Submarine Cable Infrastructure Defense Against Terrorist Aggression [1]

by

Robert Bannon, President
Bannon International Consulting LLC
P.O. Box 456
Tannersville, PA 18372

and

Douglas Burnett, Partner
Holland & Knight LLP
195 Broadway
New York, New York 10007

***Abstract* - #188**

As a result of the September 11, 2001 attack on the World Trade Center and subsequent terrorist related events through 2003, the focus of government agencies and multi-national corporations has been the protection of human life, the world economy, and infrastructure security and defense. In the United States, this is evident by the creation of the U.S. Department of Homeland Security in January 2003 and the similar restructuring of allied anti-terrorist efforts to prevent the occurrence of further catastrophic events in their countries. Immediate actions have been taken that are resulting in the overhaul of airport, harbor, and transportation security, ranging from advanced surveillance to active defense of vital infrastructures to prevent disruptions of services, such as global communications and the internet. A key element of terrorism countermeasures is the collection and timely evaluation of data which may forecast or thwart terrorist actions. Today, use of underwater fiber optic communications cables is the preferred technology to provide inexpensive, secure voice and data transport throughout the world. By definition, undersea cable systems, used for telecommunications, military surveillance, electrical power distribution, scientific monitoring of oceans or subsea oil and gas distribution pipeline monitoring are within the purview of the Department of Homeland Security. These critical assets have drawn the attention of terrorists; therefore, the underwater community, as well as the Information Analysis and Infrastructure Protection (IAIP) directorate, must continue to exercise pro-active security to prevent catastrophes from occurring from what must be considered a nameless and daring enemy. Therefore, protection planning and implementation for underwater systems technologies, cable stations, terrestrial backhaul facilities, maritime resources and cable ships are undergoing major refinements to safeguard against acts of terrorism and to provide secure restoration. In addition to government efforts, the International Cable Protection Committee (ICPC} considers recommendations for security enhancements for the individual facility owners and operators. Efforts including the implementation voluntary security plans by the American Petroleum Institute ("API") for off-shore structures and the American Chemical Counsel ("ACC") for the chemical manufacturing and transportation industry demonstrate that private industry is a key player in national anti-terrorism defenses. Pro-active support roles are evolving for new Unmanned Marine Vehicles (UMV), that encompass Unmanned Underwater Vehicles (UUV), Remotely Operated Vehicles (ROV), and Autonomous Underwater Vehicles (AUV) and the evolving hybrid Unmanned Surface Vehicles (USV). These maritime robotic vehicles are capable of supporting faster, more accurate surveys, deeper burial of fiber optic systems, advanced cable locating technologies, and expanded subsea surveillance. Risk assessment of theatre specific events has resulted in the demand for Unmanned Surface Vehicles (USV) patrolling littoral areas and critical subsea infrastructures. This paper addresses the evolving subsea infrastructure protection environment, representing industry, governmental, and judicial positions on infrastructure defense. It also addresses preventing physical aggression risks to vulnerable underwater infrastructure by implementing new sensor suite developments and maritime surveillance considerations.

Response to Terrorism

America's immediate response to the October 12, 2000 attack on the U.S.S. Cole (DDG67) as it sat in the Aden, Yemen port was one of outrage and disbelief, but as time passed this terrorist attack faded from the minds of the general public as Americans went back to their lives. It was not forgotten by the families and friends of the 17 who died and the 39 injured while waiting refueling in a foreign land. It was not forgotten by the U.S. Navy or the President. In the end though, the United States hunted for the terrorist cells responsible for this act, and the Navy re-fortified its vessel force protection and foreign and domestic port security. Then as smoke and clouds of ash rose from where the World Trade Center towers once stood, Americans realized that we were under attack by a dauntless and ruthless enemy like no other that we have ever faced

[1] The opinions expressed herein are the personal views of the authors and do not represent the views of the Office of Homeland Security,the Department of Defense, or The International Cable Protection Committee (ICPC).

on U.S. soil. We were on that day, and every day since, facing human instruments of rage, filled with the ideology that America and the West are corrupt and must be brought to its knees, even at the cost of their own lives.

The U.S. Intelligence Agencies have been accused of overlooking pertinent facts and information that streams into that community on a daily basis. Their analytical computers and the networks which link them together were described by "Feds Online" as being "woefully outdated computer systems". Had the United States overlooked telltale signs and salient information that could have led to the prevention of these catastrophic events? We, in the United States, are now focused on the use of sophisticated technologies and robust communications networks to provide advanced screening of the volumes of data arriving daily, and to support investigations and official communications should future calamities of this magnitude occur again anywhere in the world.

Information access is critical for preventative security measures as well as to the post disaster control environment. For example, preventative security measures for airports, harbors and land-based transportation hubs would include global biometric identification systems, including face, handprint, fingerprint and retinal scanning technologies as well as cargo bar-coding which also provide material handling identification records and a bill of lading. Further biometric identification techniques could include national ID smartcards for all individuals, especially those accessing critical infrastructures, such as port ISO container storage areas. These all require fast, efficient fiber optic links for the transfer of data in a "close to real-time" global environment. For these communications links to be effective worldwide, they require protected underwater fiber optic systems that transport data between continents, and secure interfaces to backhaul facilities for terrestrial distribution to harbor masters, customs and others that require immediate and timely access to the type of data that could be provided.

