Exhibit E

Pegasus

Version 3.0

Product Description

August 2018

NSO_WHATSAPP_00045591

Cyber Technologies

COPYRIGHT AND DISCLAIMER

We make no representation or warranty regarding the accuracy or completeness of this document and reserve the right to alter its contents at any time without notice. Functionality and specifications featured in this document are subject to change without prior notice and vary between configurations.

Please contact us for current product features and specifications. Any supply of the products featured in this document will be subject to the terms and conditions of the relevant contract.

CONFIDENTIALITY

This document contains confidential information and may be used solely for the purpose for which they were provided, that being evaluating the possibility of acquiring a license to use one or more of our solutions or, following purchase, receiving product support, training material, and/or user guides. If you have not received our prior written permission to use this document, you should immediately destroy all copies of it and cease using it in any way.

The licensing, use, sale and implementation of all products referenced in this document is subject to customer provision of the following: signed and stamped End-User Certificate and an import and/or export license issued by the relevant authorities.

Cyber Technologies

TABLE OF CONTENTS

Cyber Technologies

Q Cyber Technologies

1 OVERVIEW

Q Cyber Technologies—a world leader in the field of cyber product development—owns and develops Pegasus, a cutting-edge cyber-intelligence solution.

Pegasus enables law enforcement and intelligence agencies to remotely and covertly monitor, collect, extract, and analyze valuable intelligence resourced from the most widely-sold Android [redacted] and BlackBerry smartphone devices.

This breakthrough solution, developed by veterans of elite intelligence agencies, enables governments to address the communication-interception challenges found on today's highly-dynamic, cyber battlefields.

Pegasus—using its capabilities to capture new types of information from mobile devices—bridges a substantial technology gap to deliver complete and accurate intelligence that furthers your security operations.

Since 2009, this system has been used by security and intelligence organizations around the globe—a rigorous vetting process ensures that Pegasus is only made available to organizations that fight crime and terror-related activities.

1.1 Overcoming Smartphone Data-interception Challenges

The rapidly growing and highly-dynamic mobile communications market—characterized by the introduction of new devices, operating systems (OS), and applications on an almost daily basis—necessitates rethinking traditional intelligence paradigms.

Changes in the communications landscape pose real obstacles that must be overcome by the world's intelligence and law enforcement agencies. Challenges include,

- **Encryption:** Now mainstream, most applications, services, and devices store and transmit data in an encrypted fashion.
- **Abundance of communication applications:** The communications market is bursting with messaging applications, all of which are IP-based and use proprietary protocols and encryption. Messaging applications are central to a target's personal and group communications as they offer easily-available and secured infrastructures.
- **Roaming targets:** Persons-of-interest are constantly moving between countries and networks.
- **Accessing personal and private data:** Targets carry their smartphones—which hold vast amounts of personal data—everywhere with them. Normally such data is not sent over networks; it is only available on an end-user's device and cannot be intercepted in traditional ways.
- **Masking:** Targets with multiple, virtual identities use any number of free services to hide their presence and activities—this approach makes them seemingly impossible to trace and track.
- **SIM replacement:** SIM are frequently replaced to avoid interception attempts.
- **Complex and expensive implementations:** Increasingly complex communications require more network interfaces—setting up interfaces with mobile network operators (MNO) is a lengthy and expensive process requiring regulation and standardization.

Q Cyber Technologies

1.2 Limitations of Standard Interception Solutions

Standard and legacy interception systems leave valuable *intel* unavailable to intelligence agencies. Since these systems only deliver partial results, organizations are left with substantial intelligence gaps. Commonly used systems are outlined below.

Lawful Interception

Lawful Interception (LI) requires in-depth relationships with local MNO—public-switched telephone network (PSTN), cellular, and Internet—who enable the legal monitoring of text messages and voice calls.

Today, however, most contemporary communications are comprised of IP-based traffic—characterized by encryption and proprietary protocols—which is extremely difficult to monitor using switch-based solutions.

IP-based traffic, even if intercepted, typically carries vast amounts of technical data unrelated to the content and metadata being communicated. Consequently, analysts spend much time going through irrelevant data that, at best, provides only a partial view of a target's communications.

The number of interfaces required to cover relevant MNO both increases costs and widens the circle of persons who might potentially leak sensitive information.

Tactical Man-in-the-Middle Interception

Tactical *Man-in-the-Middle* (MITM) interception solutions effectively monitor voice calls and text messages when targets are within range of MITM tactical teams.

Most of the available solutions only work on 2G GSM networks—they downgrade a target's device to a GSM-based network which, in turn, noticeably impacts user experience and functionality. However, since most communications are encrypted, even solutions that cover 3G and 4G networks are only capable of intercepting a small portion of a target's communications.

MITM solutions require that well-trained, tactical field teams be physically near their targets. On the other hand, sending tactical teams within range of a target can pose serious risks to both the team and the entire intelligence operation.

Malicious Software (Malware)

Malware is intended to enable access to a target's mobile device; however, it requires target involvement for successful installation.

Targets are increasingly sophisticated and well aware of the sensitivity of their communications —they are unlikely to fall into a malware trap particularly when multiple confirmations and approvals are needed before the malware becomes functional.

Malware is vulnerable to many commercially-available, anti-virus and anti-spyware packages. Further, the limitations of their security wireframe and protection, leads to transparency issues—visible traces are easily detected on a mobile device.

By addressing and resolving smartphone data-interception challenges, Q Cyber Technologies enables users to *draw back the curtain* behind which criminals and terrorists hide.

Q Cyber Technologies

2 CYBER INTELLIGENCE FOR THE MOBILE WORLD

Q Cyber Technologies' Pegasus is a globally-positioned, cyber-intelligence solution—it is unique in its ability to successfully infiltrate the market's most popular smartphones—those with Android and BlackBerry operating systems.

Pegasus deploys an invisible software (SW) component (agent) on a target's device which extracts and securely transmits data for intelligence analysis.

The agent's installation vectors, which feature remote and tactical methodologies, require zero to minimal engagement with targets—one click at most!

The highly-secure installation mechanism and agent are completely transparent—NOT a trace exists on either device or network.

2.1 Benefits of Pegasus

Organizations that deploy Pegasus achieve unmatched intelligence collection from targeted mobile devices—the solution overcomes smartphone data-interception challenges, as well as the limitations associated with standard interception methods.

