Security Operations Center (SOC) Design Considerations 2018/11/01

Mission

To provide an effective, pragmatic, constant and comprehensive overwatch of the client's area of operation, exploration, and/or interest using the best practices, protocols, methods, and technologies of intelligence, and to safeguard the distribution, transmission, and storage of information and data gathered in the overwatch process.

Threats

The process of providing an effective, pragmatic, constant and comprehensive overwatch of the client's area of operation, exploration, and/or interest will be in direct conflict with many of the intentions and interests of other actors in the same space. These include, but are not limited to: nation-states, non-native embedded nation-state actors, non-nation-state actors, terrorists, and both internal and external corporate espionage. In addition, the actual physical environment, weather, and limited regional infrastructure present a real and significant threat to day-in/day-out operations.

Best practices

Best practices will be based on the belief that the SOC will operate in an increasingly hostile environment with active attempts to disrupt, defeat, compromise, or destroy the facility. Within the context of this environment, best practices will include a deliberately difficult to detect architecture with a non-conventional "flattened" structure leveraging COTS components, a robust rapid replace/repair/" bug-out" capability with a high redundancy in backup storage, and deliberate cyber countermeasures.

Intelligence sources

Sources for the SOC will include, but not be limited to: OSINT, HUMINT, IMINT, MASINT, GEOINT, SIGINT, mission-specific sensors, and surveillance assets.

OSINT (open source intelligence) – will be developed from area-of-operations-(AO) specific media sources, including social media and international media sources. Where applicable, additional dark web material will be developed to augment the OSINT material.

HUMINT (human intelligence) – will be developed from area-of-operations-(AO) specific individuals and groups and from international individuals and groups. Where applicable, additional dark web material will be developed to augment the HUMINT material.

Passive HUMINT will be gathered from social media monitoring for client-specific references with subsequent drill-down on sources, as appropriate.

Active HUMINT will be gathered from a deliberately deployed reward-based open-source surveillance network (Infinite-Eyes).[1]

IMINT (image intelligence)

Passive IMINT will be gathered from social media monitoring for client-specific references with subsequent drill-down on sources, as appropriate.

[1] https://leantaillabs.com/os-surveillance

Active IMINT will be gathered from a deliberately deployed reward-based network (Infinite-Eyes).

MASINT (measurement and signature intelligence)

Passive MASINT will be gathered from open and contracted surveillance assets and from "organic sensors" derived from social media postings, webcams, etc.

Active MASINT will be gathered from client-controlled mission-specific surveillance assets.

SIGINT (signal intelligence) – advanced signal intelligence will not be a part of the SOC but will be provided by external sources. cellular signal capture and monitoring will be employed.

Mission-specific sensors – sensors developed for the client to address specific needs in petroleum development and production, logistics, and storage.

Surveillance assets – other contracted and allied surveillance assets will be accessed by the SOC as determined and directed by the client.

Technical doctrine

The doctrine for technology will be COTS-based, will be deployed in a lean/nimble manner with a minimum digital or physical "footprint" that can be deployed in 24 hours, taken down in 12 hours, and in an emergency, can have critical/sensitive elements removed within 1 hour. The elements and infrastructure will include active and aggressive security countermeasures at a high level of granularity.

Commercial-Off-The-Shelf – for reasons of cost, support, and speed to deployment, almost all elements and infrastructure will be commercial-off-the-shelf products. As a functional rule, if it cannot be acquired and/or shipped from a "big box" store, it is problematic. Further, for reasons of security and robustness, no single vendor or product line will function for the full infrastructure architecture.

Lean / Nimble with minimal digital or physical "footprint" – the elements and infrastructure will exist in a "sealed" WiFi environment and will communicate by WiFi within that environment. External to the "sealed" environment, active monitoring and WiFi spoofing will be deployed. This eliminates cabling, hubs, switches, etc., and allows for the constant monitoring of all digital communication and relies on "shared drives" on devices in contrast to conventional servers.

Active cyber security at a high level of granularity – the architecture is deliberately "flattened" to use COTS desktop defenses/mitigations in contrast to server-targeted defense/mitigation tools. Operating at a higher cycle of detection/mitigation in service to the end-user market, and at a lower price-point, this moves potential threats outside the range and methods of conventional server-targeted attacks and leverages the rapid detection/mitigation cycle provided by COTS desktop solutions.