Telecommunications has long been considered the life blood of major customers, providing pertinent information to multinational corporations. Therefore these major customers, and consequently the telecom service providers, have escalated the priority of their concerns about infrastructure security and the resultant chaos caused by a major breach. There has been a joint focus by owner/operators and the large system users directed at network redundancy, route diversity, and survivability of the customer privileged and confidential data. Physical security always existed at switching centers and facility offices, and it has expanded to include remote security access to cable stations and landing sites. In addition to identify personnel in the station, these security systems rely on remote monitoring technologies to protect the fiber optic networks and the system interrogation station provides restoration routing instructions for attending personnel in times of service interruptions. Today, because of the use of advanced multiplexing technologies, such as Wave Division Multiplexing (WDM) and Dense Wave Division Multiplexing (DWDM), system circuit capacity and bandwidth has increased almost exponentially, creating the demand for increased system protection. Therefore, there is increased system monitoring requirements to ensure system reliability and with the use of control technology, there exists a greater dependence on centralized monitoring and information processing at Network Control Centers responsible for restoring critical services, if a fault occurs. Before the terrorist events of the past several years, telecommunications companies' efforts were directed towards protection from cultural aggressions, such as trawling activities and anchor drags, and not toward intentional wide-scale sabotage. The realization of possible attacks on maritime infrastructure has caused the U.S. Coast Guard, which is now part of the Office of Homeland Security, as well as the facility owners and operators, to re-assess their existing protection strategies for submarine fiber optic cables. Jointly, government agencies and the service providers have taken steps to reduce the potential vulnerability of these communications systems. The IAIP directorate in the Department of Homeland Security is also focusing on possible terrorist threats to depots, harbors, ports and underwater approaches for oil and gas pipelines and power distribution cables.

Homeland Security Partnership with Commercial Telecom Enterprises

America and the world has matured rapidly in the glow of the burning towers; innocence and our sense of naïveté being forever lost, and turning us now into skeptics and realists. Terrorism is no longer looked at as something that happens abroad in Beirut, Northern Ireland or in a third world country, but it is a reality experienced in the streets of America. It doesn't discriminate by gender, ethnic origin, or wealth; it has the potential of touching or destroying all of us. Therefore, the government agencies, the public and private sectors have emphasized the urgency to assess our vulnerability and to prepare for, prevent and respond rapidly to future terrorist activities.

With the realization that government alone can not accept the burden of infrastructure protection, multi-national enterprises, both individually and collectively through trade associations, are stepping up activities to face the myriad of critical challenges including the following:

- Define potential vulnerability of communications infrastructure to both external or internal attack, that can result in the loss of the circuit capacity and needed availability.

- Infrastructure site / facility hardening, and restricting personnel access to appropriately cleared and personnel with badges.

- Development of preventative security measures, systems, and processes that counter the likelihood and impact of an attack.

- Institute extensive behavioral modifications and training of station personnel to recognize potential threats.

- Institute extensive procedural modifications and training to prevent unauthorized observers being able to record personnel movement, shipping, and staff schedules. This includes random schedule implementation.

- Establish procedures, processes, and systems to ensure business continuity in case of service interruption.

- Development of detailed restoration plans to reroute service to alternate facilities and minimize financial impact.

- Integrate current and emerging sensor technologies into system operations to detect and/or prevent the occurrence of a critical event, and to facilitate rapid restoration to system normalcy.

- Develop and implement technology replacement strategies to ensure that security systems are maintained at a "state-of-the-art" level of monitoring efficiency. This includes implementation of monitoring that prevents hackers from crashing a system by evasive behavior, obstructive software, or new technology enhancements.

- Development and implementation of Industry Standards and recommendations, such as those issued by the International Cable Protection Committee (ICPC) or other international conventions such as the CCITT to protect communications infrastructure.

Implementation of these safeguards limit the access of terrorist to sites, such as cable stations, backhaul facility locations and other critical infrastructure. The critical global communications network supports the twenty-first century personal, business, medical, and governmental data needs, therefore communications systems will receive the attention of terrorists, who intend to disrupt modern life. Therefore, we must ensure that these facility networks receive the underwater community's full attention and protection. Service interruptions of these high bandwidth underwater fiber optics communications systems result in greater than a $1.5 million revenue loss per hour. The aggressive disruption of service results in multi-million dollar repair and restoration costs, and the impact on critical data transport for major multinational industries is even greater. The impact on military, diplomatic, and government logistics can cripple personnel and support movement, therefore, emphasis on protecting global communications, especially underwater fiber optic systems from aggressive acts, is essential. Common awareness of all community interests and cross-industry requirements, have allowed the communications industry to develop protection and security that focus on preventative and anti-terrorist solutions. However, some cable owners and operators who are not members of either international organizations or private agreement clubs are not stepping up to the protection demands. Some of these parties in response to their limited finances have chosen to implement shallower and less costly burial methodologies that jeopardize cable service integrity by exposing the cable to possible faults. The shortcomings of this approach to prevention of cable faults was recently demonstrated when a specific use cable was buried out to only 200 foot water depth instead of implementing cable burial over the entire length in shallow water. In other situations of course seabed conditions, including soil density, rocks, and topography or access for future repairs, limit burial options. Failure to comply with minimum industry standards may result in multiple faults from other ocean floor community users, thus jeopardizing investor interests, and placing system integrity and reliability at risk. The non-compliance with industry norms increased the probability of service interruptions experienced on the system. And, in fact, due to high activity in the vicinity of the cable, the fiber optic system described was faulted due to anchor drags and fishing activities, luckily there were no terrorist activities identified.

