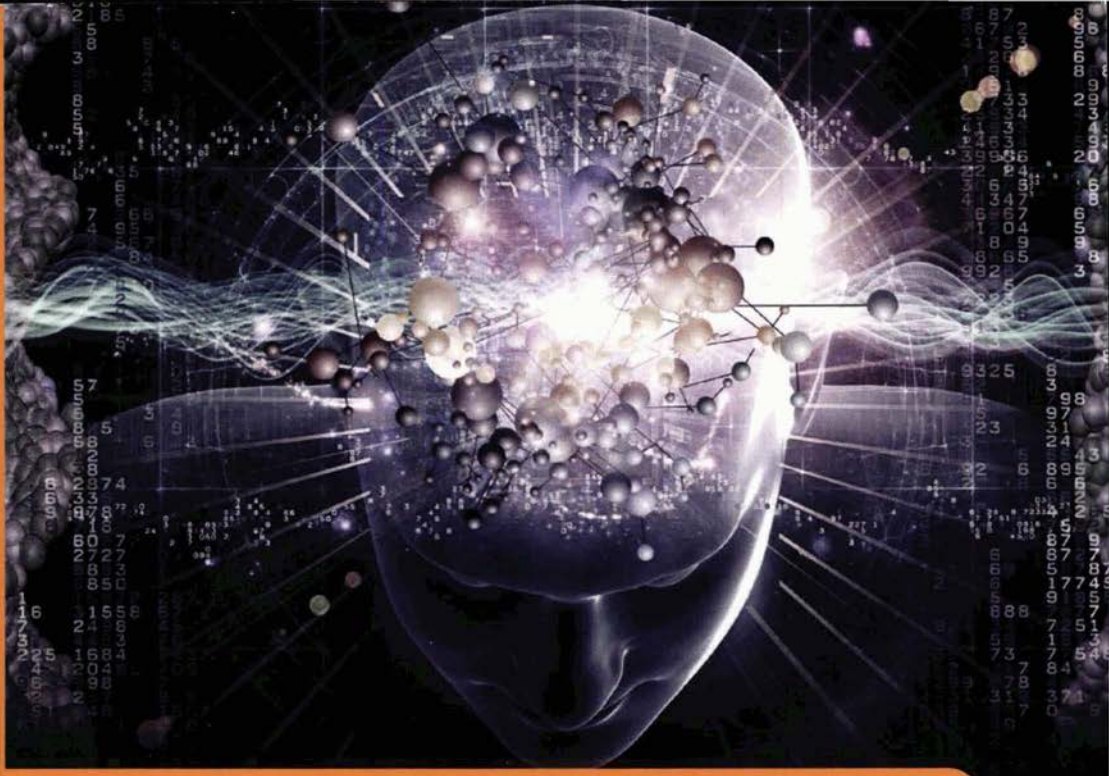


TERROGENCE

Intelligent Web Intelligence

www.terrogence.com Terrogence

About Terrogence

We are global pioneers of Virtual HUMINT™-driven Web Intelligence Services & Technology, designed to bridge crucial intelligence gaps faced by allied governments and corporations around the world.

Our WEBINT efforts are powerfully focused on Tactical C-IED, Cyber Counter-Intelligence, Enhanced Due Diligence for corporations, and more.

Table of Contents

Our Edge:

Why the Terrogence approach to Web Intelligence is right for your organization.