By making every machine a 'warrior', the structure provides a high degree of granularity in the defense architecture. Push transmissions of activity logs from all devices will be subject to automated monitoring and review by the cyber detection/defense elements. In parallel, to address insider threat, the granularity includes dual authentication (knowledge/token) for access to any device within the "sealed" environment with a push of the access logs, AES 256 encryption, and a MAC address. A white list will be maintained for all devices within the SOC.

The cyber detection/defense elements will include "honey pot" traps, "hard-crackers," and other active cyber countermeasure tools at the DMZ level of the architecture and external to the "sealed" WiFi environment. Using DNS addresses closely associated with the actual functioning

DNS addresses, the countermeasure systems in the DMZ and external to the “sealed” WiFi environment will act as both deterrents and detection systems. WiFi monitors external to the “sealed” WiFi environment will be used to detect any unauthorized transmission from or around the SOC.

24-hour set-up/12-hour tear-down/1-hour bug-out capability – using a “sealed” WiFi environment, dual authenticated devices, and a flattened architecture, the deployment/tear-down/bug-out tempo is significantly accelerated. In the most extreme case, a “bug-out” would involve the movement of 10 laptops and one encrypted multi-terabyte drive, and the encryption lockdown of all the other assets.

95% solution – the SOC is not designed to meet every operational need, but it will operate as a robust “SKIF-like” environment with external non-secure meeting rooms, cell phone privacy rooms, and other facilities external to the SOC.

Elements

The elements of the SOC are built upon, and consistent with, the defined mission, threats, best practices, intelligence sources, and technical doctrine. Further, the SOC elements are modular and scalable across the full mission of the SOC. The elements include two or more analyst monitoring groups, a shared common operating picture (COP), on-site data storage and internal communication management capability, voice over IP phone communication (VOIP), external communication and cyber threat detection/defense, and off-site cloud-based storage.

