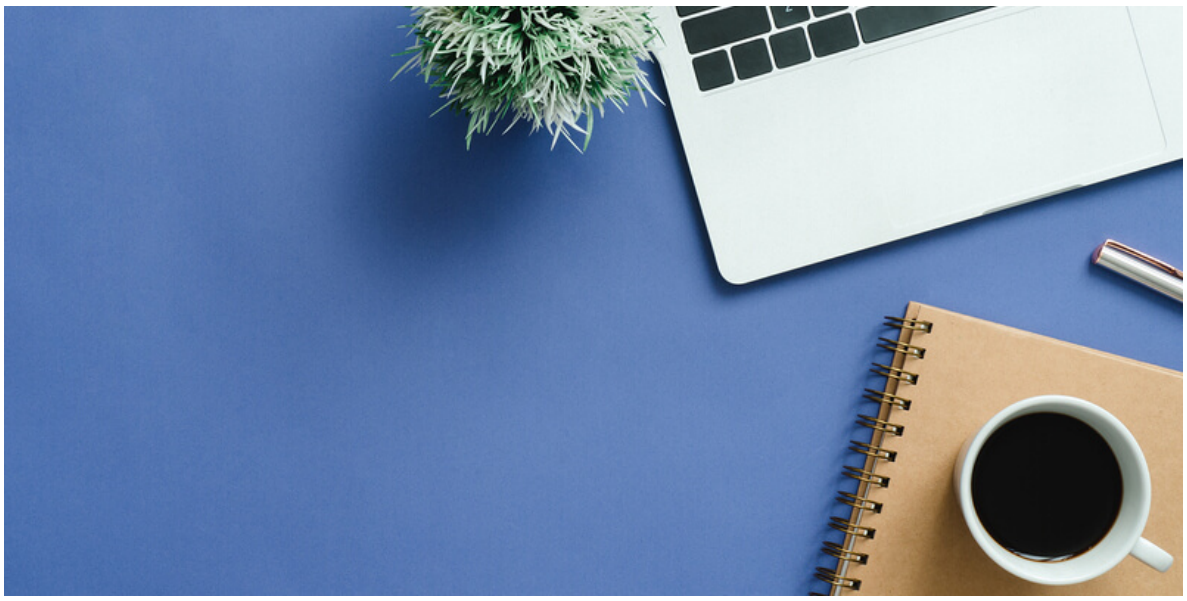
Proactive TSCM Solutions

（July 2023）

AWP
TECHNOLOGY

Brief introduction



With the rapid development of wireless communication technology and the popularization of cell phones, our privacy and information assets at work and in life are increasingly vulnerable to threats by various technical means. The traditional TSCM (Technical Surveillance Counter-Measures) generally involves routine inspection of critical working and living environments to sweep hidden cameras, bugs, etc. However, since routine inspections are conducted at certain intervals, and information security incidents usually result in huge losses, traditional TSCM solution can no longer meet the requirements of information security management in this fast changing world.

This whitepaper introduces an emerging TSCM solution, i.e. Proactive TSCM, which has the following advantages over traditional TSCM solutions:

1. Changes from reactive to proactive: from after-the-fact remediation to before-the-fact prevention and control, such as the use of electronic device detector gates to check for unauthorized electronic devices at entrances and exits, this product creates a safe working and living environment.
2. End-to-end all-round protection: from creating a safe working and living environment to proactively interfering with unauthorized electronic devices

in unsafe environments, features such as the speech protector does not allow cell phone recording during meetings to prevent information leakage.

Growing Technical Surveillance Threats

With the advancement of technology and society, we are facing more and more technical surveillance threats in our work and life. This is mainly manifested in the following aspects:

1. The miniaturization of technical surveillance devices is easier: with the maturity and popularity of the smartphone industry chain, the miniaturization of electronic devices is becoming easier and easier. This brings a very big challenge to the traditional TSCM industry, making it more and more difficult to find and detect those unauthorized electronic products, and the workload becomes bigger and bigger.
2. The social division of labor is becoming increasingly detailed, as many jobs are outsourced, environmental security is more and more difficult to be guaranteed: with the environmental greening, office equipment maintenance, cleaning and other work outsourcing, it is progressively more difficult to control external personnel to enter those environments that require information security protection.
3. Human rights and privacy awareness, making it more and more difficult to detect security threats: body searches and open bag inspections are becoming

