safe could make things more stable and bring in more business and investment. Taxes, customs fees, and prices in the country will bring in more revenue for the government.

The usefulness of UWS depends on how well developers can turn a task into a math problem with answers and map or model the operating environment. For communication and full system integration, both old and new systems must work together. Modern network-based warfare requires that all of these systems be fully linked and able to work together (Robert & Mario, 2016). This paper looks at the future of the military in today's battlespace. It looks at the current system and how secure it is. It also looks at important cyber security variables and makes suggestions for disruptive cyber security technologies and basic needs.

# RELATED WORK

Throughout the Cold War, military R&D expenditures fostered technological advancement. Due to strong ICT, internet, and consumer electronics expansion, the business is multibillion-dollar. Commercial markets drive technology due to shorter product and innovation cycles. Modern military systems utilize commercially available off-the-shelf (COTS) components to save costs and enhance performance. The use of COTS components in high-value military systems has produced additional maintenance issues over the systems' lifetime. Changing the ICT components of a deployed weapon system often necessitates costly recertification in order to continue its operation. New ICT is developed once a year; however, military systems have a longer life span, making it costly to keep up with technological progress.

Some literature discusses autonomous weapons systems. Combat UAVs were created in both the United States and abroad. They have the ability to monitor, observe, and use weapons. Some of the listed works are combat-tested systems that revolutionized UAV warfare and were designed from scratch.

## ANKA-S

In 2000, Turkish Aerospace Industries (TAI) began making UAVs. Figure 4.2 shows the TUAV system, which includes all the advance features.



**Figure 4.2** ANKA-S

The TUAV system carries out real-time image intelligence, surveillance, reconnaissance, moving or stationary target detection, recognition, and identification missions during the night and in adverse weather conditions. The flexible design of the TUAV system supports various payloads and missions. Anka-S' redundant and autonomous flight control system allowed it to safely take off and land. The Anka-autonomous uses machine learning for takeoff and landing. SATCOM antennas and national flight control computers enable Anka-S connectivity. Electronic and communication intelligence (ELINT) payloads are also included.

In 2016, it was said that the TAI was making four Anka-S drones for the military, and in 2018, it was said that the Anka-S had finished its first round of live-fire testing. Roketsan's ammunition was used to test the platform. The Anka-S carried out Turkey's first "satellite-controlled airstrike" in August 2018, according to the Turkish Presidency of Defense Industries. Anka's first flight with a domestically made engine happened in December. In 2019, Anka flew for more than 24 hours, which was its previous record. Even though Anka can only fly about 100 miles, Anka-S can fly beyond "line of sight."

## BAYTRAKTAR TB2V

Bayraktar TB2 is unmanned combat aerial vehicle (UCAV) from Turkish. It is capable of autonomous flight. The Ground Control Station's aircrew uses satellites to monitor and control aircraft, including the use of armaments.

International standards categorize it as a medium-altitude, long-endurance UAV. However, to prevent it from competing with the TAI Anka UAV, the Turkish Armed Forces have renamed it to Tactical UAV Class. Each TB2 is made up of six platforms for aerial vehicles, two ground control stations, three ground data terminals, two remote video terminals, and equipment for the ground. Each aerial platform has an avionics system that is three times as good as the other two. Its ground control system is set up so that the pilot, the person in charge of the payload, and the mission commander can all command, control, and monitor the platform.

Bayraktar's flight control system enables autonomous taxiing, takeoff, cruise, landing, and parking without external sensors. The most significant component is the flight control system, which uses real-time sensor data to conduct sensor fusion algorithms. The mission control computer system handles the controls that are specific to the mission. The aerial platform is controlled by redundant rotary and linear servo actuators that are made to fit the platform's dynamics. All of the main avionics’ hardware, software, and equipment used in the air are constantly being updated and improved to work as well as possible. The onboard systems are run by an electronic power unit that has three high-tech, well-balanced alternators and lithium-ion battery packs to back it up. In the tail of the platform is a reconfigurable, heated camera unit for flight tracking, and all payload and telemetry data are captured in the airborne data recorder. The flexible architecture of the avionics enables the aircraft to land on several airfields independently if necessary. Even in the absence of global positioning system information, sensor fusion techniques can be employed to automatically navigate and land.



**Figure 4.3** Bayraktar TB2.

## 4.2.3 KARGU by STM

STM was created in 1991 by the Turkey Defense Industry Executive Committee. This technology is developed for managing projects, technology transfer, technical and logistical support, and consultancy services. The corporation is involved in several fields, including naval platforms, cyber security, unmanned aerial vehicle (UAV) systems, radar and satellite technology, and command and control systems. KARGU is a rotary-winged attack drone with fully autonomous navigation, tactical ISR, and precision-strike capabilities that will be constructed domestically in 2020. It is a 15-pound multi-copter with a maximum speed of roughly 90 miles per hour and a flight duration of 30 minutes. The autonomously operated platform is designed for both ISR and hitting targets outside the line of sight with pinpoint accuracy. During the day and night, the platform can detect and strike mobile or stationary targets with pinpoint precision. The system consists of an attack drone with rotors and a ground control unit.