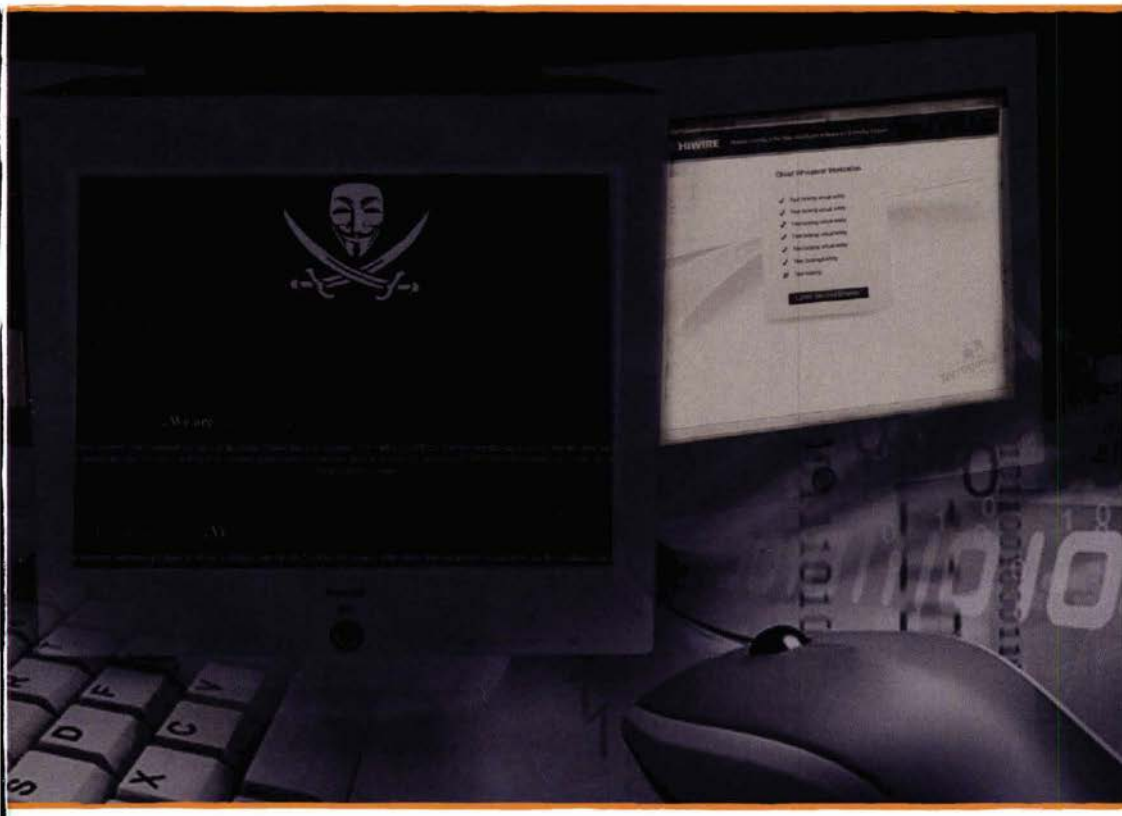
Virtual HUMINT™ Methodology

Much like a traditional intelligence agency might recruit and operate live human assets in physical spaces, in order to obtain information.

Terrogence specializes in cultivating and operating virtual entities in online spaces, that access social media platforms legitimately and act naturally, gaining trust, forming connections and ultimately collecting valuable intelligence from cyber-sources and cyber-entities of interest.

