Advanced Corporate Solutions
"Debugging" Specialists | Service Excellence since 1995

PRACTICAL OVERVIEW OF EQUIPMENT AND PROCEDURES

TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM)

"DEBUGGING"

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 necessity of Protecting Company Intellectual Property (IP) – Communication Security.

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).

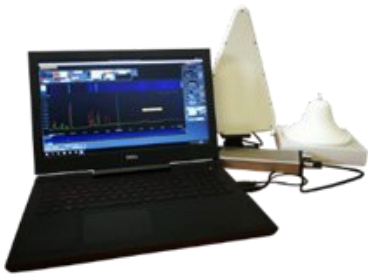
A.N.D.R.E DELUXE - ADVANCED NEAR-FIELD DETECTION RECEIVER

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

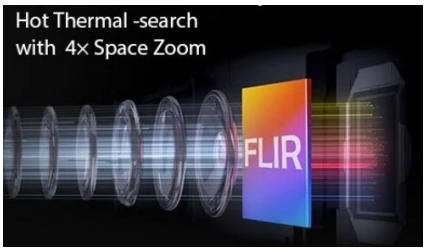
The Blackview BV8900 Rugged Phone with FLIR® LEPTON® Thermal Imaging Camera gives live thermal imaging expertise direct from a smartphone.

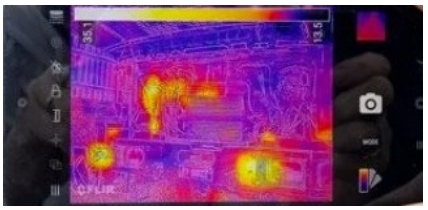
This device uses FLIR (Forward Looking Infrared) to capture shareable clear thermal imagery, video, and even time-lapse footage.

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, as long as 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.

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. If 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

REPORT PROCEDURE & COMMITMENT

ALL INVESTIGATIONS ARE CONCLUDED WITH A DETAILED REPORT TO THE CLIENT, INDICATING:

- Findings of the investigation.
- Shortcomings in the client's physical security measures that can facilitate eavesdropping attempts.
- Identified and potential eavesdropping threats and scenarios.

COMMITMENT:

- **Advanced Corporate Solutions'** investigators undertake to submit themselves to polygraph tests to affirm that they will not plant any devices on the client's premises. In the event that eavesdropping equipment is found on the client's premises, our investigators undertake to subject themselves to polygraph testing, in order to substantiate truthfulness in respect of who is responsible for planting the eavesdropping device.

- **Advanced Corporate Solutions** undertakes to allow the client to have all our equipment checked prior to and after the investigation, to ensure that no eavesdropping devices are taken onto the client's property by our investigators.

Should any eavesdropping equipment be found, the steps listed below will be followed:

- The device will **not** be removed.
- In conjunction with the client, Advanced Corporate Solutions will manage the situation to try and establish where the devices originate from.

EQUIPMENT:
CLIENTS OUTSIDE SOUTH AFRICA

- Due to the fact that TSCM equipment may be seen as espionage equipment by the Government, an authorisation letter from the Embassy for the entry of our Contractors with the necessary equipment will be required.

- A representative from Government should be requested to meet ACS Contractors at the airport to assist with Customs and clearance of equipment.

COMMUNICATIONS SECURITY

INTRODUCTION – THE TSCM PROGRAMME

Due to the advancement of Global Corporate Competitiveness, there is a growing need amongst Corporate Institutions especially at Executive Staff levels to protect all forms of communications. Communications Security encompasses all aspects of Communications transmission - Oral (spoken), Written and Data transmission, together with all relevant security techniques intended to achieve maximum possible protection of such transmission. It is of interest to note that more than 90% of the top listed Corporates in South Africa conduct a regular programme of TSCM. This proposal, however, is confined to the Oral (spoken) method of transmission and the existing current TSCM implemented to achieve maximum possible protection and security of such transmissions. It should always be remembered that information is a Corporate Asset and management, and staff have a responsibility to protect it.

COMMUNICATIONS SECURITY

GENERAL

Corporate Intelligence has over recent years, become critical to the overall protection of Corporate Assets, Property, Products, Personnel and ultimately Development. Corporate Intelligence is the acquisition of relevant information, the collation, analysis and ultimately the evaluation of such information, aimed at identifying and thus protecting the Corporate from vulnerability to threat. It can also be used as a tool against a company.

- The levels of Threat range from petty theft, Product Extortion and Fraud to Economic Espionage.
- Obviously, Communication Security is most essential in the avoidance of Corporate Espionage and thus an essential element of Corporate Intelligence.
- Corporate Intelligence implemented professionally and correctly has been found to be a most effective pro-active measure in countering the offensive activities aimed detrimentally against a Corporate and as such, must be considered essential in the overall security, policy and programme designed and implemented by that Corporate.
- The operations of a Corporate Intelligence Agency albeit “in-house” or “outsourced”, functions both offensively and defensively in achieving Security for the Corporate.