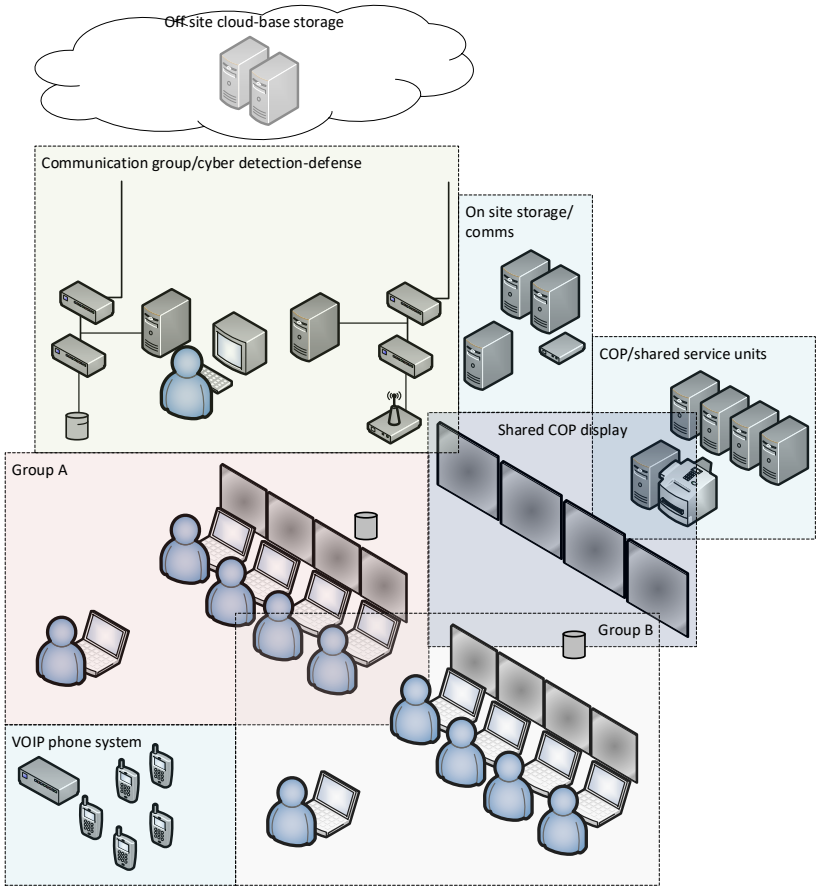

Figure 1 - Elements of the SOC

Analysis monitoring groups –using laptop-based work stations with secondary larger displays, the members of the analysis monitoring group are specialists in one or more geospatial areas with in-depth understanding in specific industries and/or client areas of interest. Any data displayed on any analyst's work station can be "cast" to a segment of the shared COP display. All work stations are protected with 2-part authentication (knowledge/token). A monitor/editor/ad-hoc fill-in substitute provides overwatch and coordination for the group. All platforms will have AES 256 encryption.

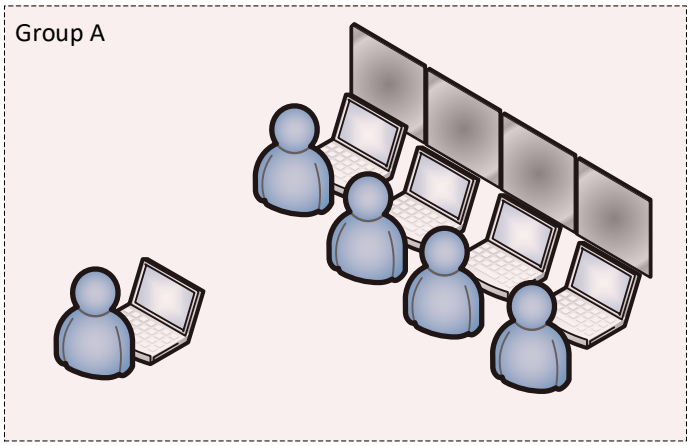

Figure 2 Analyst monitoring group

Shared COP display – the shared COP display is designed to facilitate immediate and constant situational awareness in the SOC. Built from COTS displays equipped with "cast" dongles, any display panel can receive casts from any analyst's work station. Normally the displays present an overlapping geospatial common operating picture (COP) of the client's area of interest. Feeds for the COP are sourced from the COP/shared service units and are based on a geospatial platform agnostic "marble/pebble" model.[2]

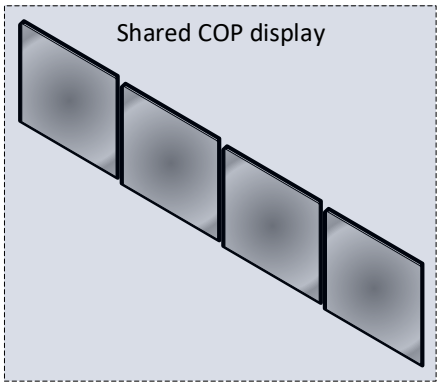

Figure 3 - Shared COP display

COP / shared service units – the units are the repositories for the layers of the COP, the receivers/interpreters for geospatial specific data feeds, and management engines for the printers/scanners/fax unit/s. Any unit can cast to any COP display and any unit can "lace" multiple

[2] https://leantaillabs.com/isocs-cop

displays for a single display on the COP. Under normal operations, a single unit is dedicated to the laced display on the COP. All platforms will have AES 256 encryption.

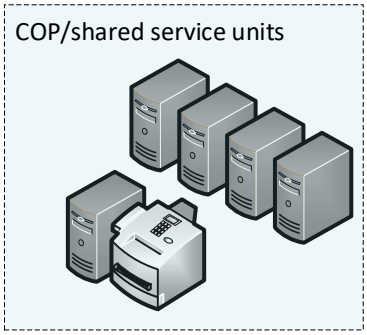

Figure 4 - COP/shared service units

On-site storage and comms – the units will track and store all data and communications including emails, systems configuration, reports, etc. Where appropriate, data will be stored in an open source massively parallel database with high cross-platform redundancy (example: GreenPlum).[3] For larger documents, the document index and blockchain encryption of the documents will be stored in the database with multiple copies of the documents in the on-site storage and the parallel off-site cloud-based storage.

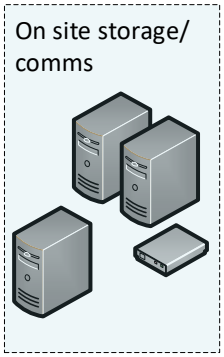

Figure 5 – On-site storage/ comms.