- **Global coverage:** Monitor targets' devices while they connect to the Internet—from any location.
- **Unlimited access to targets' mobile devices:** Remotely and covertly collect information about a target's relationships, locations, phone calls, plans, and activities.
- **Handle encrypted content and devices:** Overcome encryption, SSL, proprietary protocols, and other hurdles introduced by the complex communications world.
- **Bridge intelligence gaps:** Collect new and unique types of information—contacts, files, environmental wiretaps, and passwords—to build complete and accurate intelligence profiles.
- **Uncover virtual identities:** Ongoing device surveillance—regardless of whether or not a target switches between virtual identities and SIM cards.
- **Operate target devices:** Activate the microphone to listen in on a target's environment, turn on the camera to take snapshots, and take screenshots to collect non-communications data of high *intel* value.
- **Intercept calls:** Transparently monitor voice and VoIP calls in near real-time.
- **Monitor mobile applications:** Monitor a multitude of applications including Skype, WhatsApp, Viber, WeChat, Line, Facebook Messenger, Telegram, and Blackberry Messenger (BBM).
- **Pinpoint targets:** Obtain accurate positioning information and track targets using GPS, Cell ID (CID), and Wi-Fi.
- **MNO-independent:** Cooperation with local MNO is not required.
- **Reduce risks:** Eliminates any need for physical proximity to a target or their device during an operation.

Cyber Technologies

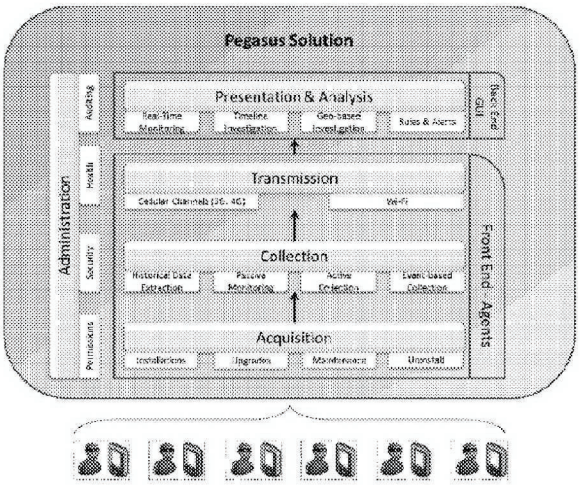
2.2 Technology Highlights

The Pegasus solution uses cutting-edge technology—developed by experts coming from intelligence and LI agencies—to offer a rich set of advanced features and sophisticated intelligence-gathering capabilities that are unavailable in standard interception solutions.

- Penetrates Android [redacted] and BlackBerry-based mobile phones—whether or not password-protected
- Endures reboot and factory resets; OS upgrades are quickly handled
- Installs an agent with zero- to 1-click—minimal to no target engagement
- Unaffected by SIM card replacement
- Monitors smartphone applications
- Extracts encrypted content from the majority of popular instant-messaging (IM) applications and secured chats
- Remotely activates and controls phone functionalities—camera, microphone, GPS etc.
- Retrieves for detailed analysis:
  - passwords
  - files
  - messages
  - emails
  - processes list
  - locations
  - contacts
  - photos
  - calendar records
  - and more
- Target remains unaware—Pegasus is completely transparent
- Leaves no trace whatsoever on a target's mobile device
- User can choose to set an automatic self-destruct mechanism
- Minimal battery, memory, and data consumption

2.3 High-level Architecture

The Pegasus system features several mechanisms which, together, deliver a comprehensive cyber-intelligence collection and analysis solution. System layers and components are shown below.



2.4 System Modules

Pegasus' central functionalities are detailed below.

Cyber Technologies

Acquire	This module is used for new agent installations, the upgrade and maintenance of installed agents, and the uninstallation of existing agents.
Investigate	As the main user interface, this layer presents collected data to operators and analysts who turn it actionable intelligence. The modules include, • **Real-time monitoring:** The collected data of one or more targets is presented in near real-time—this is critical to decision making when dealing with sensitive targets or during operational activities. • **Investigation:** Applies deep-analysis procedures to help analysts thoroughly investigate data, while investigation tools reveal crucial hidden connections and analyze events. • **Rules and Alerts (Road Map feature):** Rules are defined—based on specific incoming data or occurring events—that, when met, trigger system alerts.
Cases	Presents all active cases and their target content.
Commands	Comprehensive intelligence gathering using these extraction methods: • **Active collection:** Directs the agent to perform functions such as camera and microphone operation, screenshots, and/or retrieve files • **Passive monitoring:** Monitors new data that a device syncs with, receives, and/or sends • **Trigger-based collection (Road Map feature):** Defines scenarios that automatically trigger the activation and collection of specific types of data • **Historical data extraction:** Extracts all data existing on a target's device
Transmit	Using the securest and most efficient pathways, collected data is transmitted back to the Command and Control (C&C) servers via cellular or Wi-Fi channels.
Administration	This layer manages all system administration tasks. • **Permissions:** System administrators set up and manage users, define roles, and set permissions to data and modules. Based on this, user groups are defined on the basis of access levels as they relate to targets and cases. • **Security:** Monitors system security to ensure collected and transmitted data is clean, authenticated, and secure before it enters the system. • **Health:** Monitors the status of all hardware (HW) and software (SW) components to ensure healthy functioning—includes communication between system elements, system performance, storage availability, and fault-related alerts. • **Auditing:** Tracks all user activities and operations in the system—from log in to log out. The integrity of all audited data is maintained—it cannot be deleted or changed in any way.

Cyber Technologies

3 TARGET ACQUISITION

A target's smartphone, and the cloud accounts connected to it, offer a deep well of intelligence. Redacted – Export Controlled agent and [redacted] data extraction offer unlimited quantities of target-related data.

3.1 Agent Endpoint

Data collection begins following installation of a software-based component (agent) on your target's mobile device.

System users configure the type of data to be collected by the agent; it can be installed on smartphones that use today's most popular operating systems—Android Redacted –Export Controlled and BlackBerry.

Every agent is independently configured to collect and transmit specific types of information; this is achieved using a reliable Internet connection. The hidden, compressed, and encrypted data is transmitted to Pegasus servers along select channels at pre-defined times.

Once an agent is installed, a target's activities will no longer be hidden behind encryption protocols, the parallel use of multiple applications, and/or other communication-concealing methodologies.

3.2

Redacted – Export Controlled

Data Collection

Data is securely extracted from clouds—there is no impact, whatsoever, on the behavior of device applications and user accounts.

Data stored on mobile devices merely hints at the mass of available historical information—dating back months and even years—that can be retrieved. Cloud brings in a continual flow of information that can last months at a time.

Newly generated information is securely transmitted to the Pegasus system.

- Instant messaging
- Location history
- Account backups
- Email
- Browsing history
- File-sharing storage

Cyber Technologies

4 AGENT INSTALLATION VECTORS

Installing an agent on a target's device is the heart of any intelligence operation using Pegasus—each installation is carefully planned to ensure success.

