E.M.P CREW PRESENTS:

# TENGU MARAUDER

## Combining Robotics and Cybersecurity

COGITO ERGO SUM

EX MACHINA PARLOR

LEXICON

# Personal Bio

My name is Lexie Thach and I've been working in cyber for over 10 years now. I currently work as a lead cybersecurity engineer at a government R&D organization. In my spare time I run a local hackerspace called the Ex Machina Parlor. We've presented at DEFCON, Ivy league universities and other local security conferences.



# EX MACHINA PARLOR?

## WHAT IS IT?

We're a local hackerspace that is located in Philadelphia with 3D printers, laser cutters, robots, drones and a full server lab with enterprise emulation. One our main focuses is cyber and robotics

We have made presentations at

- DEFCON31
- DEFCON32
- Jawncon
- Local PA security conferences

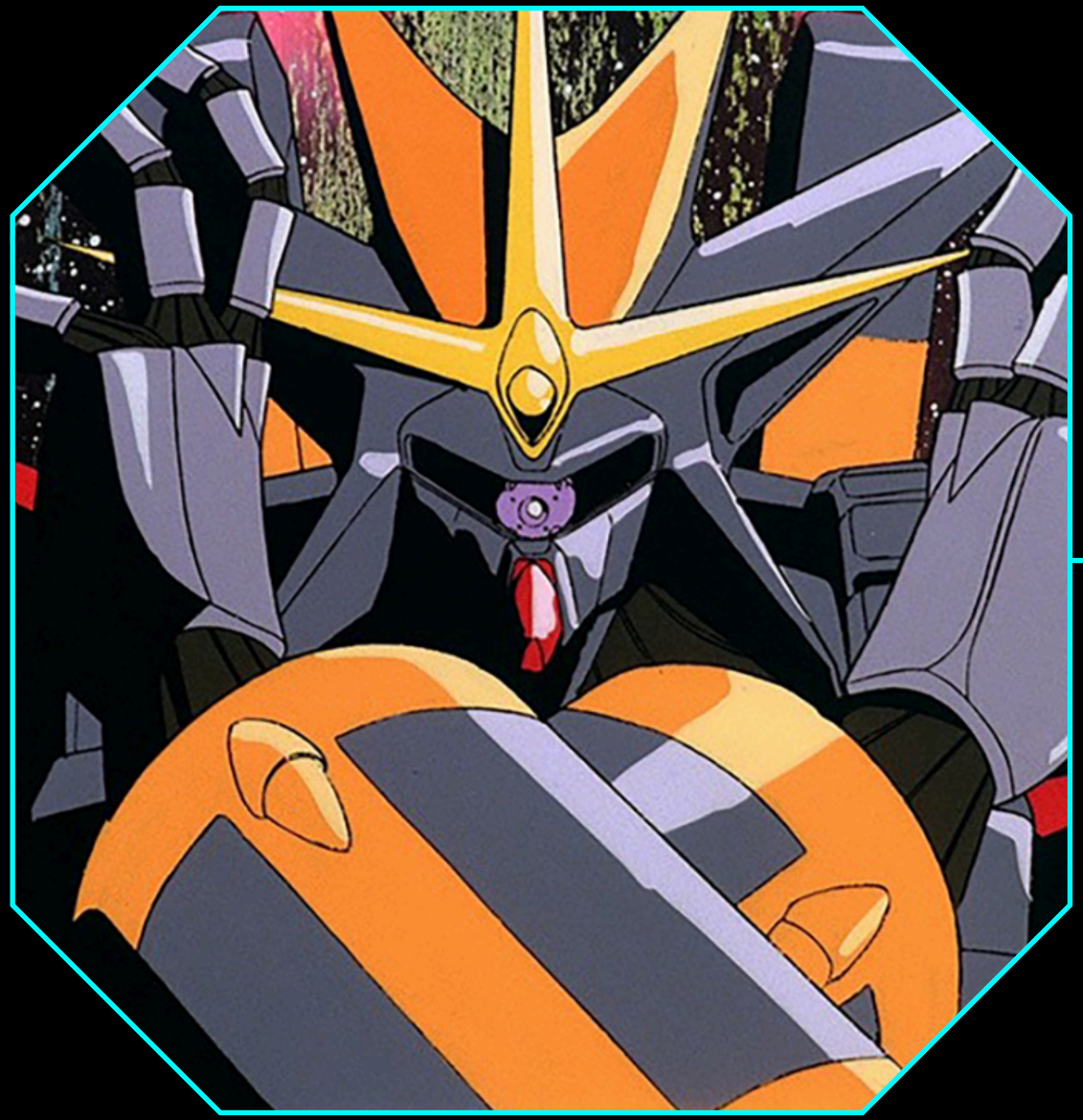
# WHAT IS A ROBOT

## DICTIONARY TERM

Robotics Definition by Standards
According to the ISO 8373 standard, a robot is defined as:

"An actuated mechanism programmable in two or more axes with a degree of autonomy, moving within its environment to perform intended tasks."

