ASV & CNL Software White Paper:

Detecting and Resolving Waterside Security Threats

September 2015

AUTOMATIC SEA VISION

CNL

Around 80% of the world's population lives within 100km from the coast/shoreline, consequently a large proportion of critical infrastructure has a waterside front. This paper has the sole purpose to highlight recent security breaches along these waterside fronts, to consider the challenges they pose, and to explore the technology available to help defend our coastal critical infrastructures from these threats. It continues by examining how this raw data can be translated into usable intelligence within the control room.

The Challenge

On 30 May, 2015, an 11m yacht with five crew on board crashed on the rocks by the Southern track, Nice Cote d'Azur international airport (NCE), France. Only one member of the yacht crew was injured and was rushed to the nearest hospital. After forensics examination this non malicious incident was classified as a genuine navigation error. The boat had entered an area where sailing is forbidden and where a monitoring solutions was supposed to be operating 24/7 in order to comply with the international airports regulations.

All airports are required to prevent any unauthorized entry in their perimeter at any time, from both land and sea. This is not an isolated incident, a similar instead took place at JFK airport not too long ago.

Following 9/11, security measures have been reinforced at international airports to prevent security incidents. However, security breaches at the maritime border are still a common threat to this type of critical infrastructures. Furthermore, such security threats are not common only at airports, but can occur at any critical infrastructure site and the consequences can be financial, brand damaging and can even cost lives.

About 70% of the Earth's surface is water-covered, and the most densely populated areas on Earth are by the coast. As a result, a large proportion of critical infrastructures are based along a waterside border, and the examples mentioned above showcase how weak coastal security could be without suitable levels of protection.

Detecting Waterside Incidents

As the above incident demonstrates, waterside security is a colossal challenge. Often the extent of vulnerability is underestimated, due to lack of awareness of the threats that an organization is exposed to. When it comes to waterside security risks in today's world, organizations inevitably will rely on: Physical Perimeter Protection, Maritime electronics and Human surveillance. Nevertheless, these types of techniques and technology can be breached as they have their own inherent weaknesses.

Physical Perimeter Protection

The illusion: Users think they are well protected by a physical obstacle

The reality: Once a waterway has been crossed, often offenders are easily able to breach fences undetected by NEITHER the general public NOR security operatives. A weapon like an RPG can also be activated before reaching the shore.

Maritime Electronics

The illusion: Electronic systems such as radars are often considered the right solution for maritime environments due to their maritime heritage.

The reality: Radars are usually very good at detecting long distance large metallic objects, however, inefficient at short distance detection as well as detecting small targets (e.g. : polyester boats, humans, swimmers & frogmen). Maritime electronics will also provide very limited interface capabilities with non-maritime systems. They have been designed and developed for maritime usage by seamen, and do not give the best of themselves in on shore based critical infrastructures environments.

Human Surveillance:

The illusion: An operator in the control room will easily detect intrusion from the waterside.

The reality: Human surveillance will only be efficient in small environments, when the operator is not distracted by having to perform other duties, and only when the weather is good. The operator will quickly become inefficient if having to monitor numerous cameras; if the weather is bad; or if the operator is distracted by other duties and is unable to monitor the cameras. Indeed, human surveillance is not the worst of solutions when it comes to intrusion prevention from the water side, however, it must be enhance with suitable cameras and supported with specially developed and installed Video Content Analytics (VCA).

Aggregating Information Sources

In terms of safety, an aggregator such as PSIM will be the only solution to provide control room operators with a comprehensive real-time view of the situation and help the operational team to address any security risks. The availability of the most current, the most accurate and above the most comprehensive and reliable intelligence becomes essential to achieve the goal.

The addition integration of an automatic VCA will also allow the PSIM platform to deliver the right information at the right time in order to support operators' decision making, which during a time of crisis is vital.

The addition of correctly added "metadata" to the video stream can further support PSIM to make the correct decision. Without a suitable VCA, a camera used on its own, even if equipped with the best motion detection, will not be able to provide the depth of capability required to detect the subtle changes in a camera scene needed to detect maritime threats. The more relevant, the more complete, the more accurate and continuous in time the information is, the more the PSIM platform will gain in right reaction support.

Usable Intelligence

A good VCA system should be put in place in order to provide a stream of information to the PSIM regarding each detected object. This type of information could be items such as: distance, azimuth, speed, size, GPS position. Having access to these details will ensure operators are able to efficiently calculate potential risks and threats.

In addition, the PSIM can instantly correlate data points with other information from other sources, such as Vessel Traffic Systems, patrol schedules. Once the PSIM is alerted to a threat, the platform will have the ability to ingest and correlate information. This information will be converted into usable intelligence that will strengthen the organization's security posture.

Within split seconds of an information raised from the VCA, the PSIM could query databases such as patrol boats or friendly vessels and filter the alarms coming through to the control room based on this. It means operators only need to focus on the small number of "exceptions" to the pre-programmed processes in the PSIM.

From here a PSIM can allow the control room to dispatch patrol teams, inform national security agencies, evacuate an area, or any number of processes that an airport or critical infrastructure may be required to do to resolve a water side security threat.

Summary

When it comes to critical infrastructure security, there is a significant difference between waterside security and land based surveillance. Water, by its nature, is constantly moving, creating waves, foam, tides and glare, which can be a cause for traditional surveillance systems to create a false alarm. The combination of a powerful dedicated VCA and an intelligent PSIM solution can bring significant differences to the detection and resolution of security breaches. Together, the two security platforms/systems can ensure the best outcome based on usable intelligence within challenging waterside security environments.

About ASV

AUTOMATIC SEA VISION (ASV), the first video content analytics (VCA) software editor 100% dedicated to marine environment, has a unique off-the-shelf solution for waterborne object detection, adding an unmatched capability to automatic surveillance systems for situation awareness on the waterside, security project in ports, coastal infrastructure (sea, lake or river) and offshore platforms.

ASV's unique technology is based on the expertise of a multi-skilled team of engineers, researchers and sailors, with a combined total of more than 40 years of experience in maritime video surveillance. For more information, please visit www.asv.fr/en

About CNL Software

CNL Software is a world leader and global provider of Physical Security Information Management (PSIM) software, designed for complete Integrated Situation Management. Our award winning PSIM technology is deployed to secure major cities, critical infrastructure and global commerce.

CNL Software's IPSecurityCenter PSIM solution sits at the heart of some of the largest, most complex and groundbreaking security integration projects in the world. Our work with leading organizations is helping to shape the future of security by offering thought leadership on key issues such as asset protection, energy reduction, process compliance and business advantage in converged physical environments. For more information, please visit www.cnlsoftware.com

Contact Us

ASV France

65, rue de la Garenne

92 310 Sèvres

France

Tel : +33 1 41 15 94 20

ASV Asia Pacific

Malaysia Office

Tel : +60 126 853 064

Email: contact@asv.fr

AUTOMATIC SEA VISION

www.asv.fr