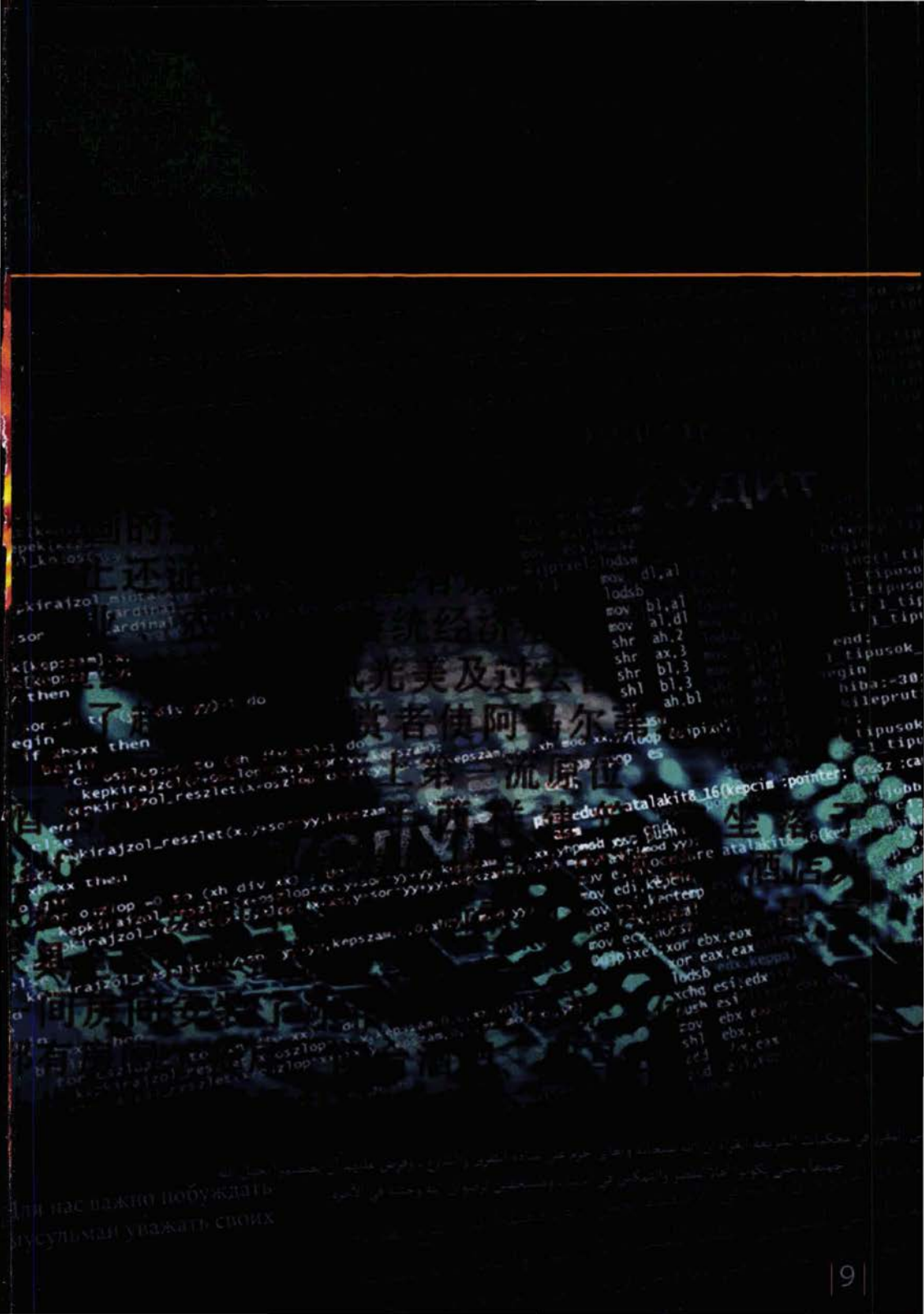
HIWIRE™ Technology

Our unique web-specific methodology developed organically over several years, culminating in an end-to-end WEBINT operations platform called HIWIRE™ (Human Interface for Web Intelligence Research and Entity) "Designed by WEBINT professionals for WEBINT professionals.The system's rich web-specific toolbox provides a technical mini-solution to every aspect of the WEBINT production lifecycle, from general source & entity management to specific video frame extraction and annotation, to assisted report generation, all seamlessly integrated in one user-friendly interface."

