SIGN4L

WIFINDER

TACTICAL CONTROL. INFORMATION CAPTURE.

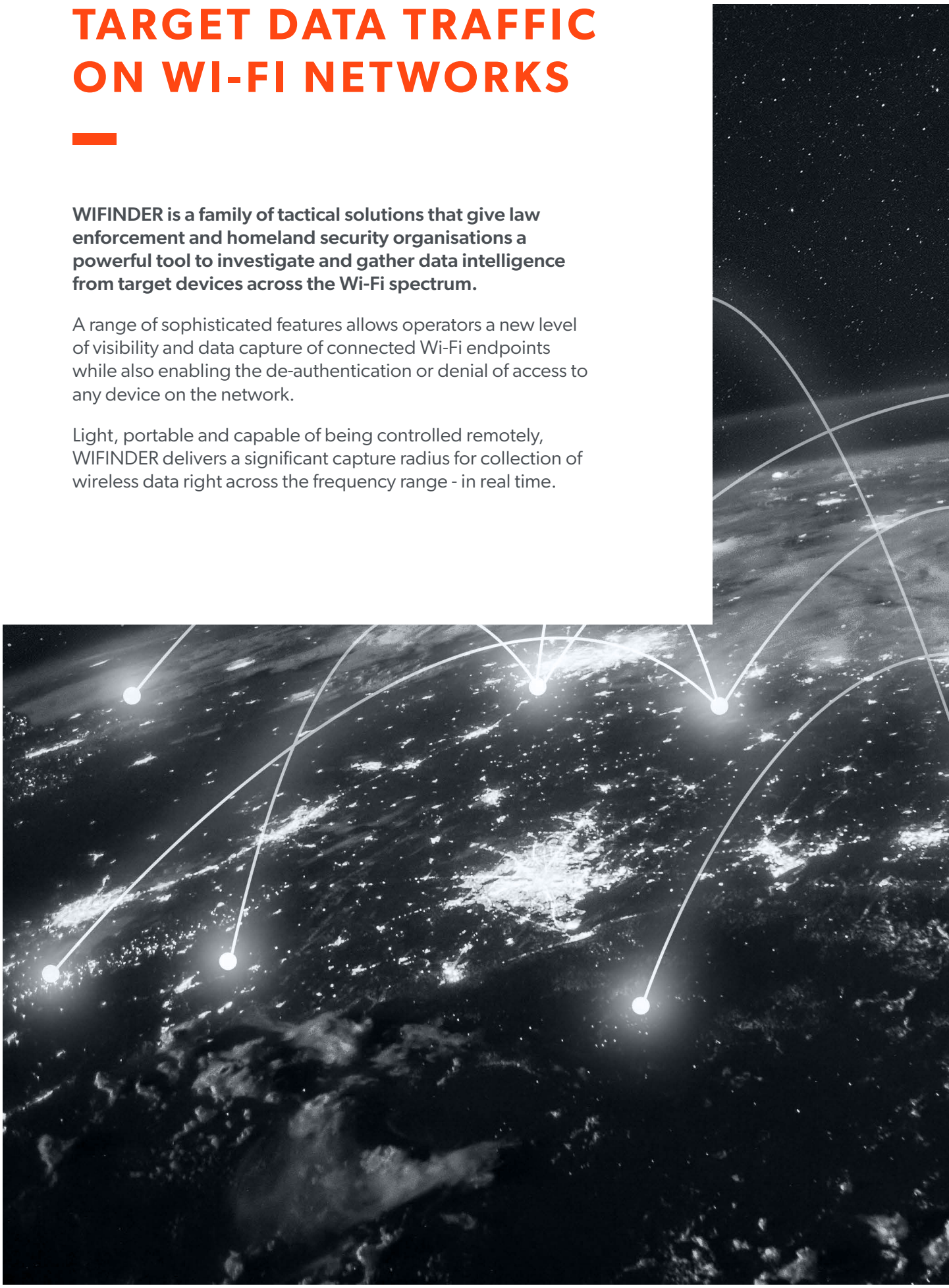
Commanding the Wi-Fi landscape with sophisticated and discreet solutions

TARGET DATA TRAFFIC ON WI-FI NETWORKS

WIFINDER is a family of tactical solutions that give law enforcement and homeland security organisations a powerful tool to investigate and gather data intelligence from target devices across the Wi-Fi spectrum.