The Pegasus system supports installation methods and vectors that are designed, as shown by high installation success rates, to satisfy varying operational scenarios. In the following sections, remote and [redacted] Pegasus [redacted] are described.

Installation Vector Comparison Table

Vector	Global	Home Country	Uses	No MNO	Field Team
Remote	✓	✓	Triggered / Covert	✓	×
Redacted – Export Controlled					
Physical	×	✓	Physical access to device	✓	✓

4.1 Remote Installation (Unlimited range)

Remote installations include both covert and social-engineering methodologies. The Pegasus solution offers many tools for composing tailored, yet innocent-looking messages—this is crucial as content credibility greatly affects whether or not a target will click a link.

Using the below methods, only a target's phone number (MSISDN) is required for a successful installation.

Covert

1. A covert message is sent to a mobile device; the target is not engaged—there is no need to click a link or open a message.
2. The message causes the smartphone to download and install the agent—the device shows no signs of change or interference.
3. The installation is completely invisible.

The Pegasus system's unique, remote installation capability gives our solution a vast advantage over other offerings found in the market.

- Covert installation process is invisible to the target and doesn't require their engagement.
- System is MNO independent.
- Activation is handled from a command and control center.
- Solution has an unlimited range and works using any MNO. Thus, the Pegasus agent can be installed on any supported device, anywhere in the world.

Triggered (Social Engineering)

System operators can choose a different approach and craft an SMS, instant message (IM), or email. This approach prompts a target to click on a message link.

- One click, whether active or unintentional, leads to an agent installation.
- The process is completely covert and there is absolutely no sign that software is being installed on their smartphone.

4.2 [redacted] Field [redacted] (Within range)

Field [redacted] include a [redacted], or even physical access to a mobile device.

Cyber Technologies

Tactical Network Element (PiXcell)

- Pegasus agent is covertly deployed once a mobile device is acquired by and connected to a tactical network solution (PiXcell)—whether it be native 3G/4G or Wi-Fi MITM.
- Pegasus solution leverages the capabilities of PiXcell to perform a covert agent installation while a target browses; there is no target engagement.
- Once installed, data is extracted and transmitted remotely—in the same manner and with the same capabilities of a remote installation.

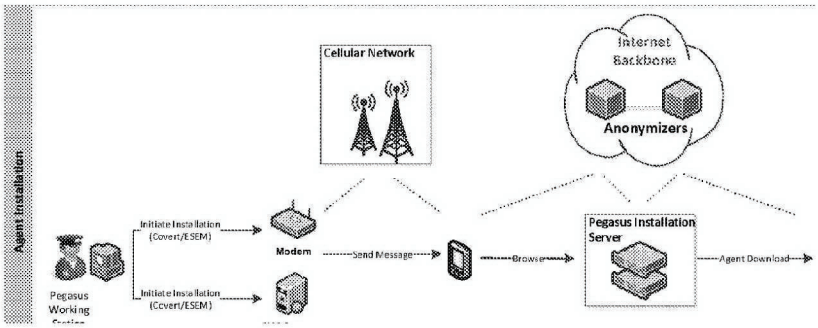
Physical

- If a team has physical access to a device, then the Pegasus agent can be installed within a few minutes.
- Once installed, data is extracted and transmitted remotely—in the same manner and with the same capabilities of a remote installation.

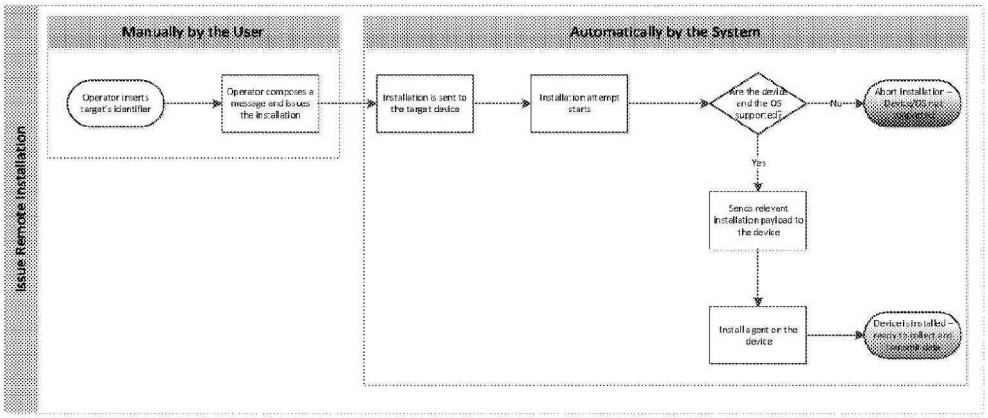
Cyber Technologies

5 AGENT INSTALLATION FLOW

The remote installation of a Pegasus agent is outlined below.



To initiate an agent installation, the system operator only needs a target's MSISDN—the rest of the installation process is performed automatically by the system; see the below image.



5.1 Device Behavior after Installation

Introduction of an agent leaves a target's mobile device totally unaffected—there is no change in the phone's behavior. The agent is designed to be lightweight, yet extremely efficient; it compresses, stores, then transmits collected data in the most efficient and economical way. This ensures that device resources, such as its battery and data plan, are wisely utilized.

5.2 Installation Failure

If a system operator initiates a remote installation to an unsupported device, OS, or browser, then the installation will be aborted. However, the target's browsing experience remains unaffected—the target's device will present the URL defined by the system operator.

Note: The system and system operator don't need advance knowledge of the device, OS, and/or browser type; this information is automatically identified during the installation process.

Cyber Technologies

6 DATA COLLECTION

Following the target acquisition stage, during which the agent is installed and the [redacted] Eye [redacted], the Pegasus system begins to monitor and collect a wide range of data from a target's mobile device.

The types of information include the following:

- **Text:** Textual information, which is usually structured and small in size, is easier to transmit and analyze; it includes text messages (SMS), emails, calendar records, call log history, instant messaging, contact list, and browsing history.
- **Audio:** Includes call recording (GSM & VoIP), environmental taps (microphone activation and recording), and other audio-recorded files.
- **Visual:** Includes photo and video retrieval, and new camera and screen shots.
- **Files:** Every mobile device contains hundreds of files such as databases, documents, and videos—some may contain vital intelligence.
- **Location:** Includes ongoing monitoring of a device's location (GPS and CID).

Data is collected by means of historical data extraction, passive monitoring, and active collection.

6.1 Historical Data Extraction

The types of historical data that can be extracted from a target's device, and sent to the C&C server, include the following:

- SMS records
- Contact details
- Call history (call log)
- Calendar records
- Emails
- Instant messaging
- Browsing history
- Installed applications
- Wi-Fi networks

Pegasus enables the extraction of all data from a device—existing *intel* and real-time additions. Other market offerings are limited to data generated after the installation and partial monitoring.

