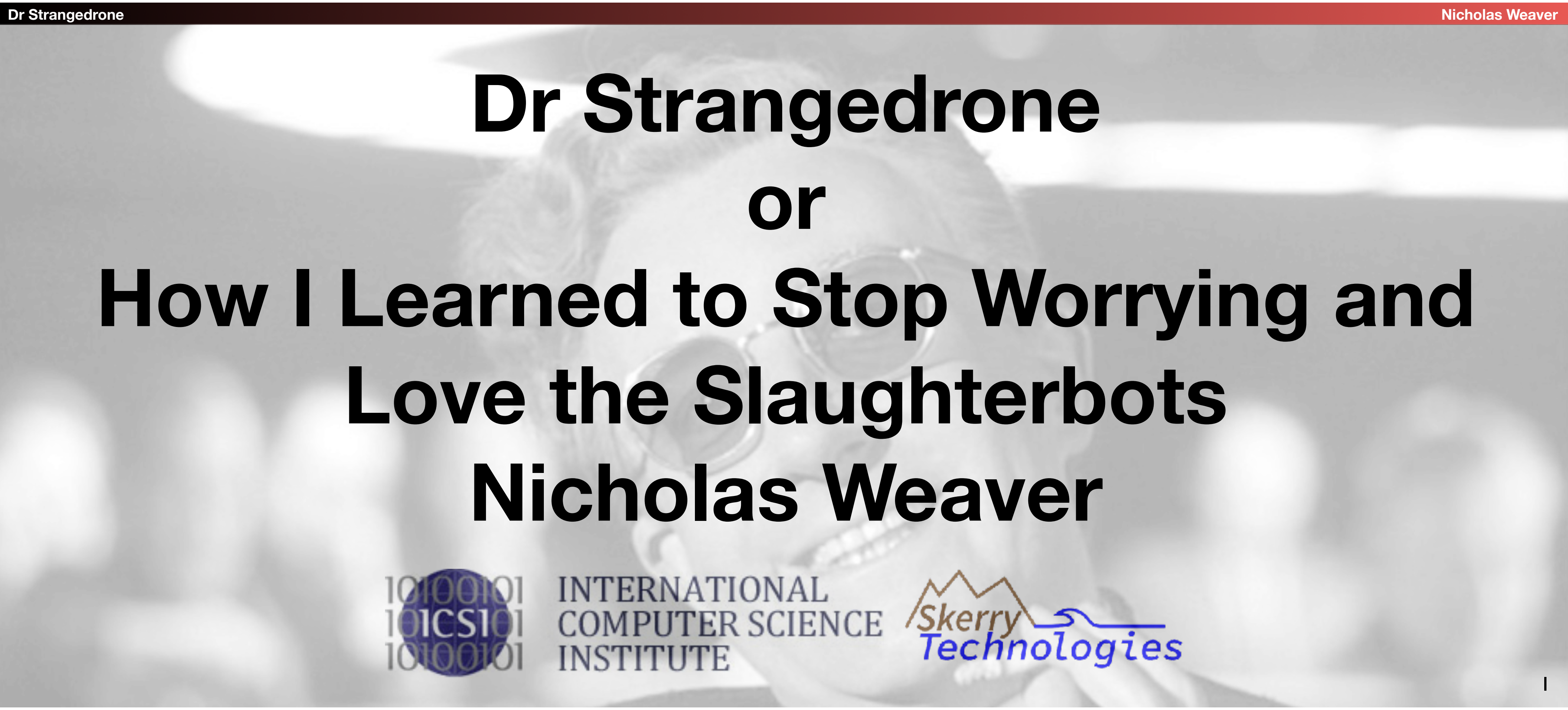


Dr Strangedrone
or
How I Learned to Stop Worrying and Love the Slaughterbots

Nicholas Weaver

ICSI INTERNATIONAL COMPUTER SCIENCE INSTITUTE

Skerry Technologies

About Me

- Computer Security/Architecture background
  - But have always been interested in small drones, especially the space driven by the hobby field
- Currently dual-hatted
  - ICSI: Computer Security Research
    - Anything good, give them credit!
  - Skerry Technologies: Drone R&D
    - Chief Mad Scientist/CEO/Janitor
    - Focus is on developing small, human-safe, and low cost fully-autonomous drones
    - I don't want to build killbots...
      I want to build ***killbot-killing***-killbots
- Security means ***thinking*** evil thoughts before other people do
- Lots of funding in the past but none for this work (yet)

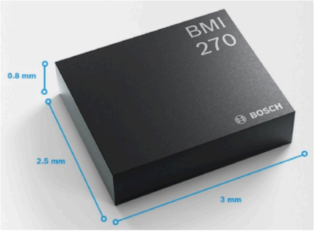
YO DAWG I HEARD YOU LIKED SLAUGHTERBOTS
SO I'M BUILDING SLAUGHTERBOTS
THAT WILL SLAUGHTER YOUR SLAUGHTERBOTS
imgflip.com

The Small-Drone Revolution

- Motors and Power
  - Low cost high-power brushless motors + speed controllers
  - Very high discharge-rate batteries
- MEMS and other small devices
  - 6 access accelerometer/gyros,
    high precision barometers, compasses, GPSs
  - Microcontrollers to implement the low-level autopilot
- Made low-cost multi-copters work and fly
  - Hovering devices are easy for humans to control

28mm diameter
1 kW max power

230g, 28 W/h energy
Peak power: 2.8 kW



A typical 6-axis MEMS IMU

The Three Development Branches

Military

Optimized for reliability and Extracting Government Money
"Low Cost" = $10k

Industrial/Prosumer

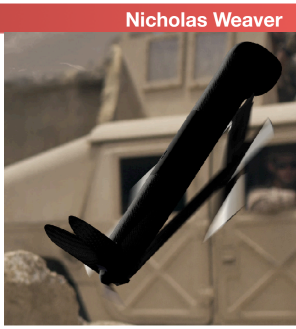
Optimized for endurance and ease of use
"Low Cost" = $1k