The burial issue has been complicated by the relatively recent intrusions since 1999 of state coastal agencies, NOAA, and some district offices of the U.S.

Army Corps of Engineers ("ACOE") who insist on often extreme burial requirements outside of the 3NM state territorial and ACOE jurisdictions[2] in permits. This is not out of concern for the protection of the cable system, but as a response to objections from local fishing industry lobbying which perceive cables has a threat to indiscriminate bottom trawling and clam dredging.

In California and Oregon, the state, with the active support of the local ACOE district offices, requires as permit conditions that cable owners to enter into one-sided agreements with fishing groups which call for exemption of liability for damage to cables from negligence, and significant lump sum and additional annual payments of millions of dollars for the life of the cable system. In New Jersey, the state is also considering extreme burial requirements to appease the demands of the local clam dredging industry. All of these states are also requiring costly video surveys of cables on the continental shelf already laid every two to five years to determine if any cable has not remained buried.

Often state and federal agencies such as NOAA and ACOE dictate that burial is an environmental issue. The fact is there is little or no scientific evidence that undersea telecom cables harm the environment. In fact the historical data and experience with undersea cables since 1866 amply supports the premise that such cables are environmentally benign. Nevertheless, under US administrative law procedures, the burden is on the cable owner to show that there is no harm. Proofing this negative result in the short period of time required in a permit application is impractical. The absence of such evidence allows the agencies to presume harm and order remediation conditions costing millions of dollars. Military applications are not immune from the tremendous costs and delays associated with satisfying various state and federal environmental agencies and conflicting permit requirements. For several years the U.S. Navy has been unable to deploy sensors and cables for underwater ranges of the U.S. coast, even though the obvious security and operational need for such systems is beyond debate.

Even within DOD, there is a stalemate between the Department of Navy and ACOE over whether ACOE, NOAA, and the states can override international law such as the United Nations Convention on the Law of the Sea (1982) ("UNCLOS") to regulate international undersea cables outside of the state's 3NM jurisdiction and beyond the 12NM U.S. territorial sea.

The Department of Homeland Security needs to aggressively cut through the conflicting interagency and federal state agency regulatory regimes and lead an effort to set a common sense and single federal undersea cable regulatory regime which will be the sole centralized source for handling permits for military, scientific, and telecom cables. The recent amendments to the Deepwater Port Act for off-shore gas terminals are one approach. In that case, the US Department of Transportation, acting primarily through MARAD and the U.S. Coast Guard, issues a single permit for construction and operation of an off-shore LNG terminal. All agencies, federal and state, must coordinate their comments and review through this one agency. Only a single environmental impact statement is used for all agencies. Decisions on the permit must by law be issued 356 days after the permit application is filed with the U.S. Coast Guard. This process balances federal and state interests while at the same time providing industry with a commercially practical timeline and predictability.

International Terrorist Law Update for Infrastructure Protection

One of the central tenets of US homeland security policy must be adherence to the norms of international law as embodied in UNCLOS and treaties to which the United States is a party such as the 1959 Geneva Convention on the High Seas, and the 1884 International Convention for the Protection of Submarine Cables. In essense these treaties garuantee the right of all nations to lay, maintain, and repair international cables on the high seas, beyond the usually 12 NM territorial seas. These protections extend to not only telecommunication cables, but to power, scientific and military cables as well. By allowing domestic US states like California, Oregon or New Jersey or federal agencies such as NOAA or ACOE to assert regulatory jurisdiction over cables beyond US territorial seas, a negative precendent is set by which foreign countries can extend their jurisdiciton over US military or scientific cables laid outside but near their territorial seas. If this happens, the ability of the US to use underwater sensors and cables to collect intelligence and scientific data beyond U.S. shores may be substantially degraded in short order.

Homeland Security to Prevent Underwater Telecommunication Fiber Optic Cable Destruction

The Department of Homeland Security will exercise its unique powers under international law to

[2] The U.S. Supreme Court has in two decisions unanimously defined state territorial sea limits at 3 nautical miles. U.S. v. California, 332 U.S. 19 (1947); U.S. v. Maine 420 U.S. 515 (1975); ACOE jurisdiction over international cables, unlike for off-shore structures and pipelines, is also limited to 3 nautical miles. 33 U.S.C. § 403; 33 C.F.R. § 329.12.

proactively diminish the prospects from injury to undersea cables by terrorist actions. When cable owners and operators report possible terrorist activities, homeland security forces, i.e., the U.S. Coast Guard, must act to protect this vital infrastructure. Under UNCLOS, nations may claim a territorial sea up to 12 nautical miles from the coastal baseline. While the United States is only a signatory to UNCLOS, it recognizes a 12 nautical mile territorial sea[3] and a 24 nautical mile contiguous zone, and a 200 nautical mile EEZ[4]. UNCLOS recognizes the right of innocent passage by foreign vessels through territorial waters. Outside of territorial seas, on the high seas, there is generally no right for a coastal nation's naval forces to board a foreign vessel without the permission of the ship's flag state.. International law, however, offers an exception in the case of vessels suspected of injury to submarine cables. Once again, however, this right depends upon adherence to international law[5].

Preparedness and Prevention Program

Intentional acts, such as vandalism, sabotage and terrorism, can be hampered, if not prevented, by an aggressive cable protection policy coupled with unscheduled cable patrols and alert parties reporting individuals found observing or photographing facilities and beach right-of-ways.