Ultimately, no security programme can be effectively implemented without adequate Intelligence (Information). Thus, it should be obvious to all concerned how necessary the need is for secure Communications within the Corporate.

COMMUNICATIONS SECURITY

INFORMATION GATHERING

The following are prime sources of information gathering:

PHYSICAL SOURCE

The human being, Management, Staff and often Associates - such sources transmit information either intentionally, frequently for personal gain or revenge, or unintentionally “careless talk”. Irrespective, every effort should be taken to employ “the Need to Know” practices.

NON-PHYSICAL SOURCE

- Communication Interception.
- Documents (Non-Oral).
- Data/Information Technology (Non-Oral).

THREAT:

Economic Espionage invariably incurs financial consequence. If successful, its high levels of sophistication, both nationally and internationally frequently incurs considerable consequences to not only corporate survival, but also Global and National economies. Regrettably, modern technological advances continually increase the sophistication of such espionage consequently requiring considerable advancement in Security Technology, Techniques and Training, Awareness and Implementation, thus an ever-greater need for the highest levels of Corporate Intelligence and Pro-active Security Responses.

RISK ANALYSIS:

Risk analysis is the application of techniques employed to identify risks and the potential effect of such risk to the Personnel and Organisation being protected.

THREAT ASSESSMENT:

Threat assessment is the determination of the imminence and level of such threat to either personnel or elements of the organisation. In the event of such threats, as detailed previously, a Corporate requires formulated policies and contingency plans to guide the protective response of the Corporate.

The overall protective strategy of the Corporate is a basic Security Policy Decision achieved by Standing Operational Procedures (SOPs) designed and implemented to attain maximum possible security for the Corporate, in any given environment, thus achieving the Secure by Policy. Such SOPs are implemented within the framework of the appropriate Corporate's policy.

In undertaking a Threat Assessment, it is accepted that the following are generally examined:

POTENTIAL CORPORATE TARGETS: "WHO?"

- Listed Companies
- Financial Institutions
- Legal Practices
- The Mining Industry
- The Pharmaceutical Industry
- Tender Boards/Committees

AIM: "WHY?"

- Intellectual Value
- Acquisitions and Merges
- Share Values
- Strategic Planning for Business or Competitive Information
- Conflict of Interest amongst Directors and Senior Management/Personnel
- Recruitment (Head hunting) of Specialist or highly knowledgeable Personnel

POTENTIAL AREAS OF VULNERABILITY: "WHERE?"

Internal

- Offices of Directors
- Offices of Executive Management
- Boardrooms
- Specialist staff workstations
- All Conference- and associated Facilities' locations
- Directors' and Executive Management's vehicles

External

- The Residences of Directors, Executive Management and identified Personnel employed on highly sensitive tasks.
- Specific Location Assignment.
- Selected Offices and Locations of persons closely associated with Contracts, Acquisitions, Legal and Financial Information/Activities, contracted to conduct business on behalf of the Corporate.

COMMUNICATIONS SECURITY

PROTECTION

INTERCEPTION TECHNIQUES: "HOW?"

The following technical and electronic instruments are most commonly used in the interception of verbal communication:

Microphones (Hardwire Eavesdropping):
The "Hardwire Bug" comprises of three elements, namely:

i. the Microphone,
ii. Wire and
iii. Line Drive Amplifier.

The Microphone is normally installed in a non-conspicuous place in the room and is supplied with power by the eavesdropper, via the same wire that carries the Microphone Audio to the eavesdropper. One does not always have to install a Microphone, as use can be made of items in the room, e.g. the Telephone Microphone, Intercom Systems, Television System and Radio Speakers can be adapted.

Radio Transmitters:
A Transmitter is one of the most versatile and flexible means of gathering information and comes in various shapes and sizes. The ideal type of Transmitter is one as small as possible, having a small signal (low watts), so that it is difficult to detect. Requiring the smallest of power sources and using the highest frequency possible, enables the use of a shorter antenna (i.e. VHF – UHF).

Carrier Current Device (Baby Sitter):
This Transmitter is connected into the electrical system of the target building. The Baby-Sitter can be installed anywhere along the electrical system of the target building but must be on the same phase. This makes it difficult to detect the eavesdropper. The Transmitter can be disguised in various things in the room without being detected, for example as a Plug Adapter. Once plugged into main sockets, the Transmitter will continuously transmit conversations using the power from the mains – to a receiver.

COMMUNICATIONS SECURITY

TELEPHONE ANALYSING

Many people are under the impression that it is only their telephone calls that can be monitored, not knowing that what they say after the telephone is "hung up", may also be overheard via the same Telephone Instrument. This is possible by using any one of the Microphones in the Telephone. Whatever ones needs, Telephone Transmitters provide the ability to discreetly and automatically transmit all telephone conversations. These are easily installed either on the Telephone Wire, in the Telephone Socket or within the Instrument itself. Telephone users will have absolutely no indication of their presence.

