

training pod carried by US aggressor squadrons flying
American-built F-16s, but references about its training
focus appear from around 2016.
Prior to 2016 most published material on Angry Kitten

refers to it as an EW warfare system or capability. Upon accepting an award in 2015, Roger Dickerson, a senior

research engineer with the Sensor and Electromagnetic Applications Laboratory at Georgia Tech Research Institute (GTRI), referred to the system as a serious technology that improves warfighter capabilities, "especially for the US Air Force air combat community." The name "Angry Kitten" is tough to forget. According to a 2013 Newsweek article, the name is an insider joke because the system can react "with the mind of a cat".

A perceptive kitty



A 64th AGRS F-16 taxiing out for a sortie with an Angry Kitten pod on the left inboard wing pylon. The footage was taken during the Red Flag 19-2 exercise in June, 2019 indicating that USAF aggressor aircraft may have already been carrying the pods for several years (Credit: US Air Force /Youtube)

GTRI is located on Georgia Tech's main campus in Atlanta. Traditionally low profile, the Institute has long



DÜRR N D T

DIGITAL X-RAY AND





been connected with US military research. Last year, its 2,900 employees undertook over US\$833 million of sponsored research for military and government sponsors on campus and at 21 field locations including AFRL's headquarters near Dayton, Ohio.

Classical defensive EW or radar-jamming since WWII has used mechanical interference – reflecting radar beams back at the sender using chaff material. Later, strike aircraft used electronics to broadcast highpower electromagnetic signals to interfere with hostile radar beams, jamming and suppressing enemy sensors. Such active countermeasures are effective but obvious because they signal one's approach to a target or objective.

Nevertheless, the US Air Force has used active EW to good effect in Vietnam and every conflict since with "Wild Weasel" F-105Gs, F-4C/Gs and later F-16C-D/Js. In addition to its stealth, the F-35 also has limited built-in digital jamming capability.

Passive EW for defensive or offensive purposes is much harder to accomplish, requiring acute senses and persistence. But with the advent of digital electronics, specifically digital radio frequency memory (DRFM), GTRI researchers could see a path to building a sensor that could passively collect enemy RF in the form of radar and other signals and use machine learning software in real time to adaptively choose an optimal jamming response from among many options autonomously... like a silent cat.

In 2013, GTRI research engineer, Stan Sutphin, was interviewed for a Georgia Tech public relations article in which he explains Angry Kitten: "We believe a cognitive electronic warfare approach, based on machine learning algorithms and sophisticated hardware, will result in threat response systems that offer significantly higher levels of electronic attack and electronic protection capabilities, and will provide enhanced security for US combat aircraft."

Sutphin elaborated that his research team was also investigating cognitive learning algorithms that could allow Angry Kitten, which the article called a "jammer", to independently assess and respond to novel opposing technology. That included the capability to respond effectively should it encounter unfamiliar hostile radar techniques. Moreover, he disclosed that as an EW engagement progressed, the system would be able to assess how effective its jamming is against the threat "and quickly modify its approach if necessary".

GTRI's team was also working to give the Kitten mimicry capability with the potential to absorb then employ an adversary's own signals to spoof it. DRFM would make this possible by recording received radar emissions, manipulating them and sending back false information that appears to be real.

"A DRFM jammer is a very effective way of adding clutter to the scene without just using unsophisticated noise-jamming techniques," Sutphin said. "You can create false targets, or hide real targets, using the enemy's own waveforms against him."

That quality suggests an ancillary use for the system, that it could potentially represent a range of threat electronic attack systems. For a US Air Force or Navy / Marine Corps concerned about training to blunt advanced Russian and Chinese aircraft and electronics systems it could not get access to, a pod with the ability to replicate what US intelligence had learned of adversary waveforms and processes would be highly prized indeed. But this additional fillip was not what was driving Angry Kitten.

Radar testbed



Electronic countermeasures pods are used to broadcast high power electromagnetic signals that interfere with incoming hostile radar beams (Photo: Tech. Sgt. Nicholas Alder/US Air Force)

During the initial phase of developing Angry Kitten the GTRI team put together a jammer prototype. It reportedly consisted of a wideband tunable transceiver system, built from commercial electronic components and custom hardware. GTRI's open architecture / open source approach was characterized as low-cost, one that enabled operators to quickly modify the system in response to changing conditions.

