

## EWA Tiger



### A Suite of Communication, Intercept, Tagging, Tracking, and Locating (CITTL) Technologies

EWA Tiger is a suite of CITTL technologies that provides the warfighter with a real-time tactical capability for communicating during active jamming and intercepting, analyzing, geo-locating, tagging, and tracking various threat RF emitters and the operators of those emitters. EWA Tiger technologies work in concert with each other or are available as independent applications addressing a specific customer requirement or operational scenario. Our technologies are mature and currently support real-world operations with various Department of Defense and national-level agencies.

Our over-arching development concept for EWA Tiger is that anywhere hostile forces conduct operations transmitting and/or receiving any form of electronic communication, EWA Tiger technologies will and can monitor, intercept, provide real-time analysis, geo-locate the emitter source, remotely tag a potential target source, and track movement of a tagged target. Additionally, our communicating through jamming technology enables the warfighter to communicate in the presence of active Jammers. EWA Tiger's suite consists of six complementary technologies that accomplish those activities. Following is a brief description of each:

**Communicating Through Jamming:** EWA CommThru provides the warfighter with the capability to communicate normally in the presence of high powered jammers. CommThru is a dual function system consisting of a CommThru Electronics Box (CommThru Box) and a CommThru Antenna, which works in combination with the SINCGARS radio translating the standard radio frequency to a new frequency operating well above the coverage of any existing Jammers. This new 'boosted' signal is then transmitted and received by another CommThru device (mounted on other vehicles or fixed facilities) which then translates the boosted frequency back down to the expected RF frequencies for SINCGARS. Thus vehicle-to-vehicle communications are maintained without making any modifications to existing radio components. Simply stated, the warfighter is able to communicate during active jamming while ensuring protection against the detonation of an IED.

**Black Hole 802.11 Intercept System:** Black Hole provides the warfighter the ability to exploit all wireless internet traffic generated on 802.11a, b, & g (WLAN) wireless networks. It is a system with four passive functional capabilities (capture, decode, search, & identify) that can produce actionable intelligence, and one active mode which enables the user to insert packets into the wireless stream to spoof the system. The system is capable of capturing over 99% of all traffic on a wireless network, decoding the captured data locally, and providing the ability to perform real-time tactical analysis of the captured data. Black Hole is designed to operate on a small Field Computing Device (FCD) with a Microsoft XP operating platform. It provides the warfighter with real-time intelligence that could divulge an adversary's current activities, planning operations, or threat identification such as Improvised Explosive Device (IED) placement, identification, etc.

**ARROW Cellular Intercept:** The ARROW Cellular Network Monitoring System neutralizes GSM's encryption to intercept, decode, display, and record a variety of cellular data. The ARROW system offers passive, real-time decryption of A5.1, 5.2 GSM and CDMA encryption protocols. Cell phone conversations can be actively monitored, recorded, and archived for further analysis. ARROW is also capable of identifying unknown cellular phone numbers, obtaining the identity of active frequency (Channels) by number and targeting of specific cell phone numbers for monitoring of incoming and outgoing calls, including recording both sides of the conversation. Additionally, all information obtained by the system is displayed in real time including: the cell ID, frequency, power of cellular phone's transmitter and the distance between cellular phone and base station. ARROW provides the warfighter with real-time intelligence that could divulge an adversary's current activities, planning operations, or threat identification such as IED placement, identification, etc.

**GeoStorm Geo-location System:** GeoStorm utilizes an Advanced Tactical Geo-location Receiver (ATGR) to locate an RF transmission source with a very high degree of accuracy. The ATGR uses two methods to geo-locate an RF emitter: Amplitude and Doppler. In Amplitude mode, a single ATGR monitors the channel(s) of interest and collects signal strength data when the target is on the air emitting. The signal strength data is processed through a set of geo-location algorithms producing a solution that is displayed as an overlay on a map via a small Field Computing Device. In Doppler mode, two ATGRs (master & slave) monitor the channel(s) of interest with the master ATGR moving around the target area. The slave ATGR can be stationary or moving. The slave ATGR captures signal data; time stamps the data, and transmits it to the master ATGR. The master ATGR correlates the slave ATGR's data with its own produced data, and then processes the resultant data thru a set of geo-location algorithms. From there, a solution is displayed as an overlay on a map via a small Field Computing Device. GeoStorm provides the warfighter with the ability to geo-locate adversaries operating various RF emitters (CW, FM, AM, and SSB devices; cellular phones; 802-11 platforms).