Characteristics of Analogue Lines:

- Information represented by constantly and smoothly varying voltage, current, amplitude, or frequency of waves and pulses.
- Do not switch suddenly between levels.
- The transmitter signal varies in relation to and is analogous (similar) to the original signal.
- With an Amplifier or a Telephone Instrument a person can listen to the audio on the line.

Characteristics of Digital Lines:

- In Audio, signals characterised by a sequence of unique pulses or digital numbers corresponding to a particular value of the Audio Signal at a specific moment of time, must be converted to Analogue to be intelligible to humans.
- With a voice logger installed, Digital Telephones can be tapped on a limited basis.
- The voice logger must be operated by one person with a security clearance. The room must be locked with a security lock and proper access control measures in place.

Telephone Threat:

- The Telephone Transmitter is in the Telephone or Online and uses Telephone Power.
- Audio Transmitter in Telephone or room, Self-Powered.
- Telephone Notification.
- Hidden Microphone in Telephone or Online in the Office.
- Room and Telephone Listening Device in Telephone or Online in the Office.
- Telephone Tap Online.

COMMUNICATIONS SECURITY

PROTECTION OF COMMUNICATION: COUNTER ELECTRONIC PROCEDURES

In conducting a Counter Measures Programme, the following services are implemented:

- A comprehensive Threat Assessment will be conducted for all designated target areas and thereafter a plan developed to best implement the TSCM. A customised approach is developed for each of our client's specific technical security situation and circumstances.
- A thorough physical search will be conducted in all designated target areas.
- A full Radio Frequency Spectrum Analysis will be performed to check for hidden Room Transmitters and Telephone connected Transmitters.
- Electrical Power Lines and other lines will be inspected with specialised equipment to locate Line "Carrier Current Device", "VLF Transmitters".
- A complete Electronic Analysis and Physical Inspection on all devices found within the target area will be conducted. The assessment will include but will not be limited to:
    - Telephones and Intercommunication Systems and Equipment;
    - Telephone Lines, including the testing for Active and Passive Devices;
    - VoIP technology testing; and
    - Identification of possible microphone modification and tampering (illicit phone system intrusions).

COMMUNICATIONS SECURITY

INVESTIGATIVE SEARCH FREQUENCY

In attempting to achieve maximum possible security provision, the TSCM Investigation should be conducted regularly, considering the following:

- Overall Facilities Sweep: Conducted monthly (to be discussed) via a Full Physical Sweep of all

Offices and Facilities as requested and to include Marking/De-marking of Wire Cables.

- Offices and Locations considered to be most vulnerable should be identified, *i.e., Directors' Offices, Executive Management Offices, Company Secretary's Office, Specialist Personnel Offices, Boardrooms, PA Offices etc.,* and these should be included in monthly TSCM investigations.

COMMUNICATIONS SECURITY

TSCM OPERATIONAL CONTROL

Due to the sensitivity, specialisation and security implications of these investigations' security, control and management should be delegated to "Crime Intelligence Security Personnel" only.

Operational implementation

TSCM can be implemented in two ways:

In-house:

Extensive in-depth research and investigation has determined that in-house implementation is considered not advisable due to:

- Constant improved technical development of Electronic Surveillance Equipment, thus increased sophistication of techniques employed by the perpetrators.
- Additional training of personnel to keep up to date with frequently upgraded or new equipment, together with regular continuation training required to achieve and maintain operational efficiency.
- The need to have existing equipment re-calibrated at least annually to maintain operational efficiency. Currently this can only be obtained by returning the equipment to the manufacturers. As yet, this service is not available in South Africa.
- When considering the financial implications of implementing the above, together with the considerable expenditure of purchasing specialist equipment and selection and training of personnel, it was found to be non-cost effective. Consequently, it is considered preferable to outsource this service.

Outsourcing:

It is recommended that when outsourcing for TSCM, the following should be implemented:

Obtain at least three (3) Tender Proposals from recognised Specialist Agencies in the field of Technical Surveillance Counter Measures. These tenders must be submitted on the basis of a detailed Brief compiled and issued by the Manager Crime Intelligence, and requiring:

- Full Company Background of the Submitting Agency.
- Details of Specialist Qualifications of the Agencies' personnel undertaking the Investigation.
- Details of the Specialist and Non-Specialist Equipment to be used in conducting the Sweep and Investigation.
- Areas, Locations and Equipment to be investigated.
- Frequency of Sweeps and Investigations.
- Full costing.
- An agreement by the Agency, that "should they be appointed to conduct the investigation, they agree to undergo Vetting and Clearance at their "Own Cost", as a condition of appointment".