Automated & Weaponized Remote Sensing:

Red Teaming Integrated Force Multiplying Technologies

Nicholas S. Caudill

School of Security and Global Studies, American Military University

ISSC231: Networking Concepts

Dr. Adam Harris

April 14, 2024

nicholas.caudill@mycampus.apus.edu

Abstract

This position paper describes plausible weapons systems that may be deployed by US adversaries today using state-of-the-art US devices and technology. This paper serves national security interests in understanding how dangerous the integration of force multiplying technology may be. Our thesis is explored through the perspective of a malicious actor with intentions to assassinate US persons and allies. This paper explores the integration of brain-machine or brain-computer interfaces, text-to-video large-language models, advanced virtual reality devices, drone warfare, and network communications methods with an underlying cloud architecture. We first introduce commercial remote sensing applications, then we describe specific devices and technologies, and lastly, we overview how these devices and technologies can be integrated into one weapons system. We discuss how a computer network connects each device, how software creates unexpected capabilities in human-controlled drone warfare, how cloud computing can be a backbone for an entire swarm of drones, and how operations security comes into play.

Keywords: brain-machine interface, brain-computer interface, virtual reality, cloud computing, drone warfare, text-to-video large-language models, computer networking, cybersecurity, automated remote sensing, internet of things

Introduction

This paper is written from the perspective of an adversary who wishes to do harm to US citizens or allies by repurposing US tools and technologies for malicious purposes. Our introduction will briefly describe, predict, and reflect upon changes within the automated remote sensing (ARS) area of telecommunications. We hope within this introduction to *prima facie* discuss the technology, discuss future trends, provide examples of relevant companies, consider regulatory concerns, and consider global implications of ARS. To red team, we explore how commercial ARS applications could be inverted for malicious intentions that are capable of doing great harm to Americans.

One ARS application is using high-altitude vehicles to perform reconnaissance from upwards of 20 kilometers above sea level (D'Oliveira *et al.*, 2016). A commercial ARS application is improving agricultural output by using computer vision to detect hazards within regions of concern (Ullo & Sinha, 2021). From a domestic security perspective, ARS can be applicable in preventing casualties of naturally occuring landslides by using "modern geospatial techniques such as aerial photogrammetry, satellite remote sensing images (ie, panchromatic, multispectral, radar images), and terrestrial laser scanning" (Mohan *et al.*, 2020). Lastly, Light Detection and Ranging technology is being augmented with digital elevation models to "provide an effective, low-cost alternative to airborne surveying" (Noh & Howat, 2015).

One global implication of ARS is the danger of cyberattacks obtaining control over unmanned automated vehicles (Petit & Shladover, 2014). "Persistent Aerial Reconnaissance and Surveillance Unmanned Aircraft Systems" are controlled autonomously by using both "Global Navigation Satellite Systems" (like GPS) and Inertial Navigation Systems which have

progressed so quickly and with such complexity to have escaped any coherent system of regulations (Colomina & Molina, 2014).

Google's Android holds a large market share over products that use technologies like Global System for Mobile communication (GSM) to power digital cellular networks used by mobile phones (Jivani, 2014). One implication is that many ethical applications of devices configured for ARS may be forced to comply with Android's monopoly, particularly when miniaturized drone products require the use of GSM. The centralized nature of a monopoly in the ARS technology sphere also raises security concerns. Some disagree that the GSM monopoly is really a threat, as Google's adoption of open architecture has resulted in Android smartphones becoming more difficult to hack than Apple iPhones, where iPhones are a "vulnerable monoculture" (Fridman, 2022). Some defend Google by arguing Google holds patents merely to protect itself, and say Google rarely offensively sues companies for patent violations, as doing so would harm Google's reputation within the open source community.

One might suspect future trends of ARS devices will improve in both capability and concerns. The explosion of large-language models (LLMs) and the internet-of-things (IoT) has made it possible for very poor countries to develop ARS devices by improving the learning rate of engineers and decreasing the cost of materials. This explosion in capability means terrorists can do more damage more anonymously for less money. On the contrary, more people get fed, quality of life improves, and defense infrastructure becomes more capable.

For optimists, the pros of ARS outweigh the cons. IEEE protocols 802.11, 802.15.1, and 802.15.4 now allow products designed for ARS to "move and connect with greater ease [as]

there are no restricting cables" (Wollschlaeger *et al.*, 2017). Unexpected features are now being found when new protocols can allow up to 100 sensors per cubic meter using 5G networks (23).

There exists many cutting edge technologies and it is important to conceptualize how computers, software, and technology could be combined by malicious actors. This paper is written from the perspective of an adversary who wishes to do harm to US citizens or allies by repurposing US tools and technologies for malicious purposes. For example, how might US national security be threatened when terrorists weaponize the combination of drones, Neuralink's brain-machine interface, OpenAI's text-to-video model Sora, and Apple's Vision Pro virtual reality device? The thesis of this paper is to describe each device and technology used within our weapons system, how a network can be structured that integrates these devices and technologies, and how a user interface can be built that brings about unexpected and devastating emergent capabilities within drone warfare.