Intelligence agencies greatly benefit from their ability to access historical data as it helps build a comprehensive and accurate intelligence picture of a target/s and their associates. Normally organizations devote months to collecting such information, with Pegasus this is achieved in minutes.

Note: Historical data extraction is a valuable option. If, however, an organization is not permitted to access and extract historical data, then this option can be disabled. The agent will only monitor newly-arrived data.

Cyber Technologies

6.2 Passive Monitoring

The agent, once installed, continuously monitors a device and retrieves—in near real time—all new data that becomes available. Data that is passively monitored includes the following:

- SMS records
- Contact details
- Call history (call log)
- Audio call recordings (GSM & VoIP)
- Calendar records
- Emails
- Instant messaging
- Target location (CID, network-based)
- Activity location; e.g., site from which a phone call originated
- Device location—monitoring a target's movements

6.3 Active Collection

In addition to passive monitoring, a wide range of active collection features are available. Active requests (actions) collect specified data based on orders issued by a system operator and/or system triggers.

Active collection allows near real-time actions to take place on a target's device—unique information is retrieved from both it and the surrounding area:

- Location (GPS and Wi-Fi-based)
- File retrieval
- Environmental tap (device microphone)
- Snapshots (front & back cameras)
- Screenshots

Pegasus' active collection capability sets it far above all other intelligence-collection solutions.

- System operators control information collection; they actively retrieve crucial data from a target's device. There is no passive waiting for *hopefully* relevant data to arrive.
- Your organization can access personal information never intended to leave a target's phone, or catch moments never meant to be captured.
- Pegasus accurately tracks a targets, takes photos, and/or records face-to-face meetings without the need for tactical teams.

Manual Actions

Active data collection is initiated by a system operator. Actions are normally issued on the basis of pre-existing target information and the need to seek specific, related intelligence.

Example:

1. Target's calendar record shows s/he is currently in a face-to-face meeting.
2. Collected location data verifies this information.
3. System operator initiates an action that activates the microphone and camera on the target's mobile device.

Further, a system operator can actively retrieve any file found on a target's device—it can be an email attachment, video sent via a messaging application, or a document synced to the device from a cloud-storage service.

6.4 Time Limitation and Selective Collection

Pegasus' capabilities enable the collection of historical, passive, and active data. A partial data collection can be performed in order to optimize resources, comply with a country's legal wireframe, or comply with a warrant issued for a target.

The following example shows how the agent collects and operates within time and data constraints.

- Data collection is only permitted during a time frame set by a warrant.
- Upon reaching the uninstall date, the agent stops sending data and removes itself from the target's device.
- If warrant conditions change, then the agent life cycle can be reconfigured.

6.5 Collection Buffer

The installed agent monitors device data and transmits it to the C&C servers.

Data transmission, on occasion, may not be possible for a number of reasons: no available data channels, device is roaming, or the agent is dormant. In such instances, the agent continues to collect new information; it is stored until a connection become available, and then transmitted.

Collected data is stored in a hidden, encrypted buffer; it is preset to hold no more than 5% of a device's free space.

Example:

Buffer can store up to 50 MB on a monitored device with 1 GB of free space.

If the buffer limit is reached, the oldest data is deleted and replaced with new data.

Transmitted data is immediately deleted from the buffer.

6.6 Description of Collected Data

The agent collects available data from supported applications found on the device—these include globally-popular applications.

Our developers understand that less popular and/or new applications can quickly come to the forefront of use—when requirements are raised, our company can choose to prioritize the development of new capabilities.

The types of data available for historical extraction, passive monitoring, and active collection are set out in the below table; they all have the potential to be collected by an agent.

nologies

Collected Data	Agent Description	Historical Extraction	Passive Monitoring	Active Collection
SMS	• Extracts history • Monitors all incoming & outgoing text messages (SMS)	✓	✓	N/A
	Redacted –Export Controlled			
Instant messages	• Extracts history • Monitors incoming & outgoing messages sent to/from a device via a multitude of applications • Covers leading IM services: WhatsApp, Telegram, Facebook Messenger, Signal, Viber and more • Collects textual messages (including group chats) • Indicates files transfers (which are retrievable)	✓	✓	Retrieval request: transferred files
Emails	• Extracts history • Monitors all emails from Gmail application and native email application	✓	✓	Retrieval request: email attachments
Call log	• Extracts history • Monitors all incoming & outgoing calls made to/from a device • Collects Cellular phone call logs • Collects call logs from applications such as WhatsApp, Telegram, and more	✓	✓	N/A
Call recording	• Records incoming & outgoing calls to/from a device • Records regular Cellular calls • Records VoIP calls made from various applications such as WhatsApp, Telegram and more	N/A	✓	N/A

nologies

Collected Data	Agent Description	Historical Extraction	Passive Monitoring	Active Collection
Contact details	• Extracts history • Monitors all contacts on a device including assigned photos • Includes contacts synced to the contact list from external services; e.g., Gmail, Facebook	✓	✓	N/A
Calendar	• Extracts history • Monitors calendar events on a device, including those synced from multiple external accounts; e.g., MS Exchange, Gmail, and more	✓	✓	N/A
Browsing history	• Extracts history • Monitors websites browsed via Chrome [Redacted - Export Controlled]	✓	✓	N/A
Installed applications	• Extracts a list of installed applications • Monitors newly installed applications • Monitors applications updates and deletions	✓	✓	N/A
Device & network information	• Monitors the following: - Device and network details - IMSI, IMEI, Wi-Fi networks, SSID, MNC, MCC - Battery level and more	N/A	✓	N/A
File retrieval	• Retrieve any file—whether on a target device's internal memory or SD card • In addition, with the cloud solution, the user can retrieve files from cloud-based services such as Google Drive. (see Pegasus 3 Product Description section 3.2)	Retrieval request: historical files	×	✓

nologies

Collected Data	Agent Description	Historical Extraction	Passive Monitoring	Active Collection
Location	• Monitors a target's location • Monitors sites where each activity was sent/received • Passive location monitoring is based on CID • Active collection is based on GPS	N/A	✓	✓
Camera snapshot	• Front and back cameras take photos - No indication appears on the device - Flash is never used - Images do not appear in the device gallery - **Note:** Images may be out of focus since the flash isn't used and the device may be in motion • Photos are sent to the C&C servers • Operator chooses the degree of image quality; size can be reduced to ensure faster transmission	N/A	×	✓
Screenshot capture	• Screen capture is taken • Image is sent to the C&C servers	N/A	×	✓
Room tap (mic recording)	• Microphone is activated to record surrounding sounds - No indication that a recording is in process - Recordings are not stored on the device - **Note:** Recording quality is affected by the device model, surrounding noise, and microphone sensitivity; the latter varies between phone models and is set by the device vendor • Data is sent to the C&C for playback and analysis	N/A	×	✓

Cyber Technologies

7 SECURE TRANSMISSION

Collected data—historical data extraction, passive monitoring, and active collection—are, by default, sent in near real time to the C&C servers. The preferred transmission channel is Wi-Fi but, if unavailable, cellular data channels such as GPRS, 3G, and LTE are used.

