CETC 中国电科

Company Overview

2024

CONTENTS

I

Overview

Profile of Privis

Privis Technology Co., Ltd (hereafter referred to as Privis), founded in 2002, is a subsidiary company of China Electronics Technology Cyber Security Co., Ltd (CCSC for short). Privis specializes in provision of comprehensive security solutions and delivery of turnkey projects to foreign customers, and cross-border technical cooperation. Its operation domains focus on security industries to satisfy the urgent needs of global customers.

- Internationally renowned supplier of **cryptography systems**
- Worldwide forerunner in the booming **cybersecurity industry**
- Trustworthy cooperator in the field of **counter-terrorism & public safety**
- Creative provider of **dedicated communications systems**

Brief of CCSC

CCSC was established by Chinese government with the approval of the State Council. As a national strategic scientific and technological force for cybersecurity, it is the only cybersecurity enterprise in China covering the two major domains of cryptography and cyber defense.

No.30th Institute of CETC
Cryptography
Army, Party and Government

China Cyber Security Company
Cryptography
Cybersecurity
Public Security
Communication

Privis Technology
International Business
Professional Company

Cryptography Trailblazer

* Chief design unit of cryptosystems of the PLA
* Top common cipher equipment supplier for the Party and government

Main Force of Cyber Defense

* Construction of nearly all common information systems, overall security solution, and major network security protection systems for the whole army.

Talents and Programs

* Academician / 1
* Chief Scientist / 2
* Chief Expert / 8
* Group Top Young Talents / 2
* National Doctoral Research Station / 3
* Doctor Degree Program/ 1
* Master Degree Program / 2

Honorary Award

* Authorized Patent / 1897
* Computer Software Copyright / 884
* Patent for Invention/ 660
* Trademark / 17
* National Scientific and Technological Progress Awards / 24
* Provincial (ministry) Level Scientific and Technological Progress Awards / 271

Milestones

21st Century

- The world's fastest quantum random number generator

- 1st 5G NB-IoT communication security module based on an independent security chip

- 1st secure government affair mobile phone
- Deep dark web information retrieval platform
- "Credit Chain" and "Trust Chain" won the National Blockchain Development Contest Awards

- 1st 10G optical encryptor
- 1st domestic 10G network encryptor

- New generation strategic network
- New generation tactic network
- 1st cloud-mode security protection system for army

- 1st cybersecurity system for telecommunications and radio network
- VPDN active detection and control platform of Public Security Department
- Electromagnetic protection of AF

1980-2000

- 1st high speed algorithm and series of chips
- 1st network based automatic KMS

- 1st domestic programmable digital switch
- 1st set of packet switch data network
- 1st set of wireless packet data network

1950-1980

- Encrypted telephone communication system for summit hot-line

- 1st analog radio encryption system
- 1st digital trunk line encryptor

- 1st digital HF strategic encrypted communication system

- 1st magnetic floppy for army

Overseas Presence

1.Southeast Asia	3.Central Asia	5.North Africa	7. Africa-Portuguese Area	9. Africa-Spanish Area	11.Europe
2.South Asia	4.Middle East	6.Africa-French Area	8. Africa-English Area	10.Central and South America	

International Business Domains

With more than 20 years of internationalized operation, Privis has accumulated rich experiences in mining customers' demands and providing matured solutions. Relying on the abundant resources and completed supply chain in the security field in China, Privis endeavors in the technical R&D and global marketing in four domains, i.e., cryptography, cybersecurity, public security and dedicated communication.

Cryptography

Cybersecurity

Public Security

Dedicated Communication

II

Products and Systems

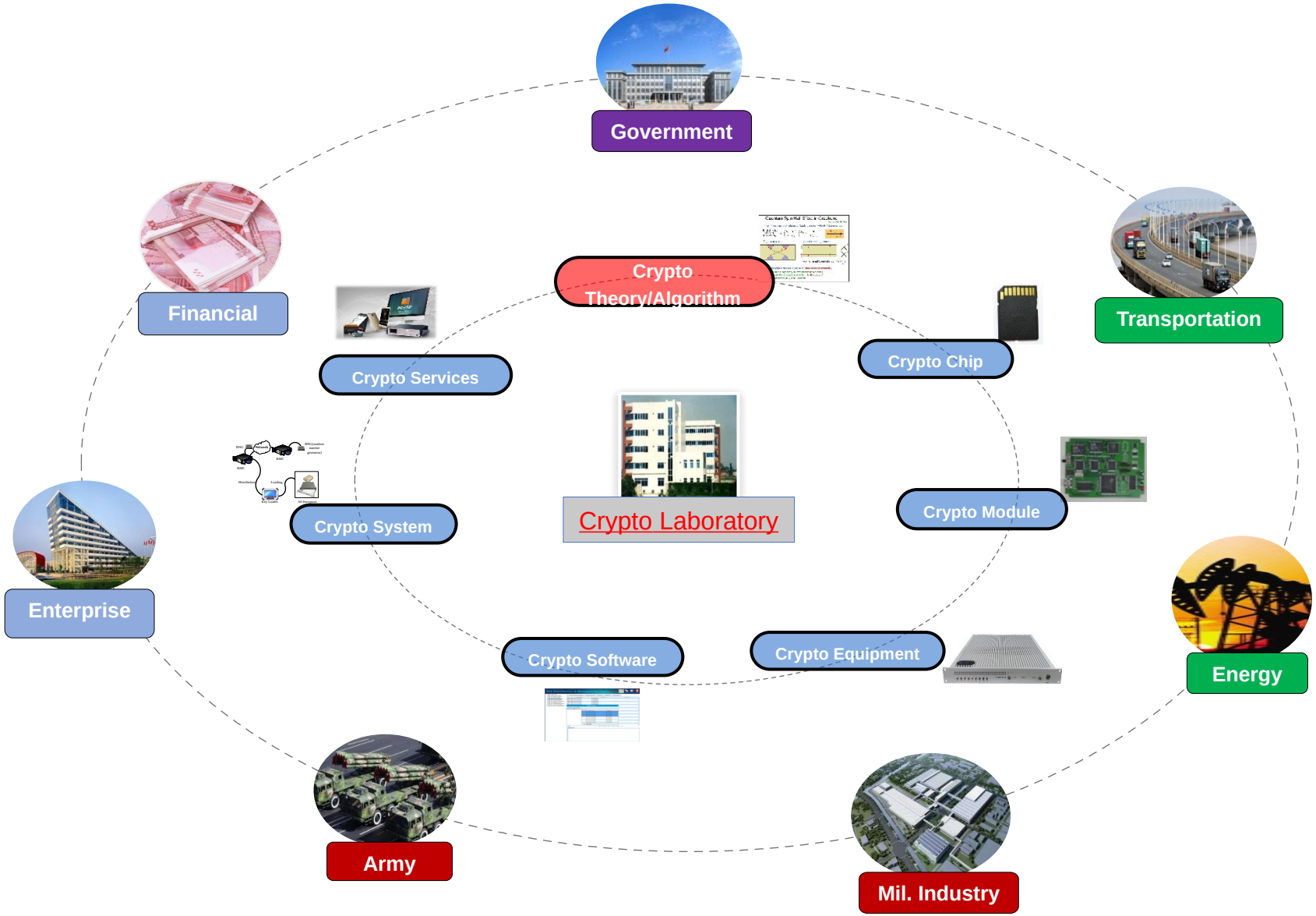
1 Cryptography

- **No.1 brand** in cryptosecurity industry in China
- Extensive overseas experience

- Full range of information security products
- Around-the-clock technical support
- Professional technical training

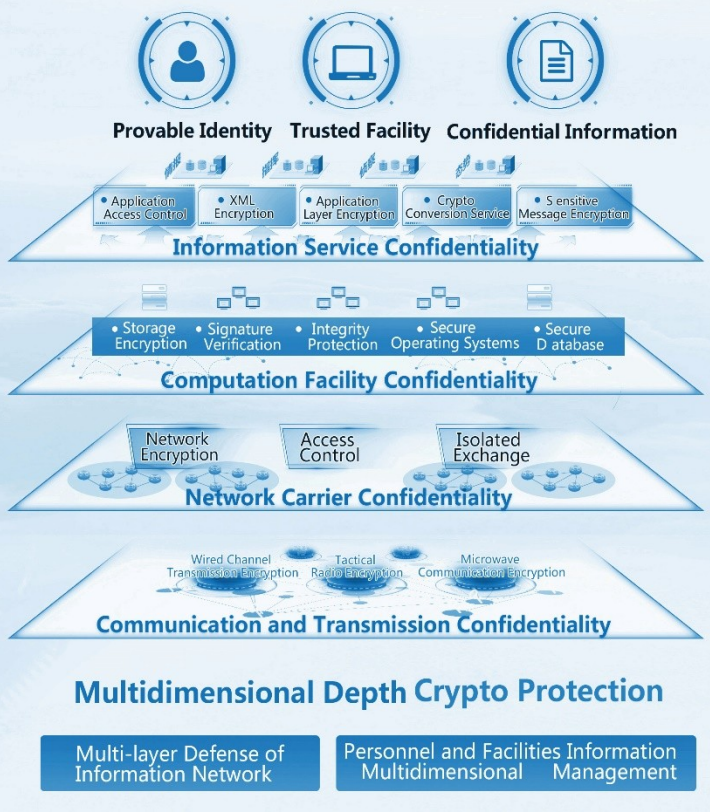
Brief of Cryptography Capability

- ✓ **State Key Laboratory:** China's only key laboratory of secure communication;
- ✓ **Product Chain:** capabilities covering theory, algorithms, chips, modules, boards, software, encryptors, systems and services, with more than 200 products;
- ✓ **Industry Coverage:** in-depth application in various industries such as finance, energy, transportation, government and military, providing all-round cryptographic protection services for the digital society.

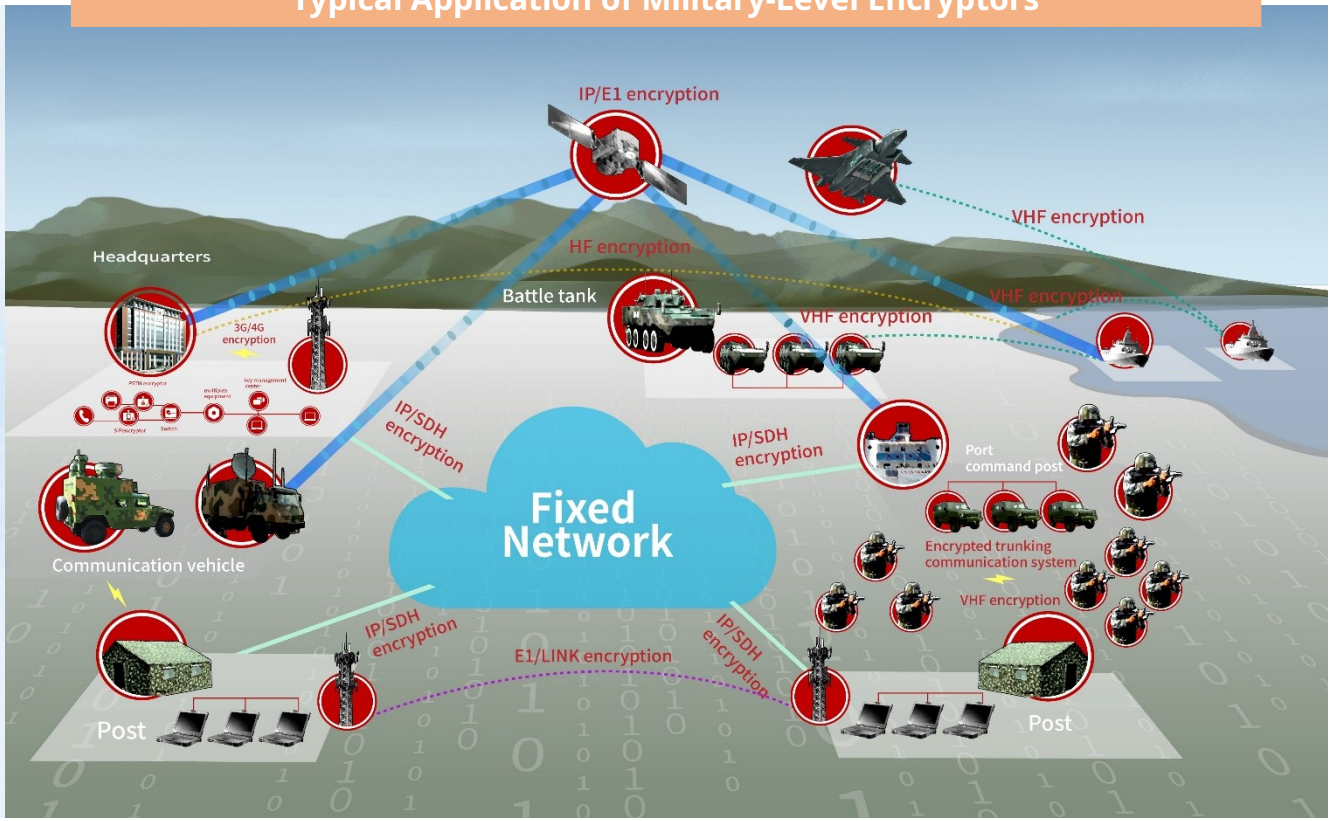


Cryptographic Mechanisms and Products

- Full range of Encryptor series
- Professional key management system
- Military-level product quality
- Compatible with various communication platforms
- High-strength digital encryption
- Plenty of practical applications