Explaining the Devices and Technologies Used Within Our Weapons System

The Neuralink implant (NI) is a brain-machine interface device that is surgically inserted into a human's skull by a robot that allows users to externally control other devices through motor-imagery or imagining one's self performing an action, like telepathy. The application of machine learning techniques on the firing statistics of neurons within the human brain allows the NI to find correlations of neural activity during a session of motor-imagery. The NI allows neural activity to be decoded from triggered electrical fields to binary strings of 1's and 0's. These bits are then transferred via bluetooth radio to a device outside of the human body (Neuralink, 2022, 52:39). Earlier this year, Neuralink went public with its first human trial where Noland Arbaugh

spoke about the impact and life changing experiences that the NI has had on his life in overcoming his personal medical disabilities (Neuralink, 2024).

Apple's Vision Pro (AVP) specializes in taking virtual reality experiences to the next level by integrating very powerful video processing chips to create a seamless spatial canvas (Apple, n.d.). "The Apple Vision Pro, boasting a superior resolution of 3680x3140, offers remarkable scene simulation capabilities, enabling more realistic and immersive environments for both experimental and therapeutic applications" (Zhang *et al.,* 2023). We will later on explore how this virtual reality platform augments the remote controlling of drones.

OpenAI has taken the world by surprise by demonstrating breakthrough capabilities in its LLM. Now, OpenAI is soon to release Sora, which builds off of earlier technological success by creating a product that generates physics-realistic movies at a resolution and framerate (FPS) that is very impressive (OpenAI, 2024). Combining Sora with geographic information systems' data, remote sensing and satellite image data, one could create high resolution 'movies' that are spatially accurate. These movies could have lengths of more or less than 1 second and might be generated rapidly to accommodate for changes within a drone's position. We explore how Sora can augment the data sent to the AVP to create surprising weapons capabilities by processing and reconstructing low-representative (sparse) visual data.

Drone technologies hold a common misconception of being solely unmanned aerial vehicles but actually may operate in land or maritime operations, like ARS eels and lobsters that can traverse the sea floor. Gerstein & Leidy (2024) identified three species of swarm behavior, but this paper will focus on the leader-follower configuration using a group of aerial drones where each drone is approximately the size of two fists. Lopez *et al.* (2021) may be incorrect in

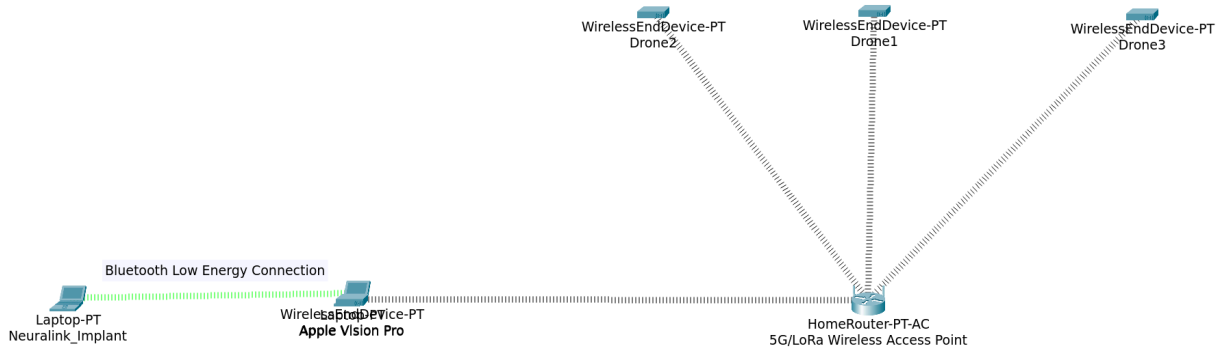
arguing that AI-controlled drones are a greater threat than human piloted drones. If the devices and software specified in this paper are integrated effectively, then one could argue that manually piloted drones could become more effective than autonomous drones. Drones are cheap weapons of war that are capable of overwhelming defenses by sheer numbers when grouped into swarms (Lopez *et al.,* 2021). Optimal swarm configurations might combine both piloting methods, like using autonomous drones to defend a single manually piloted drone. Contrary to common belief, drones do not need to be armed with explosives to kill. Cheap suicide drones could be remotely controlled up to 10 kilometers away, dropped from the sky onto a target, all the while being accelerated naturally by gravity during free fall to delivery enough kinetic energy to be fatal (Oosten, n.d.). We have outlined each device and will now describe the network that connects them together.

Describing the Network of Our Weapons System

We connect these devices and technologies with a network that uses a combination of Bluetooth Low Energy (BLE, the “preferred technology for IoT devices"), fifth-generation cellular (5G), and long range (LoRa) radio technology (Lonzetta *et al.*, 2018; Gerstein & Leidy, 2024). 5G can have multicast or broadcast capabilities by using point-to-multipoint transmissions within the radio access network (Saily *et al*., 2019). The NI and AVP would connect together via BLE as both devices “benefit from BLE’s ability to provide localized communications” (Yang *et al.*, 2020, 10). Both devices within a NI-AVP connection might have a 48-bit address of the IEEE802 standard (Nieminen *et al.*, 2015). The AVP has a more powerful network interface card (NIC) than the NI, therefore one could remotely control a drone over long-distances by using the AVP to connect with drones through a 5G or LoRa wireless wide area network (WWAN) (10).