An analysis of cable fault histories indicate that cable in water depths of greater than 1,200 meters were the least vulnerable to acts of aggression. Cable segments in water depths of less than 1200 meters experience cable faults at a rate twenty times that of the deeper segments. Records of the the International Cable Protection Committee (ICPC) support the widely held industry view that faults most frequently occurred at depths between 20 and 70 meters. "External aggression", either from natural or cultural causes, account for approximately seventy-five percent of the failures. Natural external aggression failures result from events such as submarine landslides, abrasion caused by currents or wave action, ice scour and fish bites. To date, fishing activity (trawling and dredging) and ship's anchor damage are the primary cause of man-made or cultural aggressions.

Vulnerability Assessment, Facility/Infrastructure Recovery, Risk Management and Threat Elimination

Risk management has become a highly defined regiment relying on specialized expertise, technical knowledge and the mathematical regimentation of quantitative analysis. It requires in-depth knowledge of the specific technology application, in this case underwater telecommunication systems technologies, construction implementation, systems maintenance and restoration technology. For subsea fiber optic systems it also requires knowledge of oceanographic engineering, navigation, submarine survey techniques and soil dynamics.

Telecommunication companies such as AT&T and C&W, have cable protection and restoration groups trained to combat service interruptions and aggressive fault events. These individuals are specialists trained in the following:

- Identification of potential risk sites based on historic fault data
- Establish risk boundaries with USCG and NOAA One controversial approach, apparently favored by Australia's new draft regulations is to establish corridors within territorial seas where international cables land. In these corridors, bottom fishing is prohibited. New Zealand also uses protected waters where undersea activities such as trawling are prohibited to protect its undersea electrical power and telecom cables in its territorial seas. In both cases surveillance and protection of cables is enhanced. In New Zealand's case, the historical data shows an additional benefit in that the marine environment in the protected areas has shown a tremendous rejuvenation in the protected areas since fishing was prohibited.
- Evaluation of ramifications and potential collateral damage (i.e., protected reef ecco-system)
- Cable Station facility right-of-way protection
- Establishment of protection and restoration procedures for Cable Owners' Club and non members' cables

However, due to the underwater environment, infrastructure rebuilds and restoration to the original facility routes can be extremely expensive and time consuming because faulted cables must be recovered to the surface, repaired on a ship, often in extreme sea states, and reburied beneath the ocean

[3] Presidential Proclamation 5928 (54 F.R.77) Within territorial seas, a coastal nation's naval and police forces can board foreign vessels which it believes will violate national laws and for national defense.

[4] Presidential Proclamation 5030 (48 F.R. 1061) In the Exclusive Econmic Zone ("EEZ"), the nation can regulate offshore structures used to exploit natural resources which are defined as oil, gas, minerals, and sedentary marine life. . Cables not associated with these activities are not subject to reguation, unlike oil and gas pipelines which can be reguated in the EEZ

[5] Article 10 of the 1884 Internatinal Convention on Protection of Submarine Cables provides for such boardings by the commanding officer of a naval vessel to obtain evidence if the officer believes an infraction of this treaty such as injury to the cable has occurred.

floor to meet ICPC and AT&T protection recommendations and requirements.

Chemical and Biological Disasters Provides Mapping Techniques for Cable Disaster Assessment

Many of the traditional defense contractors involved in mapping, simulation modeling and related information analysis are examining the need for advanced data fusion technologies for emergency management for natural and man made disasters. The requirement for these information analysis tools are driven by the Department of Homeland Security (DHS) IAIP and FEMA organizations. Their goals are to manage the following disasters:

- Airborne Toxic Gas Release
- Aquatic Toxin and Biological Threats and Releases
- Flooding
- Oil Spill and Terrorist Destruction of Oil and Gas Infrastructure
- Nuclear Radiation (both surface and subsea)
- Tropical Windstorm
- Wildfire (natural, man-made aggression and terrorist activity)
- Biological Threats (terrestrial and underwater ecco-system disasters)
- Earthquake and Land slide (natural and induced)

For the underwater community, these disasters require detailed maps, such as the ones prepared by AT&T and NOAA for the fishing industry to pinpoint underwater cable systems and oil and gas pipeline routes. Computer simulations can allow for DHS and infrastructure owners to perform risk management assessments, strategically place response sensitive assets and recovery systems, and develop environmental and infrastructure damage mitigation procedures.

Electronic Charting Display and Information Systems (ECDIS) is transforming the accuracy of navigation and precision location records of critical assets. Subsea precision location is a daunting challenge for those involved in repair and restoration, due to the inaccuracies of manually prepared maps and charts. The use of Digital Global Positioning System (DGPS) still only provides relative location to the surface. The U.S. Navy through their implementation of ECDIS-N and the concentrated efforts of the National Imagery and Mapping Agency (NIMA) will produce Digital Nautical Charts (DNC) and Tactical Ocean Data (TOD) libraries that will promulgate oceanographic data on critical infrastructure and cable routes. These maps will be used by HS and others to assess and manage potential risks and threats.

United States Coast Guard and Border Patrol Intervention Planning

On March 1, 2003 the United States Coast Guard (USCG), along with 21 other federal agencies, were combined into the Department of Homeland Security (DHS) to protect American people and critical infrastructure from further terrorist assaults. DHS Secretary Tom Ridge in his January 22, 2003 confirmation hearing testified, "The Coast Guard's fundamental responsibilities – preparedness, protection, response, and recovery – cut across all facets of the department's mission."