VOIP phone system – phone service within the SOC will be via VOIP on both desktops and on handset units. All platforms will have AES 256 encryption.

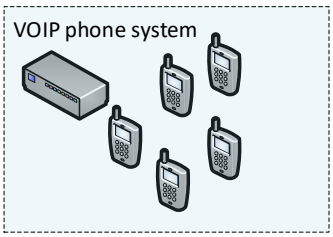

Figure 6 - VOIP phone system

[3] https://greenplum.org/

Communication group / cyber detection-defense – all Internet communication will be through a parallel pair of equivalent firewalls, detection/monitoring systems with transmission into the SOC via a multi-frequency/multi-channel WiFi architecture. Integral to the cyber detection defense will be monitoring platforms for OSSIM (open source security information and event management) and Open VASS (vulnerability assessment system) monitoring/analysis. The units will also monitor for log on/off data, persistent outbound data, etc. Further, the systems between the firewalls will be equipped with "honey pot" traps, "hard-crackers," and other active cyber countermeasure tools.

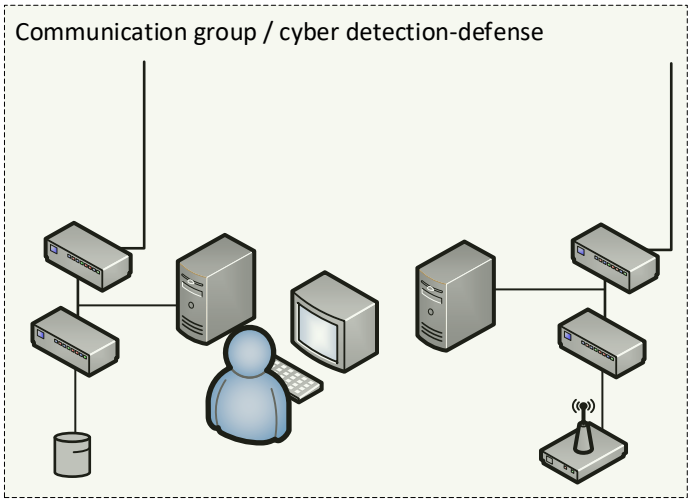

Figure 7 - Communication group / cyber detection-defense

Off-site cloud-based storage – encrypted off-site storage will be cloud-based with duplicate/redundant platforms and geolocations as supplied from two or more vendors.

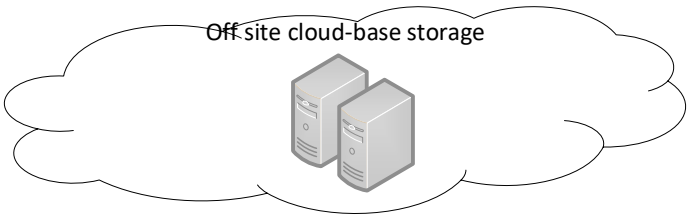

Figure 8 - Off-site cloud-based storage

Because the SOC elements are modular and scalable across the full mission of the SOC, the "plus-up" cost of adding to the SOC is predictable and based on known cost. In addition, the sealed and secure WiFi environment allows the nimble integration of units on an as-need basis. In short term expansions, this means faster ramp-up of capability and a predictable costing profile.