The NI would be used to control the lead-drone. The AVP would allow the controller with a NI to see from a drone's perspective by installing cameras on a drone and transmitting that visual data. The NI-AVP connection would communicate through a BLE WLAN while the AVP-Drone connection would communicate through either a 5G or LoRa WWAN. Because a great distance exists between the controller and drone, the controller needs to both connect wirelessly with a drone and needs that drone to be equipped with cameras so the controller can direct a drone to targets. Since one with a NI can use motor-imagery to control the cursor of a mouse or keyboard telepathically, a trained drone controller should be capable of controlling the movement of the lead-drone telepathically and from a great distance. Since the NI uses BLE, the user would not be able to connect directly with a drone due to BLE's limitations in bandwidth and distance. The NI, in theory, should be capable of indirectly controlling a drone by communicating with that drone through the NI-BLE-AVP-LoRa/5G-Drone network, where the AVP merely acts as a middle-man repeater/converter. In one sense, our weapons system is converting BLE to either 5G or LoRa transmissions using the AVP.

Figure 1. (Made with Cisco Packet Tracer)



The NI should be able to control a drone by first communicating neural intent to the AVP, where the AVP would forward those communication frames via the 5G or LoRa WWAN, which could then be forwarded to a drone. We might expect powerful, new, and unexpected capabilities to be found by summing the parts. The user should in theory be capable of controlling drones wirelessly and from a great distance, possibly up to 10 kilometers away or more.

The network of this weapons system has three main nodes. A drone controller's neural intent is encoded from motor imagery neural data to bits and frames, those bits and frames are then sent from the NI to the AVP through a 2.4 Ghz BLE connection. The intent data (which represents how the controller wishes to manipulate the drone's rotary blades) is then sent over long distances from the AVP to a drone through the 5G/LoRa WWAN within the area of operation. There is a case to be made to use LoRa instead of 5G as the access point between the swarm and the AVP.

LoRa WWANs are capable of transmitting data over 100 square kilometers and are great for battery-dependent devices like miniaturized drones (Devalal & Karthikeyan, 2018, 286). LoRa WWANs have the advantage over physical or wireless LANs by having double AES encryption and by using the IEEE 802.15.4/2006 Annex B standard, which makes LoRa more secure than other WLANs/WWANs, which is great for warfare operations (285). LoRa WWANs are standardized by the LoRa alliance; a good LoRa WWAN uses a star topology network architecture (285). LoRa modulates with a chirp spread spectrum which is often also used by militaries (286). LoRa saves battery life by adopting the ALOHA method which only sends frames when absolutely necessary (287).

Drones could also be configured to report GPS coordinates obtained via satellites to the AVP, where the AVP then combines the drone's camera footage with OpenAI's Sora model. When adding geospatial data, infrared satellite data, and other remote sensing data, one might be able to create an accurate and dynamic real time movie of the drone's perspective that is displayed on the AVP. We tentatively omitted GPS satellite communications from Figure 1.

It is worth more research into LoRa and its integration with drone networks. For example, if each drone can only transmit 27Kb/s over LoRa WWANs, could it be possible to overcome this limitation by increasing the amount of drones within the swarm? If 10 drones are each transmitting 27Kb/s of sparse video feeds and the 11th drone reports only the GPS location, the group as a whole might be able to transmit 300Kb/s total, which could then be transmitted to the AVP for further processing. Lastly, the lead-drone could be the only drone that needs to receive instructions from the remote controller. The lead drone could pass controller instructions through a 5G WWAN as a work-around. The final solution might consider drones capable of participating in a combination of GPS, 5G, and LoRa networks to deliver the necessary data to the AVP.

The downfalls of LoRa WWANs are serious. Only 27 Kilobytes can be transmitted over a LoRa WWAN, which would be very challenging when trying to send both GPS data and sparse video data simultaneously (Devalal & Karthikeyan, 2018, 290). Furthermore, LoRa might not meet the real time requirements of controlling a drone from long distances using telepathy; kamikaze-ing a drone would require very time sensitive adjustments if monitored and controlled by a human (290). Other sources have argued LoRa can transmit a maximum packet size of 256 bytes. LoRa is just one example of a low-power/long-range WWAN; other options are SigFox or

Weightless-W (Noreen *et al.*, 2017). Let us now describe the vision system that allows the controller to view targets from the drone's perspective in real time and from great distances.

Human-Machine Interface: The Vision System

By combining OpenAI's Sora model with the AVP, drone camera feeds, and local geospatial data, the controller should be able to view high resolution spatial videos of the lead-drone's perspective. If the lead-drone were to be destroyed or lost connection, another lead-drone would be automatically chosen by network settings. One might ask "Why would one need Sora at all? Would it not be more efficient to simply transfer the raw video feed of a drone to the AVP?" The answer is that it is more optimal to have Sora reconstruct the raw video feed by providing Sora with a 'skeleton' video feed (sparse video data) together with CSV geospatial data. Since 5G and LoRa are not the fastest connections, these data minimizing efforts are necessary. This allows the controller to pilot a drone and see from the drone's perspective in real time by combining virtual reality, text-to-video LLMs, and telepathy.