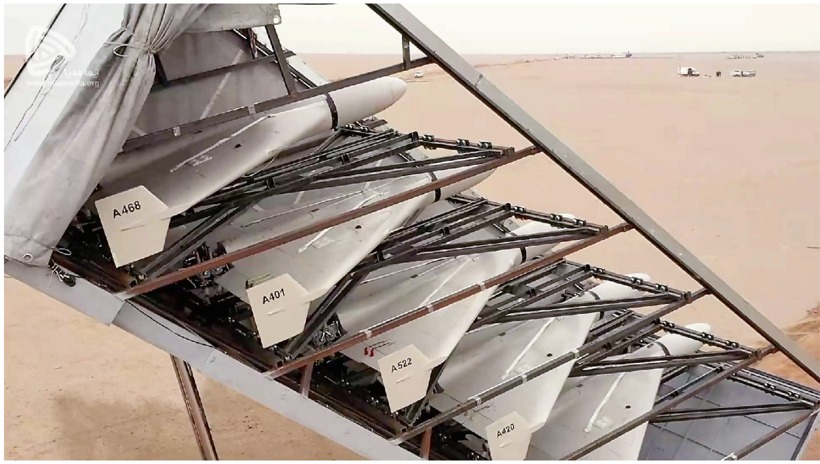
Hobby

Optimized for performance and crash-ability
"Low Cost" = <$250

Proliferating Military Options

- US: Switchblade 300
  - Fixed wing, grenade sized payload, tube launched, 15 minute endurance
- STM Drones from Turkey
  - Alpagu: Fixed wing, grenade sized payload, tube launched, 15 minute endurance
  - Kargu: Quadcopter, 1.2kg warhead
- Iranian Shahed 136
  - Fixed wing and tip-up container launched
  - Although really best thought of as a $20k cruise missile, not a drone



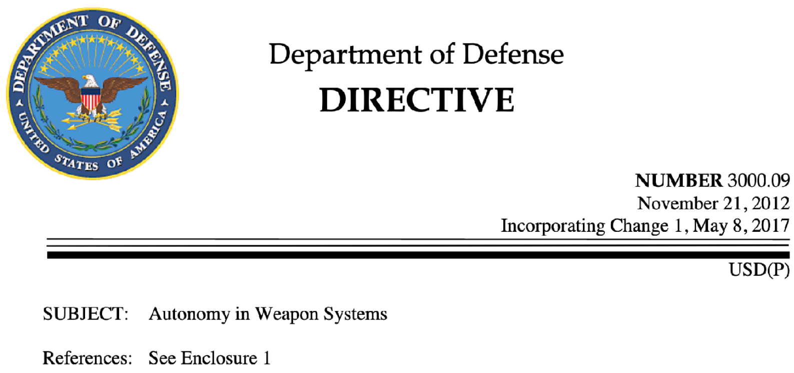


The Common Control Model: Human In The Loop

- Drone contains a low level autopilot
  - May have the capability to navigate waypoints etc
- Human receives a real-time video feed
- Human then directs the drone's high level movements
  - Target selection is entirely a human operation
- Some claims of "AI"
  - But nothing robustly confirmed:
    AI mostly seems to assist humans

Current Reluctance Towards Autonomy

- Within the US military:
  - Huge emphasis on maintaining human judgement on the use of force
  - Nothing in the US inventory is considered a Lethal Autonomous Weapon System
- Outside the military:
  e.g. Future of Life Institute
  Stop Autonomous Weapons
  - Producers of the "Slaughterbots" video



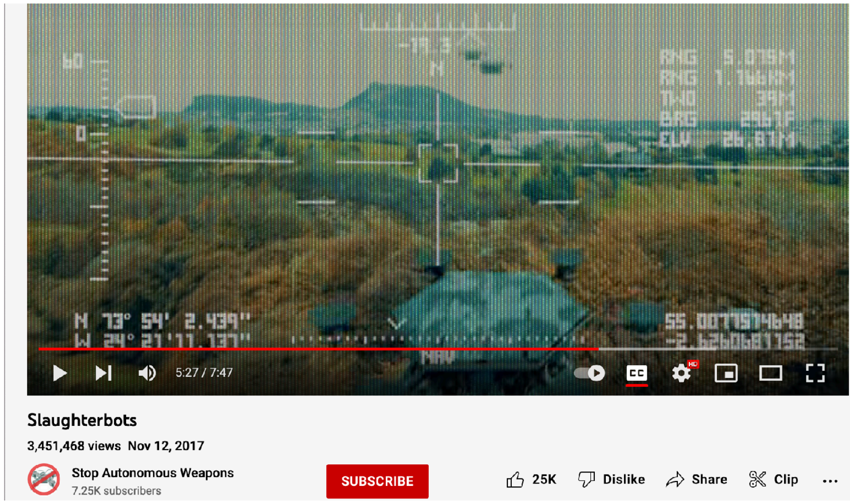
Department of Defense
DIRECTIVE

NUMBER 3000.09
November 21, 2012
Incorporating Change 1, May 8, 2017

USD(P)