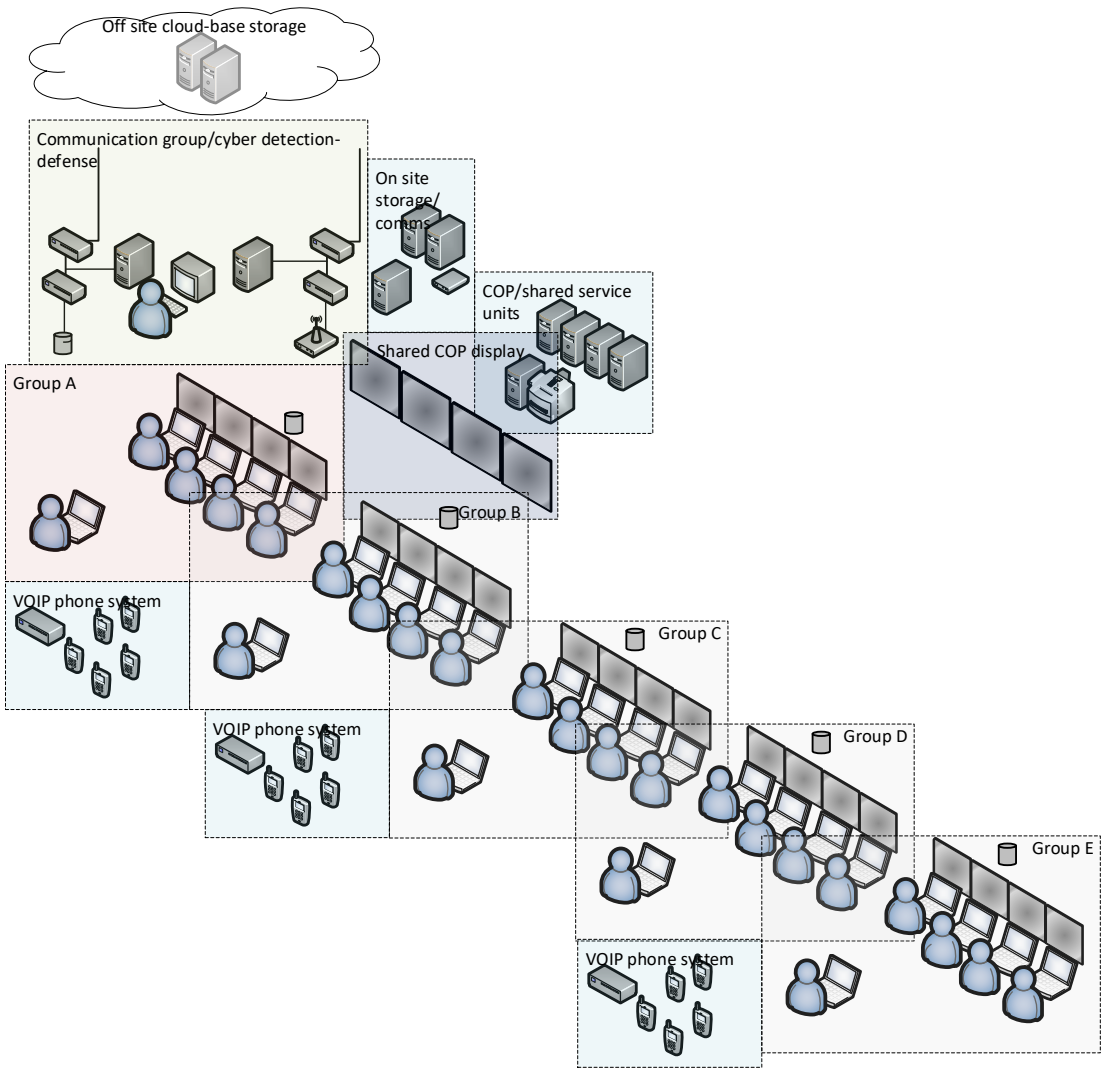

Figure 9 - Expanded SOC

Products

In coherence with the mission or providing an effective, pragmatic, constant and comprehensive overwatch of the client's area of operation, exploration, and/or interest, the products will be defined, created and distributed based on the needs of the client.

Immediate first-person sourced "FLASH" traffic via voice/text – generated on an immediate as-needed basis by any member of the monitoring/analysis group and delivered by voice and/or text, the intent of the product is to provide immediate actionable intelligence of situations, events, or actions with a high probability of significant impact on the targeted area of interest. Typically, the product will be hyper-local, will include an assessment of the anticipated impact, and will include the source of the intelligence providing the basis for the product. This is an exception to routine products and reflects both urgency and importance.

Immediate first-person sourced text - generated on an immediate as-needed basis by any member of the monitoring/analysis group and delivered by text, the intent of the product is to provide immediate actionable intelligence of situations, events, or actions with a high probability

of impact on the targeted area of interest. Typically, the product will be hyper-local, will include an assessment of anticipated impact, and will include the source of the intelligence providing the basis for the product. This product is the standard for normal communication of actionable intelligence.