Sora is necessary for converting a skeleton of the collected video feed into a comprehensible version. Sora is necessary for overcoming limitations when transferring tiny amounts of information. Since 5G cellular and LoRa have limited bandwidth and high latency between the controller and a drone, a passive transfer of only the bare minimum of a drone's visual data is needed. WWANs are limited in communicating throughout the electromagnetic spectrum largely because of the half-duplex nature of many WWAN species, moreso with LoRa than 5G. Wireless networks often use at least 70 percent of their bandwidth just for network management alone (Lammle, 2022, 423).

After the controller's NI sends a frame to a drone, that drone replies by sending a frame to the AVP. A continuous feed of very compressed sparse video data and controller instructors are sent through our weapons system's network. The final product has the AVP use OpenAI's Sora model to reconstruct the original video of a drone's perspective using the skeleton of the original visual data collected by the drone's camera. A high resolution geospatial landscape of the drone's first-person perspective is generated for the controller on the display of the AVP.

Devalal & Karthikeyan (2018, 289) specify that audio and video cannot be transferred through LoRa. A solution to LoRa's limitations is to adopt OpenAI's Sora model or similar technologies to bypass limitations in bandwidth and distance while attaining the battery-saving and security advantages LoRa offers. Since we are sending a skeleton version of a video feed from on-drone cameras, data could be sent at optimized intervals. It is not necessary to transfer a 60 FPS video when LoRa could transfer a 1 FPS video and have Sora process and reconstruct that video to be similar to the original 60 FPS video. This would enable users to be capable of seeing landscapes from the drone's first-person perspective through the AVP's display in real time. Later on, we will discuss the merits of offloading computations of the AVP to a dedicated supercomputer using cloud architecture.

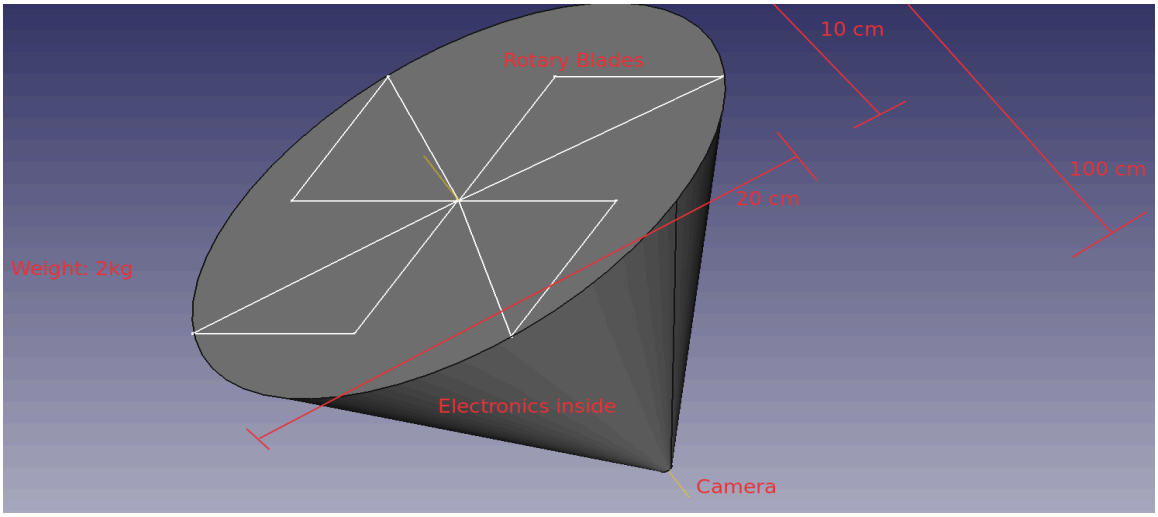
Drone Architecture

Since our drones are designed to kill, a swarm of ten drones might send three drones to execute a target. Drones would be manufactured in the shape of a cone pointing downwards to maximize aerodynamics, to minimize air resistance, and to optimize the force multiplying effects of gravity. A camera is placed pointing towards the ground at the tip of the cone. Above the

spherical top of the cone would be helicopter-like rotary blades with several degrees of freedom at the base.

Between the camera and rotary blades would lie the electronics and batteries needed to facilitate WWAN communication and to power the drones. A wireless NIC is placed inside each drone or at least inside the lead drone (Lammle, 2022, 429). This NIC might be a SX1278 LoRa module that connects to an Arduino microcontroller inside the drone's cone-shaped body (Semtech.com, n.d.). The size and specs of each drone would be determined by kinematic equations from physics. Furthermore, following kinematic equations show that one hypothetical 2Kg drone might not need to fly more than 100 meters in altitude to deliver a directed free fall with enough force to kill.

Figure 2. (Made with freeCAD)



A swarm might operate in ad hoc mode if the LoRa or 5G WWAN is not considered an access point (AP). One might assume APs are stationary ground objects and not designed for dynamic flight. Terrorist groups with an excess of resources might use SIGINT aerial vehicles to

extend the perimeter of WWANs. It might be interesting to explore leader-follower drone configurations where the lead-drone acts as a local wireless access point. Thus, WLANs in infrastructure mode might be preferable for leader-follower drone configurations (Lammle, 2022, 433).

