Cyber Investigation Unit (CIU)

Threat Countermeasures

Information Operations and Atmospherics

Identify | Investigate | Disrupt | Counter

The Cyber Investigation Unit (CIU) for Threat Countermeasures provides the capability and capacity to identify, track and remove Illegitimate and Disruptive audio, video, photo/image, and written content posted on Web Sites and Social Media. The CIU measures target population sentiment, behavior and tendencies based on illegitimate posting and content that pose threats to National Defense, National Security, Civil Order and Authority and the Safety of Citizens, Communities and Populations.

This CIU acts as an **Investigative, Intelligence, Atmospherics and Information Operations Unit** combined into a single entity that identifies threats and conducts threat countermeasures similar to counterintelligence operations using elite and proven Cyber Investigation and Intelligence systems, methods and techniques including Artificial Intelligence. The CIU we deliver will have the following capabilities:

✦ Disrupt the Illegal Operations of Bad Actors by Interrupting, Interfering, and Stopping and their Web- and Social Media- Based Communications,

✦ Initiate timely Communication Countermeasures that Invalidate, Refute or Disprove the Disruptive Web and Social Media Messaging,

✦ Take Down (Remove) Negative Social Media and Web Site Audio, Video, Photo and Written Content that Pose Threats to Civil Society and that may Instigate Crime, Violence, Protests, Disorder, or Insurrection,

✦ Conduct Sentiment Analysis of the Population and Communities to Determine the Effect of Posted Audio, Video, Photo and Written Content and Materials including the Trends of their Opinions and Beliefs and their Support or Disapproval of the Negative Content and Materials,

✦ Conduct Behavior Analysis and Pattern Analysis of Individuals, Groups and Networks to Project and Anticipate the Intent of Potential Disruptive Activities,

✦ Utilize Cyber Manipulation Tools and Methods to Reduce the Rankings of Web Sites with Negative Content to Prevent them from being Listed or Displayed by Search Engines such as Google, Bing, Yahoo, DuckDuckGo, Baidu, etc.

Fully Operational CIU with Highly Trained Cyber Threat Analysts in 60-Days

Our Cyber Teams deliver *fully operational CIUs with fully trained customer personnel within 60-Days* at prices that most investigative or intelligence agencies can afford. This means we deliver all cyber forensics hardware, software, database, and communication systems, and we train inexperienced

customer personnel to become *Cyber Threat Analysts*, *Supervisors and Managers* who operate at professional levels.

After our Cyber Team completes the CIU, we continue to provide cyber forensics investigative and intelligence support in actual cases and intelligence operations for a period of one-year. We remain in place until your CIU is highly proficient in Cyber Forensics; they successfully reduce, nullify and eliminate threats, arrest criminals and prosecute crimes and maintain civil order and the safety of citizens.

US Armed Forces – Information Operations and Atmospherics

Torres AI CI integrates Information Operations (IO) and Atmospherics into our Cyber Intelligence Systems and Methods to form a complete understanding of the digital operational environment. For example, we employ Information Operations to influence action among and between targets in order to identify and track their activities, movements and locations. We then employ Atmospherics to measure the impact of target activities and messaging among the people and populations within the areas of interest. With this information we can employ countermeasures to mitigate the bad intents of the targets.

Leading Architect in the Integration of AI into Cyber Forensics Systems and Methods

Torres AI CI is the architect and leader in the integration of Artificial Intelligence (AI) with Cyber and Digital Forensics to advance threat investigative, intelligence and countermeasure operations. For example, we are the first incorporate AI into our Cyber Investigative and Intelligence systems and processes to identify, track and capture targets, to collect and present key evidence for prosecution and to remove threatening content from a wide range of digital platforms and sources. Our AI methods and techniques include technical, behavioral and sentiment analysis to identify criminal organizations, groups and individuals to quickly advance investigation, intelligence and countermeasure efforts.

The CIU – a Covert Operation

It is essential that the CIU remains a "Non-descript", "Covert" and "Top Secret" unit to avoid detection by Bad Actors while CIU Cyber Analysts conduct countermeasure and counterintelligence operations. Maintaining covert operations is critically important to ensure that targets are not alerted to cyber-based countermeasure and counterintelligence activities targeting them. The Bad Actors that use the Web and the Dark Web (Darknet) are always alert and cautious in their cyber activities to avoid detection by law enforcement and intelligence agencies, so any mistake by CIU Cyber Forensics Analysts will cause these targets to change their tactics.

We teach CIU personnel that all Cyber Forensics Operations are "Covert" to ensure that Bad Actors are unaware of the CIU's presence, or its Cyber Forensics Tools, Methods, or Systems to maintain operational security and integrity. The Cyber Forensics skills we teach customer Cyber Forensics Analysts include both method and technology.

Contracted CIU for Customers without Capability or Resources

Torres AI CI is prepared to provide CIU Forensics Services and perform CIU duties when the customer does not have the resources to maintain his own CIU. In these cases, we provide the customer with CIU services from a remote Torres AI CI location that performs all Cyber Forensics duties working directly with the customer's designated Law Enforcement or Intelligence personnel.

Each of our CIU locations are covert and protected from physical and cyber intrusions. Our CIU services are customized based on the needs of the customer. For example, we can provide 24-hour services for periods of weeks, months or years, or focus on specific cases or operations.

Torres AI CI Training – Accredited AI and Cyber Training Institute

Torres AI CI is an accredited AI and Cyber Training Institute in multiple Artificial Intelligence and Cyber Systems, Technologies, Techniques and Methods. Upon successful completion of AI and Cyber training, our Instructors will present AI and Cyber Investigative, Intelligence and Countermeasure students with certifications registered with the Accrediting Organization.

As the author of several AI and Cyber Systems, Technologies, Techniques and Methods, Torres AI CI is the Accrediting Organization for its own AI and Cyber training courses. As such Torres AI CI will deliver training and award accreditations to Law Enforcement, Justice, Defense, Intelligence, National Security and Educational agencies and institutions to conduct their own internal training and present certifications to their own students.