TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) "DEBUGGING"
ADVANCED CORPORATE SOLUTIONS (ACS)
30 YEARS' SERVICE

ANNIVERSARY OF SERVICE EXCELLENCE 30 Years

Address: 1st Floor HB Forum Building, 13 Stamvrug Street, Val De Grace, Pretoria, Gauteng, South Africa, 0184
Postnet Suite 62, Private Bag X 025, Lynnwood Ridge, 0040
Office Tel: +27 (0) 12 349-1779 | Riaan Bellingan: +27 (0) 82-491-5086
Email: info@acsolutions.co.za | Website: www.acsolutions.co.za

OVERVIEW OF EQUIPMENT AND PROCEDURES

TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) "DEBUGGING"

TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) "DEBUGGING"

ADVANCED CORPORATE SOLUTIONS (ACS)
30 YEARS' SERVICE

INTRODUCTION

For many businesses, intellectual property protects more than just an idea or a concept – it protects genuine business assets that may be integral to the core services of the business and overall long-term viability.

Intellectual property can consist of many different areas, from logos and corporate identity through to products, services and processes that differentiate your business offering. It's when these ideas are used without permission that an organisation can suffer. Almost all businesses have undoubtedly benefited from the internet, where products, services and marketing communications can reach vast audiences at relatively low costs - but this has also increased the chances of intellectual property theft. Companies of all sizes are at risk of having their unique ideas, products or services infringed upon, even if they are on the other side of the world, making intellectual property protection more important than ever.

A main contributing factor in corporate espionage and the use of listening and video devices is the increasing sophistication, durability, and ready availability of items on the market. In South Africa, bugging devices can be readily bought over the counter and through popular online retailers, and the devices are smaller and capable of being on for longer periods to capture information. This is making the corporate spy's job even easier.

The threat of corporate espionage is real. Advanced Corporate Solutions (ACS) provides all-encompassing and comprehensive Technical Surveillance Countermeasures (TSCM) Investigations. The most modern and technologically advanced equipment, available in South Africa, are used during our TSCM Investigations.

TSCM PROGRAMME

Herewith more information about the TSCM Programme and the Equipment we make use of.

TABLE OF CONTENTS

TSCM EQUIPMENT

We make use of state-of-the-art equipment, purposely built to perform specific tasks during our assessments. Our equipment register consists of the following:

OSCOR™
BLUE SPECTRUM ANALYSER

The OSCOR Blue Spectrum Analyzer is a portable spectrum analyser with a rapid sweep speed and functionality suited for detecting unknown, illegal, disruptive, and anomalous rogue transmissions across a wide frequency range. The OSCOR Blue is designed to detect illicit eavesdropping signals, perform site surveys for communication systems, conduct radio frequency or RF emissions analysis, and investigate misuse of the RF spectrum. It sweeps 10 kHz to 24 GHz or 10 kHz to 8 GHz (depending on the model) in one second to quickly detect transmitting electronic surveillance devices and ensure that spectrum activity is captured.

MESA - MOBILITY ENHANCED SPECTRUM ANALYSER

The MESA is a portable, handheld RF receiver that detects known, unknown, illegal, disruptive, or interfering transmissions. The MESA features unsurpassed mobility and ground-breaking features, not found in any other spectrum analyser. First in its class, the MESA is purpose built to locate unknown signals throughout a wide frequency range up to 6 GHz. It DETECTS: RF, Wi-Fi, Bluetooth, Cell phone signals and Illicit transmissions. (Eavesdropping “Bug” Detection).

A.N.D.R.E DELUXE - ADVANCED NEAR-FIELD DETECTION RECEIVER

The A.N.D.R.E Deluxe is a handheld broadband receiver that detects known, unknown, illegal, disruptive, or interfering transmissions. The ANDRE locates nearby RF, infrared, visible light, carrier current, and other types of transmitters and quickly and discretely identifies threats using its wide range of accessories specifically designed to receive transmissions across a 10 kHz to 6 GHz frequency range. Technical security specialists will appreciate the portability and responsiveness of the ANDRE. It is an excellent complement to an OSCOR Spectrum Analyzer/Raptor as a preliminary non-alerting tool.

RAPTOR RXI ULTRA-FAST-SCANNING COUNTER-SURVEILLANCE RECEIVER

The Raptor RXi is an ultra-fast-scanning counter-surveillance receiver for quickly detecting surveillance transmitters. The RXi scans from 10 kHz to 26GHz in under 4 seconds, detecting even the briefest pulsed transmissions. Featuring a fast Core 2 Duo processor, its multiple software tools and demodulators detect frequency-hopping, burst mode and spread spectrum devices as well as analogue audio and video signals. The 'Waterfall' display mode gives an intuitive display of signals over time. The RXi is fully portable, operating either from an internal rechargeable battery or an external supply. Its integrated antenna system provides wideband performance from 10 kHz to 26GHz.