Programmers can direct a drone by prompting LLMs with commands like “fly between two buildings” (Schmidt, 2024, 10:00). This application can simply be included in our architecture by having controllers simply imagine the words “fly between two buildings,” where the NI converts these thoughts into bits that may be sent to a drone through our WWAN. Controllers then have three options to control a drone: by imagining commands as sentences, by imagining one controlling the rotary blades of a drone, or a combination of both. One might wonder if the drone’s perspective in video could be compressed down into LLM tokens, and then have those tokens sent over the 27Kb/s LoRa WWAN to the AVP, where the AVP converts that tokenized sparse video data into a form that may be displayed for the controller on the AVP’s video display screen.

Operations Security

For network security, the WLAN and WWAN should use MAC address filtering, EAP-TLS, and geofencing precautions to harden the network, assuming such tight constraints allow for these security features in the first place (Lammle, 2022, 618). The drones themselves and the customized AVP should be secured with both digital and physical multi-factor locks and keys. The worst case scenario is for an attack to be stopped because an adversary intercepts or disables our drones through cyberattacks, aerial anti-aircraft missiles, or physically arresting the human controller. Thus, the drones should be equipped with countermeasures to deal with

anti-aircraft missiles, like flares. Areas of operation should have the physical perimeter secured around the controller with security guards. Control over air and cyberspace should be obtained and maintained.

Furthermore, the human controller should be secured in a command and control center behind multi-factor locks and keys, preferably within an underground bunker or space station. It may be necessary to have the network communications from the AVP go through a decentralized wired network to bypass connectivity issues of a solid concrete bunker that might be several hundred meters below ground (Lammle, 2022, 639). Cameras, guards, and other protection level 1 precautions should be in place during operations (FAS, n.d.). Inspirations for Cyber OPSEC might be obtained from *USAF Doctrine 12: Cyberspace Operations* (USAF, 2013, 8). Inspiration for airspace control procedures may be obtained from *Joint Publication 3-30: Joint Air Operations* (Joint Chiefs of Staff, 2021, II-4). Inspiration for physical and signals OPSEC might be found in *US Army regulations 530-1: Operations and Signals Security* (Army, 2005, page 8 §II 3-3).

Leader-follower swarm configurations might be configured to have the leader drone be the most expensive piece of hardware in the entire swarm. The leader could act as a local WLAN virtual controller to manage APs. One threat vector against our swarm is one rogue drone entering our drones' proximity and establishing itself as an AP to perform peer-to-peer attacks (Lammle, 2022, 452). Ad-hoc networks are more vulnerable to cyberattacks, so swarms might favor infrastructure networks, as mentioned earlier (452). Since there are many limitations for our weapons system, security might not be perfect and some tradeoff decisions will need to be made, like settling for MAC address filtering over more dedicated encryption methods (456).

Geofencing might be useful as well, where drones could deny communicating with any devices, e.g., more than 100 meters away (457). It may even be good OPSEC to hide which drone is the leader and protect it within the center of the group. Firewalls between nodes within our network might also improve OPSEC/INFOSEC.

Terrorist OPSEC relies on decentralized cells to escape detection and to move faster than bureaucratic nation-states. To strengthen INFOSEC, within the frames that are sent by drones or within communication networks involving terrorist websites, a terrorist might embed/inject/append artificially-generated child sexually exploitative content (AGCSEC) to prevent amateur or professional OSINT efforts like internet/IoT web scraping.

In fact, a terrorist might even write a script that identifies the source of web crawlers scraping a terrorist's website by using nmap, and then forward that identifying data and evidence (of collecting/downloading AGSCEC) to every publicly known law enforcement agency (LEA) in order to get OSINT amateurs arrested for downloading AGCSEC. This 'AGCSEC-wrapped INFOSEC' sends lists of IP addresses collecting CSEC to LEAs. A terrorist might even configure their router or PC to append AGCSEC to every frame and packet that leaves their TOR-network node so that they have leverage on anyone that communicates with them and refuse to comply with their terroristic demands. Wrapping frames and packets might also deter IoT web scrapers, meaning INFOSEC becomes OPSEC. In an ironic way, LEAs would be protecting the terrorists by adopting these methods. A LLM like Falcon could probably provide step-by-step instructions describing how to embed every frame with AGCSEC that is to be sent by hosts running Whonix operating systems (OS) and might also generate the AGCSEC itself to counter CSEC-verification techniques used by Homeland Security.

Figure 3.