As a result of the expanded HS role, the USCG budget has grown to meet the growing HS security demands both at home and overseas, and to meet President Bush's strategy for maritime homeland security. The USCG Integrated Deepwater System (IDS) implementation is essential to military operations under Title 10 U.S. Code, and "to push out our maritime borders, giving us more time to identify threats and more time to respond," [6]

The USCG patrols and protects 95,000 miles of U.S. open shoreline, 25,000 miles of navigable waterways, 3.4 million square miles of exclusive economic zone, and 361 seaports that contribute $750 billion annually to the gross national product. The Port Security Unit of the USCG conducts over 45,000 law enforcement boarding of vessels each year. The USCG has the responsibility of preventing terrorist attacks, reducing maritime vulnerabilities and protecting population centers, ocean industries and critical infrastructure. As this paper states, underwater telecommunications is essential to international communications, effecting all phases of life ranging from bio-medical information flow to financial data transfers to material logistics, therefore protection of the telecommunications infrastructure is of critical concern to the USCG as well as industry. Therefore the USCG provides a multi-layered maritime security defense, extending hundreds of miles to sea, to deter, detect, disrupt and destroy terrorist threats to our highest valued targets, i.e., seaborne commerce which relies on underwater fiber optic communication systems.

To achieve its goal, the USCG must enhance and modernize its security capabilities by implementing the "system of systems" IDS. The IDS force structure relies on helicopters, fixed wing aircraft, unmanned aerial vehicles (UAV's), such as the Textron, Inc/ Bell

[6] President George W. Bush, Remarks at Port Elizabeth, NJ, June 24, 2004.

Helicopter Eagle Eye, Island-class patrol boats, such as the USCGC Matagorda, cutters and integrated C4ISR[7] to implement the layered defense structure required for coastal defense, maritime law enforcement, and interdiction. IDS serves as a USCG force multiplier initiative that will allow for increased surveillance of underwater cable routes and other critical infrastructure.

Communications Infrastructure Protection

Cable burial has proved to be one of the most effective forms of system security and cable protection. In the past, the standard was 1 meter burial of cable systems out to water depths of 1200 meters. As fishing and trawling activities extended into deeper waters for a wider variety of fish, as part of a comprehensive cable protection involving education, monitoring, and enforcement, AT&T recommended that cables be buried out to 1800 meters water depth when practicable for cable protection considerations. Other members of the cable owners associations adopted the AT&T recommendation which was considered the best protection against service interruption from fishing activities and anchor drags. As the fishing community pressed to new depths for tautog, monk fish, etc., burial protection evolved to 1.2 - 1.5 meter burial out to water depths of 2500 meters[8]. It is expected that the increased burial depth will provide a 60% reduction in man-made aggressions. It is commonplace in Asian port cities, such as Hong Kong, to bury cables between 5 and 10 meters below the harbor floor to protect against anchors being dropped directly on the cables. However, if a cable is faulted and service interrupted, the ability to locate and retrieve a deeply buried cable for repair is greatly impaired due to limited access to high power water jetting systems and deep de-trenching systems, therefore, replacement of a damaged section is often less time consuming and cheaper than de-trenching and extraction for repair.

With the new threat to communications infrastructure, deeper retro-burial and re-survey of shallow water routes and shore approaches in pre-assigned usage lanes becomes even more critical to system security. Burial lanes serve as a form of protection to delicate eco-systems, however, it pinpoints fiber optic systems for would-be terrorists, and therefore, deeper burial is required to prevent disasters. If the subsea bottom is not within the soil stiffness range below 150 kPa, or where water currents erode burial material, the use of flexible conduit such as uriduct, and even subsea matting, should be installed to protect the cables. However, burial and protection techniques require approval from state regulatory agencies, and the shoreline construction must be reviewed and approved by the Corp of Army Engineers as well as by coastal resource management organizations (CRMC's). In some cases, the facility provider has implemented directional drilling to provide deep burial beneath beaches, to avoid surf zones, and to prevent disturbing ecologically frail environments. The deep directional drilling techniques provide excellent protection from sabotage. Both the ICPC and the CCITT recommend consideration of these protective actions employed by the cable owners and installers where feasible.

Unmanned Marine Vehicles (UMV) for Protection and Maritime Perimeter Defense

Unmanned Marine Vehicles (UMV's) encompass surface, subsea and bottom crawling unmanned vehicles used for surveillance, maintenance and protective warfare against terrorist threats. Advanced sensor systems, visual observation with CCD's and IR and thermal scanning are becoming the backbone of identifying possible terrorist threats and acts of aggression to cables and other subsea infrastructure. Underwater approach corridors are becoming extremely congested in major metropolitan areas such as New York, with the at-sea approaches narrowing to less than 1400 meter separation. In addition, in gulf areas and along fishing beds, trawlers are fishing deeper and closer to the cables. Therefore, surveillance of cable routes by a variety of UMV's is rapidly approaching critical need.

Fiber optic systems have been installed through areas that earlier coaxial installations avoided. The next generation of submarine cables to be installed will be faced with harsher bottom topography requiring more rigorous installation tools and jet assisted plows for initial burial. These topographical features and soil density in the less desirable cable routes have created the need for more powerful Post Lay Inspection and Burial (PLIB)systems and Remotely Operated Vehicles (ROV's) capable of operating at greater depths. Because of terrorist activities, and greater probabilities of natural aggression occurrences increased protective measures must be implemented to protect these fiber optic communication channels.