Typical Application of Military-Level Encryptors



Terminal Encryption


Secure Walkie-talkie


PSTN Encryptor

Channel Encryption


IP Encryptor


Link Encryptor


V/UHF Encryptor

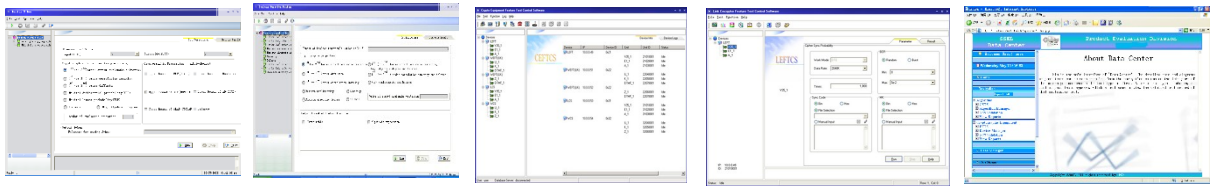

HF Encryptor

Key Management


Key Generator


Mgt. Terminal

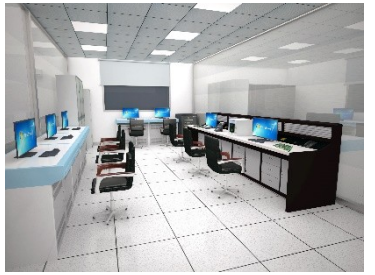
Relying on the only State-level Key Laboratory in cryptographic field in China, the laboratory is to nurture a professional team of cryptography for the customer, empower trainees with the ability of algorithm design & Implementation and cryptographic equipment test & evaluation, and finally, lay a foundation for the future development of cryptographic industry in customer's country.



Dedicated Software

Dedicated Hardware

- **ADIL Lab**: How to design and implement cryptographic algorithms
- **SSEL Lab**: How to evaluate security strength of encryption algorithms/devices
- **ToT Training:** Provide abundant training to transfer the complete crypto capabilities



2 Cybersecurity

- **The technology leader** in the cyber security field in China
- An active cyberspace trailblazer delivering up-to-date solutions to global customers

Cyber Security Solutions

Cybersecurity Governance

- Security Operation Center (SOC) Solution
- National Firewall Solution
- Social Media Monitoring and Management Solution

Cyber Protection

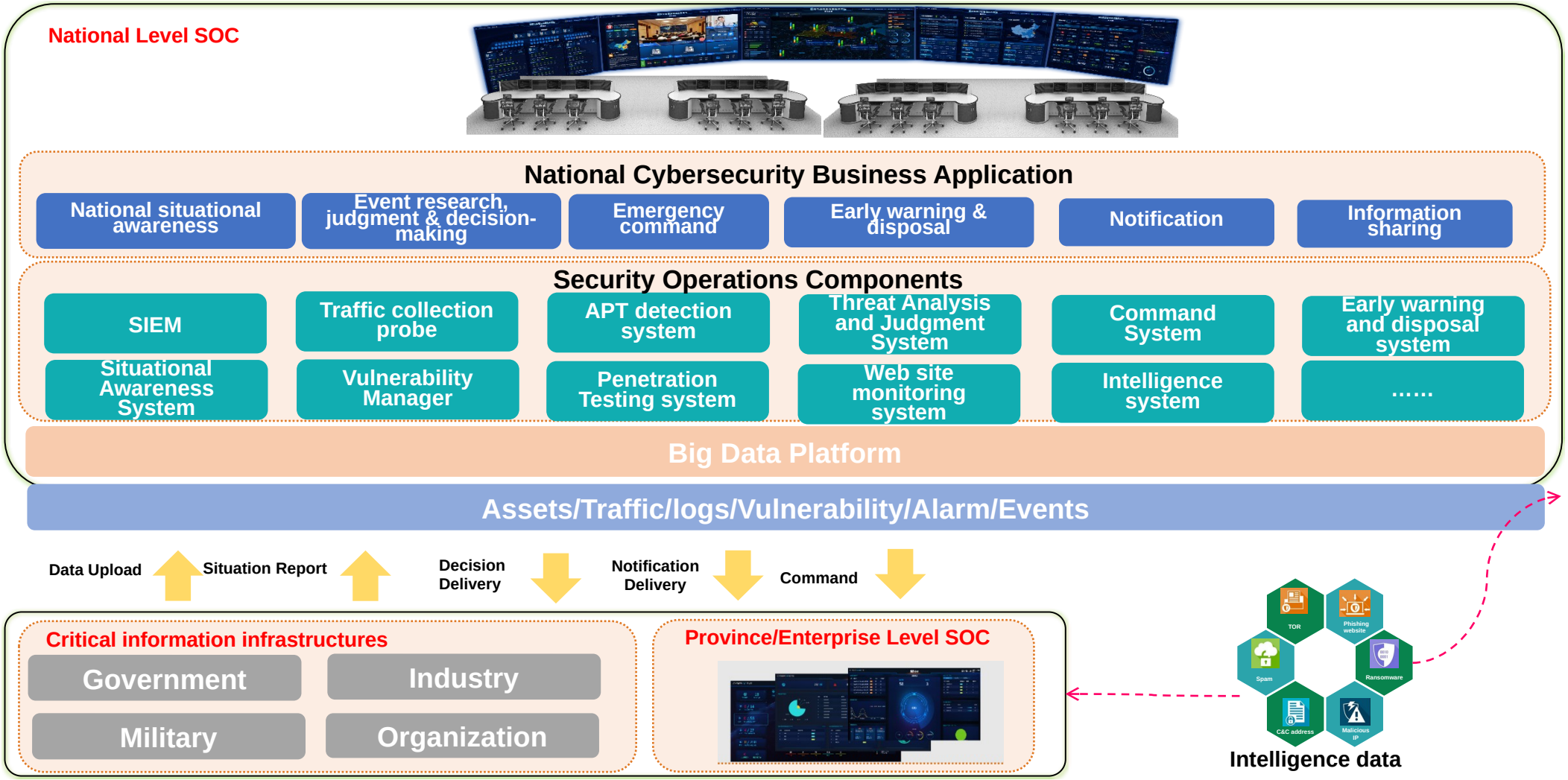
- Military Information System Network Security Protection
- Cybersecurity Protection Product Series

Talent Training and Competence Output

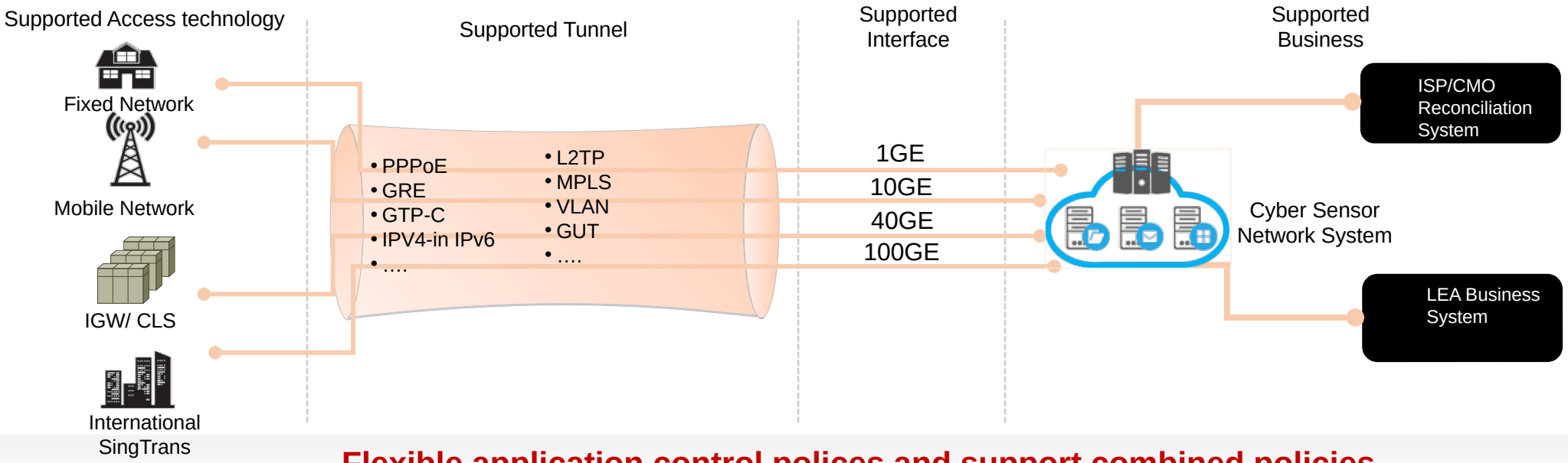
- Cyber Range Platform
- Cybersecurity Training

Security Operation Center (SOC) Solution

SOC system is the technical focus for national cyberspace administration, it is capable to strategically coordinate all the organizations and powers to realize nationwide cybersecurity awareness and pre-warning, situation-based decision and emergency command. It is also a strategic decision-making and command coordination engineering to ensure the security of national critical information infrastructures.



National Firewall Solution



Flexible application control polices and support combined policies

Five-tuples based	Mobile info based	APP based	For HTTP website	For HTTPs applications	For VPN	Action
Source IP address Destination IP address Port IP + Port IP + Port + Time IP Segment	IMSI/IMEI/ MSISDN IP CELL (Location) IP + Mobile APPs	Facebook Twitter YouTube WhatsApp Viber WeChat Other OTTs	URL Domain names Keyword in URL string Keyword in contents	Domain names Server IP SNI	IPsec/ PPTP/L2TP TOR	Monitoring Block Redirect QoS Throttling

Social Media Monitoring and Management Solution

Social Media Monitoring Solution

- Key Account Monitoring
- Hot Topic detection
- Early Warning
- Key Subject Monitoring
- Comprehensive Search
- Relationship Analysis
- Report

Action

Social Media Management Solution

Reputation shaping

Public opinion Guidance

Solution Features

- Account Generation
- Account Management
- Account Cultivation
- Task Push
- Directional Information Release