SUBJECT: Autonomy in Weapon Systems

References: See Enclosure 1



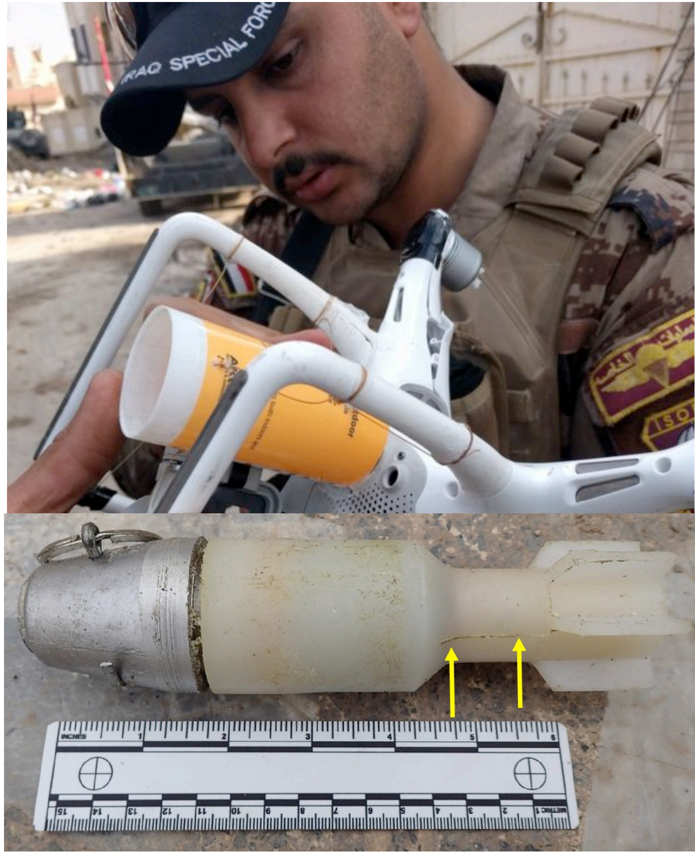
Slaughterbots
3,451,468 views Nov 12, 2017
Stop Autonomous Weapons
7.25K subscribers

But What Happened When Military Meets Consumer?

- Not all military operators have military-grade budgets
  - Rebellions, drug gangs, and overmatched defenders
- But all want to achieve military-grade effects
- In computing, a rough rule:
  "Drop a 9 and you drop a 0":
  - Going from 99.99% reliable to 99.9% reliable drops the price by a factor of 10
- Remember:
  - "Good enough for government work"
    used to mean you were doing ***too good a job***...

Recent Evolution: 2017
The ISIS Air Force

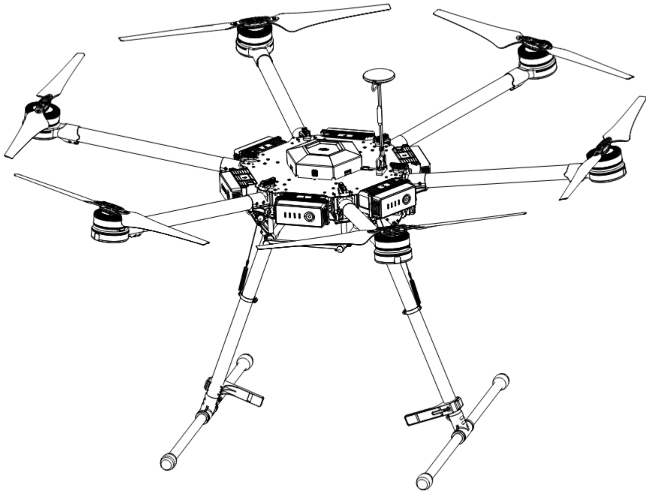
- Took commercial quadcopters and fixed wings
  - Added mechanism to drop payload
- Took grenade-launcher grenades and added tail-kits
  - 3D printed or mass produced with injection moulding
- Initially a huge impact but eventually countered through jamming



From Bellingcat

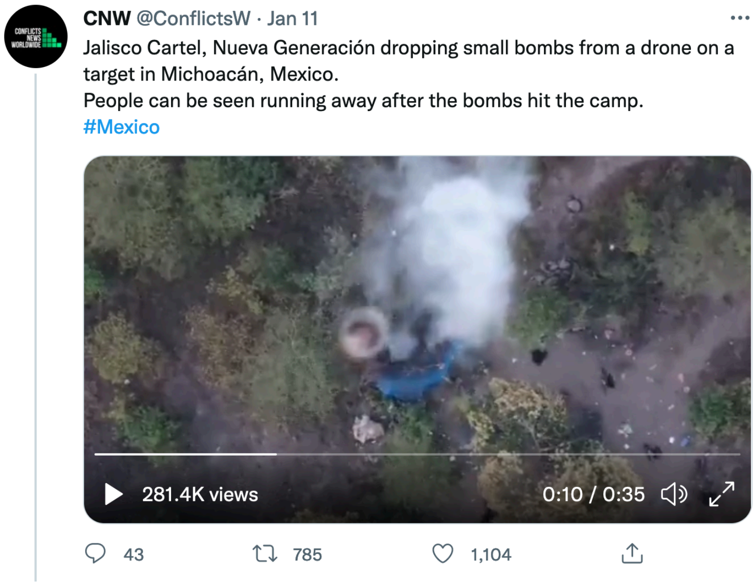
Recent Evolution: 2018
Maduro Assassination Attempt

- On August 4, 2018 someone attempted to assassinate Venezuela's ~~Dictator~~ President Nicolás Maduro
  - He was giving an outdoor speech at the time
- Attacker used two DJI Matrice M600 multicopter drones
  - Max payload: 5kg, cost ~$10k/each
- Attack failed
  - One drone exploded in mid-air, one crashed in a building
  - Cause of failure is unknown, but jamming is a possibility