KESTREL TSCM® PROFESSIONAL SOFTWARE

Kestrel is a highly evolved TSCM specific, operator centric SDR application, with advanced capability to meet TSCM specific and evolving challenges of professional technical operators, working in the private sector, and within the national security apparatus, who are faced with a modern moving target threat model, in combating the growing threats of cyber-espionage. The Kestrel TSCM ® is not a simplistic desktop spectrum analyser, offering limited capability, but rather, it is a highly deployable, mission scalable, travel friendly full featured TSCM focused product.

TALAN 3.0 TELEPHONE AND LINE ANALYSER

The TALAN represents a state-of-the-art capability to detect and locate illicit wire taps on both digital and analogue telephone systems. It provides the capability to perform multiple tests to analyse communication lines for eavesdropping devices. It includes a built-in automatic switching matrix for testing all pair combinations. For example, if a cable has 8 conductors, there are 28 combinations of pairs to test and it can automatically switch through all combinations, performing test functions and storing data for comparison. With new enhancements built into the TALAN software interface, users can now also test Internet Protocol (IP) packet traffic on Voice over Internet Protocol phones and systems. Data can be stored and exported to USB or Flash as data files for further analysis, sharing and reporting.

ORION™ 2.4 HX NON-LINEAR JUNCTION DETECTOR

The ORION 2.4 HX Non-Linear Junction Detector detects electronic semi-conductor components in walls, floors, ceilings, fixtures, furniture, containers, or other surfaces. The ORION is made to detect and locate hidden cameras, microphones, and other electronic devices regardless of whether the surveillance device is radiating, hard wired, or turned off. The ORION can locate small electronics such as SIM cards in walls, floors, ceilings, packaging, fixtures, furniture, or containers.

BLOODHOUND SHEARWATER 2000

(To test for hidden and live microphones on telephones and lines, please visit www.shearwatertscm.com)

Bloodhound is an Acoustically Stimulated Microphone Detector which is an electronic system for use by Technical Security Inspection Teams for detecting audio eavesdropping. The system works by detecting the radiated field created whenever a microphone detects sound. The Bloodhound operator can either listen to the detected audio or establish acoustic feedback. The Bloodhound is used to detect:

- Amplified wired microphone systems
- Telephone Attacks – Both base band and attacks using R.F. modulation techniques

- Radio Microphone Attacks and
- Video camera surveillance.

The Bloodhound system can also be used for:

- Cable tracing and
- Carrier Current device detection.

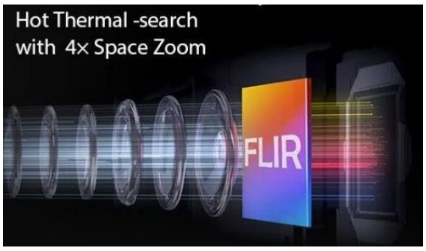
VIDEO POLE CAMERA

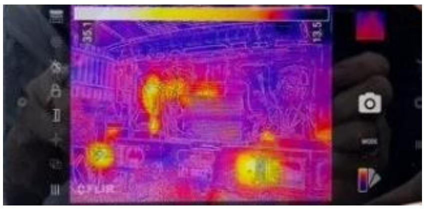
The camera provides white LED illumination for colour inspection in dark areas, such as drop ceilings, behind immovable objects, around corners, other difficult to reach areas and in dark situations.

SEEK SHOTPRO THERMAL IMAGING CAMERA

The Seek ShotPRO is the most advanced thermal imaging camera for professionals. Photos and videos are analysed immediately with new on-board thermography tools. Spot measurements and temperature boxes are created for time-saving reports. Problems are precisely diagnosed with 16x higher resolution.

BLACKVIEW RUGGED PHONE WITH FLIR® LEPTON® THERMAL IMAGING CAMERA





The Blackview BV8900 Rugged Phone with FLIR® LEPTON® Thermal Imaging Camera gives live thermal imaging expertise direct from a smartphone. This device uses FLIR (Forward Looking Infrared) to capture shareable clear thermal imagery, video, and even time-lapse footage. The thermal imaging technology is used in the field of Technical Surveillance Counter Measures (TSCM) Investigations to determine if there are any hidden electronic devices in a specific area. Electronic devices have multiple methods of accessing power to function and this invariably leads to the emission of heat. The device can further be used to identify and locate rogue Wi-Fi access points in a target area.