Data Processing

Big Data

AI

Social Media Crawling

Social Media

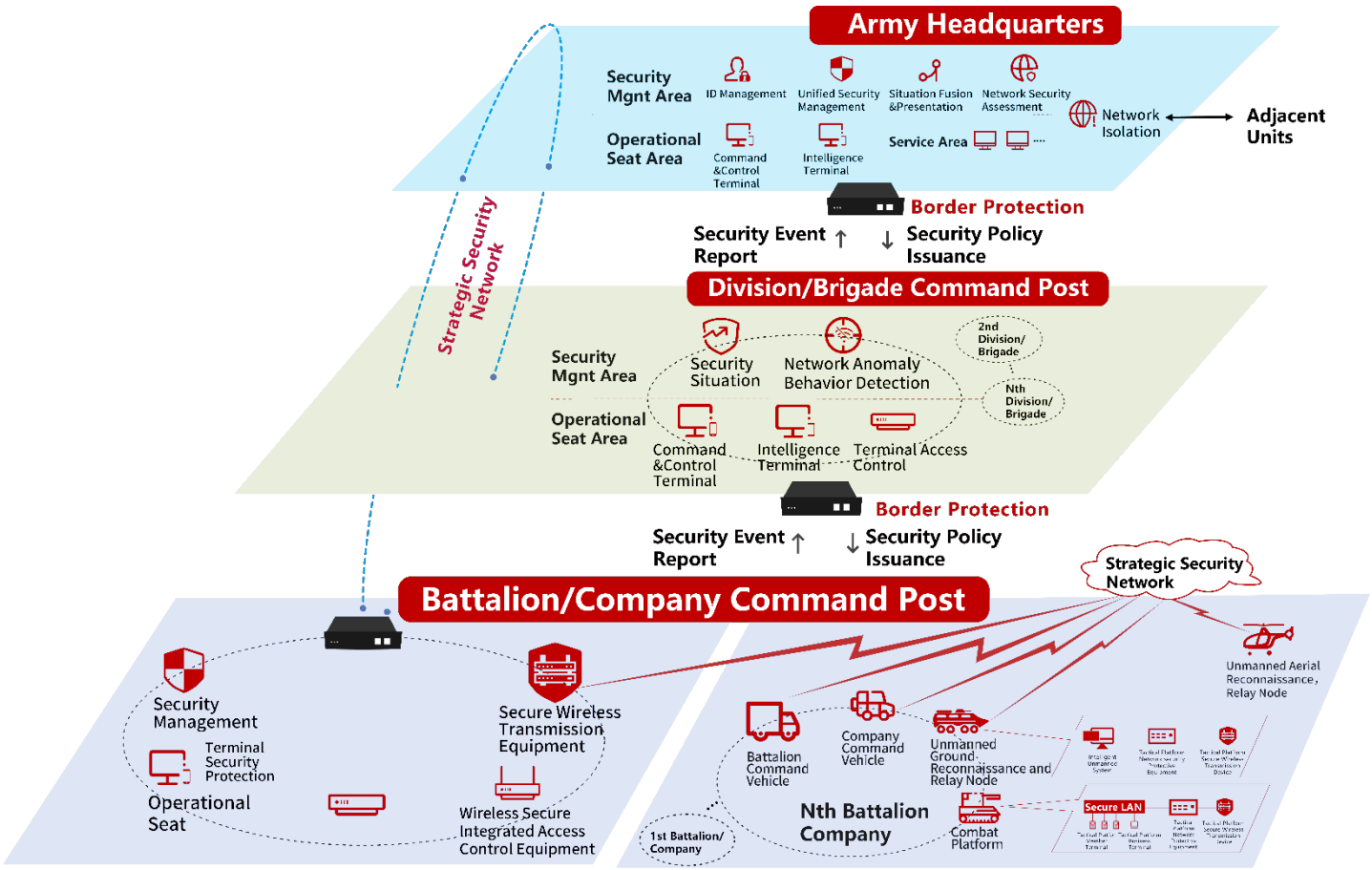
YouTube

TikTok

Military Information System Network Security Protection

According to the security protection requirements of the military information system (MIS), it adopts abundant security mechanisms to ensure the network security of the fixed and the mobile military units at all levels. Meanwhile, for the wireless environment of the battlefield, through comprehensive security measures, it provides network security protection for the tactical platforms.

- Adopt top-level design concept, perform systematic research and development of equipment, and build a defense-in-depth security protection system.
- Taking channels, networks and terminals as protection objects, it realizes comprehensive security management in all dimensions.
- It can be tailored to meet the requirements of systematic/flat deployment of the security protection systems from headquarters to combat vehicles.
- The security protection process is organically integrated into information processing, and the security capability is embedded in the information system.



Cybersecurity Protection Product Series

- **Cybersecurity Protection Products proactively safeguards data, systems, and applications by preventing all kinds of attacks from happening with our amount of cyber protection experiences and best practice. Relying on our customized solution, network breaches will be curbed and cyber assets will be assured as your network requirements.**

Website Cloud Protection Platform

Anti-DDoS System

NGFW

Distributed WAF

Intrusion Detection System

Terminal Protection System

Network Access Control (NAC)

Email Protection System

Cyber Range Platform

Based on the virtualization technology, the cyber range is a platform that simulates and derives the network architecture, system devices, operating environment and operation state of business process in the real cyberspace. The platform can support the training of security talents, confrontation drills, and test and assessment of network devices for overseas customers.

Training

Defense Training

- Emergency response
- System reinforcement
- Forensic analysis
- Tracking and tracing

Confrontation Training

- Vulnerability mining
- System intrusion
- Brute force practice
- Privilege escalation

Device Evaluation

Security Audit

- System restoration
- Risk assessment
- Vulnerability verification
- Audit report

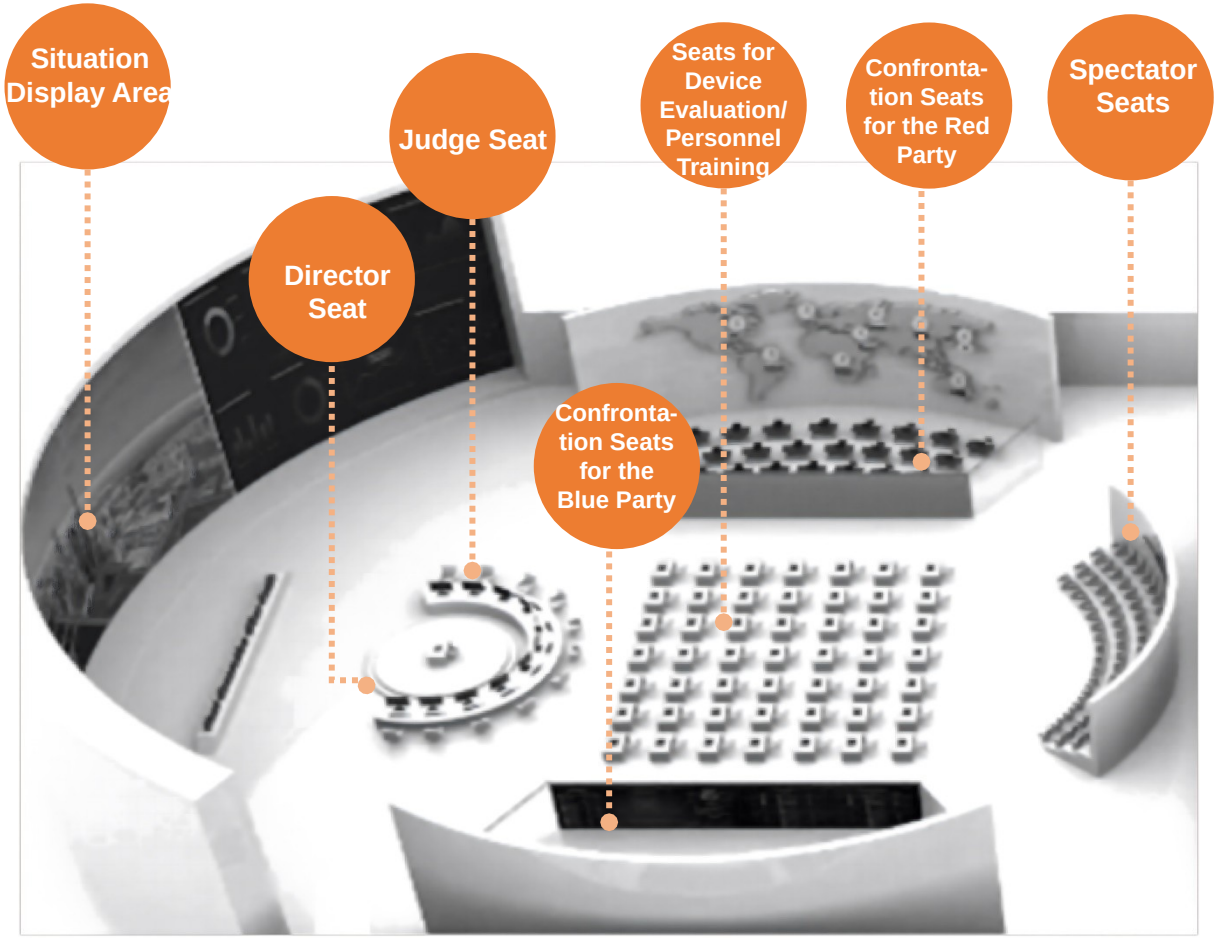
Performance Tests

- Kill-immunity test
- Covert test
- Pressure test
- Contrastive test

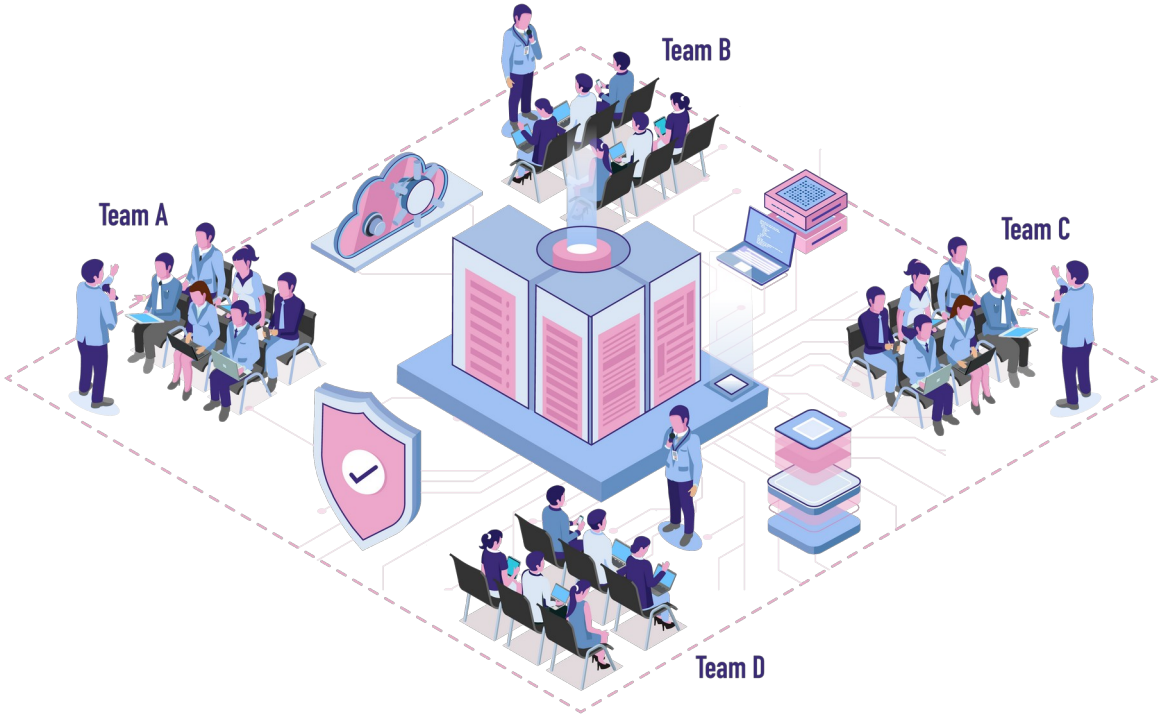
Confrontation Drill

Confrontation Drill

- Leadership and command
- Strategy execution
- Practical training
- Tactical deduction



Cybersecurity Training



Phase 3: Joint Development & Technology Transfer Training
Duration: 360 days
Content: Crypto algorithm design (210 days), cipher strength evaluation (90 days) network attack and defense tool development (60 days)

Phase 2: Advanced Training
Duration: 95 days
Content: Mobile security-iOS (25 days), Wireless Security (23 days), IoT Security (9 days), Cloud Security (38 days)

Phase 1: Comprehensive Basic Training
Duration: 191 days
Content: Reverse analysis (7 days), Binary vulnerability (30 days), Malware analysis (45 days), Pentest-Red Team (42 days), Incident Response-Blue Team (10 days), Mobile security-Android (41 days), ICS Security (16 days)

3 Public Security

- **Leading** role in public security industry of China
- Extensive relevant experience domestic and oversea
- State-of-the-art technology & products
- Complete solution to various scenarios

What Do We Focus On

01

Tactical Intelligence & Reconnaissance

Complete product series which cover wireless interception, long-range monitoring and intelligence analysis. Based on cutting-edge technology, rich experience in this field and customer-centered service, we already offered the best solution to our user all over the world.

02

Wireless Signal Control & Management

Based on latest technologies, wireless signal control & management is to help our user to establish comprehensive mechanism to manage and control surrounding wireless signal, including jamming, direction-finding, etc.