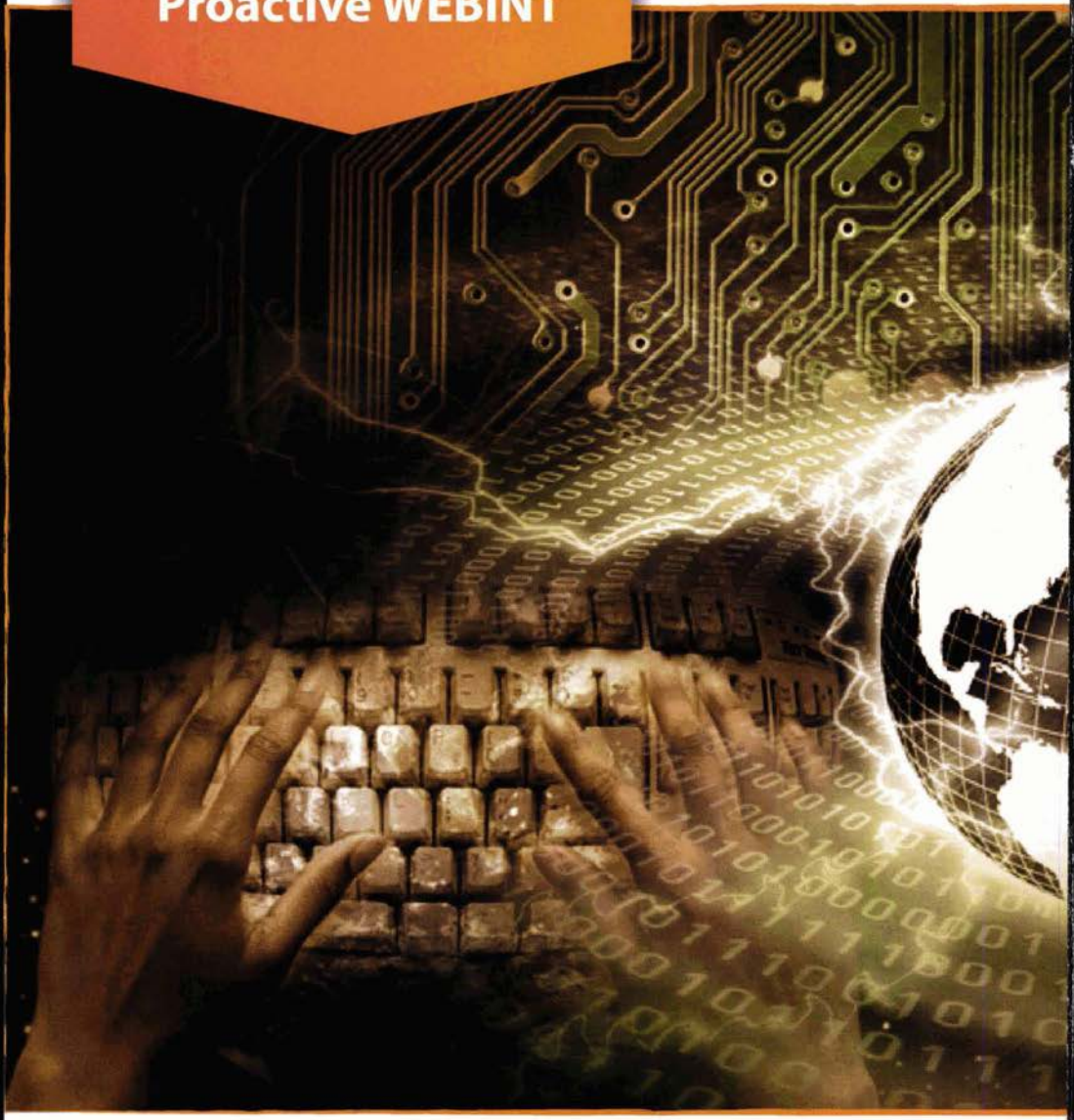


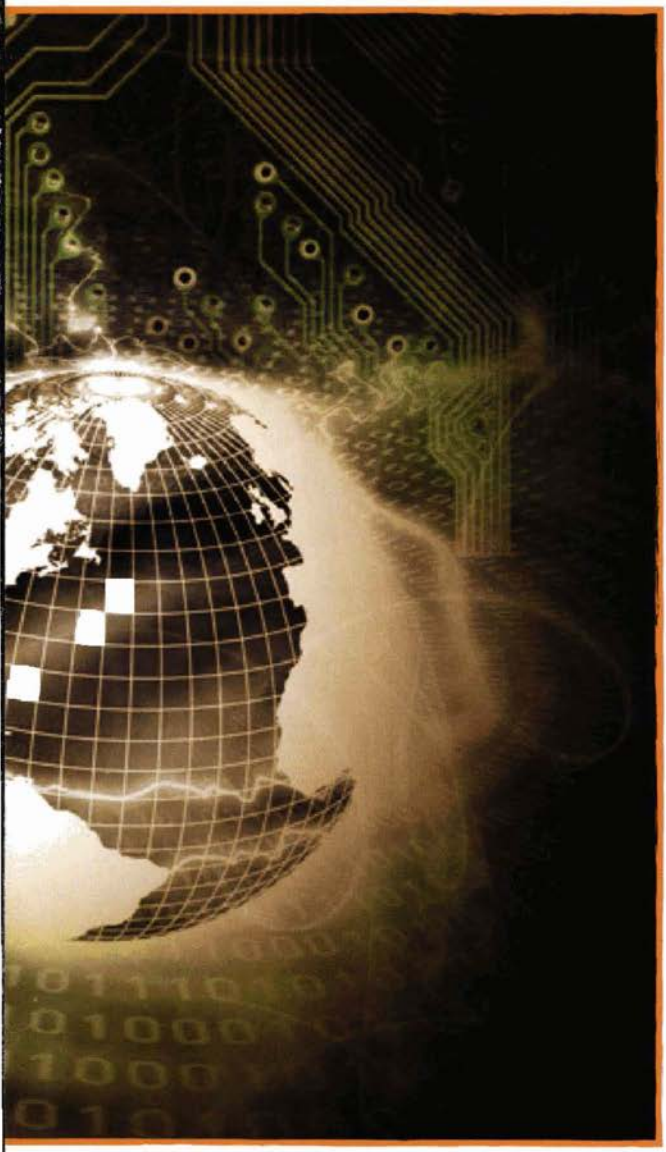
Extended Language Capabilities

Dedicated to the highest levels of source-accurate, contextually relevant deliverables, Terrogence employs an array of seasoned operational linguists, enabling us to cover an unusually wide swath of critical open and deep web sources in Arabic, Farsi, Urdu, Hindi, Turkish, Russian, Spanish, French, Polish and more.