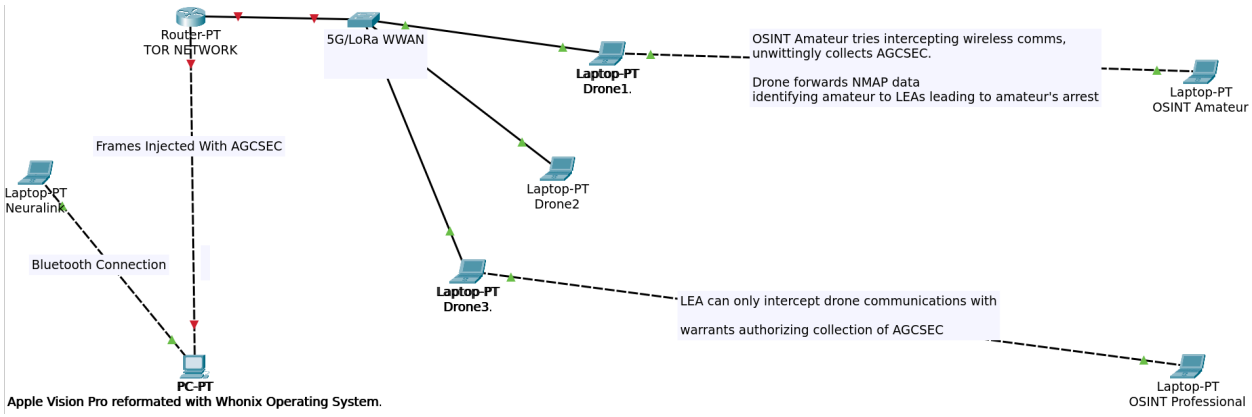
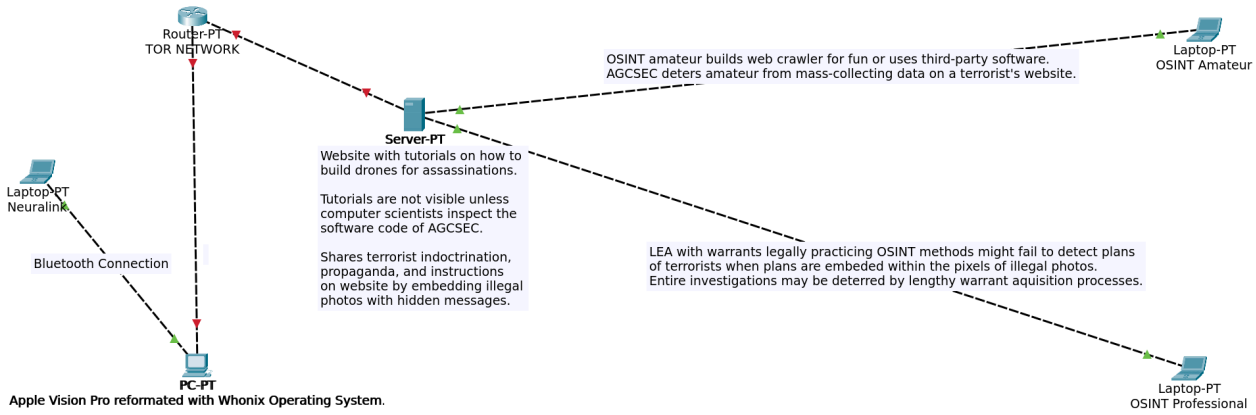


Figure 4.



Cloud Supercomputers

Infrastructure as Code (IaC) means devices in our weapons system may act as resource light terminals where supercomputers do a majority of the computational work, which opens the door for virtual botting and automation (Lammle, 2022, 704). We propose developing a supercomputer that handles all computation within the entire network thus far described. Thus, the physical devices involved (NI, AVP, drones) will act as resource-lite GUI/terminals.

We propose reformatting each device by imaging onto them the barebones Arch Linux OS so that more sophisticated OSs can be displayed on a virtual machine powered by our supercomputer (cloud). Thus, each user/controller interface in the stack might appear as a user-friendly OS, but in reality is really a hollowed display sent over the network by a supercomputer. This may allow for video feeds of a drone's perspectives to be sent over LoRa WWANs since the data is processed by the supercomputer rather than the other three main devices (nodes).

Thus, it makes no sense for any device to have any OS locally installed besides Arch Linux as any more complicated and user-friendly OS can be computed by supercomputers in the cloud, given one has an internet connection. This makes one wonder, can iPhone/Androids receive and store their complicated OS, obtained through cellular networks, while offline or after being power-cycled—where Archlinux might be the only actual OS physically imaged on the device? In this hypothetical yet plausible scenario, the complicated OS might be temporarily stored as cached memory.

Building Supercomputers for Cloud Architecture

Our first requirement is to decode, process, and compress neural intent data for transmission to the drones. The current NI can do this on-chip, but this is poor design when computation can be done on the cloud. Our second requirement is to compress, transmit, decompress, process, and display drone video recordings in real time. The third requirement is to discard a majority of the computational work done onboard the AVP and replace it with nothing but a powerful NIC, motherboard, and necessities for Arch Linux and virtual reality display.

From here, we rebuild the AVP OS with our cloud supercomputer so the controller can visualize a drone's perspective in real time, in high resolution, and at high frame rates. Thus, a duplex connection to the supercomputer Platform-as-a-Service (PaaS) cloud is required to facilitate our dynamic intent-and-response communications weapons system.

