CYBER-SECURITY PRODUCT LINE

3Net Labs has developed a suite of advanced Cyber-Security Hardware and Software systems which utilize Artificial Intelligence and leading-edge compression and encryption.

TRACKER1 (TRAK1)

Trak1 surveils a security perimeter looking for all digital devices in the area and alerts the user and the wireless command center in real-time. Create a secure 360' digital fence. Suitable for home, business and military use. Full location monitoring and protection.

SEEKER1

Seeker1 is a more powerful version of Tracker1 which includes many additional features which are suitable for the needs of government agencies and law enforcement.

GOVERNMENT/LAW ENFORCEMENT PURCHASE ONLY

SPECIAL DATA PROCESSING (SDP)

SDP finds the GPS location of mobile devices. Mobile devices can be located anywhere in the world, when connected to wireless, cellular, or satellite networks. SDP will find them and return their GPS coordinates. SDP supports tracking movement over time. SDP tools are used retrieve the data undetected.

Prior contract for SPD 1.0: **$9.05 million per year**
Prior contract for SPD 2.0: **$1.57 million per year**

RANSOM-AI

Ransom-AI cyber security programs monitor your computer networks looking for security breaches used by computer ransomware hackers. These AI programs were used by various US intelligence agencies and their contractors **to protect their own networks.**

RANSOM RESET

Ransom Reset attempts to undo the damage caused by a ransomware attack **without the need to pay the ransom**.

RANSOM HUNTER

Ransom Hunter tracks down the cyber hackers that are involved in a ransomware attack and neutralizes them using a variety of cyber countermeasures and adaptive AI.

Cyber Forensics Analytica (CFA)

CFA conducts analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion. Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis. Provide technical summary of findings in accordance with established reporting procedures. Check recovered data for information of relevance. Perform file system forensic analysis. Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within enterprise networks.

Prior contract for CFA 1.0: **$7.05 million per year**

Visit our site: www.3netlabs.com