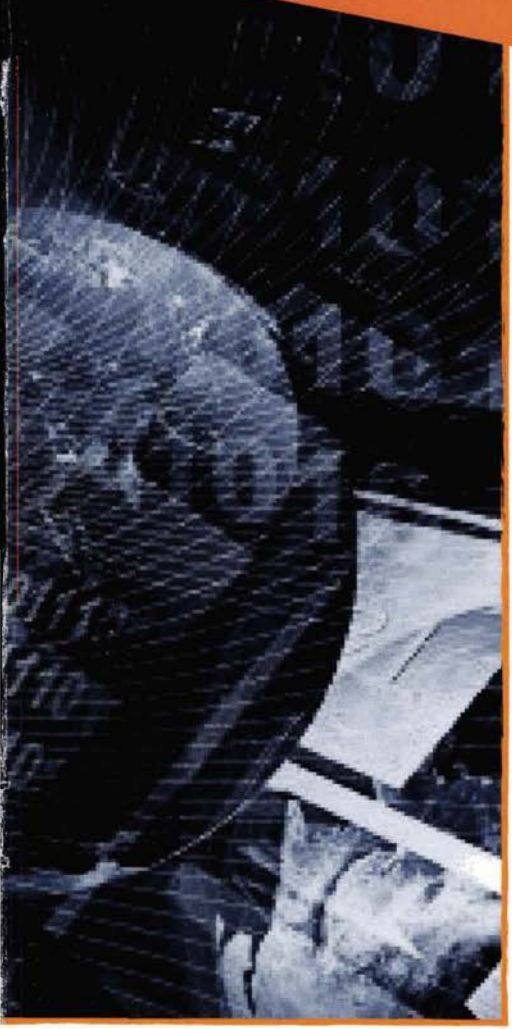
Proactive WEBINT





On the dynamic web, Terrogence is more of a human in the room than a fly on the wall. We guide our Virtual Entities to interact like actual human users. Going a step beyond, we actually elicit information by carefully guiding online discussion, often drumming up interest and facilitating communication by employing multiple virtual entities in a single operation.