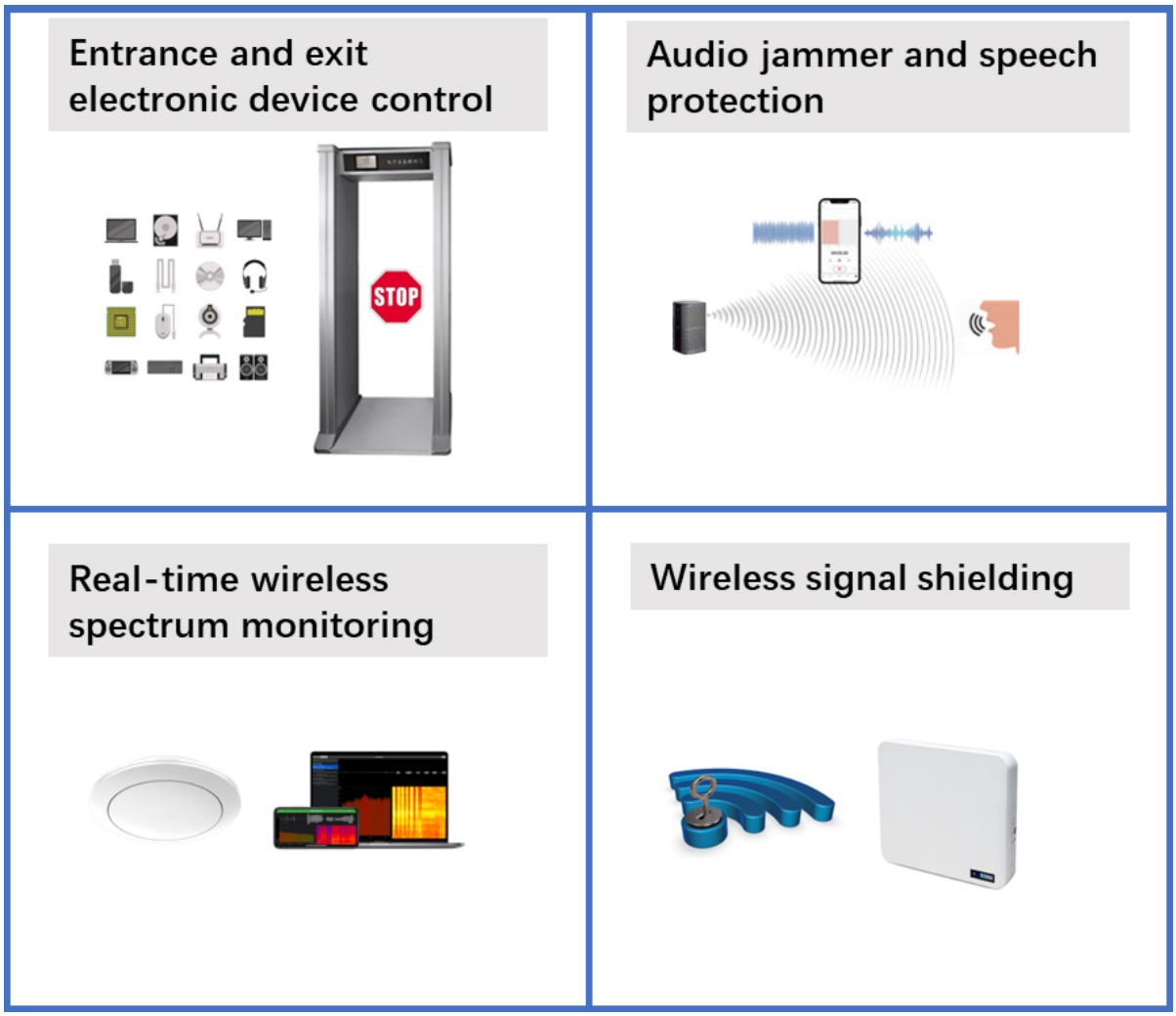
more and more uncivilized, or even illegal, and new humane technical means must be introduced to find and detect security threats.