The agent, which uses several compression and encryption methodologies, can exclude irrelevant, non-textual content from documents before transmitting them.

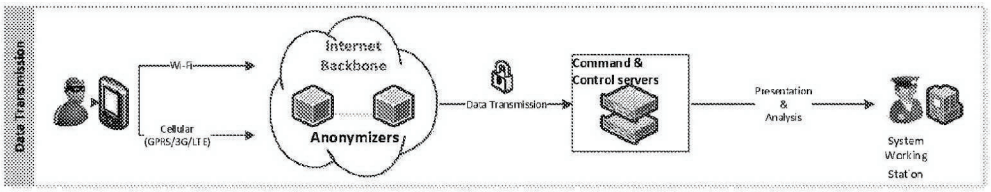
Due to Pegasus' tremendous capabilities, and the remarkable efforts invested in its design, the data usage is tiny—normally only a few hundred bytes. This guarantees that collected data is easily transmitted, and has minimal impact on a target's device and data plan.

Section *6.5 Collection Buffer* notes that if data channels are unavailable, then the agent continues to collect new information, stores it in a dedicated buffer and, when connectivity returns, transmits the data. Factors that can affect data transmission are noted below.

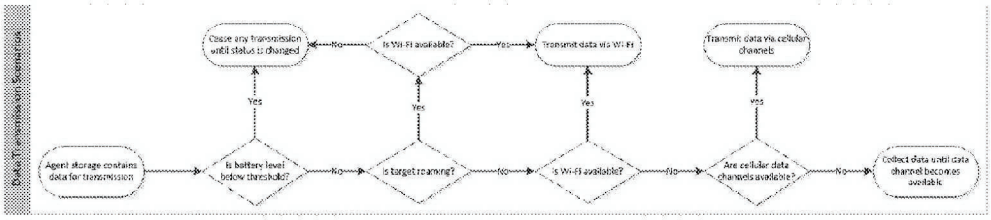
- **Low battery:** If a device's battery has only 5% remaining power, then all data transmission processes are stopped until the device is recharged.
- **Roaming device:**
  - Cellular data channels used by roaming devices are expensive; therefore, by default, data transmission is handled via Wi-Fi.
  - If Wi-Fi is unavailable, then transmission stops.
  - System operators can, however, choose to transmit data over cellular channels—though this can lead to high data-plan charges.
- **Dormant agent:**
  - The agent is set to dormant under the following circumstances:
    - Target enters a country whose expensive roaming charges could draw attention
    - Target enters a country with high with exposure risk.
    - There may be legal and/or contractual limitations on use in given countries
  - The agent continues to passively collect and then store data. Upon departure from the country-of-risk, collected data is transmitted to the C&C servers.

Communication between the agent and the central servers is indirect—it is handled via an anonymizing network—thus trace-back is infeasible.

The below image shows the Pegasus system's data transmission process.



Channels and scenarios for transmitting collected data are set out below.



7.1 Data-transmission Security

The connection between agent and servers is encrypted with strong algorithms and also mutually authenticated; transmitted data is encrypted with a unique and asymmetric encryption.

The encryption of data and transmissions is pivotal, but attention must be given to data, battery, and memory use—the target must be kept unaware.

It is inconceivable that a target would discover an active agent. The agent, installed deep in the device, is well beyond OS privilege controls and is untraceable by antivirus and anti-spy software.

7.2 Data Hashing

The authenticity of collected data is guaranteed; it is sent in encrypted form and is digitally signed to prevent tampering. Data is timestamped as follows:

- At creation
- Upon arrival at the C&C servers

7.3 Anonymizing Transmission Network

Agent invisibility and source security are the guiding principles of the Pegasus solution. An Anonymizing Transmission Network (ATN)—a network of anonymizers—is deployed at every client's site to ensure that it is impossible to trace back to an operating organization thus ensuring full deniability.

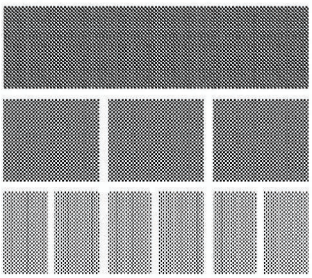
ATN nodes are spread worldwide and enable agent connections to be redirected along separate paths before reaching the C&C servers. This ensures that the identity of the communicating parties is obscured.

Note: Our 24/7 Support Center monitors security alerts arriving from all client systems; however, while the Support Center can see security alerts, they cannot view any collected target or operational-related data. Should there be a security incident, the client must immediately follow Support Center guidance and directions.

Cyber Technologies

8 MONITORING AND INVESTIGATION

Collecting intelligence on hundreds of targets and devices generates vast amounts of data that require visualization, presentation, and investigation.



Collected data is displayed in an easy-to-use, intuitive user interface (UI).

- Collected data is organized per case
- Each case consists of related targets
- Target profiles show installed agents; e.g., devices with Pegasus agents

The Pegasus system includes a set of operational and collaborative tools that help organizations transform data into actionable intelligence. Tool functionalities include the following:

Timeline investigation	Review and analyze activities in chronological order to best understand the flow of events.
Geographical investigation	Review target and case activities on a map: • View their historical locations • Investigate their routine • Simultaneously view and compare multiple target trails
Data enrichment	Enrich collected data with user input to help retrieve, filter, and analyze data: • Add comments and tags • Write summaries and conclusions • Add translations
Entity management	Manage targets that are tagged per case, location, and/or subjects. For example, • Operation [name] • Country [name] • Drugs • Terror • Serious crimes
Advanced search and filters	Search and filter to prove or strengthen a theory, or investigate events. User categories such as case, target, topic, types of data (location, calendar records, email), terms, names, numbers, code words, dates and times, etc.
Notification and action rules	*Roadmap* feature that will define rules to, • Generate notifications • Issue actions

8.1 Data Export

This section holds information on features, tools, and other systems used to export data from the Pegasus system.

Third-party Systems

Pegasus is an end-to-end system that provides its users with collection, presentation, and advanced investigation tools. Additionally, the system can export html files that may be integrated with compatible, third-party analysis systems.