A Human-Intelligence Approach to Big Data

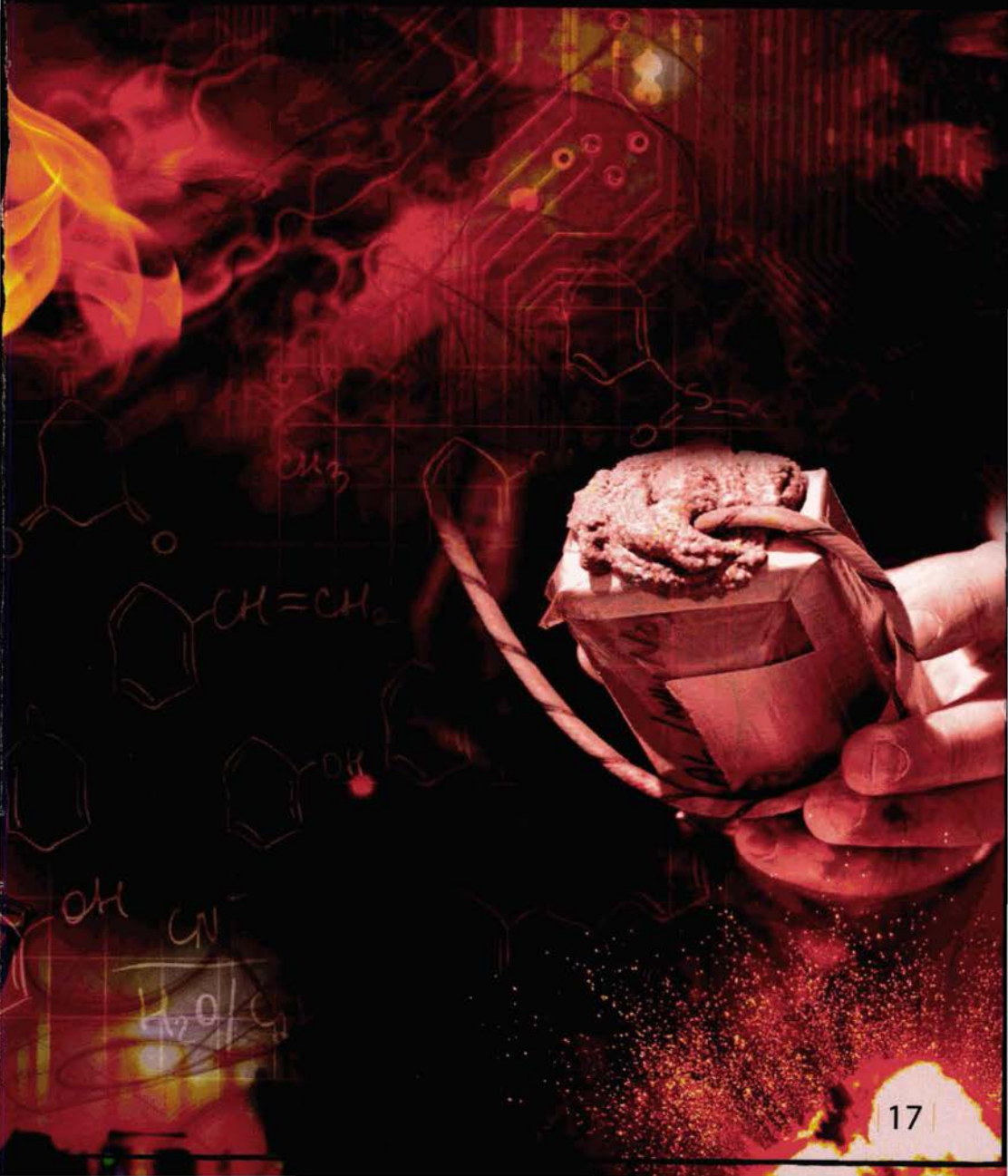


Terrogence is predicated on the idea that big data merely provides context to the specific intelligence derivatives that can be coaxed from it with a virtual human touch. Our HIWIRE™ system, together with the methodology that inspired it, embodies a proactive, human-centric approach to WEBINT, as opposed to a techno-centric, passive approach of many crawler-based intelligence solutions and methodologies.