A range of sophisticated features allows operators a new level of visibility and data capture of connected Wi-Fi endpoints while also enabling the de-authentication or denial of access to any device on the network.

Light, portable and capable of being controlled remotely, WIFINDER delivers a significant capture radius for collection of wireless data right across the frequency range - in real time.



KEY FEATURES

- Significant capture range
- Discrete and portable form factor
- Real-time collection of Wi-Fi emitters and metadata
- Intelligence gathering across multiple Wi-Fi connected devices

WIFINDER: TACTICAL SMART PHONE

WIFINDER provides undercover security personnel and officers with a powerful covert device to monitor or jam Wi-Fi networks, and mobile Wi-Fi devices in the range of a WIFINDER enabled mobile phone. The solution can be used for existing Wi-Fi networks such as public hotspots, home and company networks, or to create custom Wi-Fi hotspots that provide full intelligence on all connected devices and their online activities

WIFINDER allows the undercover officer to appear as a civilian public Wi-Fi user browsing the internet or streaming video content, even as the smartphone conducts network intrusions or intelligence data capture of targeted devices.

Components

Mobile phone: Off-the-shelf Android smartphone that runs the covert WIFINDER application.

Covert Wi-Fi Adapter: Custom phone case with hidden Wi-Fi adapter.

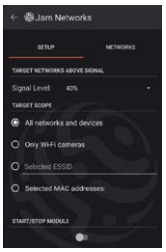
WIFINDER App: Covert Android application that is installed on the smartphone and contains the core data-collection functionality.

WIFINDER Headquarter: Windows application installed on a computer. The software configures the smartphone for operation and retrieves, analyses and displays the collected data. It also can remotely control WIFINDER enabled devices.

Six Powerful Functions

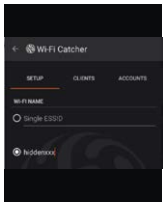
Wi-Fi Analysis

Wi-Fi Analysis allows the capture and recording of intelligence and evidence data from access points within Wi-Fi range of the device. This reconnaissance technique can be deployed when scoping out premises for target devices or when suspects meet nearby and basic intelligence about the suspects' devices is required.



Wi-Fi Jammer

The Wi-Fi Jammer enables jamming and denial of service to all – or select – mobile phones, cameras, IoT devices and other endpoints on a network.



Wi-Fi Catcher

The Wi-Fi Catcher feature can initiate Wi-Fi hotspots for single or multiple network names to capture Wi-Fi devices and gain access to device and traffic information.

Bluetooth Scanner

Bluetooth devices identification including and recording of intelligence.