Recent Evolution:
The Mexican Cartel Air Force

- Basically the same strategy as ISIS
  - Small quad-copters as airborne bombers
- May be using improvised explosives rather than military grenades
  - No significant counter-drone jamming currently in use (yet)

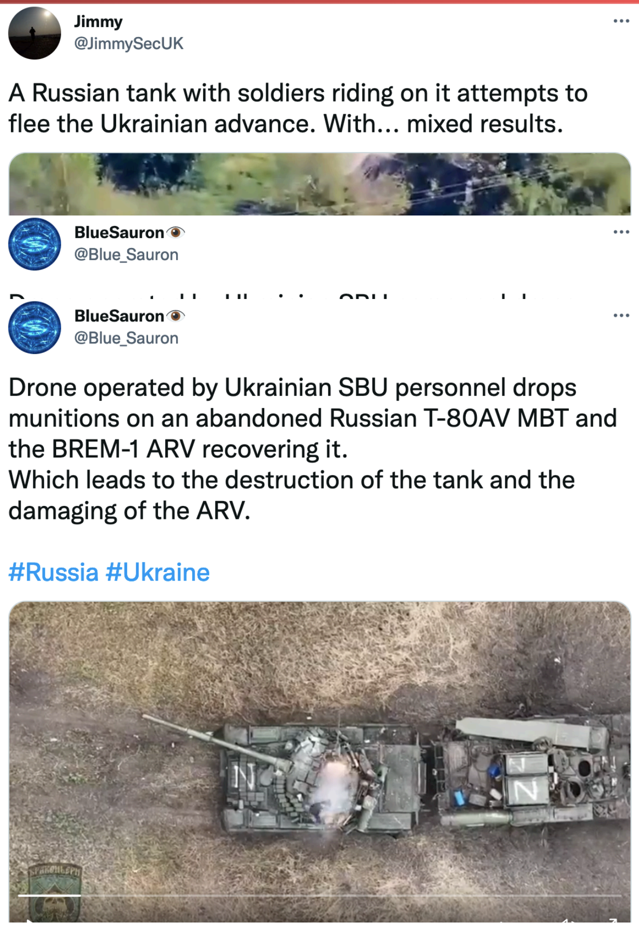


CNW @ConflictsW · Jan 11

Jalisco Cartel, Nueva Generación dropping small bombs from a drone on a target in Michoacán, Mexico.
People can be seen running away after the bombs hit the camp.
#Mexico

Today:
Ukraine vs Russia

- Wide variety of drones in use
- Small quadcopters for reconnaissance
  - Enables precise artillery targeting
  - Enables high-quality propaganda videos
- Small quadcopters with 1-2 grenades
  - Mostly grenade-launcher grenades with tail-kits
  - Using hacks like "turn on auxiliary light->release grenade" for modified DJI drones
- Pretty high precision
  - <2m error dropping from 75-125m altitude



Jimmy
@JimmySecUK

A Russian tank with soldiers riding on it attempts to flee the Ukrainian advance. With... mixed results.

BlueSauron
@Blue_Sauron

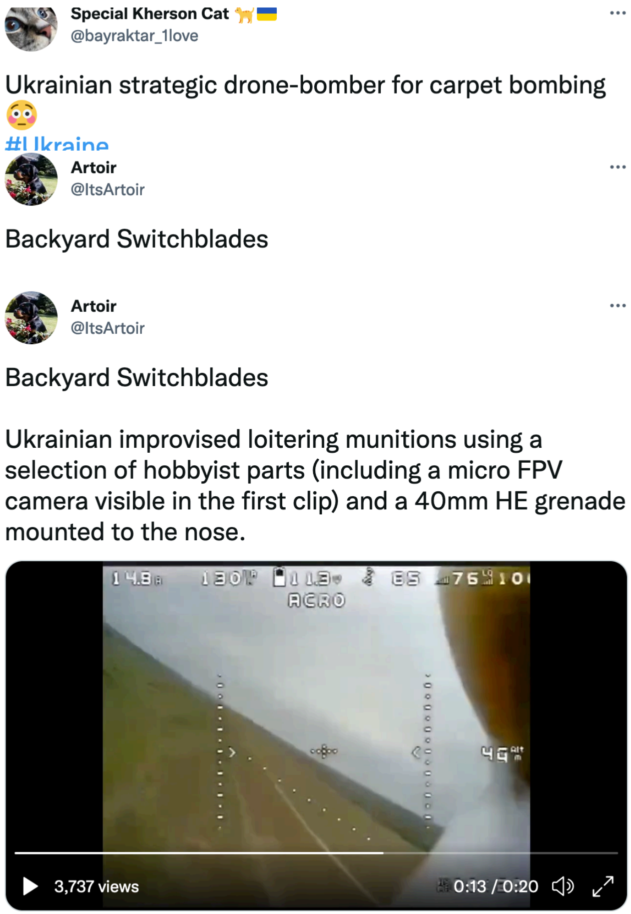
BlueSauron
@Blue_Sauron

Drone operated by Ukrainian SBU personnel drops munitions on an abandoned Russian T-80AV MBT and the BREM-1 ARV recovering it.
Which leads to the destruction of the tank and the damaging of the ARV.

#Russia #Ukraine

Today:
Ukraine vs Russia

- Heavy-lift drones with multiple bombs
  - Some with >6 bombs
  - Some hex or octocopters, not just quad-copters
- Fixed-wing "Backyard Switchblade"
  - <$150 flying wing, <$100 FPV/radio kit, grenade
- Remarkably permissive electronic-warfare environment
  - DJIs operate with near impunity...