Export Authenticity

Collected data maintains its integrity—it cannot be changed or altered by system users. Users can, however, add explanations and additional information by means of descriptions, tags, and comments. This leaves the data unchanged, but it does add a useful reference layer.

All exported data is 'sealed data'—including hashes—and is admissible in court.

Report Generation

Generated reports can be securely transferred to organization stakeholders. The system generates reports based on data filtered according to parameters:

- Timeframe
- Cases and targets
- Types and categories of collected data
- Tags
- Comments
- Free text
- Location

9 AGENT MAINTENANCE

Installed agents require maintenance in order to support new features, bugs fixes, and changes to settings and configurations.

Agents can be uninstalled when a target is no longer a focus-of-interest for an organization.

9.1 Agent Upgrade

New agent versions are regularly released—for first time installation or as an upgrade to an existing agent. Latest versions provide new functionalities, bug fixes, support for new services, and/or improvements to the agent's overall behavior.

The time required for an upgrade is short and the process simple—there is no target engagement and the target's device is completely unaffected.

- A system operator requests the upgrade and, once initiated, it is completed within minutes.
- If the target's device is turned off or has a poor data connection then the upgrade is delayed until the device is reactivated and/or the data connection improves.

Updates are crucial—they keep the agent functioning and operational, and improve and repair security issues that can arise due to the ever-changing smartphone and communication environments.

9.2 Agent Settings

Agent settings are initially defined during installation:

- Data to be collected
- Preferred channels of communication with the C&C server
- Frequency with which the agent communicates with the server

Agent Uninstall

When an intelligence operation is completed, or a target is no longer of interest, then the agent can be uninstalled; this process is quick and has zero-to-minimal effect[1] on a target's device.

If an agent is operational on a device and communicates with the C&C servers, then—regardless of the initial installation vector—it is simply and **remotely** uninstalled. Under certain circumstances, a physical uninstall is also possible.

1. System operator issues a request for agent uninstallation.
2. Uninstall command is sent to the device.
3. No trace whatsoever will ever be found on a device.

Uninstalling an agent doesn't affect any data collected to date. Prior to the removal process, all collected data is transmitted to the C&C servers where it awaits investigation and analysis.

[1] In some cases, uninstall may lead to device reboot; however, this will only occur after agent removal is completed.

Cyber Technologies

10 OPERATIONAL SECURITY

Q Cyber Technologies devotes extensive resources towards keeping our clients and products secure and, equally important, invisible to targets. The Pegasus architecture ensures no client trace-back or agent detection.

10.1 Self-destruct Mechanism

The Pegasus agent carries an automatic self-destruct mechanism that the system operator can choose to activate due to specific operational considerations.

If there is a chance of agent exposure then the self-destruct mechanism is automatically activated; then, when the risk has been removed, the agent can be re-installed. The agent has sensors that help detect security risks such as those noted below:

- **Anti-debugging—**agent continuously monitors debugging activities; e.g., device rooting, connections to forensic tools, and/or connection to an emulator.
- **Agent manipulation—**agent endlessly monitors its own code and performs checks for changes and/or abnormalities.
- **Device mirroring—**agent ceaselessly monitors the environment on which it is running and will immediately detect device duplication or changes.
- **Unresponsive agent:** If an agent is unresponsive or doesn't communicate with the servers for a set period of time[2], then the agent automatically performs uninstall to avoid remaining on an unused or unsupervised device.

10.2 Security Alerts Monitoring

Our Network Operations Center (NOC) monitors Pegasus security logs 24/7—if there is any suspicious activity or an alert, an immediate investigation begins.

- Support Center updates the client and shares known information.
- Nagios, the security monitoring system, is transparent and also available on client premises.
- NOC follows a protocol:
  - Verify which type of security alert was triggered.
  - Actions to be taken by the support team and client.

[2] Default period is 21 days but can be reconfigured for a shorter period of time.

Cyber Technologies

11 AUDITING

Pegasus is a mission-critical system that supports covert, operational intelligence activities. System operators and analysts are well trained and understand the system's capabilities—especially the collection of highly-sensitive and critical data.

- System's auditing mechanism enables:
  - Compliance, where relevant, with country-specific regulations
  - Access to auditing tools that access correct system usage—from log in to log out
- Audited data is only available to persons who are designated as auditors by the system administrator.
  - They can review data and filter it according to date, user, or user action
  - Example: Review all actions performed by a given user on a specific date
- A user can only connect to one Pegasus workstation at a time.
  - Supports reliable and accurate auditing
  - Example: If a user connects to another workstation, then the initial connection automatically ends
- Audited information is stored in a protected database.
  - Data cannot be deleted or altered by any level of system user
  - This safeguards data integrity and viability
  - If required, audited information can be exported

Cyber Technologies

12 ROLES, PERMISSIONS, AND ENTITIES

Pegasus is an intelligence system that collects, generates, and stores large volumes of critical data.

Q Cyber Technologies understands that gathered data can relate to high-profile and/or sensitive targets and, as such, our company provides a mechanism for managing the compartmentalization of data according to user permissions.

The system's highly-flexible permissions architecture makes organizational changes extremely easy to update. Users are allocated roles, tasks, and related permission levels. On the basis of these parameters, users can access permitted data and use specific sets of tools—all of which assist them in meeting both mission and organizational objectives.

12.1 Roles

Roles are characterized by predefined sets of activities, tools, modules, and permissions. New and existing users smoothly transition into and within the Pegasus system. Roles include,

Administrator	• Creates and manages system users, their roles, and assigned permissions • Gives users access to system modules, and the ability to conduct operations and view data
Supervisor	• Manages acquirer, analyst, and operator roles • Views all operations performed by subordinates • Approves and conducts critical operations; e.g., agent uninstall & data deletion
Acquirer	Dedicated user who deals with the entire life cycle of an agent on a target's device—installation and maintenance to uninstallation
Analyst	• Runs investigations and can only read, query, and analyze collected data • Analysts add comments, tags, and descriptions to the data to aid in interpretation
Operator	• Conducts installations, deploys new agents, and changes existing settings • Views data and issues active data collection requests
Auditor	• Dedicated user with only auditing-section permissions • Can audit system usage and all user operations—from log in to log out

Authentication and Authorization

The security and integrity of your Pegasus system is ensured.

- System access requires authentication—the log-in process demands the use of both a username and password.
- These identifiers are stored and transmitted in an encrypted manner.

Following successful authentication, users can then access data permitted to them based on their role and associated teams and cases.

12.2 Module Permissions

User permissions are based on their **role**, as well as to the **team** and **cases** to which they are assigned.