In the face of increasing technical surveillance threats, traditional TSCM solutions have become increasingly unable to meet the requirements, which are mainly manifested in the following aspects:

1. Facing the threat of miniaturization of technical surveillance devices, the traditional TSCM work difficulty and workload has increased greatly: a reporter once visited a hotel in South Korea to find out 30 hidden cameras in a guest room. Nowadays, there are more and more electronic devices in the working and living places, and most of them are connected with wireless signals, so it becomes increasingly difficult to find out those illegal electronic devices hidden in everyday environments with traditional TSCM solutions.
2. Facing the threat of increasing number of outsourced personnel, traditional TSCM cannot meet the requirements of rapid responses: traditional TSCM service is usually on a regular basis, while the increase of outsourced personnel makes the probability of potential threats appear much higher and unpredictable. If the interval of TSCM service is shortened, or TSCM service is implemented quickly after each occurrence of outsourcing service, it will greatly increase the cost of protecting information security.
3. In the face of increased awareness of human rights and privacy and the difficulty of detection, traditional TSCM can do nothing: traditional TSCM services have detection equipment limitations, thus it cannot adapt to the dynamic changes in the environment. Therefore, the inspection of portable electronic products is not only inefficient, but also there is a very high ratio of missed inspection.

Proactive TSCM Solution

Faced with the growing threats to information security, and in response to the problems of traditional TSCM solutions, we propose the "Proactive TSCM Solution", which consists of the following four parts:



- **Entrance and exit electronic device control** is used to prevent unauthorized electronic devices from being brought into or taken out of the protected area, securing the protected area even in the event of a very high turnover of people.
- **Real-time wireless spectrum monitoring** is used to detect unauthorized wireless communication devices lurking in the environment, through real-time monitoring to achieve long-term and seamless protection.
- **Audio jammer and speech protection** is used to jam eavesdropping and recording devices to prevent them from functioning properly, which can be

used in high-level information security areas or for call protection in emergencies, improving the flexibility of information security protection.

- **Wireless signal shielding** is used to shield the communication of wireless communication devices, which can be used in high-level information security areas or emergency information security protection, and improves the flexibility of information security protection.

These four components complement each other to provide an end-to-end solution in facing increasing technical surveillance threats.

Entrance and exit electronic device control

Working principle:

Non-linear junction detectors have been used in the TSCM industry for many years and have proven to be an effective means of detecting electronic devices. An electronic device detector gate is a gate array of multiple non-linear junction detectors that performs high-speed scanning of people in the detected area to discover the electronic devices they are carrying, and displays the location where the electronic devices are located, thus realizing the control of the electronic devices at the entrances and exits.

Application Scenario:

Electronic device detector gate is placed at the entrance to area requiring information security protection to prevent personnel from bringing unauthorized electronic devices into or out of the protected area. This solution does not require close non-linear junction detector scanning of personnel, body searches and bag openings, and is very accurate and efficient. Its application scenarios include:

1. The entrance and exit control of information security protection area: to prevent hidden cameras, bugs and other technical surveillance devices from

being brought in and out of information security protection areas, it ensures the security of every moment of the protected area.

2. R & D companies: to prevent unauthorized electronic devices, such as USB flash drives, SD cards, cell phones, etc. from being brought in and out of the high-level R & D environment, in order to avoid the leakage of the core intellectual property, such as code, product design, etc.
3. IC companies, electronic product developers, etc.: In addition to preventing the leakage of core intellectual property, but also to prevent the loss of R & D samples.
4. Electronic equipment manufacturers: to prevent the theft of components and products.

Real-time wireless spectrum monitoring

Working principle:

Multiple real-time wireless spectrum monitoring terminals are arranged at locations requiring information security protection to collect wireless signals within the working range and aggregate the information to the Spectrum Analysis Center. The Spectrum Analysis Center analyzes the operating frequency bands, modulation and demodulation types, data formats, encryption modes, communication protocols, etc. of various signals, and analyzes the changes of these signals in the time and spatial domains through artificial intelligence to determine whether security threats exist in the environment.

Application Scenario：

Deploying real-time wireless spectrum monitoring equipment in places that need to be protected makes it easy to detect wireless communication terminals that have been deliberately left behind in the environment, such as hidden cameras and bugs. Long-term monitoring also makes it possible to discover wireless communication terminals that are lurking in the environment but are constantly waking up. Its application scenarios include:

1. Information security protection area: prevents unauthorized wireless communication devices such as hidden cameras and bugs from being brought into the area that needs information security protection by the personnel, and ensure the security of the protected area at all times.
2. Hotels: prevents residents from installing hidden cameras in guest rooms.
3. Public places: prevents visitors from installing eavesdropping devices or hidden cameras in places that require privacy protection, such as public restrooms.