Special Kherson Cat 🐈🇺🇦
@bayraktar_1love

Ukrainian strategic drone-bomber for carpet bombing 😳
#Ukraine

Artoir
@ItsArtoir

Backyard Switchblades

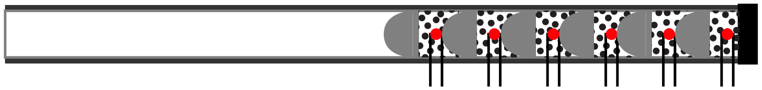
Artoir
@ItsArtoir

Backyard Switchblades

Ukrainian improvised loitering munitions using a selection of hobbyist parts (including a micro FPV camera visible in the first clip) and a 40mm HE grenade mounted to the nose.

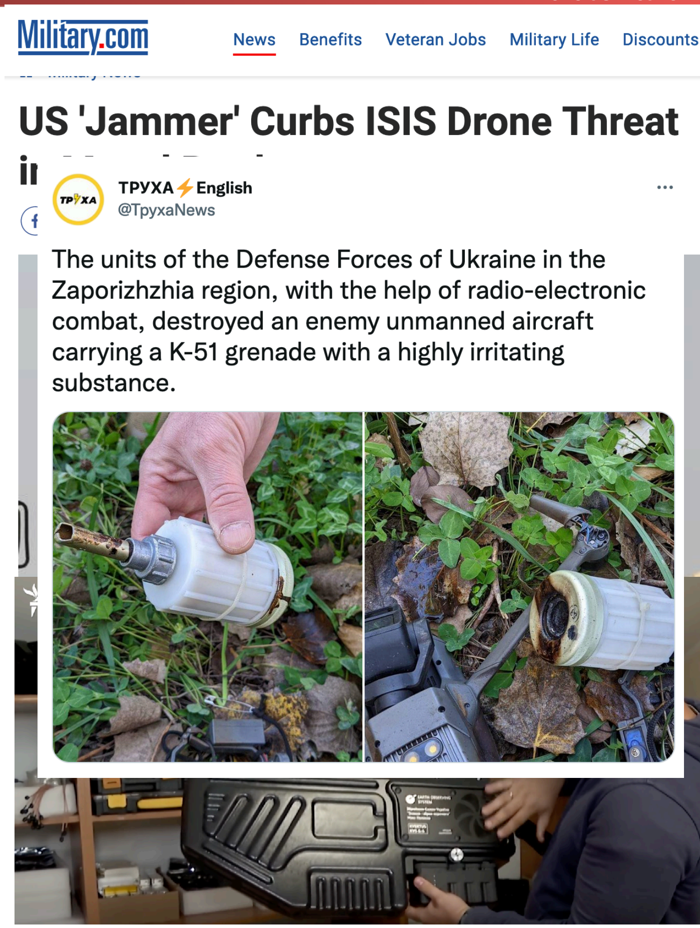
A Common Payload: ~200g of Mass

- ~200g == grenade launcher warhead
  - Primary armament of most small militarized-drones
- There are alternatives
  - 1.5 kg == Claymore antipersonnel mine
  - 3.4 kg == Warhead from a sensor-fused munition
- But there are possible alternatives too:
  - Tungsten-carbide beads in sticky hydrofluoric acid
  - 6-12 round stacked-munition gun
- Common theme: Precision
  - a 200g warhead right on the target beats an artillery shell 50m away



Countering Today's Threat

- Civilian drones are particularly vulnerable to jamming
  - Very limited frequencies, no meaningful spread-spectrum wide-band receivers
- Also vulnerable to hacking/hijacking
  - Many with very poor/nonexistant cryptography
- Also easy to triangulate the controller
  - Many literally broadcast their location and where they launched from
- Military drones are harder but still vulnerable to jamming etc...

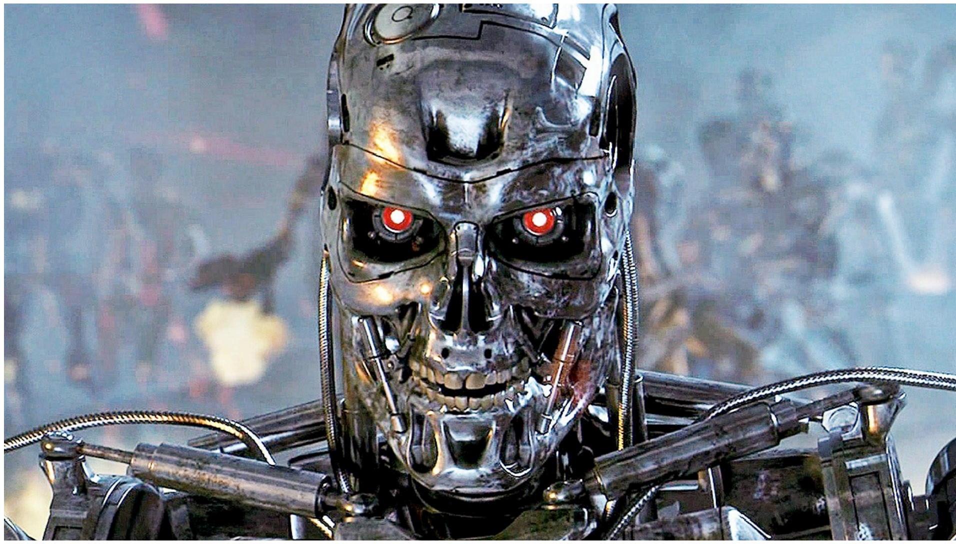


US 'Jammer' Curbs ISIS Drone Threat i

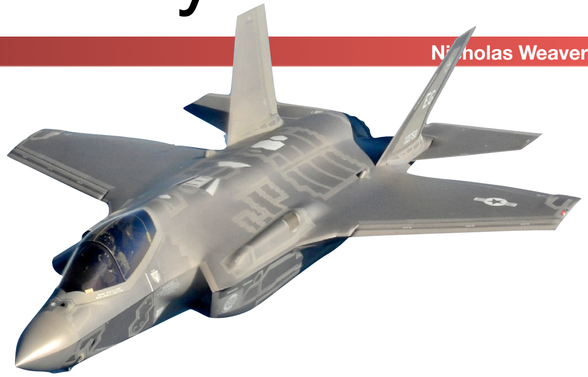
The units of the Defense Forces of Ukraine in the Zaporizhzhia region, with the help of radio-electronic combat, destroyed an enemy unmanned aircraft carrying a K-51 grenade with a highly irritating substance.