Daily listing of "INT" material with prioritization by "INT" manager – generated once a day prior to the first work shift in the client's area of interest, this product is a general summary of the intelligence of the previous 24 hours and is to ensure a consistent level of situational awareness across the client's area of interest.

Weekly listing of analysis metrics, scheduled, and anticipated events – generated once a week at the beginning of the work week, this is an analysis and anticipatory product providing a general review of trends and a forecast of events internal and external to the client's efforts and area of interest.

Monthly summary of trends and scheduled events – generated once a month at end of the month, this is a comprehensive summary of events and trends with analysis. The product is to provide situational awareness for the month with analysis of critical data.

Geospatial flicker – generated by the placement of reported events, environmental events, etc., on the common operating picture, this product can be moved forward and backward chronologically to assess the geospatial profile of events and trends over time.

Sensor communication architecture

The sensor communication architecture will address the needs of very large-site deployments, medium sites with personnel, small sites with occasional personnel presence, mobile surveillance on land and sea, and remote areas. Although not an integral part of the SOC, the sensor communication architecture will provide critical data to the SOC and to allow the SOC to perform surveillance overwatch.

Communications

Cellular communication covers most of the world, and in many developing nations cellular connectivity and coverage exceed the coverage available in developed nations. Where there is no reliable cellular communication, a combination of a wireless mesh architecture and a satellite uplink will be deployed.

Sensor elements

The suite of sensor elements includes: stand-alone weather/airborne contaminate monitor units, stand-alone special mission sensors for industry-specific sites, event-driven surveillance devices, sensors and short-range 360 camera units, sensors and long-range electro-optical/FLIR units, and fixed and mobile tethered drone units.

Industrial-specific sensor platforms – based on a ruggedized version of an Arduino-dedicated processing platform, the industrial-specific sensors detect specific chemicals in the air and/or water and can be programmed to report on a scheduled basis or an on-demand basis. Powered by batteries and/or solar panels, the units can communicate through a variety of radio and cellular protocols, including a self-healing/self-configuring wireless mesh with peer-to-peer relaying of data to centralized hubs for up-linking.

Autonomous surveillance platform (ASP) – based on a lightly modified wildlife camera and powered by battery and/or a solar panel, the ASP triggers on heat or movement, captures images in light or in infrared, and transmits the image via cellular modem. The units are capable of being remotely configured and reconfigured as needed. As the units are derived from a COTS product and designed for long-term outdoor deployment, they are both low-cost and resilient. Further, as the units only transmit on triggering events, they do not present a significant burden in monitoring or system bandwidth use.

Sensor platform with short-range 360 cameras – based on a ruggedized version of an Arduino-dedicated processing platform and equipped with a short-range day/night camera, the units can be programmed to report on a triggering event (movement in a specific area), a scheduled basis, or an on-demand basis. Powered by batteries and/or solar panels, the units can communicate through a variety of radio and cellular protocols including a self-healing/self-configuring wireless mesh with peer-to-peer transmission of data to centralized hubs for up-linking.

Sensor platform with electro-optical (EO)/FLIR cameras – based on a ruggedized version of an Arduino-dedicated processing platform and equipped with long-range electro-optical/FLIR cameras, the units can be programmed to report on a triggering event (movement in a specific area), can scan over a series of preprogrammed views, or can be remotely manipulated from the SOC. Powered by line voltage and/or batteries and solar panels, the units can communicate through a variety of radio and cellular protocols including a self-healing/self-configuring wireless mesh with peer-to-peer transmission of data to centralized hubs for up-linking.

Tethered drones – tethered drones are quad, hex- and/or octa-copters that are tethered to a base station and receive power via the tether. By virtue of the tether, the size, payload, and flight time of the drone are not restricted by the onboard power supply. Very large sensor arrays can be deployed for hours/days at a time so long as a reliable power supply is provided to the tether. The size and capability of the platforms are defined by the mission and can include electro-optical sensors, thermal, and other sensors. The platforms can either feed the control and sensor data up and down the tether or use radio and/or Wi-Fi transmission. By the available power and altitude, Wi-Fi can be transmitted over a large area providing ground assets with live feeds from the platform to cell phones and tablets. At 60 meters (200 feet) altitude a tethered drone has a to-the-horizon view of 27 kilometers (17 miles) and with a standard electro-optical/FLIR package can detect a human at 4.8 kilometers (3 miles).