Audio jammer and speech protection

Working principle:

The audio jammer uses ultrasonic mixing technology to emit ultrasonic signals that cannot be perceived by the human ear, but can be picked up by the microphone in cell phones and voice recorders. The ultrasonic have strong directionality and large sound pressure level, which can cover the normal speaking voice, making the audio picked up by the microphone just meaningless noise, thus avoiding verbal information leakage.

Application Scenario：

You can apply the audio jammer in any scenario where you need to protect the conversation, or you can choose the right audio jammer according to different application scenarios to achieve the best jamming effect. Its application scenes include:

1. High-level confidential conference rooms: audio jammer can be installed on the conference table and under the table to form a full coverage of jamming signals to interfere with the possible existence of eavesdropping devices in the conference room.
2. Centralized management of cell phones during meetings: Uniformly placing cell phones centrally outside the conference room makes it difficult for participants to accept the possibility of missing important calls. You can arrange audio jammer in the conference room, and then uniformly place cell

phones in it, which not only protects the confidentiality of the meeting but also avoids the possibility of missing important calls, which is more acceptable to the participants.

3. Prevent apps or viruses in the cell phone from eavesdropping on the conversation: there may be malicious apps or viruses in the smart phone, in order to prevent them from eavesdropping on the conversation, it is necessary to jam the microphone of the cell phone during the important conversation.
4. To protect the temporary initiation of the conversation: some important conversations cannot be carried out in a confidential conference room, this time there is a need for a portable, but also more covert audio jammer to protect the temporary initiation of important conversations.

Wireless Signal Shielding

Working principle:

Wireless signal shielding equipment shield wireless communication signals within its operating range in order to disable the communication capability of wireless communication terminals within its coverage area.

Application Scenario：

Installing wireless signal shielding equipment in the desired environment can interrupt the communication of malicious electronic devices in the environment to protect privacy and information security. Its application scenarios include:

1. High-level confidential conference room: wireless signal shielding equipment can be installed in the conference room to shield possible hidden camera or eavesdropping devices in the conference room, interrupting their communication.
2. Prevent apps or viruses in the cell phone from eavesdropping on the conversation: there may be malicious apps or viruses in the smart phone; in order to prevent them from eavesdropping on the conversation, you can turn on the wireless signal shielding equipment to interrupt the communication of the cell phone in the important conversation.

3. To protect the temporary initiation of the conversation: some important conversations cannot be carried out in a confidential conference room, this time you need a portable wireless signal shielding equipment to protect the temporary initiation of important conversations.
4. Dangerous goods storage areas: for those areas where cell phone communications easily cause explosions, such as gas stations, etc., wireless signal shielding equipment can be used to prevent cell phone communications.

Combined use of multiple technical means

Working principle:

For cases with high information security protection requirements or complex usage scenarios, the four proactive TSCM solutions mentioned above can be used in a comprehensive manner, including entrance and exit electronic device control, real-time wireless spectrum monitoring, audio jammer and speech protection, and wireless signal shielding.

In order to facilitate unified deployment and management, the equipment in above four types of solutions can be uniformly connected to a "Security Risk Assessment and Management Center" for unified management and data collection of these equipment, so as to carry out unified assessment of security risks in the management area, provide early warning and take timely action.

Application Scenario：

A variety of technical means are used jointly to cope with complex or high information security requirements of the scene, such as:

1. High-level confidential conference room: a variety of technical means to cooperate with each other to form a full range of protection

1) Place the electronic device detector gate at the entrance of the conference room to prevent unauthorized electronic equipment from entering the conference room.
2) Installation of audio jammer on and under the conference table to interfere with the possible existence of eavesdropping devices in the conference room.
3) Installation of wireless signal shielding devices in the conference room to block the possible hidden camera or eavesdropping devices in the conference room to interrupt their communications.

2. Complex information security protection scenarios: different technical means are applied in different areas with different requirements, with flexible deployment and low cost.
   1) High-level confidential area: multiple technical means are used jointly.
   2) Areas with high information security requirements such as R&D department: electronic device detector gate.
   3) Other areas with lower information security requirements: real-time wireless spectrum monitoring.

Summary

The development of wireless communication technology and portable electronic devices has brought a lot of convenience to our work and life, but it also brings great threats to privacy and information security protection. Traditional TSCM solutions can no longer meet this fast-changing and increasingly complex environment, turning passive into active and adopting proactive TSCM solutions is the only way to protect our core information assets and make our communication more secure.

www.tekforbiz.com

Official AWP distributor