Countering The Countermeasures:
Human On The Loop with Fail-Deadly Autonomy

- Drone has sufficient on-board computation for self-contained autonomy
  - A set of targets, operation area, and objectives
- IF communication works...
  - The human can override or augment targeting decisions...
    But the drone will make its own decisions in the absence of explicit direction
  - Necessary because the drone still needs to work with the speed of automation...
- IF communication fails...
  - System goes into full autonomy mode:
    Carry out the mission



So Lets Jump Forward And Think Evil...
We are in charge of part of Atropia's Military



- A relatively small budget: $100M/yr for both R&D and procurement
  - AKA a F35 and change
  - AKA <1/3 the military spending of Luxembourg
- Our Grand-Strategy Objective:
  Anyone who wants to invade us (*including the United States*) will suffer
  - Our goal is ***not*** victory, but a defensive posture:
    The other side's "victory" will taste of ash, and any potential adversary will know this

Atropia's Resources For "Operation Killbot Insurgency"

- $100M/yr budget split 50/50 between procurement and R&D
    - We have a few really good technical people and a fairly good intellectual base
- We have a single medium tier circuit board fabrication facility (if not, add $$$ to build this...):
    - 8 layer, 3mil/3mil, blind/buried VIAs
    - Semi-automated assembly capable of dealing with 0201 sized components
    - Pitched as "economic development" (which it is, in addition to be dual-use)
- We have good relationships with China
    - And a small network of mules that can get us backpacks full of stuff as well

Our Threat Model:
Recent Invasions and Interventions

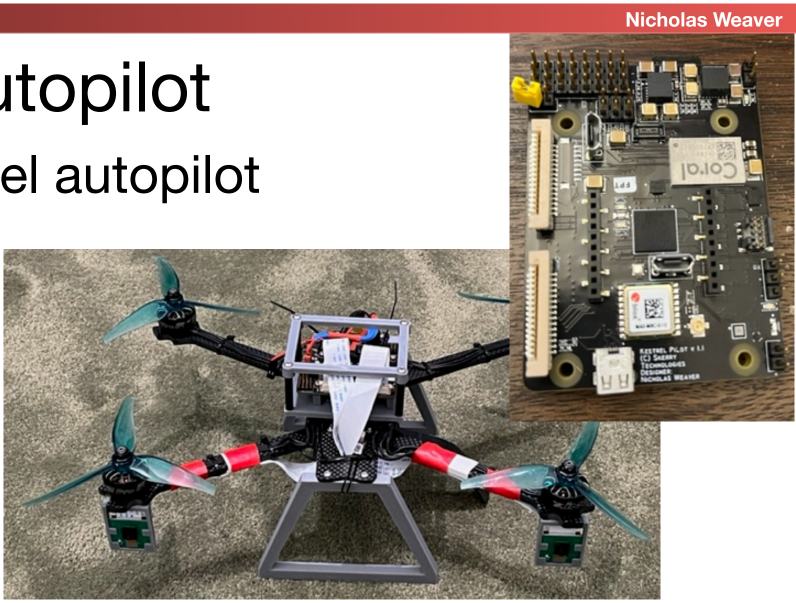
- US/NATO in Libya & Yugoslavia
  - Need a military strategy that can ceed the skies (above 50m) and still survive
- US in Iraq
  - Need a military strategy that guarantees a ground invasion will meet an insurgency
- Russia in Ukraine
  - Need a military strategy that can counter tanks, artillery, and remote logistics
- For all cases:
  Need to be able to directly counterattack very soft targets
  - Attack opponent-country energy, military, and logistics nodes

Our Tactical Objective:
Place a Small Payload in the Right Place

- Focus is almost entirely on small payloads
  - 200g for anti-personnel, unarmored targets, and anti-infrastructure, 4kg for anti-armor
  - But have to get super-close and super-precise
- This requires being super fast-reacting
  - Decision cycles measured in fractions of a second
- Why we can't do "Human IN the Loop":
  - We need our systems to see and exploit opportunities without asking "is it OK?"

Start With A Common Compute Platform

- Example of what's possible: Kestrel Autopilot
  - Microcontroller with GPS, IMUs to run the low level autopilot
  - Raspberry Pi CM4 for compute
  - Slot for cellular modem
  - AI accelerator
  - 2x 2-lane MIPI CSI2 camera interfaces
    - 1080p 30FPS video
    - Up to 64 megapixel still with digital pan/tilt/zoom



- Hardware cost in quantity: $200-400 depending on options
  - Quality of the cameras, inclusion/performance of the cellular modem, options on the Compute Module

Just How Much Does Dropping Reliability Save? Compare to the upcoming F35's processor

- Kestrel:
  - Raspberry Pi CM4: 1.5 GHz, quad core processor, up to 8 GB RAM, SD card (128 GB Flash)
  - 2x 4k HDMI output for graphics if desired, 3840 x 2160 resolution
    - Only one populated for debugging purposes
  - Offloads all hard-real-time processing onto dedicated coprocessor
    - 400 MHz single-core ARM with 1000 DMIPSs, 2MB Flash, 1MB DRAM
    - Realtime OS imposes a lot of compromises:
      Far easier to segregate the real-time components into a separate device
  - $200-400
- L3 Harris ICP (short):
  - 2x CPU processors, 512MB DRAM, 256MB Flash, ~2900 DMIPS/core
  - 2x Graphics processors, 256MB DRAM, 2560×1600 resolution
  - $???? (but it is frightfully expensive, and isn't even rolling out until next year!
    Current F35 computer is 1/25th as capable!)