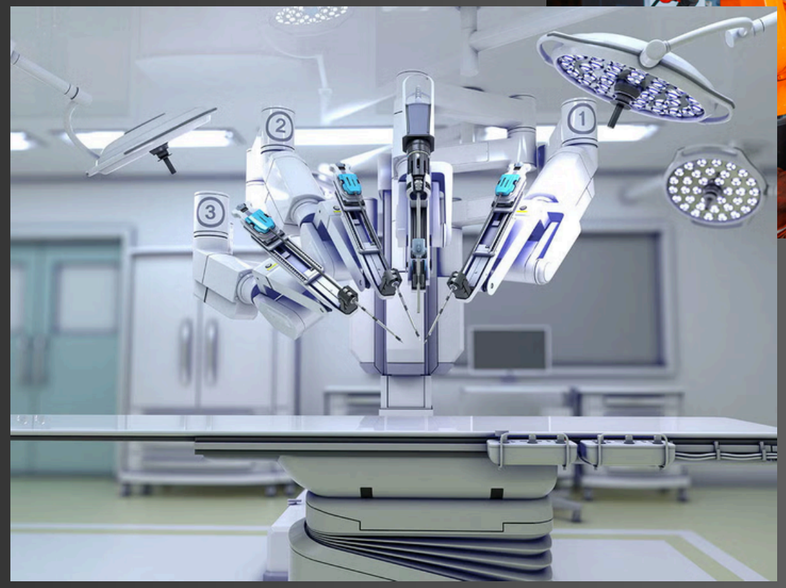
Broadly defined as a machine capable of carrying out a complex series of actions automatically, often programmed by a computer.