MOBILE FORENSICS - MALWARE AND SPYWARE ANALYSIS

Mobile devices, which include smart phones and tablet computers, provide increased functionality and ease of use to people, anywhere and anytime. Smart phones are the new computers. These devices contain a tremendous amount of personal and even business information. With rapidly increasing advances in technology, everyday life is starting to depend on these wireless technologies, but it brings greater risk and some unique security threats.

Mobile device malware (malicious code) has increased exponentially over the past few years. The sophistication of these exploits has also increased exponentially, making detection and eradication very difficult. Anyone can install eavesdropping software on your smart phone if they have access to your phone even for a few minutes. This can result in them gaining access to all your private data such as SMS, emails, pictures, location information, call logs and even listen in on actual calls.

Some malicious code will even allow the attacker to switch on the microphone of the device unnoticed and listen in on conversations or use the camera to secretly take pictures.

Our associate company Dynamdre can assist in mobile device investigations to gather information from mobile devices which may contain infected and malicious data. Please visit www.dynamdre.co.za and contact Dynamdre direct for further information and assistance.

Laptop Computers: Two (2) phases of malware analysis are conducted as described below:

Phase 1: Static Malware Analysis
Static analysis of malware entails the investigation of executable files without going through the actual instructions. The static analysis can validate whether a file is malicious, give information about its functionality, and sometimes provide information that will allow you to create simple network signatures. It is basic and can be quick, but it is mostly useless against sophisticated malware, and it can miss significant behaviours.

Phase 2: Dynamic Malware Analysis:
Unlike static analysis, dynamic analysis executes malware to observe its activities, comprehend its functionality and identify technical indicators which can be used in revealing signatures. The dynamic analysis can reveal domain names, IP addresses, file path locations, registry keys, additional file locations and can also classify communication with an attacker-controlled external server for command-and-control intentions or to download other malware files.

WI-FI SECURITY ASSESSMENT

In the face of the COVID-19 pandemic, most companies adopted a "working from home" policy. This had an adverse effect on companies, changing the way we work and operate, and introducing new Information Security Risks. During these trying times, perpetrators have made it clear that they are not resting, and they are not backing down! In fact, we have seen a substantial increase in these types of attacks over the last couple of months.

With "working from home" policies becoming the new norm, it now poses significant security risks, mainly due to companies and ICT teams having to rush, to put in place applications and services that enable remote work as well as more insecure connections.

In a recent survey conducted across 300 remote office workers and 300 ICT professionals, the results showed that 57% of remote workers use communication tools such as Zoom and Microsoft Teams, which have had well-publicised security problems in recent months.

Risky cyber-practices were shown to be particularly prevalent amongst working parents included in the study, who face additional distractions such as childcare and home-schooling. Of this cohort, 57% insecurely save passwords in browsers on their corporate devices while 89% said they reuse passwords across applications and devices. Additionally, 21% allow other members of their household to use their corporate devices for activities like schoolwork, gaming, and shopping. Despite the additional security risks posed by the huge rise in remote working, 57% of ICT professionals surveyed said they have not increased their security protocols in this period.

It is a well-known fact that home networks, and more specifically home Wi-Fi networks are far less secure than corporate networks, which poses another significant risk to business. In many cases, once a Wireless router has been installed, we find a place in our home for it and forget about it. As long as all our devices are set up and connected via the Wi-Fi network, that is all that matters, right? Wrong!

Probably many of you do not realise it, but the Internet router is one of the most important devices in our home. It is the gateway to our Internet access and prone to exploits by cybercriminals who can sneak into our devices and get access to our system. Let us not forget that we live in the age of data breaches, ransomware attacks, and many other online threats. Thus, one should be worried about the security of our home network and take all the needed security measures to increase Wi-Fi security.

Dynamdre, in conjunction with Advanced Corporate Solutions (ACS), conducts formal Wi-Fi Security Assessment within the residential (home) environments, registered to and owned by executive management from numerous organisations. The Dynamdre Wi-Fi Security Assessment provides organisation's executives with insight into the resilience of their home information security posture to withstand attack from unauthorised users, and the potential for valid users to abuse their privileges and access.

Technical Controls and Security Assessment focus areas include, but are not limited to the following:

- Identification of Rogue Wi-Fi Access Points.
- Default Credentials (Router Based Access and Wi-Fi Passkey)
- Unencrypted Wi-Fi Networks
- Legacy / Weak Encryption
- Outdated Firmware Version
- Network Segmentation
- DHCP Functionality Check
- Wi-Fi Passkey Strength Test
- Residential Wi-Fi Vulnerability Assessment