A major development in the Unmanned Underwater Vehicle (UUV) arena is the use of Autonomous Underwater Vehicles (AUV's) for survey and video

[7] C4ISR is a U.S. Navy initiative incorporating command, control, communication, computers, intelligence, surveillance, & reconnaissance (C4ISR) platforms and sensors.
[8] Burial depth options depend not only on econmics but to an even larger degree on available technology, the density of the seabed subsoil, the bottom toorgraphy, and the precense of rock or coral which limit burial.

recording observation. In the past 25 years, UUV's have developed from scientific laboratory prototypes and sensor test beds to essential support systems for ocean industries. AUV's are unmanned robotic vehicles, free of umbilical cables, utilizing advanced program languages and protocols to define missions, i.e., seabed survey without fixed communication links to the surface vessel. AUV's have become viable with the incorporation of advanced fuel cells and battery developments, which provide a 40 to 50 hour mission operation window, depending on payload configuration and vehicle speed.

This new generation of AUV's has performed programmed tasks such as a 320 km under-ice lay of fiber optic cable and highly precise side scan survey of the ocean seabed for commercial fiber optic telecommunication systems. AUV's, such as the HUGIN 3000 equipped with chirp sub-bottom profiler and dual frequency side scan Sonar, manufactured by Kongsberg Simrad, is now being ordered by vehicle operators and survey companies, for deepwater seabed survey work. It should be noted that the current HUGIN 3000 configuration evolved from mine counter-measures research, requiring bathymetry and image identification functions, HUGIN effectively detected mines in depths ranging from 80 to 200 meters from altitudes ranging from 9 to 30 meters from the seabed.

AUV's could carry out and record periodic cable ground conditioning surveys to establish a baseline to facilitate detection of new mine-like objects found on the seabed near cable paths. This function would be an adjunct to surveys carried out to meet cable environmental requirements under state and federal permits. As threat levels increase, AUV security patrols could be initiated to compare the seabed conditions with previously recorded and updated bottoms surveys. Its processing capacity is capable of effectively conducting post lay inspection or even processing current conditions compared to prior surveys to aid in planning remedial maintenance burial operations.

The burial of cable systems during initial installation is achieved using cable plows. There are a variety of designs that are based on earlier technologies from AT&T Bell Labs and Cable and Wireless. But once a system is installed, Post Lay Inspection and Burial (PLIB) and maintenance retro-burial activity is accomplished by the Remotely Operated Vehicles (ROV's). These ROV systems are required to provide cost effective performance under reasonably harsh environmental conditions. In addition to burial operations out to water depths of 3600 meters, the ROV's must operate in surface water currents up to 6 knots, mid column water currents of 4 knots, and operate in bottom currents of 1.5 knots, and bury in soil densities up to 150 kilo Pascal (kPa). Additionally, these ROV's must be launched in Sea State 5 conditions, and recovered in Sea State 6. the operational sea state criteria requirement mandates the use of an integrated Launch and Recovery System (LARS), which has migrated to an extendable A-frame that can allow the ROV to interface with the water more easily than the knuckle-boom cranes that were previously used.

The system design and operational requirements for this new generation of vehicle provides for "graceful operational degradation", so effective mission performance is achieved. Engineered risk mitigation and system redundancy have limited the need for abrupt operations termination due to single sub-system or component failure. Because of the expenses associated with cable repair, the operator of ROV systems must minimize the repair vehicle down time. It is, therefore, important that provision be made for electrical and hydraulic subsystems degradation before final failure, where practical, to allow for operations to be completed or gracefully terminated before the ROV resurfaces.

Redundant subsystems on the ROV's provide additional mission confidence. The operating personnel have ready access to display of diagnostic information in order to properly assess vehicle system failures.

The newest ROV's operate through fiber optic links, which will provide for all command controls and transmission of sensor signals. Copper conductors are still used for electrical power. Reliability of the system mean time between failure (MTBF) and ease of maintenance time to repair (MTTR) are of paramount importance. Sensor systems can now process data locally on the ROV's, due to component miniaturization, and the increased speed of the onboard processors. However, due to the increased number of sensor suites on the ROV's, the amount of data transferred from the ROV to the surface control van has increased drastically with the capability demands. The latest manufactured design for ROV umbilicals provide up to 4 Gb/s bandwidth for telemetry, video, and other data transfer. Special application ROVs needed for advanced survey, sensor suite platforms and surveillance technologies will utilize a 10 Gb/s fiber optic link. The operational requirements for these ROV's may resemble the following:

- 500- hp. ROV with removable jetting package
- Ability to jet in 150 kilo Pascal (kPa) soil
- Operate at water depth of 3600 meters or greater
- Perform survey operations and bottom sampling

- Initial Burial / retro-burial of submarine cable system up to 2 meters below subsea floor
- Locate and track buried fiber optic cable system
- De-trench / Uncover buried submarine cable system to depth of 2 meters
- Determine burial depth +/- 2 cm
- Dredge holes for placement of special equipment and sensors
- Grip and Cut submarine cable, rope, tow cable
- Grip and Cut anchor chain
- Disengage debris (i.e., otter boards, trawling equipment and fishing gear) tangled on cable
- Attach lift lines for recovery of cable, optical amplifier , and associated submersible plant
- Perform IR , thermal and/or visual inspection and video recording of submarine cable system in exposed areas, buried areas, sites of natural / aggressive cable faults or acts of terrorism
- Provide electronic detection and surveillance of fiber optic cable system
- Provide acoustic inspection of all types of surface laid and buried submarine cable systems
- Data logging / recording of all visual, electronic and acoustic data, including Global Positioning System (GPS) information for interface with fiber gyro system
- Perform cable/equipment bottom positioning with +/- 6 cm accuracy
- Position cable protective matting with manipulators
- Install / remove Uriduct with manipulators
- Recover artifacts with manipulators

The UMV marketplace is rapidly evolving due to the 2002 and 2003 terrorist activities throughout the world. Corporations who previously did not feel threatened by global events have chosen to react to possible terrorist threats, and are investing in surveillance systems and UMV's that protect water approaches from ribbed hull inflatable boats (RHIB's), SCUBA divers, small disposable AUV's that might carry explosives, and even swimmers approaching their sites.