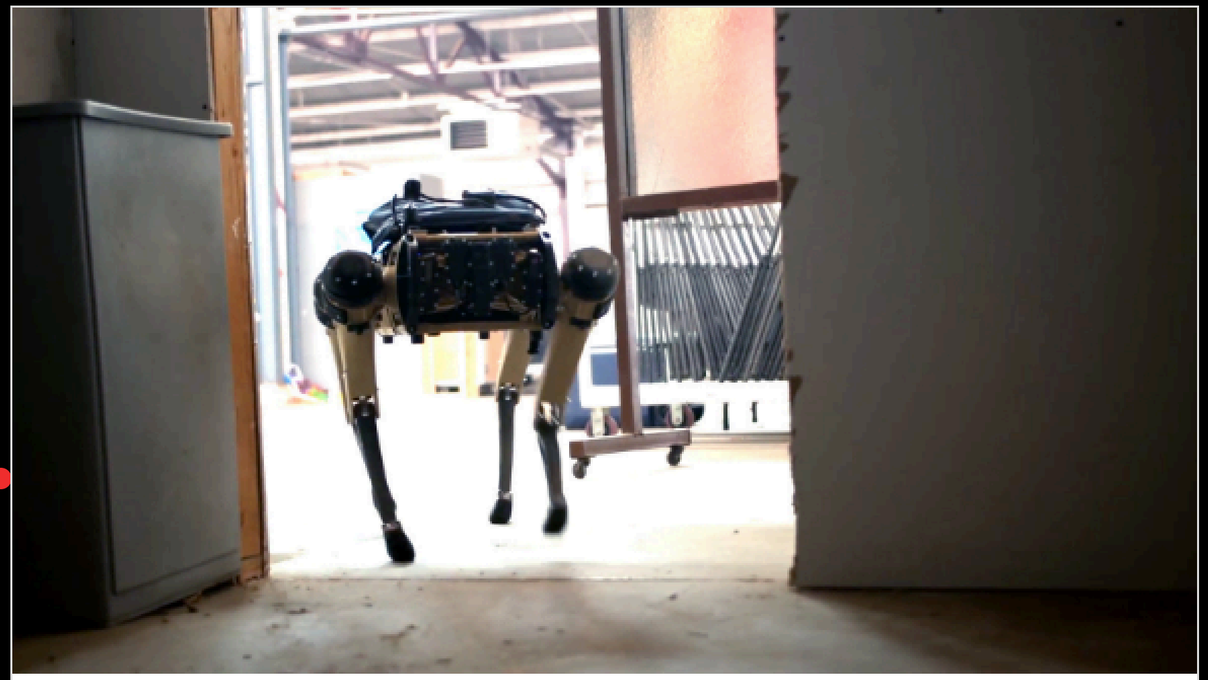


# USE CASES

## REAL WORLD SYSTEMS

- Industrial automation
- Drones and autonomous vehicles
- Healthcare robotics



**Dog-like robot jams home networks and disables devices during police raids — DHS develops NEO robot for...**

Smart home defenses crumble when the NEO dog arrives.

Tom's Hardware / Jul 23, 2024

# MODERN DAY UNITS 1

## COMMON THREATS AND THEIR IMPACT

At the 2024 Border Security Expo a Quadruped Unmanned Ground Vehicle (Q-UGV) NEO was unveiled. Produced by Ghost Robotics NEO is equipped with an antenna array that is designed to overload home networks, thus disrupting devices that rely on Wi-Fi and other wireless communication protocols. It will thus likely be effective against a wide range of popular smart home devices that use wireless technologies for communications.


**Ukraine blinds Russian target seekers with drone-on-drone combat**

Opinion: Ukrainian forces have found success in downing Russian spy drones with cheap, first-person-view drones, analyst Federico Borsari finds.

# MODERN DAY UNITS 2

## COMMON THREATS AND THEIR IMPACT

Ukraine disturbs Russian reconnaissance and targeting capabilities by participating in drone-on-drone combat and using modern electronic warfare tactics. Showcasing affordable and flexible techniques in modern warfare, this approach mixes commercially available and military-grade drones to intercept and disable opponent UAVs. The strategy underlines how weaker countries might use drone technology to get tactical benefits against more powerful military forces.