Core Areas of WEBINT Expertise

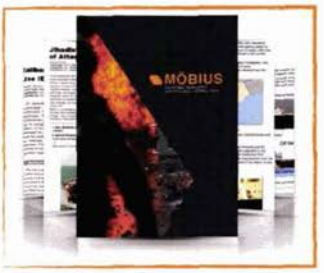
Physical Threats Intelligence

The IED is here to stay, and as deadly as ever. Terrogence are deep inside the web of terrorist and insurgent online organization, in the user-access-restricted portions of networks where old TTPs are perfected and new TTPs developed.



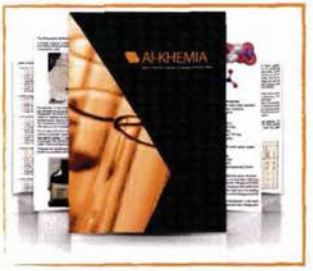
Subscription Reports for Counter-Terrorism

Al-Khemia™ - Al-Khemia™ delivers an in depth analysis of real-life explosives recipes as they appear in hard-core terrorist forums and knowledge bases. Exposing these recipes and components is key to rooting-out the IED threat from its source: the makeshift-labs and workshops where modern day IEDs are created.



Möbius™ - Möbius™ deals with the deployment of explosives in Improvised Explosive Devices (IEDs) of all types, representing current capabilities in manufacturing IEDs, Vehicle Borne IEDs, body worn IEDs, detonators, camouflage etc.

TGAlertS™ - Outright threats or developments of imminent interest in the deep web are disseminated in near-real time via the Terrogence Alert Service (TGAlertS™). In order to avoid inundating subscribers with the low threshold of "just news", TGAlertS™ dig a level deeper, providing context and interpretation.



Hydra™ - Hydra™ paints a rich picture of extremist use of the internet, with particular emphasis on hardcore Jihadist peer-to-peer platforms. Each month the report examines the latest publications, potential targets and underlying motivations of internet terrorist activists around the world.

Looking Glass™ - Looking Glass™ analyzes the behavioral patterns of prominent Jihadi-web entities who are often experts in the field of explosives and IED manufacturing, as well as the main disseminators of such information over the web.