The integrated machine learning algorithms of KARGU allow it to run autonomously and be manually controlled from a distance of up to nine kilometres. It can also build algorithms for image processing in real-time and deep learning. When the drone detects a target, it locks onto it using an explosive charge. The attack consists of three variants: (1) an explosive/fragmentation variation for humans and light vehicles, (2) a thermobaric variant for damaging structures and bunkers, and (3) a shaped charge for heavier armoured vehicles. KARGU is able to return safely to the operator if no target is found. The drone has LIDAR, a daylight camera, and an infrared camera. It is highly autonomous, can follow a predetermined flight path, and utilises deep learning algorithms to independently seek, track, and identify targets. The latest version of KARGU is rumoured to be capable of tracking and murdering human targets autonomously utilising facial recognition and artificial intelligence. STM is also developing the operation of swarm drones, which allows a number of drones to coordinate their operations in order to search efficiently and simultaneously attack several targets. KARGU was reportedly deployed against insurgents along the Turkey border.

# COMPUTING SUB-DISCIPLINE - CYBERSECURITY

Cyber security is the way businesses and governments manage security risks and the actions they take to protect the privacy, integrity, and availability of data and assets used in cyberspace. The concept is made up of standards, rules, and groups of protections, technologies, tools, and training in order to make the cyber environment and its users as safe as possible (Schatz et al., 2017). Cybersecurity technology has not kept up with the rapid growth of information technology, leaving systems and users vulnerable to both new and old dangers. These are some of the threats to technology and computer systems that could jeopardize cyber security. Cybersecurity can make it harder for attacks to succeed and lessen the damage to those that do (Scarfone et al., 2009).

UWS depends on aircraft and ground control being able to talk to each other well through secure real-time satellite communication, a ground network, and a radio transmission link. As the complexity of networked embedded control technology grows, it will become more vulnerable to cyberattacks, and these weaknesses must be carefully looked at. In modern warfare, all systems are increasingly interconnected and tend toward non-conventional warfare (NCW) circumstances. First, sensors that communicate with the outside world, like GPS or autonomous surveillance-broadcast, can be tricked into sending false data. A researcher has shown that GPS signals from military-grade drones can be falsified. Attackers could take control of a UWS if they got into the ground control station. Malware was found on UAS ground control stations that recorded keystrokes during UAS operations (Shachtman, 2011) At Creech Air Force Base in Nevada. Key loggers were used to get people's passwords, which made it possible for more complex attacks to happen.

On the basis of past intrusions, it seems anticipated that UWS will be subjected to more frequent and severe cyberattacks in the future. Security on the UWS is extremely crucial. A UWS that has been hacked might not be able to do missions like active warfare, combat support, military or police surveillance, firefighting, or search and rescue in the wilderness. If the hacker acquires access to any onboard weaponry or utilizes the UWS itself as a physical weapon, a compromised UWS might disclose confidential information and represent a grave threat to troop lives and property. The number of dangers will increase when numerous UWSs are combined into a network. Then, the communication links between network nodes will create new attack vectors. As shown in Figure 4.4, the UWS Communication Network needs to be protected from outsiders.



**Figure 4.4** UWS Communication Network

The UWS Project team must act as though the already-established hardware layer is unreliable. Consequently, it makes sense to prepare for the worst-case scenario. Therefore, you require a multilayered security approach that encompasses both avoiding intrusions and mitigating their effects. Encrypting data is required to keep it secure. Although data encryption prevents hackers from directly viewing the commands transmitted to a UWS, it does not prevent sensors from being faked or ground stations from being compromised. If a hacker has the proper tools, it is difficult to prevent them from faking sensors, and it is difficult to prevent a hacker from seizing control of a ground control station due to the complexity of their operating systems, which are vulnerable in a variety of ways. To make the UWS more resistant to assaults, UWS engineers must first determine the system's susceptibility to various types of attacks. Most of the time, a fault detection system can immediately recognize if someone is attempting to cause the vehicle to fail by dramatically modifying its condition, and efforts must be taken to thwart the attack. A stealth attack that impairs the operation without activating the ship's fault-detection systems is hence more dangerous. Multiple digital and physical UWS components must be securely integrated in order for a cyber security system to be secure.