Use of Unmanned Surface Vehicles (USV's) for Surveillance and Surveys

Another UMV that has recently gained attention as a result of the attack on the Cole is the Unmanned Surface Vehicle (USV). For the U.S. Navy the USV will play a significant role in the littoral battle zone, blue water and brown water engagements, and as surveillance and interdiction vessels in harbor and ports. For the USCG, the USV will be used for harbor and port surveillance and as the surface platform for a small electric ROV used for hull and dock inspections. But several of the most important roles that USV's will assume will be under the auspices of the department of Homeland Security. USV's will become their workhorse for infrastructure protection.

Likewise, underwater cable companies will employ USV's to provide continued surveillance of cable landing sites, shallow cable crossings, patrol depot areas and provide surveillance of underwater approaches to cable ships and maritime assets. The USV will become the high speed platform for transporting an inspection AUV to the site of a cable break to assess the damage and to determine the cause. The USV will be equipped with the capability of transmitting video and AUV survey data back to either the host ship or to headquarters for analysis.

Use of Unmanned Air Vehicles (UAV's) for Future Infrastructure Surveillance

In the recent past, the cable owners significantly enhanced their ability to detect surveillance by simply redesigning the programs already in place for traditional cable protection and training their personnel to consider possible terrorist actions in addition to traditional threats to cable systems. These traditional procedures are described in ICPC Recommendation No. 6 and include:

- Radar and visual monitoring of vessel traffic from cable stations with clear views of cable landings.
- Vessel monitoring systems
- Air patrols[9]

[9] Typically, private air patrol services under contract, require the aircraft with a trained observer to be airborne within 30 minutes of being alerted to a fault. In addition, these aircraft fly random cable route patrols; their pilots become very familiar with normal traffic and ship identification. On occasion, it may be possilby to utilize Coast Guard aircraft to assist. ICPC Recommendation No. 6 at 5.2 notes in part:

> Air patrols are typically flown throughout the year. However, in areas where fishing vessels are concentrated over cable grounds during a certain season, the flights may be concentrated into that season. Randomizing the day of the week and time of the day of the flights is recommended. In this manner fishermen do not become comfortable fishing over a cable all week except during the regular flight. Fishing vessels spotted by the air patrol are hailed on VHF radio and informed of that they are in the vicinity of a submarine cables. Additinally, leaflets can be dropped indicating the location of the cable. Identifying numbers and names can be crossed

- Sea Patrol[10]

- Terrestrial Patrol[11]

Use of the above practices enhanced to detect terrorist surveillance may impose relatively little extra expense to cable owners already following ICPC Recommendation No. 6. The crucial element required and in many cases missing is to use these practices for antiterrorism defense is training cable station personnel, pilots, patrol skippers and other vendors to be aware of the threat of terrorism, terrorism surveillance tactics, and the importance of documenting and promptly reporting conditions or suspicious events to supervisors, local security, and recently established National Maritime Intelligence Center.

The Department of Defense has included billions of dollars for the development of Unmanned Air Vehicles (UAV's). These UAV's are not the drones of the 1990's, nor are they isolated laboratory projects. Because of military funding, these UAV's have evolved to integrated sensor platforms built on rugged airframes that have multiple detection and observation systems required to meet the requirements of government agencies and the military. In the recent Iraqi War, the Predator preformed in an outstanding manner, proving the value to expanded unmanned observation. CONOPS (Concept of Operation) have defined detailed data gathering techniques for these UAV's, and major defense contractors such as Northrop Grumman Corp., Boeing, and Lockheed Martin are looking to commercialize their platforms for homeland security and other surveillance operations. The commercial versions of these aircraft would utilize the benefits of the Navy's Tactical Control System (TCS) to fly cable routes and return to base after the completion of an aerial survey.

The USCG has selected and agreed to purchase the Eagle Eye unmanned tilt rotor aircraft from Bell Helicopter Textron, which is a subcontractor to the Lockheed Martin Deepwater Program. The Eagle Eye will fly coast and port surveillance missions, beginning in 2006. It will be replaced by a USCG version of the Global Hawk in 2016.

In addition, Northrop Grumman will market the Sea Scout, which is a USCG version of its Fire Scout unmanned helicopter, and it will be operational in 2005. These same vehicles can be marketed to the telecommunications and the gas and oil industries because they both invest in infrastructure that spans both the continents and ocean floor. Both environments require aerial patrols and repetitive surveillance as part of their preventative maintenance and protection programs.

To further UAV development and other defense systems, the Department of Homeland Security plans to create a technology development office called the Homeland Security Advanced Research Program (HSARPA), which would operate similar to the Pentagon's DARPA.

Conclusion

Protection of submarine infrastructure is ongoing. Protection today does not guarantee protection tomorrow. Thomas Jefferson is credited with having said "The price of liberty is eternal vigilance." This applies as well to security for undersea cables and sensors so vital to the nation's wellbeing. In the case of government, a centralized federal agency to coordinate permitting and security for all undersea cables is desirous and long overdue. For industry continued recognition of the value of partnering with government agencies on security issues must be an essential part of system planning. Together government and industry can do much to deprive the terrorists of easy targets to attack.