Navigation and Vision

- Primary sensors are visual
  - Multiple cameras for both stereo/optical flow
  - Use normal light, near IR, and some cheap thermal
- Longer distance navigation is primarily terrain-map and inertial
  - GPS should assume to be jammed in most cases
  - Requires detailed mapping, but hey, 128GB SD cards are only $20
- Can operate autonomously at just-above-the-treetops level
  - But we are cheating: Sacrificing a little reliability for much lower cost

Use to build a common software suite

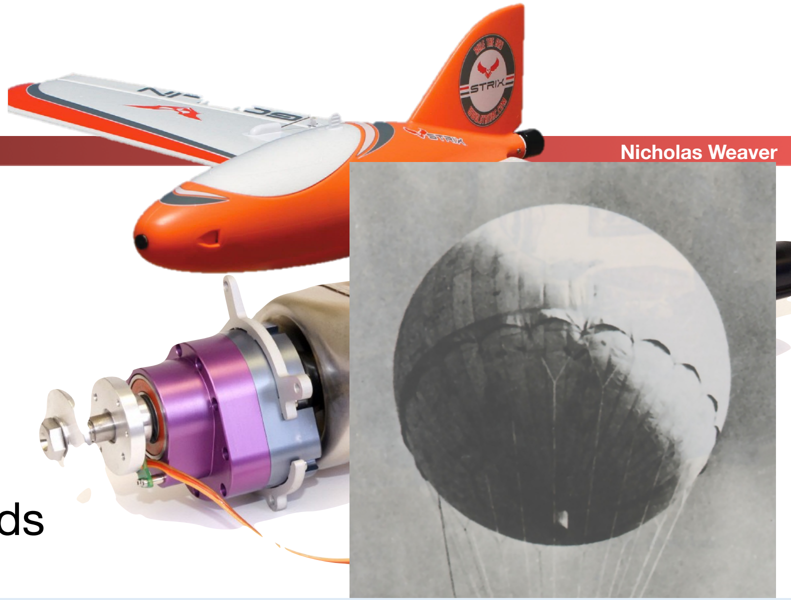
- Steal as much as possible
  - Ardupilot for low level autopilot:
    Then restructure for cleaner code and higher performance
  - OpenCV for initial computer vision pipeline:
    Then restructure for cache-aware, higher performance on the standard computer
- Build higher level common components
  - Visual-based detection/target identification
  - Terrain following & navigation
  - Common networking/communication/coordination layer
    - Not really a "Swarm", but more a "situational awareness" model:
      Flood broadcasts to nearest neighbors

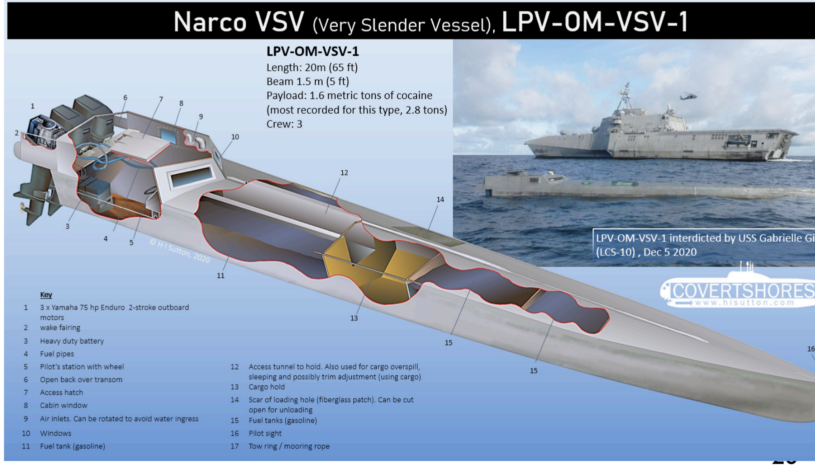
Then Power Some Basic Platforms

- Quadcopters: Two sizes
  - Small quad, 200g payload, $300
    - Anti-personnel programs
  - Large quad, 2-4kg payload, $600
    - Anti-armor and hard targets
- "Ankle Biters"
  - A mechanum-wheel chassis with quadcopter props to "hop", $350
- Fixed gun-mounts & camera mounts
  - Automated fixed-turrets and sensor packages ($100-1000 + the gun itself)
- Chinese knockoff robot-dogs? $4000
- Power "perches" to keep systems charged
  - Also provides wired Internet backhaul points

More Interesting Platforms

- Small fixed wing
  - $150 chassis, 10-50km range, 200g payload
  - $300 version with pop-out wings and tube-launching
- Larger fixed wing
  - $15,000 prop-driven mini-cruise-missiles loaded with quads
    Launched from a stack in a modified 40' container
- Balloon bombs
  - Carry 20 fixed-wings on a weather balloon:
    Intercontinental Strike
- Narco Sub
  - Carry 500+ fixed-wings in a semi-submersible
    low-profile boat





Narco VSV (Very Slender Vessel), LPV-OM-VSV-1

LPV-OM-VSV-1
Length: 20m (65 ft)
Beam 1.5 m (5 ft)
Payload: 1.6 metric tons of cocaine
(most recorded for this type, 2.8 tons)
Crew: 3

LPV-OM-VSV-1 interdicted by USS Gabrielle Gi
(LCS-10) , Dec 5 2020

Key

1	3 x Yamaha 75 hp Enduro 2-stroke outboard motors
2	wake fairing
3	Heavy duty battery
4	Fuel pipes
5	Pilot's station with wheel
6	Open back over transom
7	Access hatch
8	Cabin window
9	Air inlets. Can be rotated to avoid water ingress
10	Windows
11	Fuel tank (gasoline)
12	Access tunnel to hold. Also used for cargo overspill, sleeping and possibly trim adjustment (using cargo)
13	Cargo hold
14	Scar of loading hole (fiberglass patch). Can be cut open for unloading
15	Fuel tanks (gasoline)
16	Pilot sight
17	Tow ring / mooring rope

Note on Stealth...