03

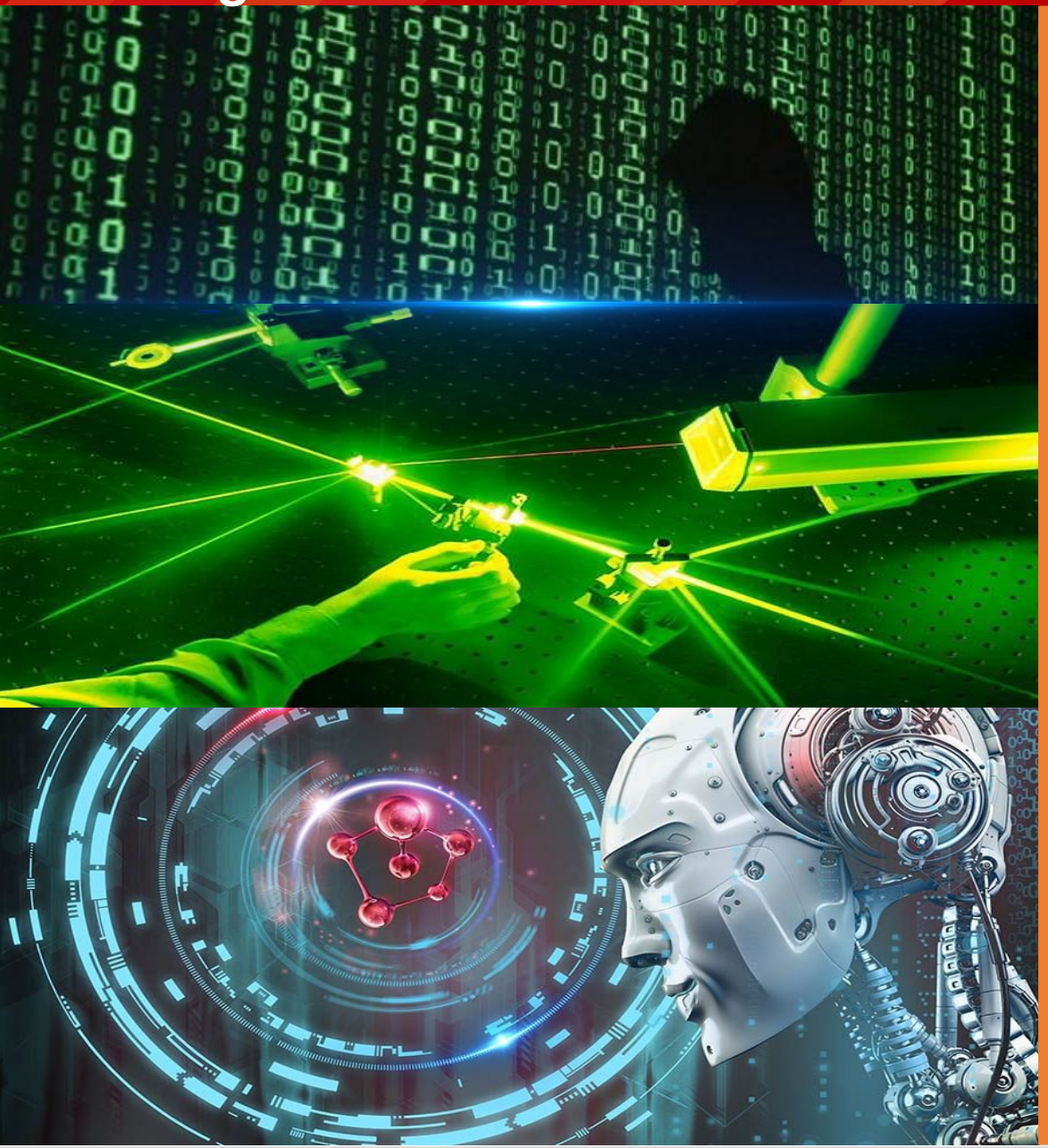
Information Leakproof

Besides network attack, there is many other ways to steal sensitive information from our system, including electromagnetic signal interception, laser monitoring, voice recovery device, etc. It is used to prevent EM leakage from critical infrastructure.

04

Digital Forensic

World-wide leading integrated solutions provider of digital forensic software, hardware, training, case assistance, consulting, and authentication services which fully covers computer/mobile/video forensics, forensic data recovery, and lab.



01

Intelligence &
Reconnaissance

Strategic Interception System

LI (Lawful Interception)

As typical strategic interception system for telecom monitoring, LI can make surveillance on specific targets (telecom subscribers) or all subscribers of telecom companies. It can be classified as Active LI and Passive LI.

To deploy and run a LI system, deep cooperation with local telecom companies is necessary. Sometime it will be a big problem for our customers.

Tactical Interception System

The significant benefit of tactical interception system is that it can work without coordination of the local telecom companies.

Tactical interception system can be divided into active system and passive system. The active system transmits telecom signal while the passive system doesn't.

Unlike LI that is a comprehensive system which consists of various components or subsystem, the tactical interception system is much simpler, and it can be a fixed equipment or a vehicular system which can work independently.

LI

Lawful Interception Gateway (LIG)

LIG is referring to the **mediation system** between multi telecom operators' network and multi Lawful Interception Center (LIC) in LEA.

Telecom Monitoring Center (TMC)

A set of monitoring system assists LEA to intercept targets of communication networks based on the national laws. Assist to monitor **target Voice, Location and SMS**.

Active Approach

Big Data Analysis Platform

The **Big Data** Analysis platform can fuse multi-dimensional communication data and provide **various intelligent application services** based on the ML and AI engines, including tracking, behavior and other analysis.

Massive Signaling Interception System (MSIS)

A collection,decoding and analysis system based on massive signals data of mobile operators. Assist to monitor **massive CDR, SMS and Location.**

Massive Voice Interception System (MVIS)

Collection and retrieving massive voice data from mobile operators passively. Assist to monitor massive and target **Voice content.**

Passive Approach

Product Series

Active System

IMSI Catcher

Collect IMSI and other wireless communication information of mobile terminals under the coverage. It can automatically transmit all kinds of collected information to the digital analysis platform for correlation and comprehensive analysis of data.

Vehicular active locator

Active locator

Based on fake BTS principle, the system can help user to rapidly locate target position via signal measuring continuously under different network scenarios. It also can be used for communication control.

Manpack active locator

Active Interception & Locating System

Active Interception & Locating System is widely used in IMSI catching, interception and positioning of various reconnaissance scenes. System can collect the IMSI, IMEI (2G) and other identity information of all cellphones in the signal coverage, and use the catching information to realize the functions of target recognition, target online alarm, forged call, forged SMS, communication blocking and target positioning etc. Through internal network redirection technology, the system can also intercept the voice and SMS of the target cellphone in GSM network.

Passive System

Passive GSM Interception System with A53 Solution

Enhanced version of Passive GSM Interception System. It is latest version with most advanced technology over the world. With special A53 controller, the system can realize surrounding massive GSM channel interception even if A53 algorithm has been deployed.

Vehicular passive locator

Manpack passive locator

Drone-borne passive locator

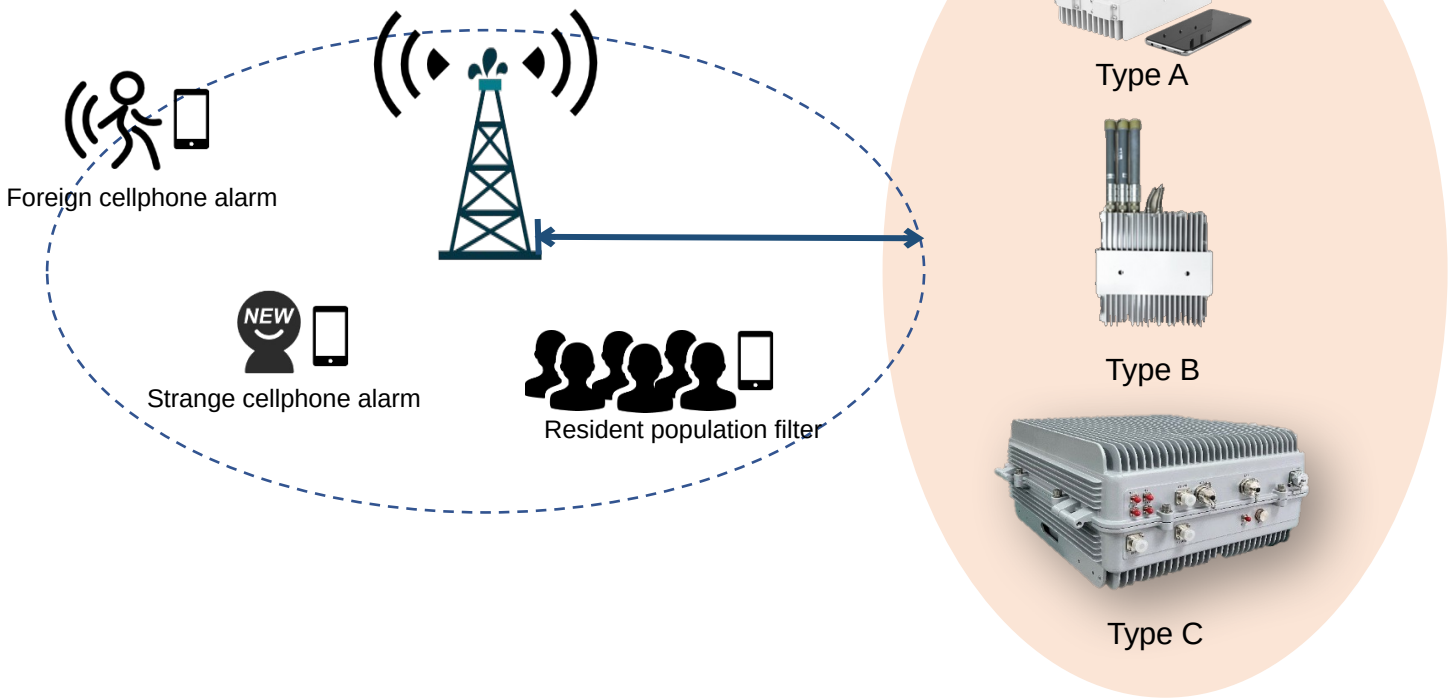
Passive Locator

Based on passive principle, the system support long range DF function and realize precise locating without affecting target operation.

Voice collecting

Laser surveillance system

Highly Sensitivity Optical Fiber Forensics System (Wall Mounted)



IMSI CATCHER

Highlights

- Various model for different scenarios
- Support one-button scanning configuration
- Support the full coverage of 2/3/4/5G NSA
- Support outdoor unattended work
- Support foreign cellphone alarm
- Support strange cellphone entry alarm
- Support automatic reporting of alarms to the background system
- Support remote maintenance, remote version upgrade, and remote alarm processing
- Support 3G/4G wireless and wired data transmission

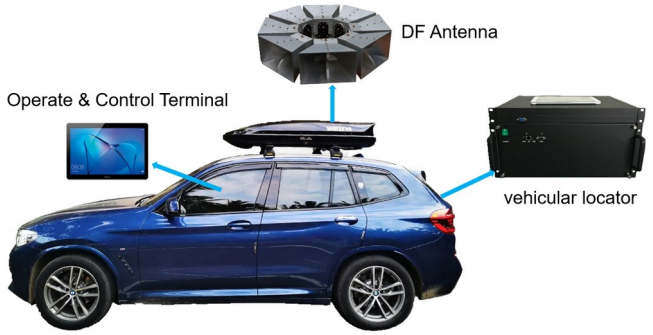
As first and useful tactical interception system in our product series, IMSI Catcher can be deployed on specific position to collect IMSI and other wireless communication information of mobile terminals under the coverage. It can automatically transmit all kinds of collected information to the digital analysis platform for correlation and comprehensive analysis of data. The system can realize resident population analysis, strange cellphone identification, blacklist/whitelist management, overseas cellphone incoming alarm and other functions, which greatly improves the efficiency of regional management.

Direction Finding & Locating

Vehicular Active Locator

Manpack Active Locator

- Active locator is consisted of full standard integrated equipment based on active mode.
- Support IMSI catching and communication control
- When working, system will actively collect 4G/5G cellphone information within the range of operation, and once the target information is collected, it will be absorbed to measure the uplink energy of the target, and then find the target to achieve active positioning.



Vehicular Passive Locator

Manpack Passive Locator

- Passive locator adopts software-defined radio technology to realize accurate direction finding and locating of target cellphone. The system is highly integrated, and the whole process of locating is efficient, accurate, covert, and non-perceptible to the target (target phone will NOT be affected during the whole locating process).
- Passive mode to support covert operation and silent mission, no radiation, non-perceptible to targets.

Active Interception & Locating System

Vehicular active interception system is a vehicular solution that focus on voice & SMS interception and Locating for target cellphone under LTE/WCDMA/GSM network. This solution adopts the vehicle-mounted form and active working mode. When the target cellphone is captured and registered to the system successfully, the system can be used to play role as Man-in-Middle and intercept communication content, call and SMS, of specified target. In addition, with accessorial individual positioning device, the precise positioning of the target can be implemented.

Functions & Features

- Support simultaneous operation under LTE/WCDMA/GSM telecom carrier network.
- Support working under the network with A5/0, A5/1, A5/2, A5/3.
- Real time verification and KC evaluation for selected targets.
- Records voice sessions, SMS messages and call related information of selected targets.
- Quickly detects cellphones location within the working area.
- Supports the Successive Approximation Positioning (SAP).
- Selective block for registered cellphones.
- IMSI/IMEI identities capture and collection.
- Support target's MSISDN acquisition.