IMSI Grabber

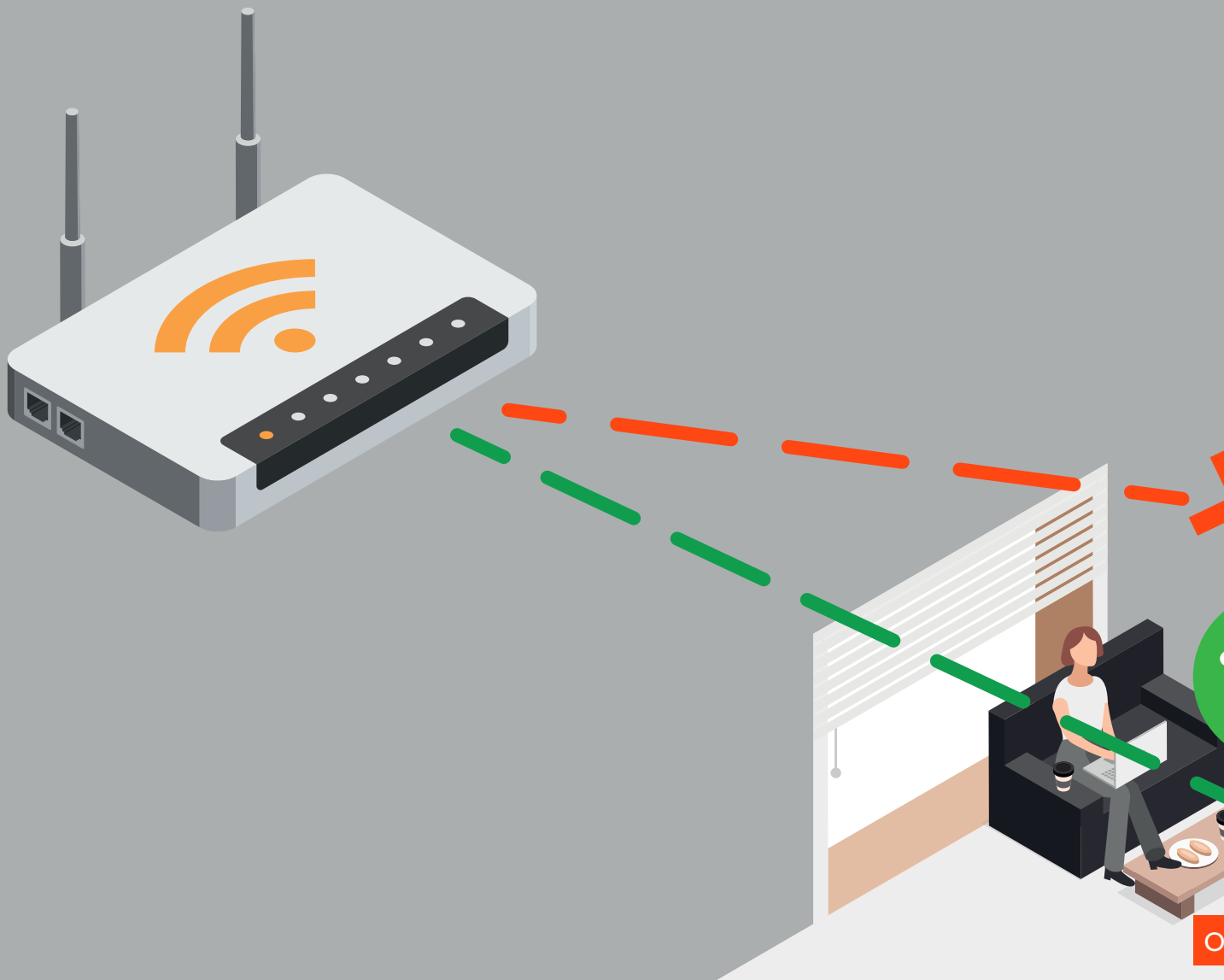
The IMSI Grabber records and correlates the international mobile subscriber identifier of cell phones in the vicinity.

Hotspot Login Injection

The customisable Hotspot Login Injection feature can be used to capture a suspect's Facebook, Google, X or other account credentials, using the Wi-Fi Catcher or Network Monitor features.