# SECURITY IN ROBOTICS

## EMBEDDED SECURITY

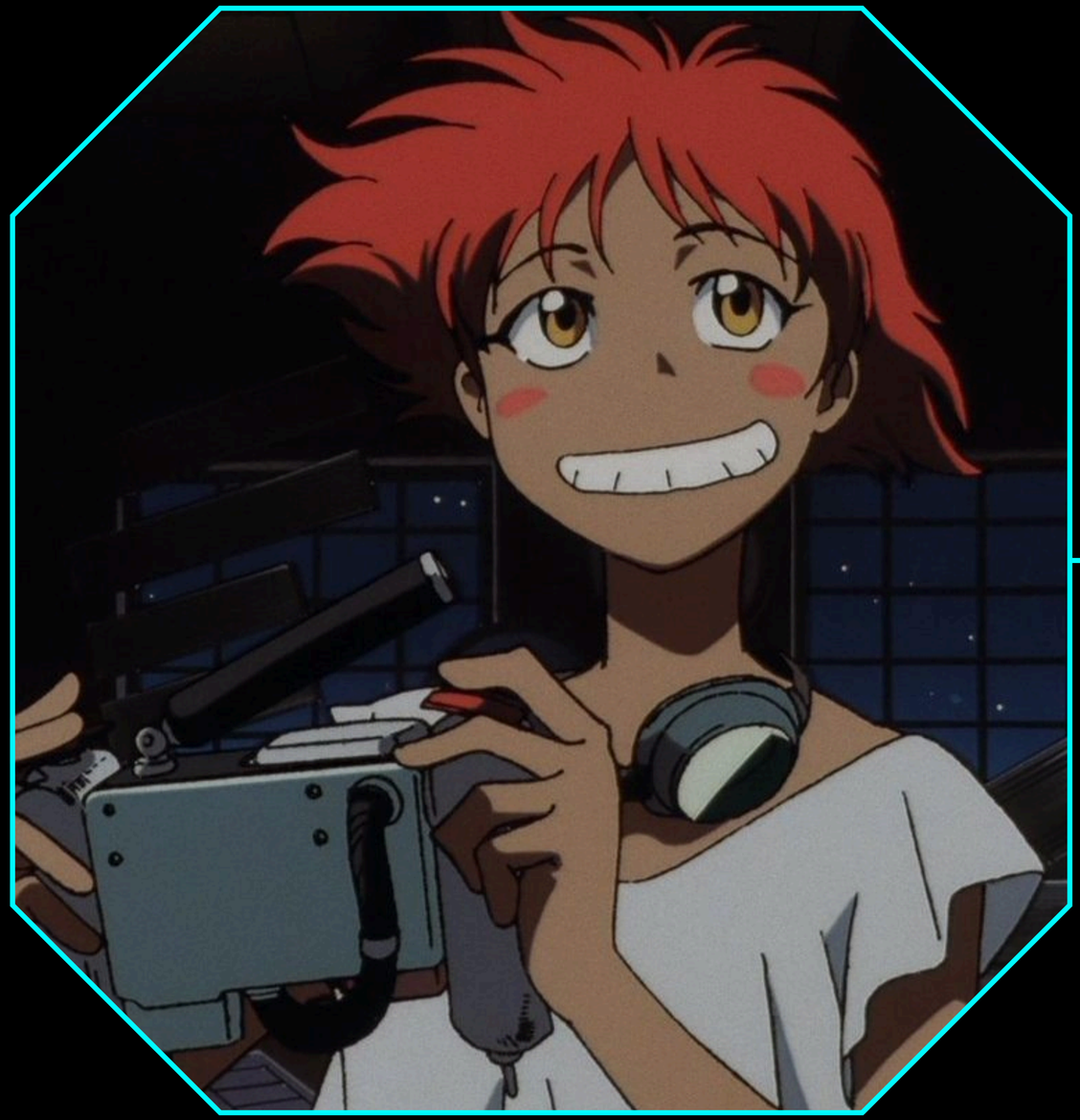
Protection of microcontrollers, firmware, and communication channels in robotic systems.
Robots interact with the physical world — attacks can cause real harm
Embedded systems have limited resources → harder to secure
Common vulnerabilities: firmware tampering, unsecured interfaces, wireless attacks
Key facts:
70% of IoT/robotic devices have at least one serious security flaw
Attacks on embedded systems can lead to full system compromise
Securing robots protects safety, data, and autonomy


REFERENCE: MIT Article

# CYBER & ROBOTS

## WHY I THINK IT'S IMPORTANT

- Cybersecurity is an integral part of our lives whether we like it or not
- With the innovations of technology we tend to forget the dangers
- We're living in a super fast changing world with AI, ML and automation.
- Robots will continue to become more and more intertwined in our daily lives.
- We need to understand the benefits and concerns of this technology frontier even if we're afraid to.



# TENGU

## DICTIONARY TERM

Inspired by the fabled Tengu—birdlike, red-faced creatures from Japanese folklore noted for their mix of knowledge and mischief, the Tengu Marauder project Originally viewed as disruptive spirits, Tengu developed into masters of martial arts, flight, and spiritual strength and guardians of holy places. The design of the Tengu Marauder reflects this duality by combining attacking and defensive powers in robotics and cybersecurity. Like its namesake, the project questions limits with purpose and accuracy, running on the brink of cunning and control.

# MARAUDER

## URBAN DICTIONARY

A marauder is typically defined as someone who roams around in search of things to steal or attack, often linked to raiding or plundering. In the context of the ESP32 Marauder, the term is repurposed to describe a compact, portable tool built on the ESP32 microcontroller for wireless network reconnaissance and penetration testing. It "marauds" Wi-Fi environments by scanning networks, sniffing packets, performing deauthentication attacks, and exposing vulnerabilities—essentially acting like a digital raider in the wireless spectrum.

E.M.P CREW PRESENTS

# BREAKSLIDES

WE'LL RESUME SHORTLY

# BACKGROUND

## THE INITIAL CONCEPTION

In 2023 for DEFCON31 one of our crew built a proof of concept interceptor drone called the Strix Interceptor using ardupilot, a HackRF SDR, DragonOS and a donated 3DR X8 drone from Carnegie Mellon
However that iteration ran into a lot of issues with programming and interoperability
We learned a lot from that experience and wanted to share what worked and what didn't in our next project

TENGU

MARAUDER

# DEVELOPING THE TENGU MARAUDER

## COMMON THREATS AND THEIR IMPACT

The new goal now was to pare down the original idea into a more accessible project that people could crowdsource their own parts. We wanted this to be achievable with a Raspberry Pi, 3D printed parts and a flipper zero.