Each of the three main devices might now be viewed as a software-defined network where each device has an application programming interface to interface with the supercomputer (Lammle, 2022, 719). We hope the supercomputer cloud will allow a LoRa WWAN to bypass the real time video streaming limitations of the AVP-LoRa-Drone network by using OpenAI's Sora to reconstruct the sparse JSON dataset of the original video. Forbes writes "Machine learning PaaS providers include Google Cloud, Vertex AI, Cirrascale, Lambda, CoreWeave, and Paperspace" (Forbes, 2023). "The concept of cloud computing is…where processing information does not need to happen at the source" (Nel & Jooste, 2016, 56).

Lammle discusses networking concepts are moving towards IaC (Lammle, 2022, 721?). The consequence of this movement means IaCs will now be essentially built from prompting LLMs. In other words, the building of a supercomputer for our weapons system's communication network is in large part the output of a LLM. Thus, to design our supercomputer is a matter of typing well-phrased English commands into a textbox, where the LLM will provide us with step-by-step instructions to build our supercomputer and entire weapons system. One could imagine integrating LLMs with robotic builders to completely automate the physical task of building our supercomputer and weapons system. It is likely that this service is already being provided within the market.

Conclusion

The thesis of this paper was to describe each device and technology used within our weapons system, how a network can be structured that integrates these devices and technologies, and how a user interface can be built that brings about unexpected and devastating emergent capabilities within drone warfare. We have shown how cheaply manufactured drones can kill from great distances using telepathy. The implications of this weapons system will likely mean more sanctions and regulations will be placed on the devices and technologies involved, from microchip-manufacturing to the dissemination of software in order to prevent hostile state and non-state actors from harming US persons and allies. One might suspect that the psychology of US citizens will not change in light of these advancements in weaponry since society has now long been accustomed to and desensitized by the nuclear gun barrel pointed directly at them.

This paper, in a holistic view, has demonstrated how AI and machine learning can improve the performance of drones and real time communications with those drones. We showed how cloud computing is necessary to "manage the amount of [visual] data generated" by offloading the processing of that data away from the individual nodes themselves and onto supercomputers (Nel & Jooste, 2016, 60). While the IoT and cloud computing allows "data to be processed faster," these methods now allow humans to be slaughtered more quickly en masse by fewer malicious actors and with less financial resources (61). If IoT is an "interconnected network of machines," the NI shows that humans are now deeply intertwined within this network of machines, which possibly paves the way for the merge, singularity, and transcendence (60). One solution to drone and CBRN threats is to digitize or informationalize our brains and minds to transcend the limited biological carbon body (Caudill, 2023; Chalmers, 2010; Chu, 2014).

References

Apple. n.d. Vision OS. *Apple Developer*. Retrieved April 5, 2024, from https://developer.apple.com/visionos/labs/.

Army. (2005). *Operations Security: Operations and Signal Security*. Army Regulation 530–1. https://irp.fas.org/doddir/army/ar530-1-2005.pdf .

Caudill, N.S. (2023). Human-Machine Interaction: Revealing Security Concerns Posed by Artificial Life. *Automated Intelligence Community College.* https://doi.org/10.5281/zenodo.10968007.

Chalmers, D. (2010). *The Singularity: A Philosophical Analysis.* Journal of Consciousness Studies 17:7-65.

Chu, T. (2014). *Human Purpose and Transhuman Potential.* Red Wheel/Weiser.

Colomina, I., & Molina, P. (2014). *Unmanned aerial systems for photogrammetry and remote sensing: A review.* ISPRS Journal of Photogrammetry and Remote Sensing, 92, 79–97. https://doi.org/10.1016/j.isprsjprs.2014.02.013.

Devalal, S. & Karthikeyan, A. (2018). *LoRa Technology - An Overview.* Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2018, pp. 284-290, doi: 10.1109/ICECA.2018.8474715. keywords: {Batteries;Logic gates;Wireless fidelity;Chirp;Conferences;Embedded systems;IoT;LoRa;LoRaWAN;LoRa Alliance;Embedded Systems}.

D'Oliveira, F., Melo, F., & Devezas, T. (2016). *High-Altitude Platforms - Present Situation and Technology Trends. Journal of Aerospace Technology and Management*, 8(3), 249–262. https://doi.org/10.5028/jatm.v8i3.699.

FAS. (n.d.). *DCID 6/3 - Manual.* (n.d.). Irp.fas.org. Retrieved April 11, 2024, from

https://irp.fas.org/offdocs/DCID_6-3_20Manual.htm#Confidentiality%20Requirements.

Forbes. (2023). *NVIDIA Bets Big On Public Cloud To Deliver Its AI Supercomputing And Omniverse Platforms.* Forbes. Retrieved April 11, 2024, from https://www.forbes.com/sites/janakirammsv/2023/03/23/nvidia-bets-big-on-public-cloud-to-deliver-its-ai-supercomputing-and-omniverse-platforms/?sh=64b5dac2aedc.

Fridman, L. (2022). *Nicole Perlroth: Cybersecurity and the Weapons of Cyberwar | Lex Fridman Podcast #266*. https://youtu.be/hy2G3PhGm-g?si=Kv-HIO5oZ14XvyW6.

Gerstein, D., & Leidy, E. (2024). *Emerging Technology and Risk Analysis: Unmanned Aerial Systems Intelligent Swarm Technology.* Homeland Security Operational Analysis Center operated by the RAND Corporation. https://www.rand.org/pubs/research_reports/RRA2380-1.html.