- Stealth is ***old*** technologies
  - 1970s-level on how to design surfaces to scatter
- We will use multiple strategies
  - Most systems will just fly very low:
    Hide in the ground clutter from the air, and not be seen from the ground
  - Many systems naturally stealthy:
    Styrofoam, plastics, etc are transparent, and many components are just small
  - Some custom "stealth boxes":
    Non-structural enclosures to scatter radio
- Also, we will invest in counter-stealth
  - Although this is outside our current focus here:
    Turn 5G cell-towers into a multi-path radar network would be a good orthogonal bit of R&D

Defense Philosophy:
Building a Defensive "Dark Forest"

- The defensive battlefield is filled with various sensors
  - On drones, fixed locations, and everywhere else...
  - These sensors communicate with neighbors, but only "talk" when they see something
    - Low bandwidth but high reliability communication
- If an enemy is spotted:
  - In low-threat mode: wait for human confirmation
  - In hot-war mode: If spotting system can engage a target of that type, engage immediately
  - Spotting system also broadcasts to neighbors the presence/type/numbers/location of hostiles
- In this environment, being detected means death
  - "Spot to Shoot time of 0"
- Aka "The Pre-Planned Killbot Insurgency"

Hiding The Killbot Insurgency

- Small systems just hide
  - Either connected to the power grid (preferred) or with a small solar panel...
- Some pre-packaged pods of killbots
  - Keep under cover and have someone drag them out
  - Or in-place camouflaged
- Large systems (e.g. the prop-powered cruise missiles) hide in plain sight
  - Place in 20' or 40' containers...
    And use a lot of containers just for storage, utility, etc...
  - Every container in the country becomes a JDAM-sponge

Offensive-Defense Philosophy: Logistics Targets in the Near

- Use mass attacks of long-range prop-powered cruise missiles
  - A few will use terminal autonomous target recognition with an explosive payload
  - Most however will release small swarms of small quads and ankle-biters
- Some deployed systems attack immediately
  - Recognize and target weaker things:
    Containers, aircraft, personnel, open hangar doors, etc...
- Some deployed systems run and hide
  - Lurking autonomous killbots really disrupt material handling

Offensive-Defensive Philosophy: Long Range Strike

- Multiple systems for low damage intercontinental strike
  - The balloon bombs, the narco subs
- So need to target very soft targets
  - But there are a large number of them
- Logistics nodes within the US
  - E.g. Travis AFB, use the same strategy of anti-personnel lurking
- Refining infrastructure & power substations
  - Get 20% of the refineries in the US and you will cripple the US economy
  - Get 20 power substations at the same time and you will overwhelm the availability of spare parts

And Then Bulk Build and Sell It...
Atropia: Provider To The World

- Most platforms are <$1k
  - So with $50M to purchase that gives 50000 killbots a year!
- Sanctions are not going to be that effective:
  - If someone can buy 5000 of X on Digikey, embargoes don't work
  - Buy 5k component sets, build boards, repeat as supply chain changes
- Internal use: build at cost...
  - Gotta build up the nice pre-planned killbot insurgency
- External use: only mark up 2x-5x
  - But only for volume sales:
    Don't sell 1000 killbots at $10k/each, sell 10,000 at $3k/each

Implications

- The defender has a substantial advantage
  - Limit on small killbots is endurance:
    Some hacks for limited long-range strike but most systems are 5-50km range
- Autonomy can only be fought with autonomy
  - Computer reflexes can only be countered with computer reflexes:
    Human decision cycles are just too slow...
- So invest in both mobile killbot-killing-killbots and auto-turrets
  - Very low cost distance-fused munitions: Goal should be <$5/fuse

So Love the Slaughterbots...

- This trajectory seems inevitable
  - Being able to build a defensive structure like this is very valuable:
    I'd bet that a significant effort is currently underway in Taiwan along these lines.
- Major territorial invasions already have an awful track record
  - This just makes it even harder
- Quantity has a quality all its own
  - US military procurement is specifically broken when it comes to dealing with swarms of killbots

And For the US Military in Particular

- This is not the only future of war... But it is a significant probability
  - And it specifically targets weaknesses in the US military procurement model:
    Expensive means you can only be in a few places
- Even the smallest units will need fully autonomous killbot-killing-killbots
  - This needs to be a major priority
  - Either auto-turrets with super-cheap distance-fused munitions and/or their own pet killbots
- And we need ***HUMAN SAFE*** killbot-killing-killbots for civilian areas
- Perhaps more integrated internal design & manufacturing?
  - As soon as a MILITARY contractor gets involved, prices go up 10x and latencies go up by years...
  - And reforms so the US government can just hire people at market rate!
    Instead of paying contractors to pay people at market rate and the contractor gets 50% on top
- This is an upcoming arm's race:
  Get a head start and work on killbot-killing-killbots now

And in the mean time... We Should Also Worry About the Mineshaft Gap