Items	Description
Support Network	LTE-TDD/LTE-FDD/WCDMA/GSM
Support Frequency Band	LTE-FDD:B1/B2/B3/B5/B7/B8 LTE-TDD:B34/B38/B39/B40/B41 WCDMA:B1(2100M) GSM:900M/1800M
Concurrent Band Carrier Number	Standard model: 8 carriers (Can be updated to 13 carriers)
Working Mode	Active
Number of Concurrent Interceptions	≤4 (Voice & SMS interception)
Receiving Sensitivity	GSM:-110dbm/LTE:-100dbm/WCDMA -118dbm Normally coverage up to 1000m
Transmitting Power	LTE: Single carrier 0~20w adjustable; WCDMA: single carrier 0~20w adjustable GSM: single carrier 0~20w adjustable
Peak IMSI Catching Rate	LTE: ≥1,000 /carrier/per minute GSM: ≥800 /carrier/per minute WCDMA: ≥800 /carrier/per minute

HYBRID DECRYPTION STRATEGY AGAINST A5/1, A5/2, A5/3 NETWORK

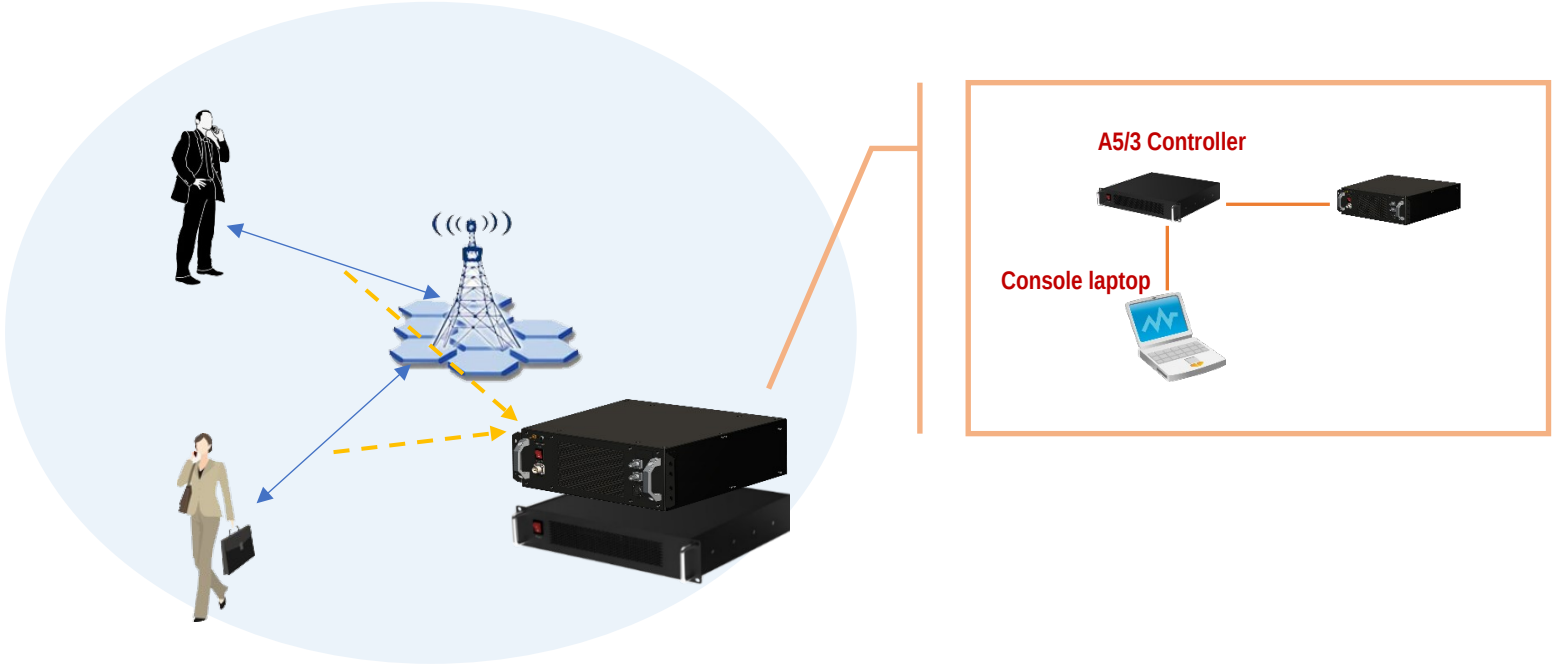
Passive Interception

Genuine semi-passive working mechanism: passive interception host for undetectable concurrent multiple channels monitoring and recording, and A5/3 controller for coping with challenge of A5/3

- Real-time A5/1&A5/2 deciphering with high-performance decryptor
- Unique A5/3 controller to crack A5/3 encrypted network

- Large area coverage
- Flexible configuration for monitoring cells and channels
- Automatically scan and report parameters of surrounding mobile network

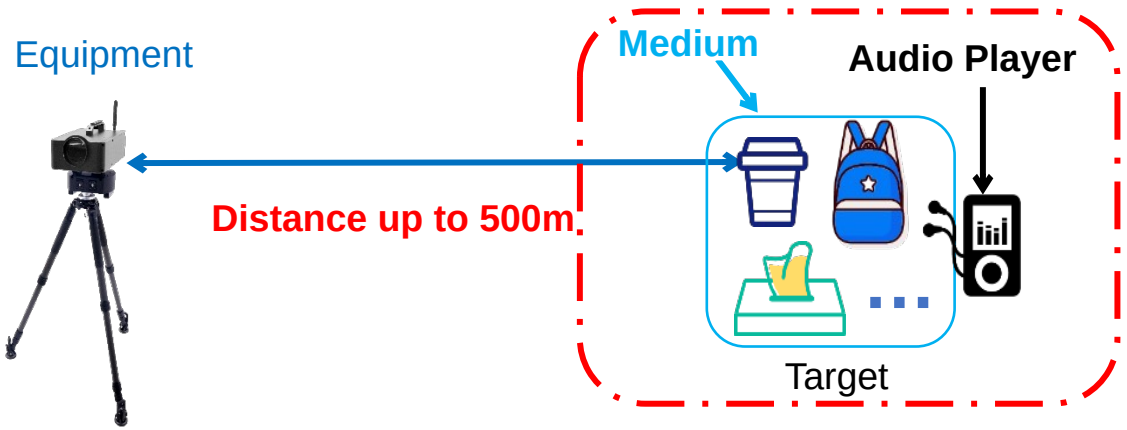
- Enhanced version of passive GSM interception system with special capability against A53 encryption algorithm.
- Extraordinary product design with state-of-the-art technology
- The most advanced solution to your requirements



The high sensitivity optical fiber forensics system can eavesdrop on the target object by The long-distance laser surveillance system is based on the diffuse reflection laser doppler technology and can achieve technical investigation on the target when the location cannot be entered under specific conditions. The equipment adopts the latest developed narrow linewidth laser as core components, efficient transmit-receive optical path, all-digital demodulation circuit, deep-learning-based agile demodulation algorithm and other core technologies. Meanwhile a high-precision electric and anti-shake PTZ is designed to improve the convenience and use effect of the equipment.

Specifications

- Overall weight <20kg(Including host, PTZ and tripod)
- Host power <30W
- Laser wave length ≥ 1500nm, invisible to human eyes
- Laser emission power: less than 150mW
- Maximum incident angle through window ±45° the angle between the laser and the vertical plane of the window
- PTZ adjustment range Horizontal angle -180°~+180° Pitch angle -25°~+45°
- Work preparation time 1 minute From power-on to normal work
- System response time after changing the target medium: within 1 minute
- Focus mode: auto focus;
- Voice frequency range: 200Hz~5kHz
- Storage capacity 128G



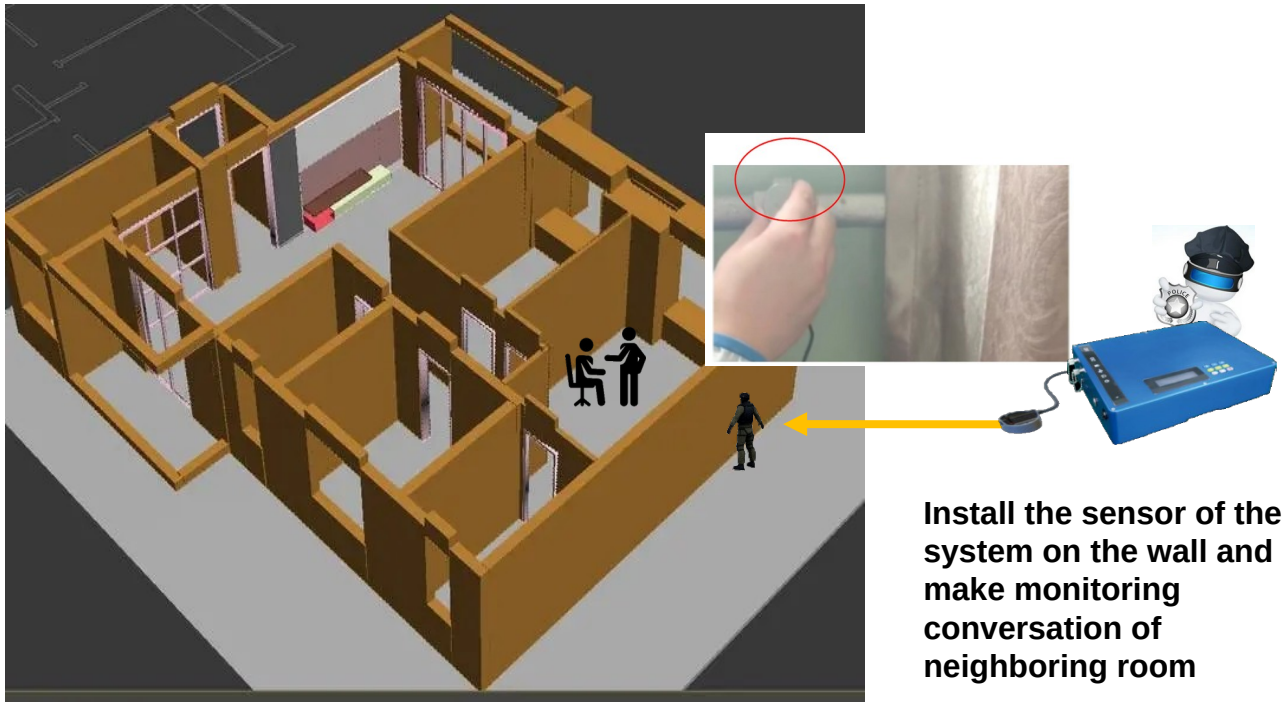
Voice real time pick up, voice data processing, storage and replay

Video real time pick up, video data storage and replay

The high sensitivity optical fiber forensics system can eavesdrop on the target object by installing a specific probe on the partition wall without entering the room of the target object. It is mainly used in hotels, guesthouses, boxes, apartment rooms and other places. Based on our unique coding technique over fiber, the system presents outstanding performance and has been adopted as major equipment in various LEA of China.

Function

- With independent operation of dual-channel audio card, it can perform stereo recording or dual-channel independent recording;
- Key content marking, key recordings can be marked with one key, which can be quickly queried and exported;
- Automatic recording setting, recording starts when it is power on, key information shall not be lost;
- Sound effect adjustment, software and hardware multi-dimensional noise reduction, better sound quality;
- Realize different probe matching, one-key debugging of system parameters;
- Support 256G large-capacity memory which can store recordings for one year
- The signal-to-noise ratio is improved to be more than 55dB, and the background noise is less than 1 15dBm.



Install the sensor of the system on the wall and make monitoring conversation of neighboring room