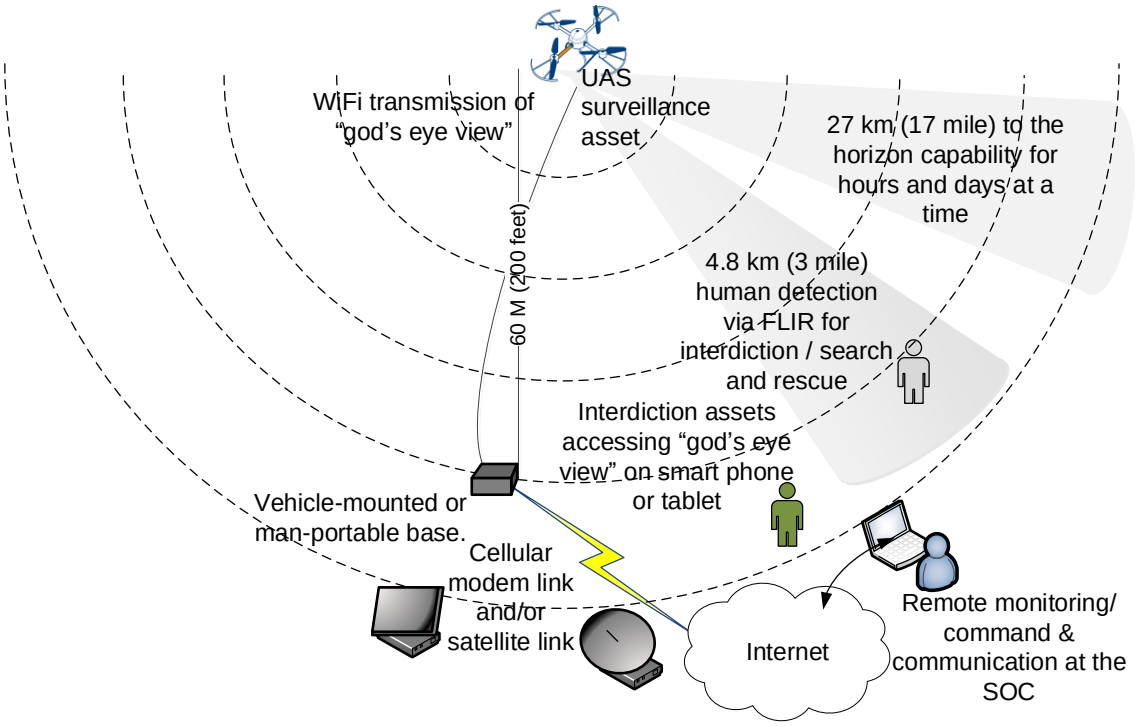

Figure 10 - Typical tethered drone deployment

The external power also allows the drones to maintain position in relatively high winds that would exhaust the power reserves of free-flight drones and would threaten aerostat platforms. By virtue of their small profile, they are less intrusive and a less overt surveillance platform. Leveraging COTS quad-, hex-, and/or octa-copter platform components, the tethered drones are low-cost and require minimal maintenance. Typically carried and launched from a 'Pelican'-like case, the drones are a single-button launch-and-retrieve system using COTS flight control software modified for a tethered platform. The tether is spooled out and retrieved automatically from the base station. As a safety precaution, the drones carry a battery to allow a controlled landing in the event of a power failure.

The best practices and methods for tethered drone use are in circumstances requiring ad-hoc sustained surveillance from a controlled base with minimal cost and minimal observable profile. They are a "best fit" for low-level, semi-covert surveillance over a sustained time. The drones can also be used over water or in desert areas and have a "follow" capability to allow them to be used from a moving sea-borne or land platform in unobstructed areas. This gives them superior littoral and desert surveillance capability.

Site specific deployment

Very large-site deployments – large-site deployments will be surrounded with a network of ASPs triggering on motion and/or heat. Images from the ASPs will be sent via cellphone and/or cell-relayed satellite modems. The ASPs will function as perimeter security for the site and will feed images directly to the common operating picture (COP) at the SOC.