**Bigfoot Remote Tagging System:** Bigfoot, an RF Tag, is a very small, battery-operated device used to emit an RF transmission from a target such that the target can be located and/or tracked. The tag has sophisticated power management features to allow use over a long period of time (months). A maritime version of the tag (Remora) is also available and provides ability to track ferrous-hull vessels (container ships). Each tag can be installed on a witting or unwitting person, material, vehicle, ship, etc. Power is supplied by installed battery or host power source. The tag can be augmented with GPS to allow data logging for later exfiltration or geo-fencing functions (on/off when inside defined geographic boundaries). Bigfoot provides the warfighter with real-time tracking intelligence on potential adversaries conducting threat activities.

**Advance Scout Intelligent Video:** Advance Scout combines a covert video and communications system with an Intelligent Video Camera (IVC) alerting solution that transforms traditional video surveillance into an intelligent, network-based, tactical video system. The system can be adapted to meet changing mission requirements and can be deployed in various configurations depending on available infrastructure. The tactical wireless intelligent video cameras transmit alert, data, and images in a localized Wi-Fi network. Data can be transmitted over a wide area using a variety of communication methods (cellular transmission, 802.11 wireless (WI-FI) or SATCOM). The IVC provides a capability to define areas of critical importance that pose the greatest threat to the warfighter. The IVC's capabilities provide for detection, classification, and behavior analysis of those identified threat areas. This also includes detecting objects and identifying them as persons, vehicles, or unknown objects. The technology operates with a rules-based engine which enables the user to automatically identify and track objects entering/exiting, appearing/disappearing, loitering near buildings or areas of concern, identify and notify user of left behind items, and the ability to create virtual tripwires ("fence"). The system provides the warfighter the ability to place low maintenance units in remote sites, control multiple systems remotely, and simultaneous monitoring of multiple systems. Advance Scout provides the warfighter with early detection and situational awareness of an adversary's threat activities.

**EWA Tiger's** suite of CITTTL technologies is assisting the warfighter in a broad array of mission sets. As mentioned above, the technologies are complementary and can be integrated in a variety of configurations to address multiple operational requirements or they can be provided as individual applications for a specific mission set. An example of integrating two applications would be combining EWA Tiger's Black Hole 802.11 Intercept System and the GeoStorm Geo-location technology. The combined capability of the two would provide an organization with the ability to intercept 802.11 data, accomplish a tactical analysis of the intercepted data, and then subsequently geo-locate the specific source of the 802.11 communication. The two applications can be integrated onto a single small field computing device provided by EWA Tiger, minimizing the logistics burden of the warfighter.

**EWA Tiger's** CITTTL technologies can also be integrated with other existing systems (i.e., jammers) to provide a broader system of systems approach to defeat specific threats such as IED's. In a jammer system of systems approach, our **EWA Tiger** CITTTL technologies significantly enhance operations focused on IED pre-detonation efforts, such as geo-locating an IED initiator device with GeoStorm Geo-location technology or intercepting RF communications (802.11, GSM cellular, or FRS) with our Black Hole or ARROW technologies that reveal an imminent IED attack. There are a multitude of ways and scenarios to utilize our CITTTL applications. **EWA Tiger** can provide specific solution recommendations and associated cost data for whatever requirement an organization is attempting to address, whether it be for a single application or an integrated solution of CITTTL technologies. Again, **EWA Tiger's** suite of CITTTL technologies is mature and ready to assist the warfighter in the Global War on Terror.