Cyber Technologies

	Agent Life Cycle	Monitor & Investigate	Data Enrichment	Archive, Delete, Uninstall	System Admin	Audit
Acquirer	✓					
Analyst		✓	✓			
Operator	✓	✓	✓			
Supervisor	✓	✓	✓	✓		
Auditor						✓
Administrator					✓	

12.3 Entity Relations

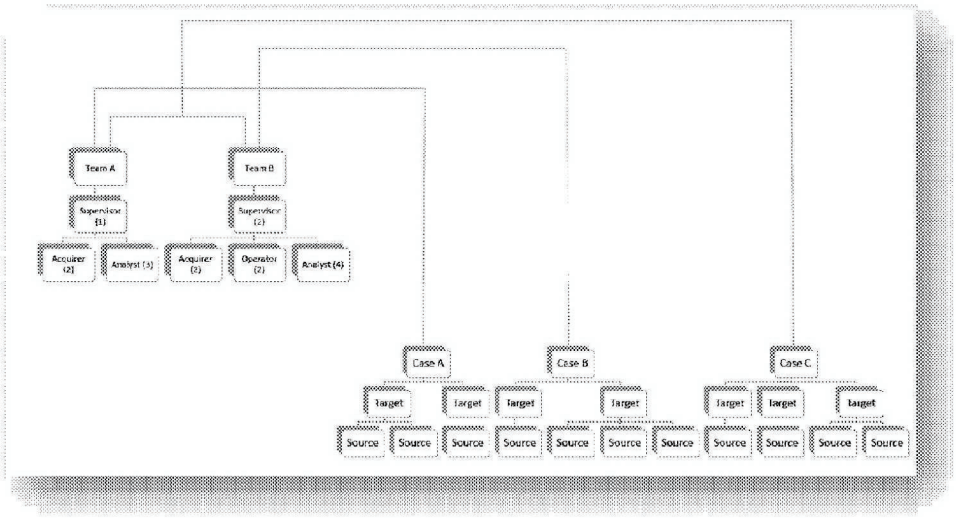
Pegasus organizes collected data according to mission cases—each case holds at least one target or person of interest.

A target may possess one or more devices. Your organization can collect data from all of them by installing an agent on each of a target's devices.

The system is designed to support compartmentalization. Access to case data is based on the roles held by the various team members—supervisor, operator, analyst, and acquirer.

The below diagram sets out the following situations:

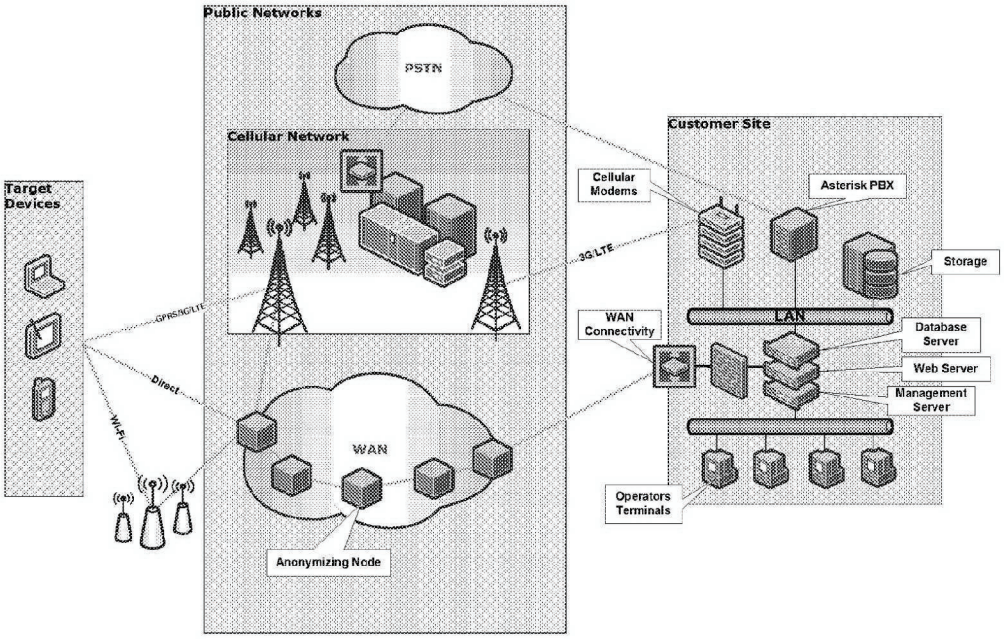
- Team A investigates Case A.
- Team B investigates Case B.
- Both Teams A and B investigate Case C.



Cyber Technologies

13 SOLUTION ARCHITECTURE

The Pegasus system's major architectural components are shown in the below image.



13.1 Client Site

Q Cyber Technologies is responsible for the deployment and configuration of Pegasus hardware and software at your site—we ensure that all is functioning correctly.

The below table outlines the main components that will be installed at your site.

System Component	Description
Web server	Responsible for, • Agent installation and monitoring • Agent maintenance: remote control, configure, and upgrade installed agents • Data transmission: receive collected data transmitted from installed agents
Communications module	• Responsible for interconnectivity • Handles Internet connection to the servers
Permissions-management module	• Defines and controls features and content • User access is permitted based on predefined criteria
Data storage	• Agent-collected data is stored on an external storage device • Data backup has full resiliency and redundancy to prevent failures and downtime

System Component	Description
Server security	• All servers reside inside the client's trusted network • Client deploys security measures • Q Cyber Technologies also puts system-related security measures in place
Hardware	• System's standard hardware is housed in racks and installed on multiple, connected servers • Responsible for advanced load balancing, content compression, connection management, encryption, advanced routing, and highly-configurable, server health monitoring
Operator terminals (PC)	• Main tool used by operators • Used to activate the Pegasus system, initiate installations and commands, run investigations, and manage collected data
Pegasus application	• User interface that is installed on an operator's terminal • Provides a range of tools—view, sort, filter, manage, and alerts—which are used to handle and analyze the volume of collected data

13.2 Public Networks

The Pegasus system only requires hardware and software installations at your premises—there is no physical interface with local MNO.

However, since agent installations and data are transferred over public networks, Q Cyber Technologies ensures that the data is transferred efficiently and securely to your servers.

Anonymizing Network

The ATN is built from anonymized connectivity nodes spread over worldwide locations; they enable agent connections to be directed along varying paths before reaching the Pegasus servers. Anonymized nodes serve only a single client who can choose to manage their setup.

See Section 7.3 Anonymizing Transmission Network for more information.

13.3 Target Devices

Pegasus' architecture allows operators to issue new installations, and monitor, actively collect, and extract data from targets' devices.