02

Wireless Signal Control & Management

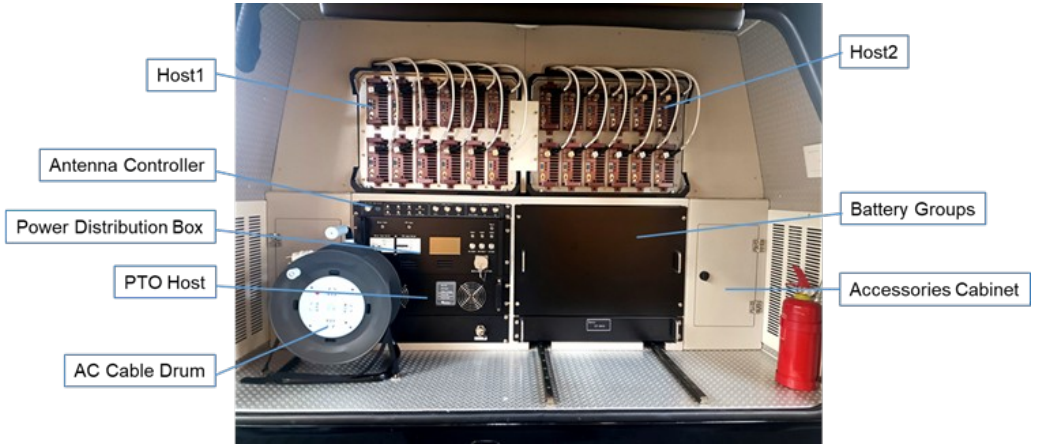
Tactical Man-pack Jammer

Photo-Frame Style Smart Jammer

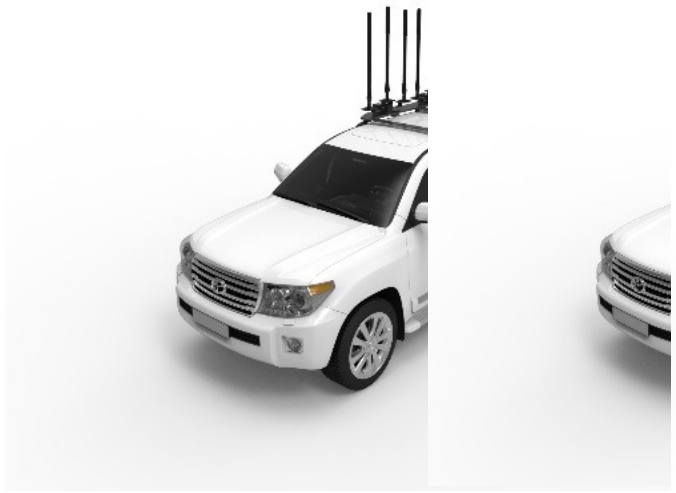
Tactical Portable Jammer

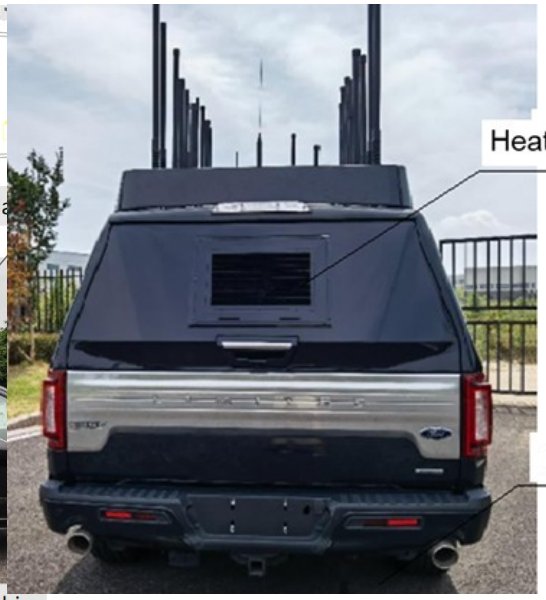
Fixed Jammer

Jamming Vehicle



1 Modular design with DDS technology, which makes it easy to maintenance and operate.
2 Standard vehicle modification solution ensure quick and high quality project overseas.
3 It covers all frequencies from 20MHz to 6000MHz.
4 Torque extraction generator and high-storage batteries install in the vehicle make sure the power supply.





System Highlights

- **Complete Solution:** System can manage both on-the-books and off-the-books terminals, and accurately find off-the-books terminals.
- **Senseless control:** While controlling the off-the-books terminals, it does not affect the normal function and usage of the on-the-books terminals.
- **Easy Deployment & Simple maintenance:** The system is simple to deploy and maintain, which does not require complex operation or professional knowledges.

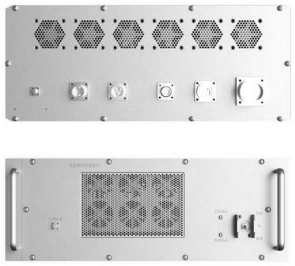
System Components

Intelligent & Distributed Terminal Control Host

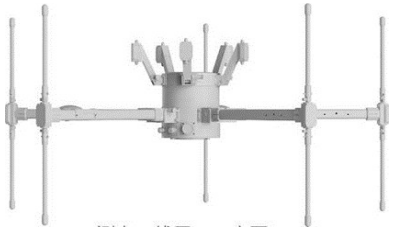
- Suitable for control radio coverage in designated areas in the building, communication and internet services of on-the-book terminals or pre-registration terminals will be allowed.
- Communication of off-the-book terminals will be blocked.
- Support full standards of 2/3/4/5G.
- Can detect and prohibit illegal smartphone from entering the control area, and once the signal of off-the-book smartphone is detected, an alarm will be immediately issued and the internet access of the illegal terminal will be blocked.
- Support whitelist for the guests. Internet access can be allowed during the temporary period, and will be automatically turned off after expiration.

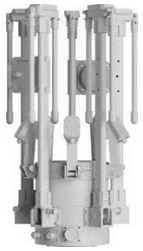
The radio monitoring and DF system can monitor, direction finding, and locate radio signals, and the equipment has various forms such as fixed, vehicle mounted, portable, and handheld. The system is applied in military and civilian spectrum management institutions, as well as industry departments such as national security, confidentiality, and civil aviation, for electromagnetic environment testing, radio monitoring, and interference detection, ensuring the normal operation of various radio services without mutual interference.

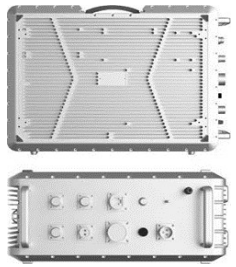
Fixed Radio M&DF



Vehicular Radio M&DF

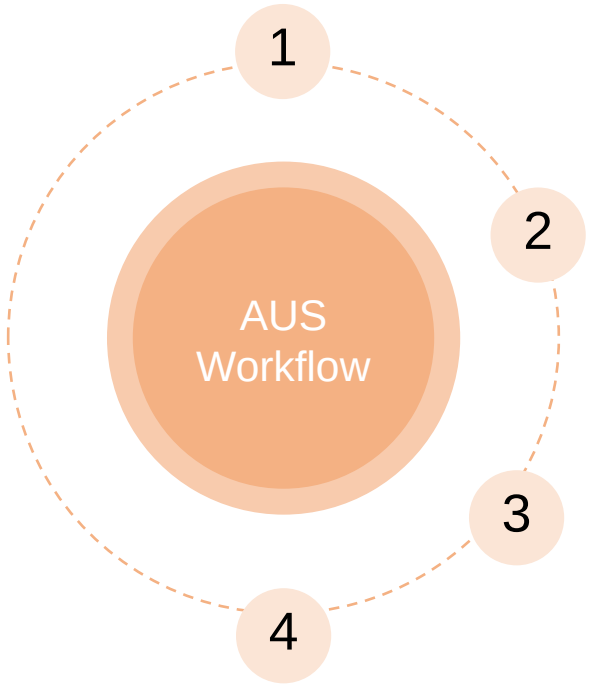






Portable Radio M&DF

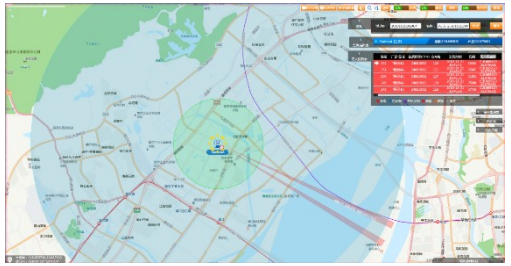
Handheld Radio M&DF



Detection

Detect drone invasion into the protection zone through radar scanning and spectrum monitoring.

Identification



Identify and confirm the invading drone through EO and spectrum library.

Tracking

Drone flight path tracking through radar, with EO video tracking and observing to judge target's intention and obtain evidence.

Disposal

Remotely controlled drone will be disposed by wireless signal jammer, and the GNSS tricker.

03

Information Leakproof (TSCM)

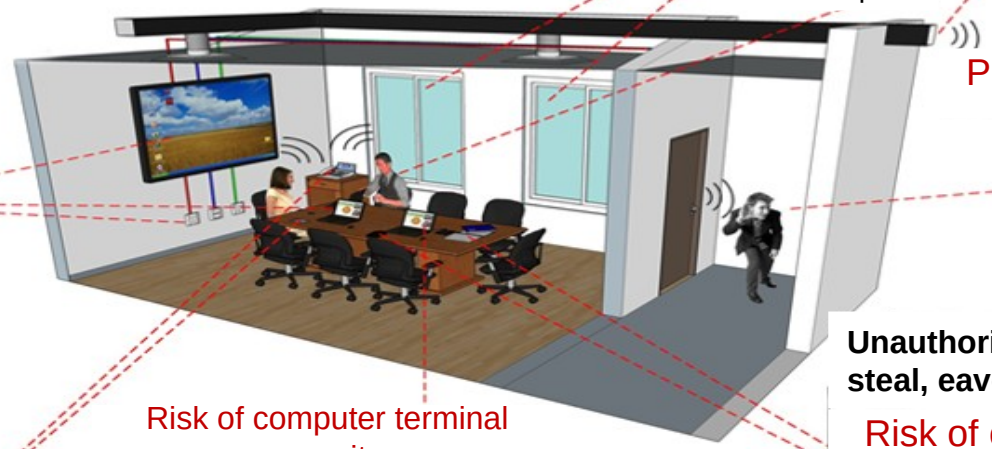
Information Leakproof

There is a large amount of sensitive information in the form of sound, optical, electromagnetic (SOE) and other forms in office or meeting room. If necessary information security measures are not taken, the sensitive information is easy to be required and restored by unauthorized personnel through technical means. If leakage events occur, serious consequences will be caused.

Risk of electromagnetic leakage

Electromagnetic leakage of information equipment and transmission leakage of power supply and communication cables

EM spectrum information restoration



Risk of sound leakage

Air sound leakage and vibration sound leakage are through doors, windows, pipes, walls, roofs and floors

Physical contact

Unauthorized personnel enter the classified area to steal, eavesdrop and secretly shoot, etc.

Risk of communication leakage

- Leakage of communication information of mobile phones, telephones, etc.
- Audio interception and location

Risk of computer terminal security

Information leakage of computer terminal by EM radiation

Risk of classified carriers leakage

Leakage of paper documents, optical discs, hard disks, USB flash disks and other carriers containing confidential information

Detecting System

Passive Mobile Detector

Non-linear Detector

Electromagnetic Spectrum Analyzer

Handheld Radio Frequency Counter

Portable Wireless Signal Detection & Orientation System

Portable All-in-one X-ray Imager

Infrared Thermo Imaging

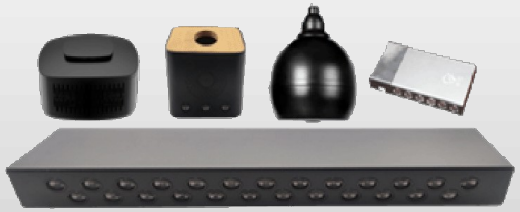
Needle-camera Seeker

Portable Laser Interception Detector

Applications cases

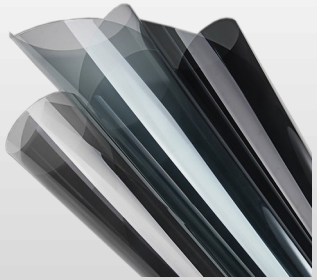
SOE Security Devices

Sound Protection



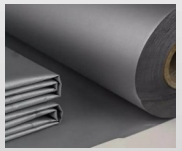
- Sound masking
- Anti-recording

Optical & Laser Protection



- Indoor Laser-interception Detector
- Outdoor Laser-interception Detector
- Anti-laser-eavesdropping film

Electro-magnetic Protection



- Performance monitor
- Mobile signal jammer
- Correlation jammer
- Shielding curtain
- Electromagnetic Security Computer
- PLC Jammer