USE CASE: COFFEE SHOP WI-FI

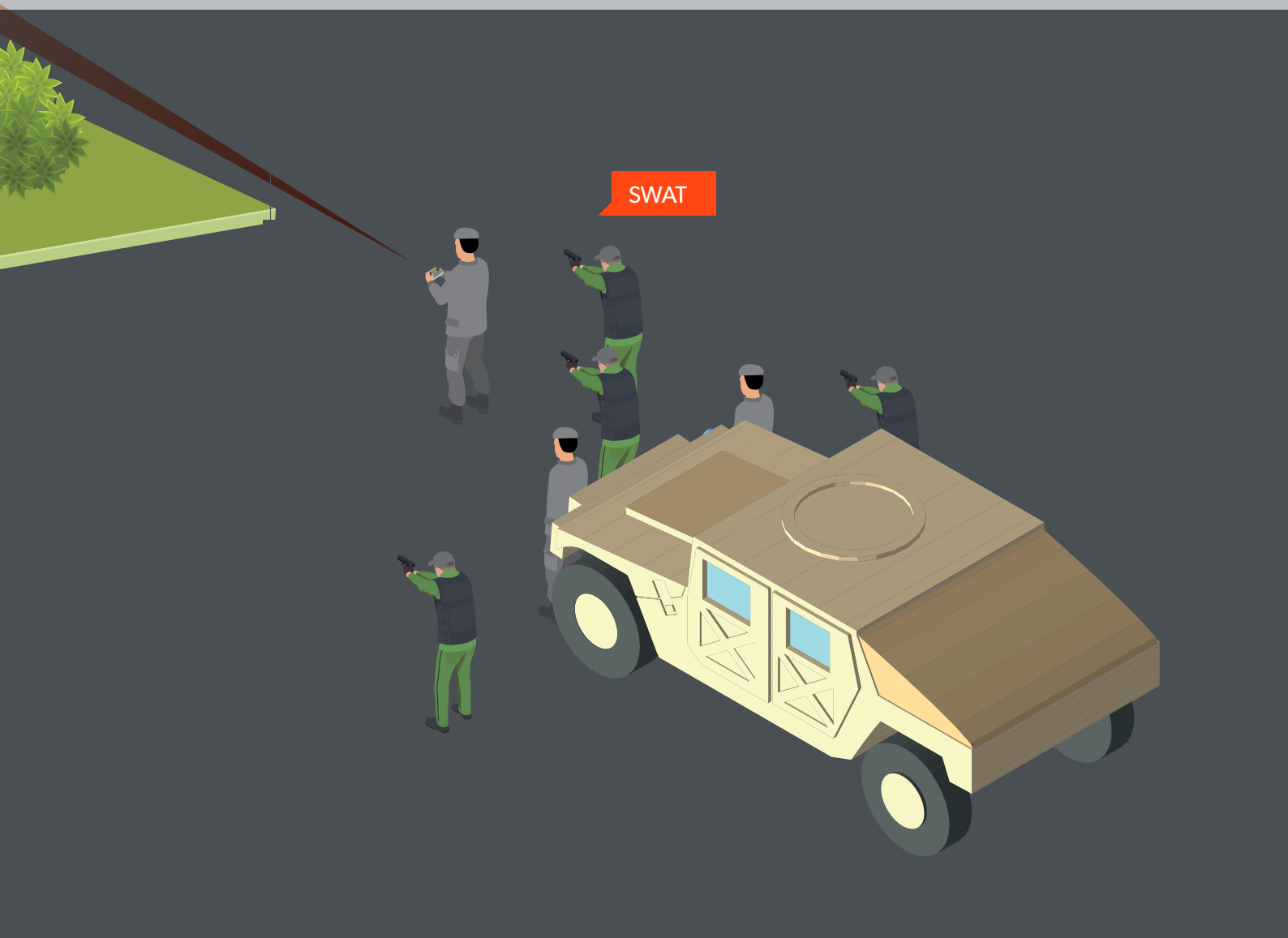
The Wi-Fi IMSI Grabber can be deployed to collect intelligence on a suspect who accesses public Wi-Fi networks, such as those provided at coffee shops. The solution can be used to collect valuable voice, data and text metadata from mobile devices that automatically connect to the Wi-Fi hotspot




latte
FRAPPE
Coffee
Coffee menu
Coffee
TARGET
PERATOR

USE CASE: CCTV

Tactical teams can gain an advantage or avoid detection by using the Wi-Fi Jammer to disable surveillance cameras and other Wi-Fi connected detection technologies. The smartphone form factor and intuitive operation delivers powerful capabilities in a compact non-intrusive package that supports mission success.



SIGN4L

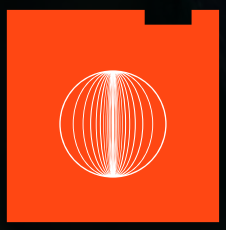
ABOUT SIGN4L

Electronic warfare (EW) systems have become an essential element of the modern battlefield, and SIGN4L is pioneering advanced technologies to secure the electromagnetic spectrum and is developing disruptive solutions to outpace adversaries.

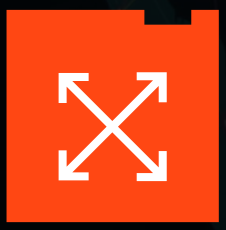
Based in Abu Dhabi, SIGN4L is the leading provider of EW solutions in the UAE and one of only a few in the region with such capabilities.

SIGN4L is part of the Electronic Warfare & Cyber Technologies cluster at EDGE Group.