This new iteration, the Tengu Marauder was designed to be a learning and development platform to understand the intersection of robotics, cybersecurity and wireless pen testing. It's important to learn these new concepts with systems presently being developed with the same capabilities and different purpose.

# WARNING

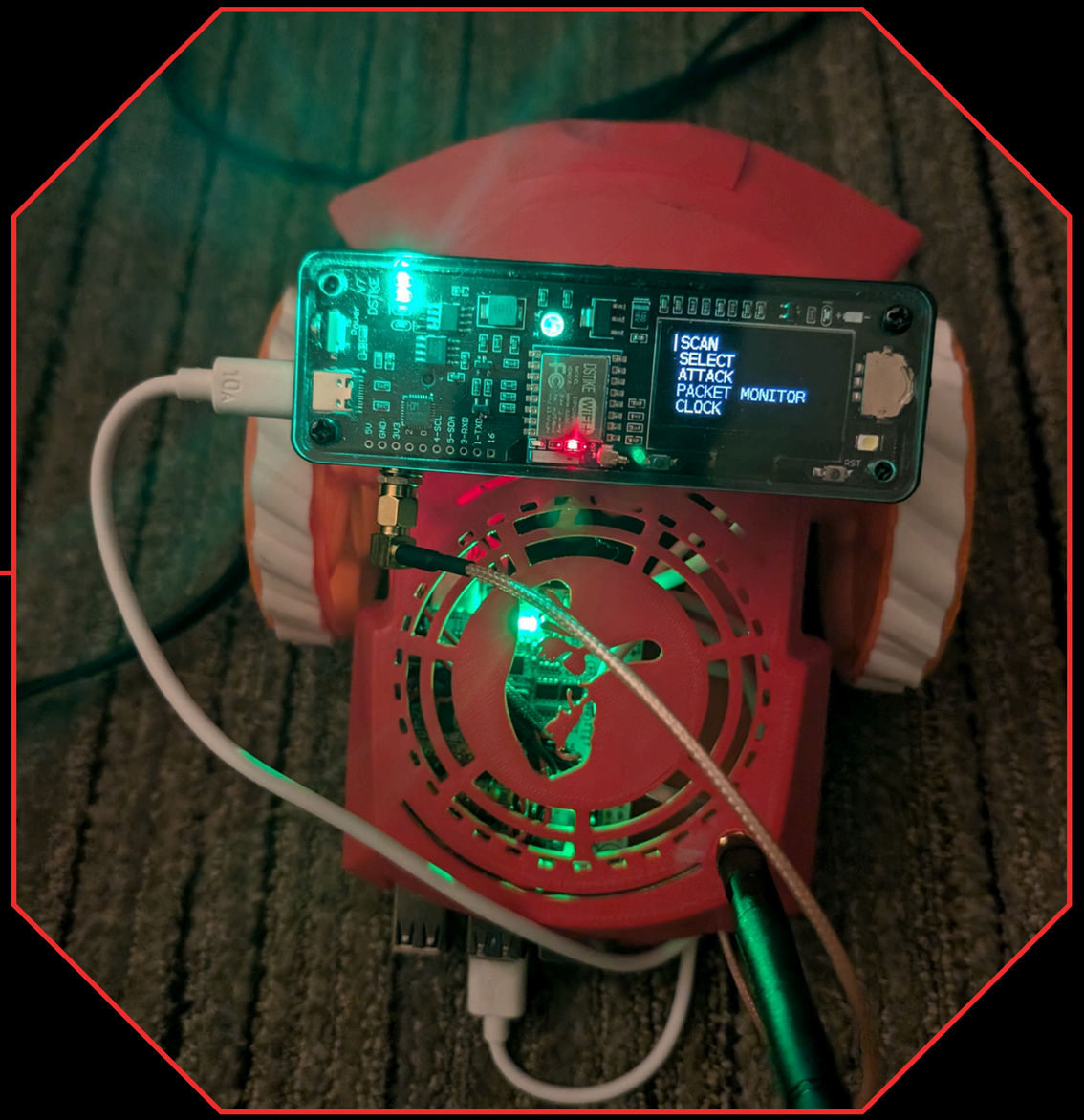
DURING THE DEMO DO NOT ATTEMPT TO DISRUPT ANY WIRELESS SIGNALS IN THIS ROOM

ANY ATTEMPT TO REPLICATE THESE TOOLS AND TACTICS IN AN UNAUTHORIZED MANNER IS ON YOU

WE HOLD NO LIABILITY OR RESPONSIBILITY ON YOUR ACTIONS SHOULD YOU CHOSE TO USE THIS ON YOUR OWN

# SPECIFIC LAWS

49 U.S.C. § 44801(5): Defines a counter-UAS system as a device capable of lawfully and safely disabling, disrupting, or seizing control of a drone. Does not cover detection-only systems. Wiretap Act and Pen Trap Statute: These laws may apply to the interception of electronic communications, including those used by drones. Unauthorized interception could result in criminal penalties. FAA Reauthorization Act: Allows certain government agencies to intercept or take control of drones that pose a security threat. These powers are not extended to private individuals or companies. DHS Regulations: The DHS has regulations that may apply to drone interception and jamming, particularly in relation to national security and critical infrastructure protection.