04

Digital Forensic

VIDEO FORENSICS

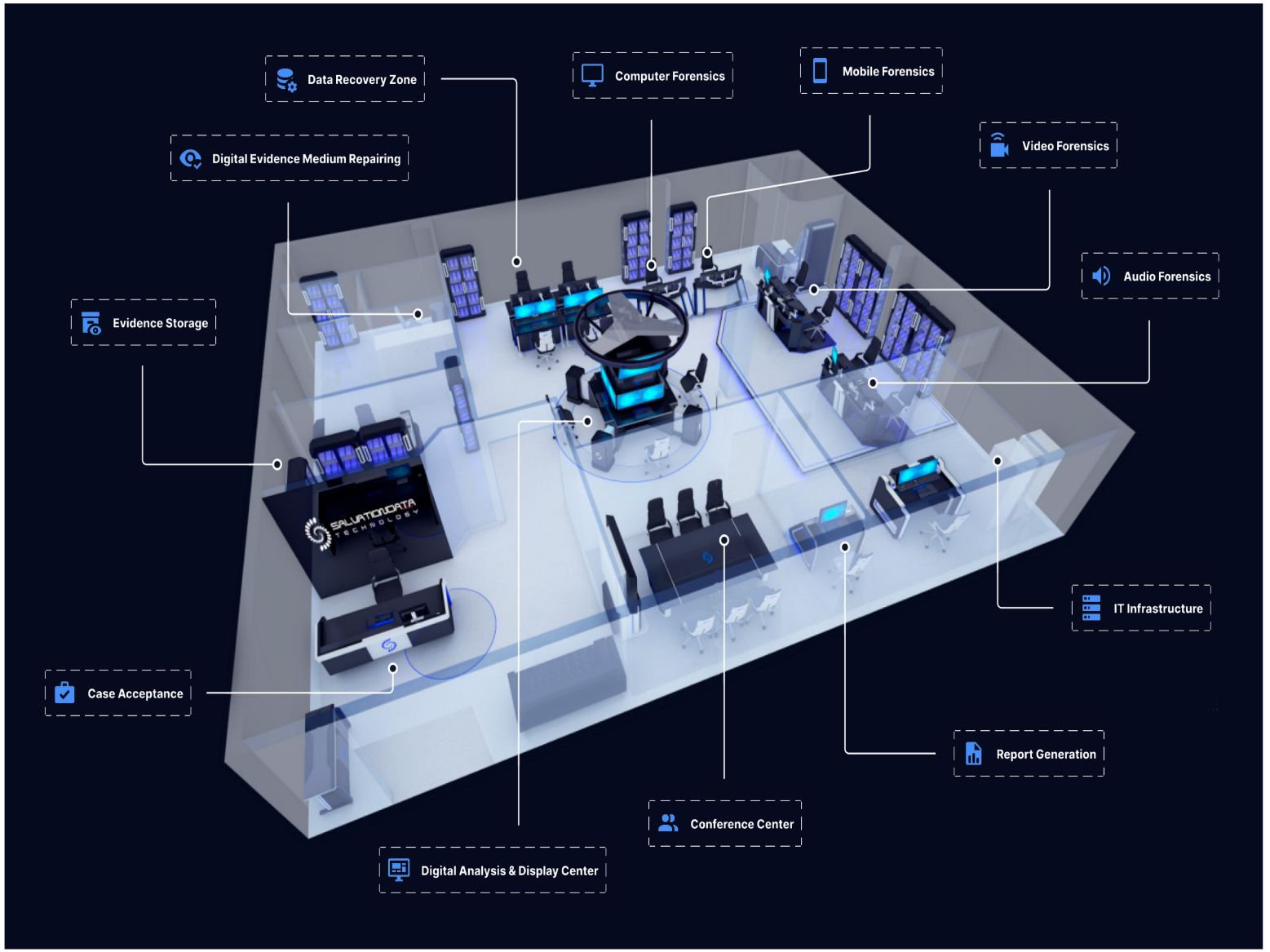
DATABASE FORENSICS

MOBILE FORENSICS

COMPUTER FORENSICS & DATA RECOVERY

Being born as the most ultimate solution for Crime Investigation, the One-Stop Integrated Digital Forensic Laboratory Solution is devoted to providing the most effective, efficient, user-friendly and professional Digital Forensic Assistance.

“Utilizing One-Stop Integrated Digital Forensic Laboratory Solution, the Digital Investigators will deal with each digital evidence confidently and comfortably!”



ASSISTANT SYSTEM

- Access control System
- CCTV Surveillance System
- Case Management System

SOFTWARE TOOLS

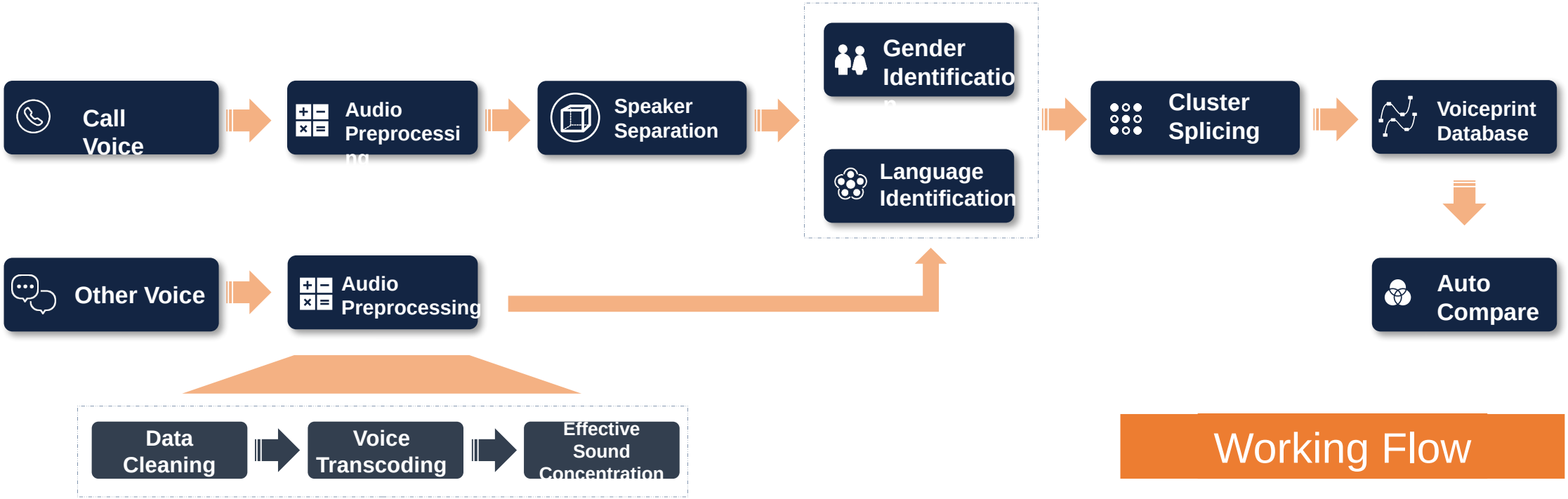
- Video Forensics
- Mobile Forensics
- Computer Forensics and Data Recovery
- Audio Forensics

HARDWARE EQUIPMENT

- Forensic Workbench
- Intelligent Forensic Workstation
- Intelligent Data Analysis and Visualization center
- Security Locker
- Conference Center
- IT infrastructure: server UPS, LAN

ONSITE INVESTIGATION

- Write-Blocker
- Duplicator
- Integrated Tool Kit



Working Flow

Highlights

- **Neural network noise reduction:** The system automatically recognizes the environment where the audio is located, and completes noise reduction processing based on neural network algorithms to some parts or the entire area of the uploaded audio.
- **Audio condensation:** It supports automatic analysis and removal of silent sound and invalid sound clips in voice files, and extracts valid sound clips.
- **Audio transcoding:** Support various audio format and video transcoding, such as: MP3, avi, silk, mpg, m4a, wav, MP4 and others, which can fully meet the voice data processing needs which were from different data sources; the system supports sampling rate conversion for audio and video with a sampling rate greater than 8KHz . Support audio multi-channel, stereo conversion to mono, etc.
- **Intelligent authentication:** Detects if the audio is speech synthesized audio. Select an audio, through the algorithm analysis, gives a judgment of "suspected yes" or "no".; Able to detect and judge if it is the audio generated by the re-recording of the original playback. Select an audio, and after algorithm analysis, give a judgment of "suspected yes" or "no".

Intelligence data cracking platform is specifically designed for the national intelligence department or government authorities who's in charge of national security, with the low consumption and high efficiency of FPGA chips based computing technology and flexible hardware programming , it provides marvelous capability for helping crack encrypted files , hard disk , mobile devices (smart phone & PCs), servers, database, WIFI , VPN, website login password , etc. ,.

HIGHLIGHTS

- 100+ applications password recovery
- World-leading Super computer engineering team.
- 20+ years served in military and Public Security Ministry.
- Practical cracking strategy by analyzing cracked ones.
- Sufficient experience in real action of intelligence data cracking.

- **World-leading Parallel Computing Cluster**
- **Variable cracking scenarios for intelligence departments**
- **Auto recognition of files and standard API**