Joint Chiefs of Staff. (2021). *Joint Publication 3-30 Joint Air Operations.* https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf?ver=GSL5OjFm-wwhdBTNEXJx9Q%3d%3d.

Jivani, M. (2014). *GSM based home automation system using app-inventor for android mobile phone.* International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 3(9). https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=812fc94d95dd140052bc00da3b74cf675fc09c42.

Lammle, T. (2022). *CompTIA Network+ Study Guide : Exam N10-008: Vol. Fifth edition*. Sybex

Lonzetta, A., Cope, P., Campbell, J., Mohd, B., & Hayajneh, T. (2018). *Security Vulnerabilities in Bluetooth Technology as Used in IoT.* Journal of Sensor and Actuator Networks, 7(3), 28. https://doi.org/10.3390/jsan7030028.

Lopez, J., Perumalla, K., & Siraj, A. (2021). *CCWS 2021 16th International Conference on Cyber Warfare and Security.* Academic Conferences Limited.

Mohan, A., Singh, K., Kumar, B., & Dwivedi, R. (2020). *Review on remote sensing methods for landslide detection using machine and deep learning.* Transactions on Emerging Telecommunications Technologies, (), –. doi:10.1002/ett.3998.

Nel, C., & Jooste, W. (2016). A technologically-driven asset management approach to managing physical assets - a literature review and research agenda for "smart" asset management. South African Journal of Industrial Engineering, 27(4). https://doi.org/10.7166/27-4-1478.

Neuralink. (2022). *Neuralink Show and Tell, Fall 2022.* https://www.youtube.com/live/YreDYmXTYi4?si=AKC3GrBSrX5W1L0K.

Neuralink. (2024). *Neuralink Live Update*. https://youtu.be/ZzNHxC96rDE?si=_zIbL7DXKBpZbmvp.

Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., & Gomez, C. (2015). *Ipv6 over bluetooth (r) low energy* (No. rfc7668). https://www.rfc-editor.org/rfc/pdfrfc/rfc7668.txt.pdf.

Noh, M. & Howat, I. (2015). *Automated stereo-photogrammetric DEM generation at high latitudes: Surface Extraction with TIN-based Search-space Minimization (SETSM) validation and demonstration over glaciated regions*, GIScience & Remote Sensing, 52:2, 198-217, DOI: 10.1080/15481603.2015.1008621.

Noreen, U., Bounceur, A., & Clavier, L. (2017). *A study of LoRa low power and wide area network technology.* 2017 International Conference on Advanced Technologies for Signal and Image Processing (ATSIP). https://doi.org/10.1109/atsip.2017.8075570.

Oosten, C. V. (n.d.). *The Physics behind the Real Danger of Falling Tools – Airitas.* https://www.airitas.com/the-physics-behind-the-real-danger-of-falling-tools/.

OpenAI. (2024). *Introducing Sora — OpenAI's text-to-video model.* https://youtu.be/HK6y8DAPN_0?si=RjCI5idIV0sIGNYp.

Petit, J., & Shladover, S. (2014). *Potential Cyberattacks on Automated Vehicles.* IEEE Transactions on Intelligent Transportation Systems, 16(2), 1–11. https://doi.org/10.1109/tits.2014.2342271.

Saily, M., Barjau, C., Navratil, D., Prasad, A., Gomez-Barquero, D., & Tesema, F. (2019). *5G Radio Access Networks: Enabling Efficient Point-to-Multipoint Transmissions.* IEEE Vehicular Technology Magazine, 14(4), 29–37. https://doi.org/10.1109/mvt.2019.2936657.

Schmidt, E. (2024). *AI and Quantum Computing: Glimpsing the Near Future.* https://youtu.be/gZZan4JMwk4?si=EpqALPd74Vsa_AH2.

Semtech.com. (n.d.). *SX1278*. Www.semtech.com. Retrieved April 6, 2024, from https://www.semtech.com/products/wireless-rf/lora-connect/sx1278#features.

Ullo, S, & Sinha, G. (2021). *Advances in IoT and Smart Sensors for Remote Sensing and Agriculture Applications.* Remote Sensing, 13(13), 2585. https://doi.org/10.3390/rs13132585.

USAF. (2011). *Air Force Doctrine Publication 3-12 Cyberspace Operations Catalog of Doctrine Topics Introduction to Cyberspace Operations.* https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf.

Wollschlaeger, M., Sauter, T., & Jasperneite, J. (2017). *The Future of Industrial*

Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0. IEEE Industrial Electronics Magazine, 11(1), 17–27. doi:10.1109/MIE.2017.2649104.

Yang, J., Christian, P., Pramita, & Neubecker, C. (2020). *Beyond beaconing: Emerging applications and challenges of BLE. Ad Hoc Networks,* 97(), 102015–. doi:10.1016/j.adhoc.2019.102015.

Zhang, Z., Mateu, L. G., & Fort, J. M. (2023). *Apple Vision Pro: a new horizon in psychological research and therapy.* Frontiers in psychology, 14, 1280213. https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2023.1280213/full.