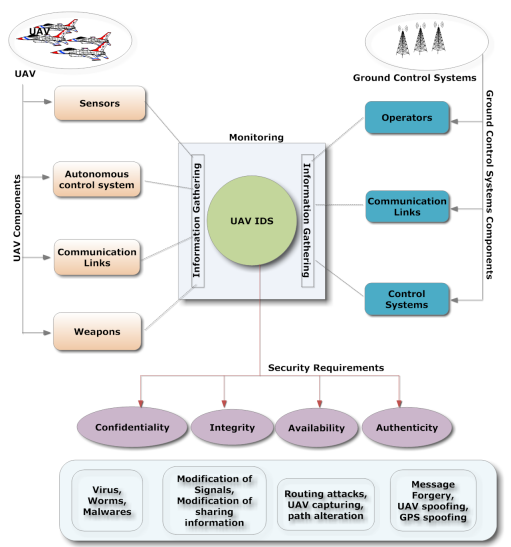
# RESULT AND DISCUSSION

Since intrusion prevention was already a component of the UWS development package, this study will concentrate on two of the five disruptive technologies that must be the primary focus if this project is to be successful (Boccardi et al., 2014). IDS and blockchain will be the first disruptive technologies to enhance UWS's cyber security.

## Intrusion Detection System

An Intrusion Detection System (IDS) is a piece of hardware or software that monitors connected networks or systems for indications of inappropriate behavior or policy violations. Any intrusion is often notified to an administrator or centralized by a security information and event management system. This system takes information from a variety of sources and employs alert filtering to distinguish between genuine dangers and false alarms. IDS must be developed specifically for UWS-based networks so that it can automatically analyze behavior or activities based on hypotheses and rules derived from the network's security standards. In this manner, it is able to identify odd or illegal behavior or acts. This system monitors system configurations, data files, and/or network traffic in order to detect potential assaults. The IDS is therefore designed to mitigate the consequences of assaults such that neither hidden nor public operations can exploit system vulnerabilities.

IDS is also designed to detect improper UWS usage. Misuse refers to any undesirable behavior that could compromise the performance or security of an entire group of UWSs. Possible attacks investigate UWS's vulnerabilities, which may stem from security problems in UWS networks, implementation flaws, or poor designs and protocols (Choudhary et al., 2018). IDS monitors signals, command traffic, control instructions, working behavior, energy consumption, and the operation of UWS components. As a network node, it also monitors the data flow and collects data from various UWS components. IDS can make communication more dependable and secure in a cost-effective and productive manner. An IDS can be implemented on a UWS or a ground control system to ensure the safety and dependability of the UWS and the ground control system. Installation of an IDS can be determined by the level of security required, such as in terms of confidentiality, availability, integrity, and authorization. Additionally, an IDS protects the UWS system from assaults and illegal operations. The UAV security policy offers simple criteria for detecting strange or potentially dangerous objects. Depending on the needs of the UAV system, these regulations can be created using various approaches or algorithms. Most UAVs on the market now include IDSs that utilise behavior-based detection techniques. Figure 4.5 depicts the suggested IDS paradigm for UWS.



**Figure 4.5.** An operational overview of IDS (*Source:* Choudhary et al., 2018).

## Blockchain

Blockchain is a technology comprised of distributed databases that are shared public or private ledgers of all digital events. Each transaction in the public/private ledger is confirmed when a majority of the agents in the system agree on what happened. Once information is in, it can never be taken out again. The blockchain has a record of every single transaction ever made that can be checked (Crosby et al., 2016). The blockchain technology is where it came from. Blockchain technology is different from most other information systems because it is not based in one place (decentralized), it is safe, it can be checked, and it can be used in smart ways.

Through the use of decentralized distributed ledgers hosted by groups of participating agents, blockchain makes it possible for many decentralized participants of any given blockchain to access, validate, and record data at the same time in a "write-once, read-many" way. For data transfers, digital fingerprints and signatures are made using cutting-edge cryptographic methods. Data integrity is kept by using consensus or protocols that are hard to hack and make sure that all nodes are in sync, as well as digital signatures that prove the content is real. Immutability means that ledgers can't be changed without the agreement of everyone in the network. If someone tries to change a block, the other people in the game will know about it. You can make "smart contracts" that automatically follow business rules when contractual or business obligations are met. The distributed nature of the ledger makes sure that all participants, no matter where they are or what kind of environment they are in, can do business with a common view (Adams et al., 2020).

Blockchains can be used to provide high-quality, verifiable data on a large scale to track all digitizable assets and transactions, such as cryptocurrency and tracking or audit data for physical or digital objects. UWS can employ block chain to infuse Internet of Things with a higher level of security and prevent data breaches by leveraging the technology's openness and virtual incorruptibility to keep things "smart." Decentralized credentialing systems based on block chain can mitigate cybersecurity risks. By removing passwords from a centralized server and replacing them with biometric and password-free authentication mechanisms, the UWS will be infiltrated in the long run.