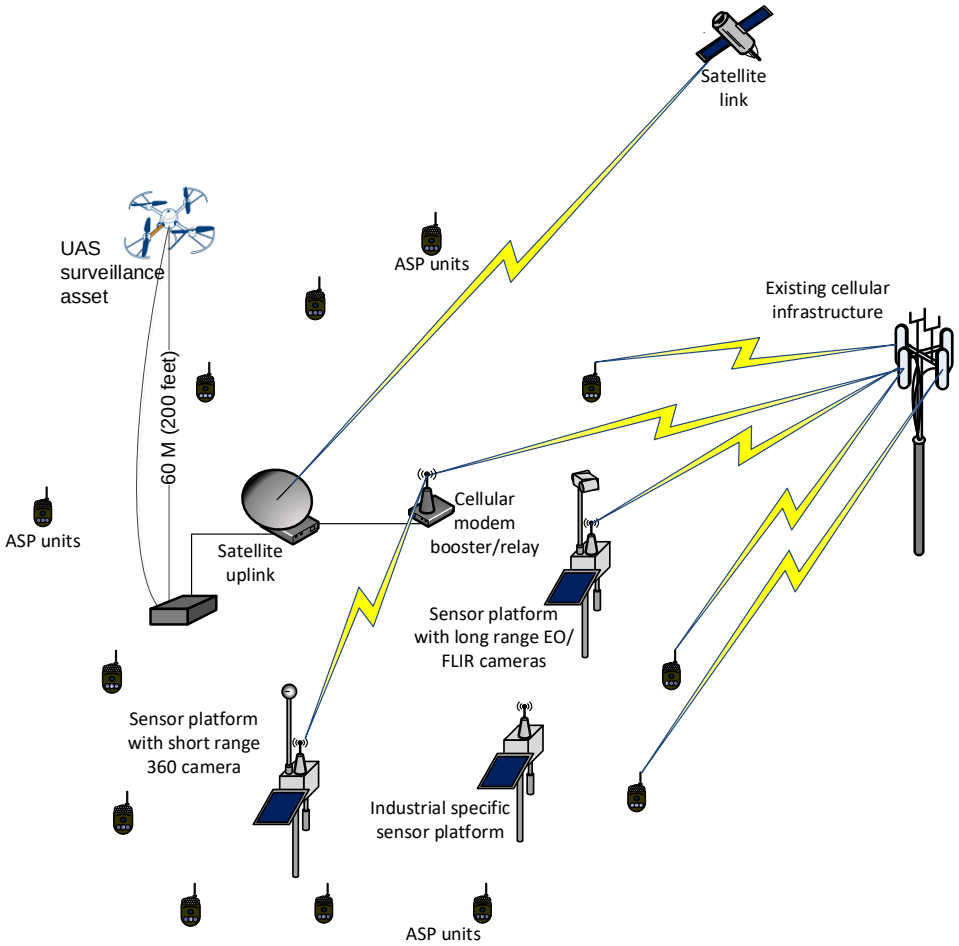

Figure 11 - Large site architecture

Within the parameter and mounted at mission appropriate locations will be a mix of short-range 360 camera units, long-range electro-optical/FLIR units, and industrial-/mission-specific sensing units. At sites where, immediate long-range sensing and detection is required, tethered auto-launch drones on fixed or mobile platforms will be deployed.

Medium sites with personnel – medium site deployments with personnel will parallel the large site deployments to a limited extent. They will be surrounded with a network of ASP triggering on motion and/or heat. Images from the ASP will be sent via cellphone and/or cell relayed satellite modems. The ASP will function as perimeter security for the site and will feed images directly to the common operating picture (COP) at the SOC. Within the parameter and mounted at mission appropriate locations will be a mix of short-range 360 camera units, long-range electro-optical/FLIR units, and industrial-/mission-specific sensing units.

Small sites with occasional personnel presence – As with the large and medium sites, similar surveillance elements will be deployed, but not at the same level of saturation. At a minimum, the sites will have a perimeter of ASP units, industrial sensors as needed, and at least one sensor platform with a short-range 360 camera.

Mobile surveillance on land and sea, and remote areas – most mobile surveillance needs will be addressed by either vehicle or sea-borne tethered drones with dedicated radio and/or satellite uplink.