Mixing open architecture with commercial electronic components was key to the prototype jammer – a new way of doing business in the EW community despite the application of so-called "agile" design to weapons systems for several years previous. Around the same time, the US Navy embarked on the development of a Next Generation Jammer (NGJ) for its EA-6B Prowler, the soon to be introduced EA-18G and potentially for the carrier launched F-35C.

NGJ too was to take an open-architecture, modular approach but its adaptive character appear not to be as flexible as Angry Kitten. That mattered to GTRI's director of research, Tom McDermott, who opined in the 2013 PR piece that, "We need an approach to more quickly evaluate advances in digital RF signal generation, and to rapidly field countermeasures without expensive hardware upgrades."







To help GTRI achieve that Aram Partizian, a researcher who teaches courses at Georgia Tech on DRFM and principles of radar electronic protection, co-devised the "enhanced radar testbed". The testbed simulates opposing radar signals, enabling rapid and realistic testing of jammers.

Like their analog predecessors, DRFM jammers rely on a "library" of known threats that are used to identify and neutralize incoming signals. Stan Sutphin explained that DRFM equipment may also include electronic-intelligence (ELINT) capability, the capacity to monitor and collect information on enemy signals and jammers. ELINT data so gathered was typically used weeks, months, or even many years later to improve US threat response techniques.



Georgia Tech Research Institute engineer Stan Sutphin is shown in an L-39 Albatros jet trainer used for EW flight testing (Credit: Stan Sutphin/ Georgia Tech)

"What we want is to perform those same ELINT analysis and adaptive response tasks in seconds – while the jamming is occurring – not months later," Sutphin said. "And obviously our system must work autonomously, because there's no time for human input."

By simulating known adversary radar signals Partizian's testbed allowed the GTRI team to quickly and cheaply infuse Angry Kitten with sensitive ears – ELINT – and algorithm-driven adaptive logic behind the secure, closed doors of their laboratory. The enhanced radar testbed not only informed development of Angry Kitten's adaptive capability, its capability for mimicry fed into the jamming system's use as a pod-carried training tool.

When Angry Kitten branched out in that direction isn't exactly clear but AFRL and the US Air Force possibly considered highlighting the training application as a way to shift emphasis from its broader potential. It may also be why GTRI still describes the system as "a test asset for radar and electronic warfare equipment."

Flying rapidly re-programmable pods with the mimicry and adaptive capabilities of Angry Kitten would not only make for good training, it may have helped the US Air Force evaluate their potential as EW combat systems. Formally, that evaluation didn't take place until April 2022 when AFRL conducted an "operational assessment of the Angry Kitten Combat Pod electronic attack system."

AFRL carried out the evaluation of "an updated version of the Georgia Tech Research Institute Angry Kitten pod" as part of its App-Enabled Rapidly Reprogrammable Electronic warfare / Electromagnetic Systems Experiment campaign. The flight tests got noticed by the US Air Force, AFRL experiment program manager Keith Kirk says, because US Air Force leaders expect to employ more open architecture software to allow agile changes in future systems.

That chimes nicely with what GTRI has been more broadly working on for the last decade, a concept and program called Electromagnetic Battle Management (EMBM) for distributed electronic warfare. A GTRI press release in January of this year characterized it as developing technology to dynamically monitor, sense, and act upon the electromagnetic spectrum using networked and distributed radio frequency systems.

GTRI senior research engineer, Breneman Whitfield, leads the EMBM project. As he says, it looks across the electromagnetic battlefield using a tool GTRI long ago began developing. "We are initially looking at the electronic warfare aspect of the larger electromagnetic domain and using GTRI Angry Kitten EW systems to perform autonomous, collaborative, netted, distributed electronic support for the development of data processing, machine learning and visualization techniques to provide decision aids," he says.

Angry Kittens placed on platforms could use their ELINT, response and spoofing capabilities to great effect. If, as defense journalist Kelsey Atherton said in a recent Popular Science article, adversary EW data can be shared from one aircraft to the entire US Air Force, "a possibility with open standards and reliable, open bandwidth, then the second day of aerial combat against a hostile jammer could go much more smoothly than the first."