# TENGU MARAUDER:

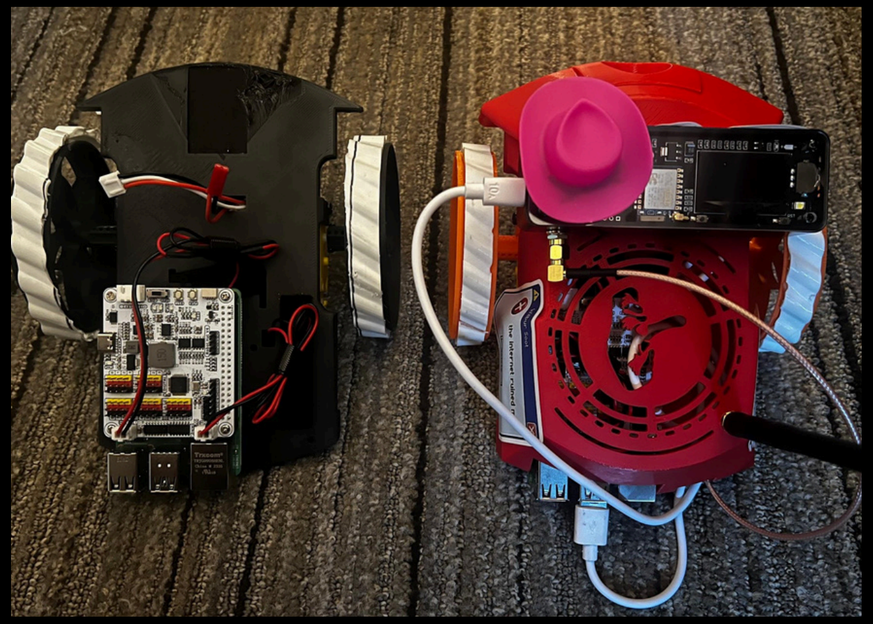
## AUTONOMOUS TWO-WHEELED ROBOT.

Key Components:

- Raspberry Pi , running Ubuntu 22.04 or PiOS ESP32* Marauder
- Main Functionalities:
- Autonomous movement, WiFi scanning capabilities , deauthentication attacks.

# HARDWARE COMPONENTS

Raspberry Pi: Running Ubuntu Pi Desktop 22.04
DStike ESP 8266: Running Marauder or other ESP wifi device
Chassis: Miniature Unmanned Ground Vehicle (UGV) platform with dual motor drivers.
SunFounder Pi Motor hat



# SOFTWARE

Python 3.X or higher

SunFounder robot-hat library with installation for motor hat on raspberry pi

Tengu Marauder code base

# BEST PRACTICES FOR SAFETY

DO NOT USE ON NETWORKS THAT YOU DO NOT OWN OR HAVE AUTORIZATION ON

HAVE A SECURE AREA FOR TESTING

# MOTOR CONTROL

## BASIC OPERATIONS

For the purposes of this demostration we will be accessing the Tengu Marauder over a secured WiFi connection as most commonly used devices such as IOT use WiFi to access different network devices.

The motor control script just uses the sunfounder hat to move the motors left, right, up and down.

Additional integrations for servos, manipulators and other devices can be added to the hat if needed.