The Internet of Things, tackling security challenges in UAV networks, and video surveillance systems, which are connected to this study, are just a few of the fields that could potentially benefit from blockchain's implementation (Barman et al., 2020; Jeong et al., 2019; Qiu et al., 2020). However, academics has not paid much attention to the prospects blockchain could present for video and data streaming applications, particularly for the benefit of UWS. Even though there have been various studies on the possible application of blockchain technology in the media and entertainment business, there has not been a thorough study of what is happening in industry and academia and how blockchain could benefit and focus on video and data streaming. Blockchain for military usage, particularly for UWS, is still up for debate, and the potential to study it further remains a concern.

# CONCLUSION

There are weapons and technologies from various eras present on the modern battlefield, making it a challenging environment. This can significantly affect the result of a conflict. This has a significant impact on cyber security, but it also makes these systems more susceptible to hackers.

Instead of employing cryptography and a VPN to safeguard UWS, IDS detects external and internal misuse, which is any undesirable action that could impair performance or security. Possible attacks examine network security holes, implementation issues, and faulty designs and protocols. As a network node, it monitors data flow and collects data from many sources. IDS improves communication reliability and security cost-effectively and efficiently. UWS was strongly advised to deploy IDS.

Numerous benefits are suggested by the research on how block chain can be implemented in numerous industries. Numerous studies have studied the potential applications of blockchain technology, but none have examined how it could facilitate data and video streaming. This demonstrates that block chain for military applications, particularly UWS live data streams, is still being considered and researched. This study advised implementing block chain for UWS decentralized credential solutions as well as biometric and password-free approaches to prevent hacking, notwithstanding this concern.

**ACKNOWLEDGEMENT**

This work was funded by the Universiti Teknologi Malaysia under Iconic Project Grant (PY/2020/04465)**.** We also thank to the Malaysian Armed Forces (MAF) for scholarship funding of this Master's Degree study.

# REFFERENCE

Adams, V., Alonso, M., Henry, W., Hyland-Wood, D. D., Jansen, W. C., Kodumudi, V., Nannra, A., Neidig, J., Nelson, M., Shenoy, N., Stevens, J., Sutherland, W. H., Taylor, I., & Tennenbaum, J. (2020).

*Potential Uses of Blockchain Technology In US Department of Defense*.

ANSI. (2018).

Roadmap For Unmanned Aircraft Systems, Version 1.0. *American National Standards Institute (ANSI)*.

Barman, N., Deepak, G. C., & Martini, M. G. (2020).

Blockchain for Video Streaming: Opportunities, Challenges, and Open Issues. *Computer*, *53*(7), 45-56.

Boccardi, F., Heath, R., Lozano, A., Marzetta, T., & Popovski, P. (2014).

Five Disruptive Technology Directions for 5G. *IEEE Communications Magazine*(52(2)), 74–80.

Choudhary, G., Sharma, V., You, I., Yim, K., Chen, I.-R., & Cho, J.-H. (2018).

*Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey* 14th International Wireless Communications & Mobile Computing Conference (IWCMC). ,

Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. (2012).

*Cyber security threat analysis and modeling of an unmanned aerial vehicle system.* IEEE Conference on Technologies for Homeland Security (HST),

Jeong, Y., Hwang, D., & Kim, K.-H. (2019).

*Blockchain-Based Management of Video Surveillance Systems* International Conference on Information Networking (ICOIN),

Qiu, J., Grace, D., Ding, G., Yao, J., & Wu, Q. (2020).

Blockchain-Based Secure Spectrum Trading for Unmanned-Aerial-Vehicle-Assisted Cellular Networks: An Operator’s Perspective. *IEEE Internet of Things Journal*, *7*(1), 451-466.

Robert, K., & Mario, G. (2016, 31 May-3 June 2016).

*Weapons systems and cyber security - a challenging union* 2016 8th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia.

Roseman, C. A. (2019).

*Targeted Weather Forecasts for Small Unmanned Aircraft Systems* 19th Conf. on Aviation, Range, and Aerospace Meteorology, Phoenix, AZ.

Scarfone, K., Benigni, D., & Grance, T. (2009).

Cyber Security Standards. *National Institute of Standards and Technology (NIST)*. (Wiley Handbook of Science and Technology for Homeland Security, John Wiley & Sons, Inc., Hoboken, NJ)

Schatz, D., Bashroush, R., & Wall, J. (2017).

Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*.

Shachtman, N. (2011).

*Exclusive: Computer Virus Hits U.S. Drone Fleet*. Wired.com.