Note: Pegasus is a mission-critical, intelligence system that maintains full redundancy in order to avoid malfunctions and failures. The system, which handles data and traffic on a 24/7 basis, is scalable to support client growth and future requirements.

Cyber Technologies

14 SYSTEM SETUP AND TRAINING

Q Cyber Technologies sets up the Pegasus system and trains your users before handing the system over to you.

14.1 System Setup

Pegasus is a turnkey solution whose system setup includes the following:

- Operating-environment
  - Client is provided with prerequisites that must be prepared
- Deployment:
  - Normally requires 15 work weeks
  - Q Cyber Technologies' personnel deploy Pegasus at the client's site
  - Setup includes hardware and software installations
  - Meeting end-user agreement particulars (e.g., adaptations) as well as client regulatory and technical environments

14.2 System Training

Once Pegasus is installed, Q Cyber Technologies personnel conduct a series of training sessions—these can take place at your site, another location, or at Q Cyber Technologies' headquarters.

The number of trainees in a session is in direct proportion to the number of operator stations.

Training content includes the following:

- Basic and advanced system usage
- Operational case management
- Web intelligence and social engineering
- System security
- Operational simulation exercises
- One-on-one, hands-on exercises

14.3 High-level Deployment Plan

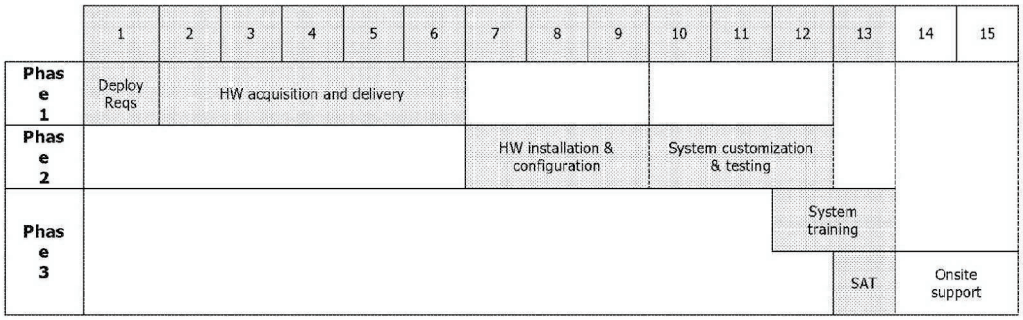
The deployment process—at your site—involves three phases:

- Phase 1 (P1): Preparations
- Phase 2 (P2): Implementation
- Phase 3 (P3): Training and Commissioning

P1	Preparations	• Analyze system deployment requirements together with the client • HW and SW acquisition, delivery, and arrival to the client's premises
P2	Implementation	• HW & SW installation and configuration per the client's contract • System customization and adaptation to local networks and devices • System testing
P3	Training & Commissioning	• Detailed system training; including practicing real-life scenarios • System Acceptance Test (SAT) by the client • Onsite support for the first two working weeks of the system

Week

Cyber Technologies



14.4 System Acceptance Test (SAT)

Q Cyber Technologies has extensive experience installing and implementing our Pegasus system.

The System Acceptance Test (SAT) covers the following:

- Sets out the scope of work
- Describes the approach and tests to be performed to validate agreed-upon system functions
- Verifies the system is fully functioning
- Validates that agreed-upon functionalities have been delivered and received by the client

The tests are divided into the following stages:

1. Functionality
2. Network and provider
3. Client-tailored

An official system hand over—from Q Cyber Technologies to you—is performed once the system has been deployed, tested, and used for demonstration checks.

Q Cyber Technologies

15 MAINTENANCE, SUPPORT, AND UPDATES

Q Cyber Technologies provides one year of maintenance, support, and upgrade services.

15.1 Maintenance and Support

Requests for an onsite support engineer to help troubleshoot and to take on greater responsibilities will be evaluated per client.

SW upgrades	• Periodic SW releases add new features and capabilities, and fix bugs • New upgrades are coordinated with the client to minimize system downtime
SW hotfix	• Dedicated SW package to fix critical bugs (unrelated to periodic SW upgrades) • SW hotfixes are provided when a new OS version is introduced for a specific platform; [Redacted – Export Controlled]
Health-monitoring system	• Connected 24/7 to the support team's NOC • Monitored by a system configured to perform the following: – Connect all major HW components and provide system's health status in real time – Monitor SW components (e.g., tunnels and 3rd party services) and send alerts if a service is down or will be affected due to technical and/or white balance reasons – Alerts for all security incidents relating to the system
NOC 24/7 tier support	• Tickets are submitted by phone, secured website, or email • NOC representatives follow support procedures to ensure each ticket is handled according to the SLA

Tier 1	Tier 2	Tier 3
Company-trained engineer provides support. • Support includes: – SW & HW installations – Upgrades – Basic troubleshooting – Configuration changes – Operation optimization	Field Service Engineer (FTE) provides proactive, best-effort support. • Dedicated engineers inspect, examine, and resolve common technical issues • If required, remote assistance is provided via remote desktop SW and a Virtual Private Network (VPN)	Technical support engineer provides support. • Support activities include all those associated with Tier 1 and Tier 2 plus, – In-depth system instruction – Advanced diagnostics – R&D-level troubleshooting

15.2 Upgrades

Our Company releases major upgrades approximately every quarter; these upgrades include,

- New features
- New devices/OS support
- Bug fixes
- Client-tailored features

Cyber Technologies

16 ABBREVIATIONS AND ACRONYMS

Abbreviation	Description
ATM	Asynchronous Transfer Mode
ATN	Anonymizing Transmission Network
BBM	Blackberry Messenger
C&C	Command and Control (server)
CID	Cell ID
CSV	Comma Separated Value
dBm	Decibel (referenced to milliwatts)
ESEM	Enhanced Social Engineering Message
FSE	Field Service Engineer
GB	Gigabyte
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HW	Hardware
ID	Identity
IM	Instant Messenger
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
Redacted –Export Controlled	
IP	Internet Protocol
ISP	Internet Service Provider
JSON	Java Script Object Notation
LAN	Local Area Network
LI	Lawful Interception
LTE	Long-Term Evolution (3GPP/4G)

Abbreviation	Description
MB	Megabyte
MCC	Mobile Country Code
MITM	Man In The Middle
MNC	Mobile Network Code
MNO	Mobile Network Operator
N/A	Not applicable
NOC	Network Operations Center
OS	Operating System
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
R&D	Research and Development
SAML	Security Assertion Markup Language
SAT	System Acceptance Test
SD	Secure Digital
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SMS	Short Message Service
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SW	Software
UI	User Interface
URL	Uniform Resource Locator
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network