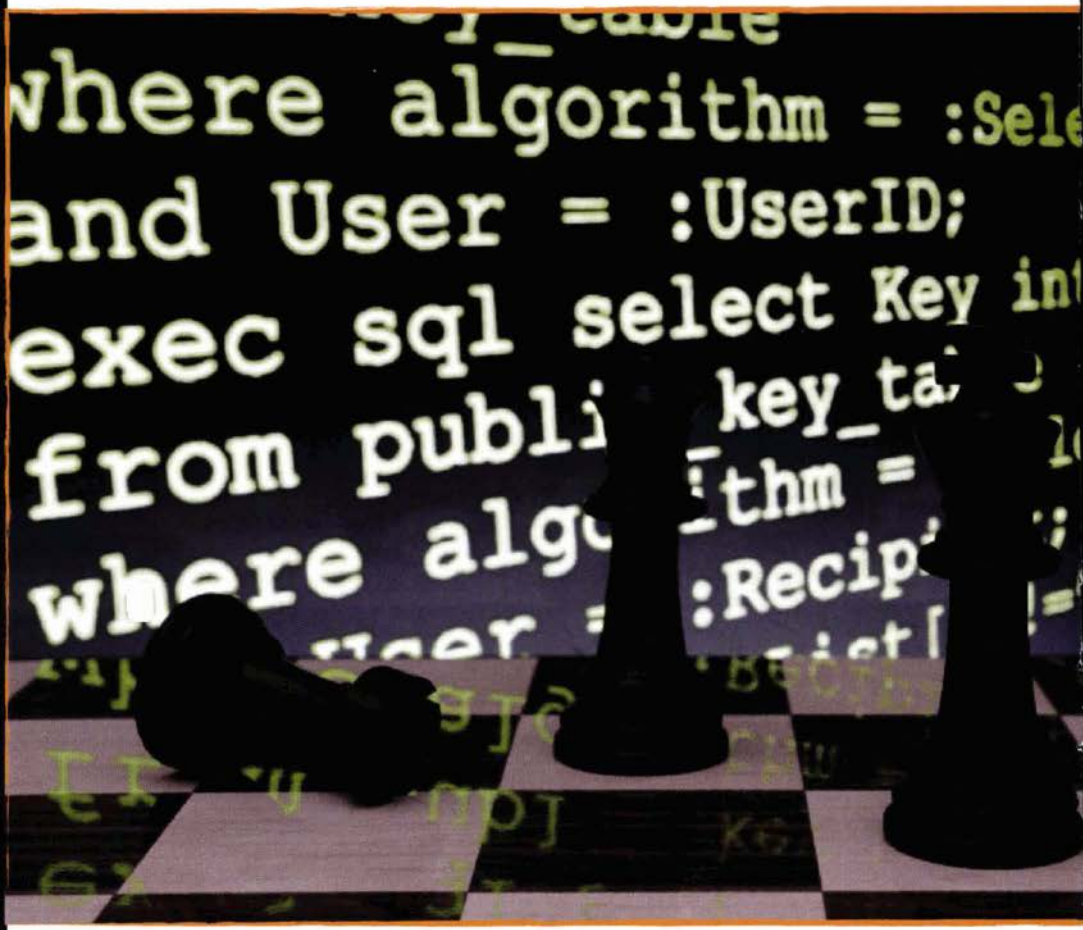
Chimera™ - As terrorist affiliations and other non-state actors continue to quest after bona fide WMDs, CBRN online knowledge bases in Arabic and other languages mature towards critical mass. Chimera™ monitors the development of this 21st century threat, exposing salient developments of CBRN knowledge shared among jihadists online.

Cyber Threat Intelligence

Mitigation of Cyber threats, like any other, is based on a multi layered approach. In the Cyber warfare arena, the obvious defense layer is that of technology layer, installing firewalls, switches and sniffers. The most overlooked layer is the Intelligence layer: knowing your Cyber adversaries and exactly what threats they pose. Intelligence as a concept is viewed as a very broad term, mostly associated with military affairs.

Today's Cyber battlefield has evolved to become very similar to a "classic" terror battlefield, with similar intelligence needs and benefits; most of the actors in the Cyber arena are either non-state actors or state sponsored actors. These activists and units "live", communicate and thrive on the internet while targeting mostly non-military targets.

Corporate Intelligence Solutions



The advanced technology and methods that lend superiority to Terrogence WEBINT operations on behalf of governments, really come into their own harnessed to the interests of global corporate entities who are even more exposed to the web. Some of the WEBINT services Terrogence supplies to corporations include:

- Enhanced Due Diligence.
- Compliance Enforcement Monitoring.
- Web Exposure & Vulnerability Assessment (Virutal Red Team).
- Commercial Sector Cyber Counter-Intelligence (Finance & Banking, Petro-Chemical & Energy, etc).

WEBINT Training & Workshops

Over the past several years, Terrogence has honed a proven methodology for harvesting applied open source intelligence from web platforms, bridging the intelligence gaps of our customers worldwide. Our methodologies and practices have been developed specifically for Open Source Web Intelligence (WEBINT) and have been tried and tested over years of intelligence production and operations.

The trainers for our web-intelligence workshops and training sessions come from rich intelligence and operational backgrounds in SIGINT, HUMINT, OSINT and HLS strategy.

www.terrogence.com