Forensic Workbench & Tower

Conference Tables & Evidence Storage

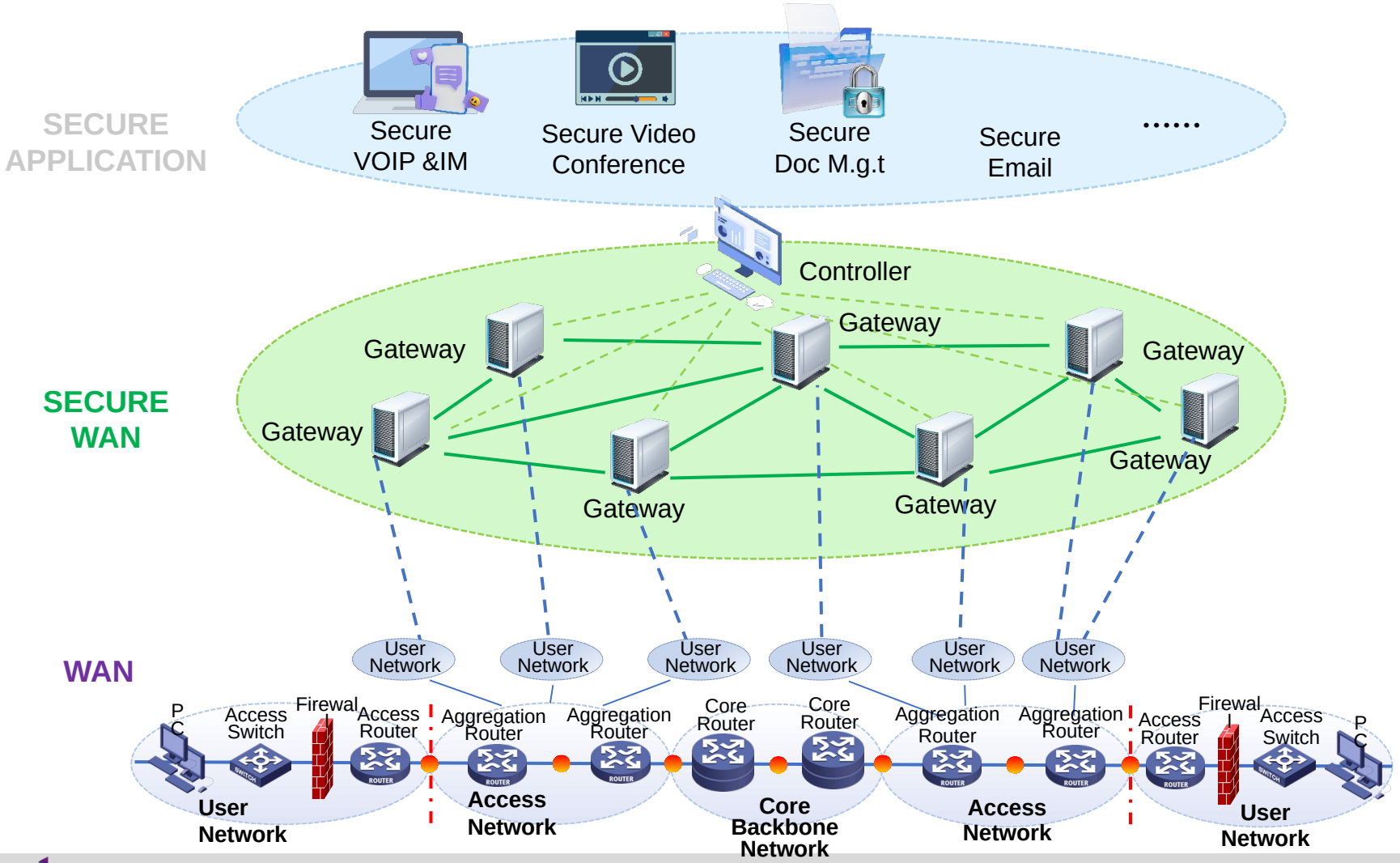
Intelligent Forensic Workstation

Intelligent Data Center

4 Dedicated Communication

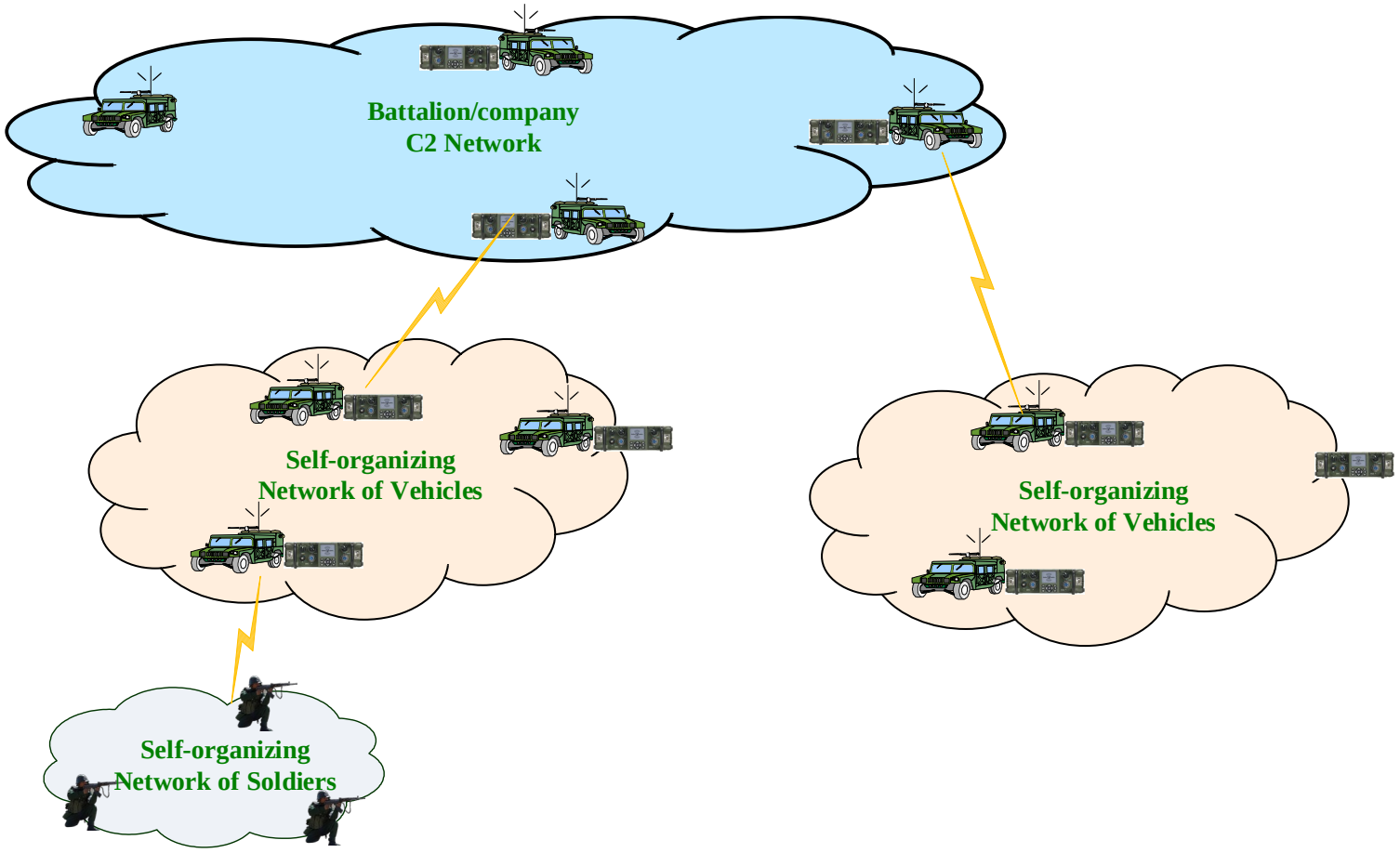
- Specialized in satisfying the dedicated communication demands of certain customers, such as military, public security departments, industrial organizations, etc.
- Offers a wide range of solutions ranging from the high-performance components and equipment, to the turnkey supply of complete systems; from strategical communication to tactical communication and other dedicated communications.

A secure wide area private network constructed for users (government, military, enterprises, etc.) on a IP-based public network (such as the Internet) or private network using software-defined technology. Various secure services can be offered to meet users' daily collaborative office, conference negotiation and other business needs.



- Reliable Transmission (Intelligent Routing, Traffic Dispatching)
- Simplified Operations (Centralized M.g.t, Flexible Access)
- Double Security of Network/Business
- Rich Secure Services (VoIP, IM, File, Conference)
- Easy to Expand (Independent of Bottom Protocols)

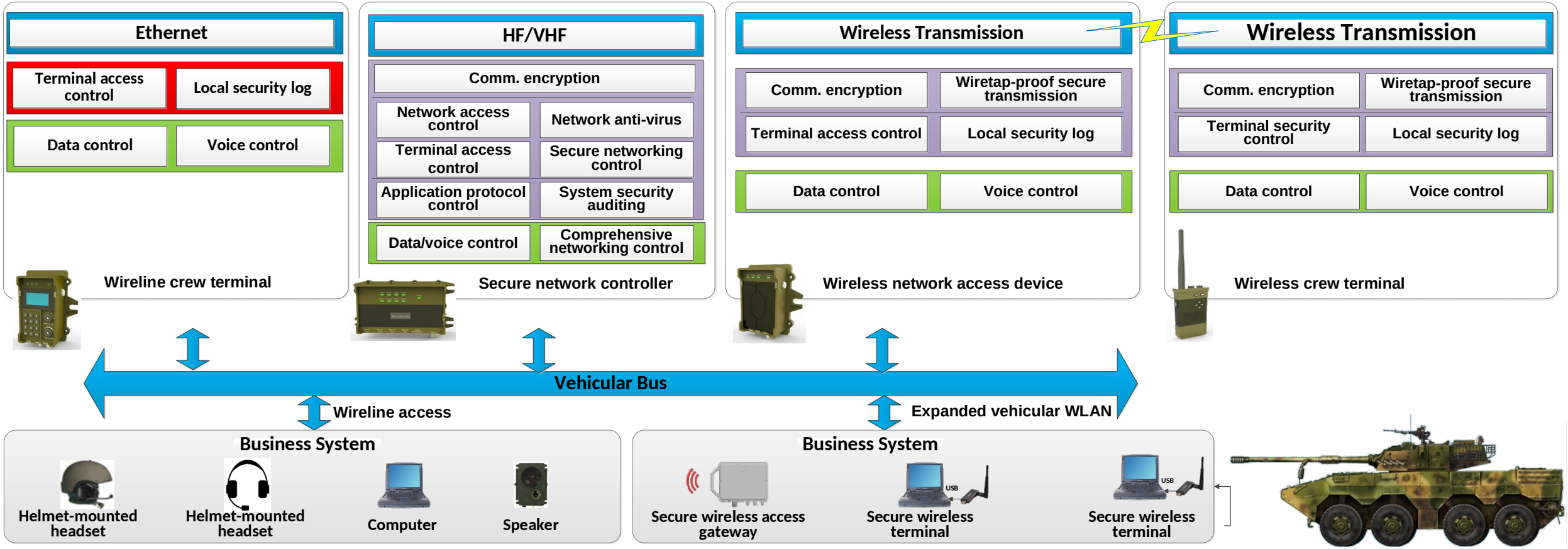
- The system adopts vehicular platform and abundant wireless transmission means to cover wide area;
- In a complex battlefield environment, it features strong resilence and survival ability;
- Wide bandwidth and security assurance enables it to provide reliable command and communication.



Dual-channel SDR Radio
(Short-to-medium distance communication)

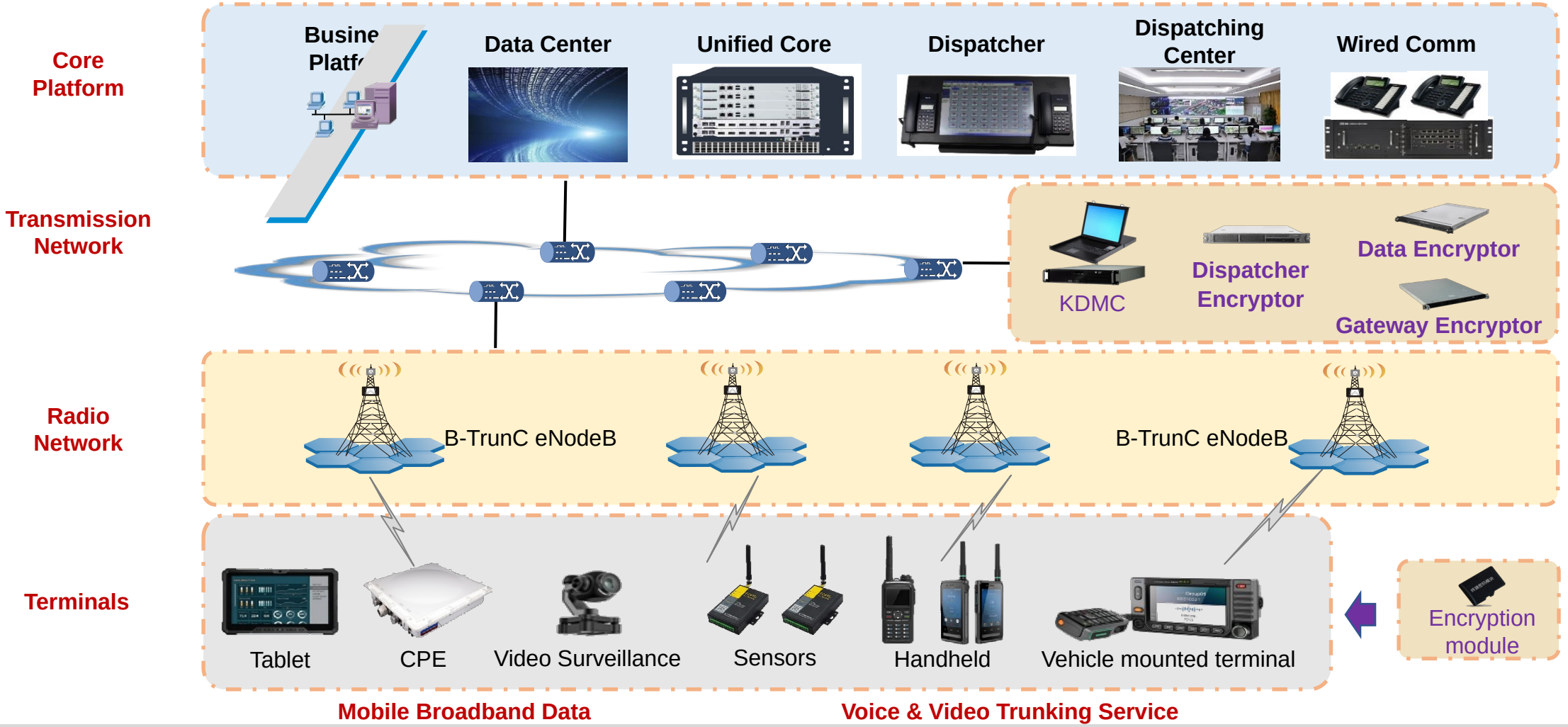
Over-the-Horizon UHF Radio
Long range communication

- The system provides secure intercommunication for various vehicular combat platforms
- Comprehensive networking of wireline and wireless channels
- Universal security control of vehicular data and voice.



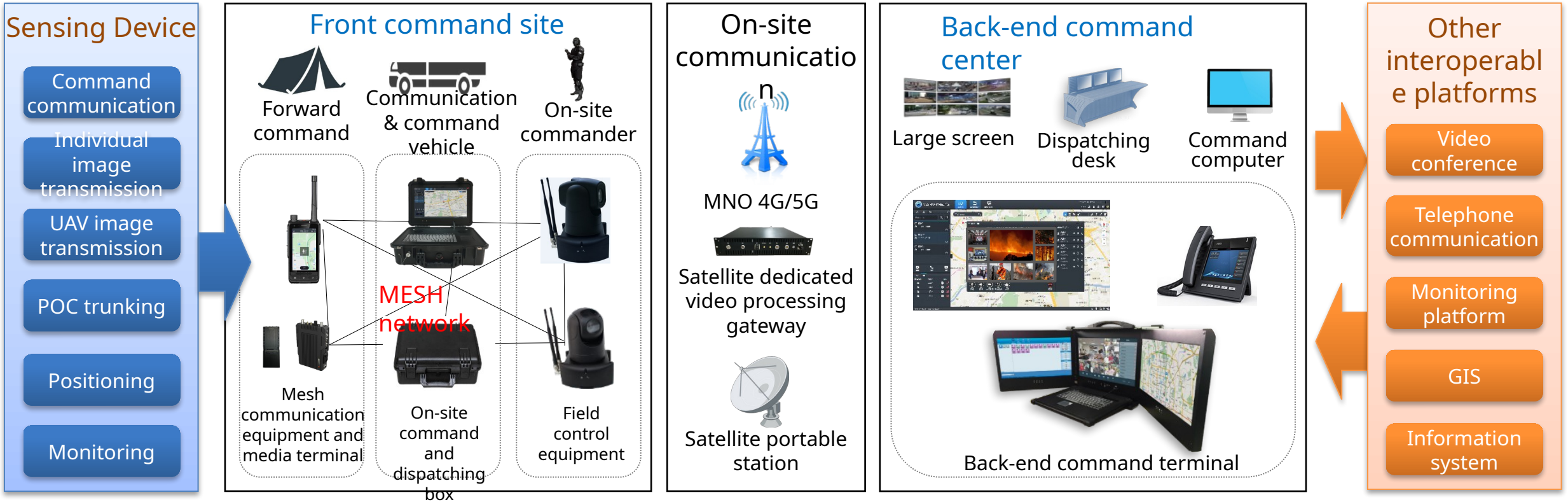
Broadband Secure Trunking System

- To satisfy the demands for dedicated communication, command and dispatching of field operation units.
- Provides traditional and advanced trunking services like video-based command, centralized dispatching, etc.
- Adopts 4G flat architecture, comply with the B-TrunC standard; offers end-to-end encryption assurance.



Self-Networking Mesh System

- **Highlighting "**the last mile" **access, the whole system consists of three parts:** on-site mesh broadband network communication and dispatching system, satellite-ground communication equipment and visual dispatching system**.** The system can transmit multi-channel videos, voice, sensing data at the same time, realizing the intercommunication of rear command center, front command posts and task sites.



CETC 中国电科

责任 创新 卓越 共享

Responsibility Excellence
Innovation Shared