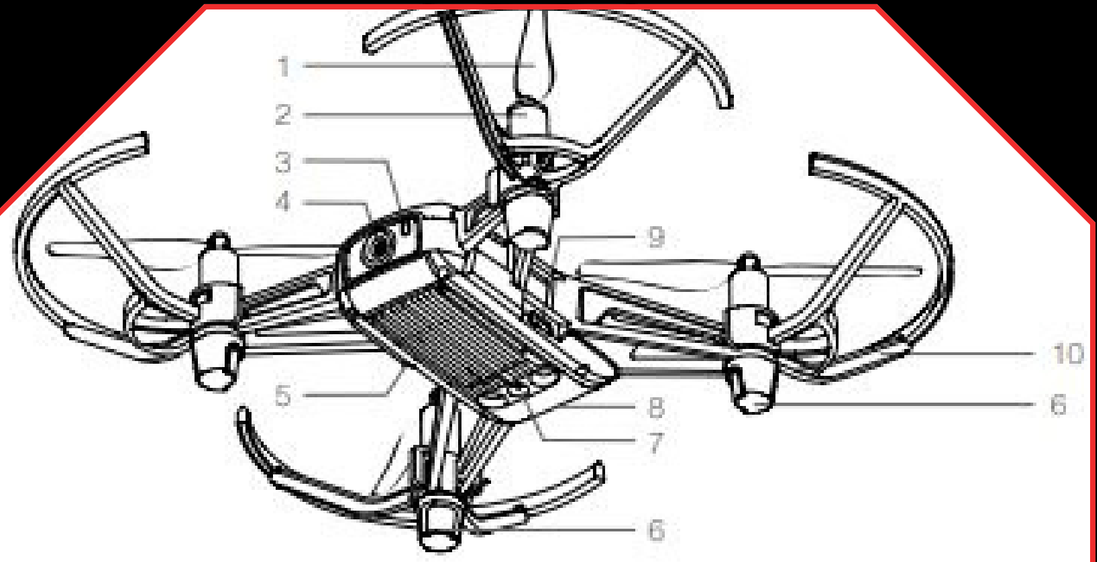
```python
import rclpy
from rclpy.node import Node
from std_msgs.msg import String
from some_motor_driver_library import MotorDriver

class MotorControlNode(Node):
    def __init__(self):
        super().__init__('motor_control_node')
        self.subscription = self.create_subscription(String, 'cmd_vel', self.cmd_vel_callback, 10)
        self.motor_driver = MotorDriver()

    def cmd_vel_callback(self, msg):
        command = msg.data
        if command == 'F':
            self.motor_driver.move_forward()
        elif command == 'B':
            self.motor_driver.move_backward()
        elif command == 'L':
            self.motor_driver.turn_left()
        elif command == 'R':
            self.motor_driver.turn_right()
        elif command == 'S':
            self.motor_driver.stop()

def main(args=None):
    rclpy.init(args=args)
    node = MotorControlNode()
    rclpy.spin(node)
    node.destroy_node()
    rclpy.shutdown()

if __name__ == '__main__':
    main()
```




1. Propellers
2. Motors
3. Aircraft Status Indicator
4. Camera
5. Power Button
6. Antennas
7. Vision Positioning System
8. Flight Battery
9. Micro USB Port

# DEMO TARGET

## DJI TELLO WIFI ENABLED DRONE

- A DJI Tello connected to a remote operator
- A laptop connecting to the Drone Simulates a unified traffic management system (at small scale)

# LIVE DEMO

## ATTACK OPERATION

Step-by-Step Guide:
Remote to RPi
Use the RPi to send movement
Serial into ESP8266
Initiate commands to scan, select and deauth

instructions via Python script.
Initiate WiFi scan and display results

## Demo Script:

```
#Start the Robot: Launch the ROS2 system
ros2 launch tengu_marauder tengu_marauder_launch.py
#Command the Robot: Use the operator interface to send movement commands
python3 operator_interface.py
#WiFi Scan: Send a SCAN command to the ESP32
ros2 topic pub /esp32_in std_msgs/String "data: 'SCAN'"
ros2 topic pub /esp32_in std_msgs/String "data: 'SCAN'"
#Display the scan results processed by the data_processing_node
```