OUR CAPABILITIES



Electronic warfare deception and concealment

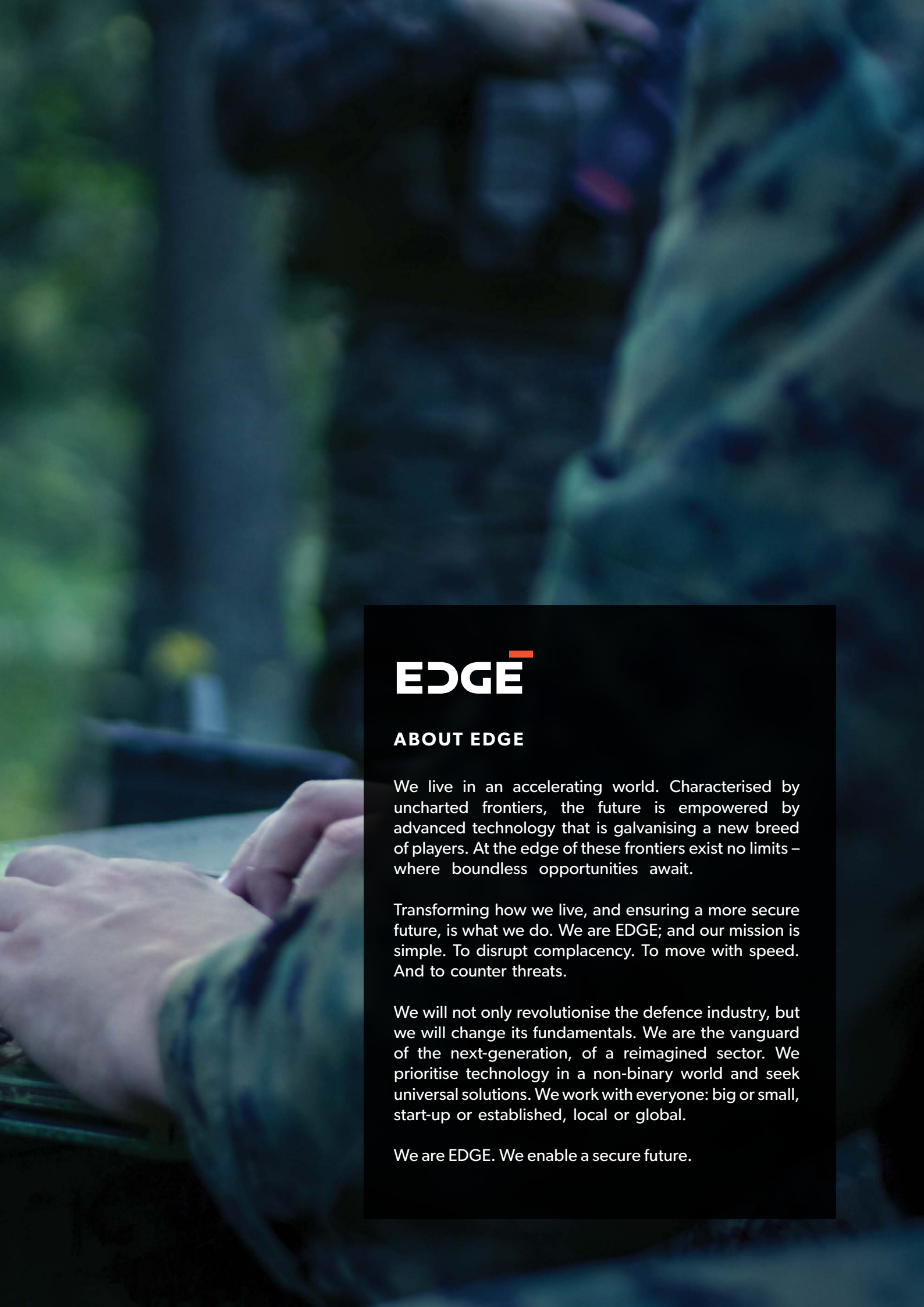


Electronic warfare protection

Electronic and communication intelligence

Electronic warfare support measures

Intelligence, surveillance, target acquisition and reconnaissance (ISTAR) sensors



EDGE

ABOUT EDGE

We live in an accelerating world. Characterised by uncharted frontiers, the future is empowered by advanced technology that is galvanising a new breed of players. At the edge of these frontiers exist no limits – where boundless opportunities await.

Transforming how we live, and ensuring a more secure future, is what we do. We are EDGE; and our mission is simple. To disrupt complacency. To move with speed. And to counter threats.

We will not only revolutionise the defence industry, but we will change its fundamentals. We are the vanguard of the next-generation, of a reimagined sector. We prioritise technology in a non-binary world and seek universal solutions. We work with everyone: big or small, start-up or established, local or global.

We are EDGE. We enable a secure future.

Ahmed Ali Alhosani

Manager, Business Development
EDGE Electronic Warfare & Cyber Technologies
+971 50 555 4566
ahmed.alhosani@edgegroup.ae

SIGN4L

EDGE HQ
Channel Street
P.O.Box: 43221
Abu Dhabi, UAE

www.sign4l.ae