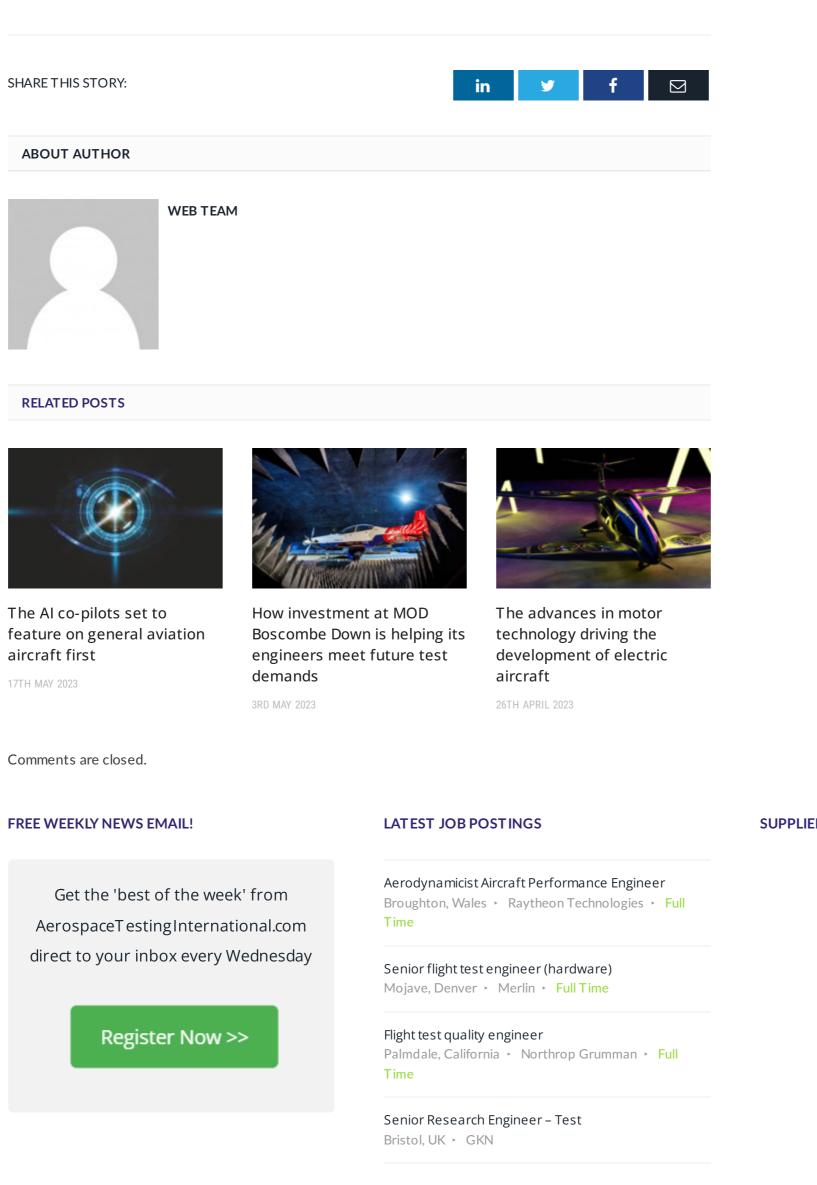
In fact, GTRI began development by assembling a software integration environment using the "Low Cost Kitten" variant of the Angry Kitten EW architecture family according to GTRI's press release, in what seems like a nod to Partizian's enhanced radar test bed.

Combined with a GTRI-developed tool called ATOM (Asset Tasking and Operations Management), Angry Kitten pods could help US combat commanders visualize the electromagnetic battlefield, understand what is happening and manage it, down to allocating scarce bandwidth to US communications and weapons systems while protecting them from enemy EW.

The threads above make sense when put together. They also indicate broader potential for the Angry Kitten-like approach to electronic warfare and cyber. Perhaps Angry Kitten was never just about airborne aggressor training. It's a much cleverer cat.



The Angry Kitten pod (blue) in early flight testing on the wing of an L-39 Albatross in 2013 (Credit: Stan Sutphin/Georgia Tech)



SUPPLIER SPOT LIGHT