# RESULTS AND ANALYSIS

## FINDINGS

- Analyze the WiFi scan results.
- Discuss potential applications and implications of the Tengu Marauder.
- Highlight any interesting findings from the demo.


```
{
  "networks": [
    {
      "SSID": "TELLO-1234",
      "BSSID": "60:60:1F:94:84:9E",
      "RSSI": -55,
      "Channel": 6,
      "Encryption": "Open"
    },
    {
      "SSID": "HomeWiFi",
      "BSSID": "34:CE:00:1A:BC:2D",
      "RSSI": -70,
      "Channel": 11,
      "Encryption": "WPA2"
    },
    {
      "SSID": "GuestNetwork",
      "BSSID": "70:3A:CB:3E:1A:C4",
      "RSSI": -80,
      "Channel": 1,
      "Encryption": "Open"
    }
  ]
}
```

# CHALLENGES AND SOLUTIONS

## STRUGGLES

Throughout the development of the Tengu Marauder, we faced several challenges.

One major challenge was ensuring reliable communication between the RPI and ESP32 which led us to use an ESP 8266 which was more accessible. A flipper was considered but was found to be insufficient in our tests. May be preferable for for sub gigahertz attacks (NFC, RFID)

These experiences taught us valuable lessons in hardware-software integration and system design.

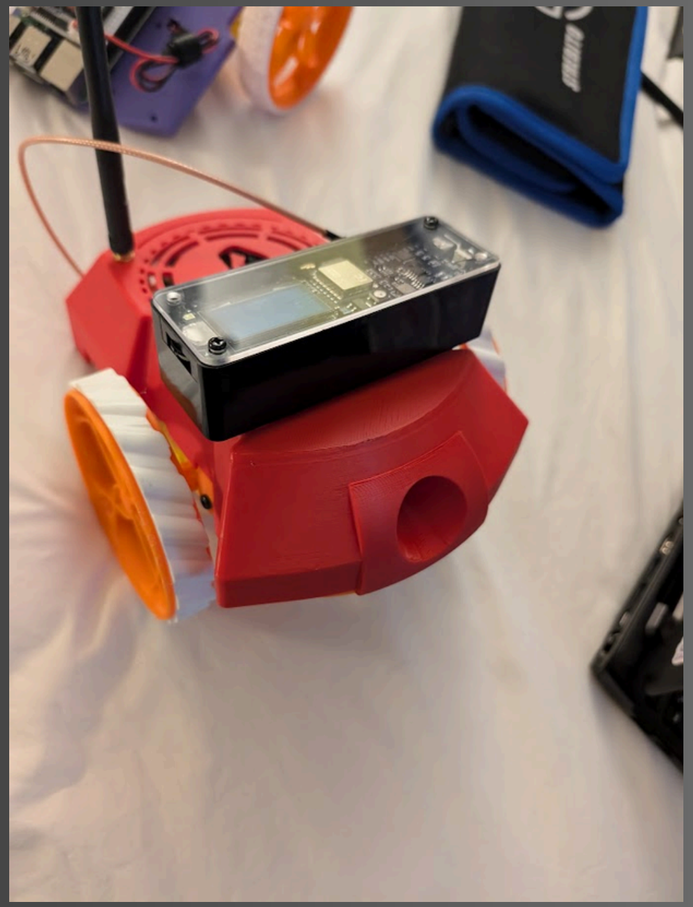
# FUTURE WORK

## PLANNING AHEAD

We have planned improvements and additional features. We aim to integrate more sensors, such as cameras and LIDAR, to enhance its navigation and situational awareness.

We also want to enhance the the robot with AI for better decision-making and autonomy is also a key goal. This can done with machine learning training over ROS2 and RVIZ

Additionally, we plan to explore new research directions, such as using the Tengu Marauder for more advanced cybersecurity tasks and environmental monitoring.




# CONCLUSION

To summarize, the Tengu Marauder is an autonomous security robot that combines commercial off the shelf robotics components with WiFi network security capabilities.

It demonstrates the potential for integrating cybersecurity with robotics to create powerful tools for both fields.

If you want to be a part of this community project or the E.M.P Crew please feel free to visit us at the Ex Machina Parlor or our website

https://exmachinaparlor.org


# Special thanks to our crew members and supporters

- Lexi3c0n (Lexie T)
- Kup (Leo N)
- Trashp4nda (Leo S)
- Riley
- Lain
- Sasha
- DeciSym LLC
- Raices
- Toool Philadelphia

LEXICON

If you have any questions please feel free to reach out!

**Lexie Thach**

@lexiecon121

COGITO ERGO SUM

EX MACHINA PARLOR

FROM THE MACHINE PARLOR

# THANK YOU