> referenced later to determine if the fishing vessels have been contacted during port visits or sent cable protection charts or if additional noficiation might be required.
> Air patrols shall be vailable on a 24-hour call-out basis in the event of a cable break. Modern night vision and image stabilizing optics can enable identification of possible cable breakers even at night. Identifying a cable breaker and collecting damages from them sends a strong message throughout the fishing community.

[10] Sea patrols are arranged under private charter; frequently using fishing vessels to patrol cable routes. ICPC Recommendation No. 6 notes, in part:

> Sea patrols are typically undertaken througout the year. However, in areas where fishing vessels are concentrated over cable grounds during a certain season, the patrols may be concentrated into that season. Randomizing the day of the week and time of the day of the patrols is recommended in order to ensure the fishermen cannot predict when the patrol will occur. Fishing vessels identified by the sea patrol to be near the location of submarine cables are hailed on VHF radio and informed of that they are in the vicinity of a submarine cable. Additionally, cable warning charts may be passed to the fishing vessel indicating the location of the cable. By recording the fishing vessel identifying number and name, the cable Maintenance Authority can later crossed reference the information to determine if the fishing vessels have been contacted previously during port visits or previously been sent cable protection charts.

[11] ICPC Recommendation No. 6 notes, in part:

> All actions for the protection of the submerged plant referred to above need to be complemented with an effective monitoring of the land cable route in order to ensure that the land cable suffers no aggression.
> For this purpose, Cable Station Managers shall establish a routine, preferable daily, consisting of a visual observation of all of the land cable routes to confirm that no construction work is being undertaken in the vicinity of the cable. Sometimes, this can be accomplished simply by delegating somebody from the Cable Station staff to follow the land cable route when driving to/from the Station, to observe it carefully and report any potentially dangerous activity.

Bibliography

ACMA 2004 (Atlantic Cable Maintenance and Repair Agreement) AT&T and ACMA, June, 2003.

Adams, Neal, **"Terrorism & Oil",** Pennwell Corporation, Tulsa, OK, 2003.

Anti-Terrorism Officer Student Guide, Military Sealift Command, MSC APMC Training Center & Fire School (East) 2001.

Bannon, Robert T., and Douglas Burnett, **"HIGH DENSITY UNDERWATER FIBER OPTIC SYSTEMS SECURITY"**, OCEANS 2002 Conference, Biloxi, MS.

Bannon, Robert T., "**Report On the International Cable Protection Committee (ICPC) Meeting"**, Naples, FL, June, 2002.

Bannon, Robert T., **"Remotely Operated Vehicle Evolution For Maintenance and Repair of Fiber Optic Systems"**, Oceans 2000, Providence, RI, September, 2000.

Burnett, Douglas R., **"International Protection of Submarine Cables, A Partnership of Cable Owners and National Governments,"** ICPC Plenary, Orlando, FL., Apr. 1998

Burnett, Douglas R., **"Legal Cable Protection In the Next Century"**, ICPC Plenary, Sidney, Apr. 1997

Canada's Ocean Strategy (Canada, July 12, 2002).

Chance, Thomas, **"Hugin's Role in Undersea Survey"**, NDIA Undersea Warfare Conference, Monterey, 2003.

Coble, James, **"Maintenance of Undersea Cable Systems"**, AT&T, June, 2002.

Collins, Thomas H. ADM. –Commandant of the United States Coast Guard**, "The Coast Guard's Closest Point of Approach to Maritime Homeland Security",** *Sea Power Magazine*, April, 2003.

Department of State Bulletin, Vol. XL, No. 1034 (Novorossiisk at 555-558, (Apr. 20, 1959).

Draft Regulation of Submarine Telecommunications Cables (Australia, February 3, 2001).

Foot, David, **"System Security for Cable Owners"**, KMI 6th Fiberoptics Submarine Systems Symposium, June, 2000.

Geneva Convention on the High Seas, April 29, 1958, 13 U.S.T. 2312, T.I.A.S. 5200, 450 U.N.T.S. 82.

Hessman, James D., **"The Challenge Ahead for a Vital Agency – DHS: A Department Born in Crisis**", *Sea Power Magazine*, April, 2003.

Hugin Mine Reconnaissance, *ON&T*, April, 2003.

Hurst, Pamela J. and William D. Miller, **"Trends in Undersea Fiber Optic Systems",** Oceans 2000, September, 2000.

ICPC Recommendation No. 6, Issue 4, **"Recommended Actions for Effective Cable Protection (Post Installation)"**, 28 October 2000.

International Convention for Protection for Protection of Submarine Cables 24 Stat. 989-1000 (14 March 1884), 25 Stat. 1424, (1 December 1886), 25 Stat. 1425 (7 July 1887), T.S. 380

Kennedy, Rep. Patrick J., **"Ocean Partnership Act: Finding the Focus Again".** Address to the U.S. House of Representatives, Washington, D.C. *Annual Review and Forecast,* 1997.

Langevin, Lou Rae, Lieutenant Commander, Judge Advocate General's Corps, U.S. Navy, **"The Regulation of Submarine Cables: Trends in International and Domestic Law"**, Naples, FL, June 2002.

Submarine Cables and Pipelines Protection Act (New Zealand, 1996).

Presidential Proclamation 5928 (54 F R. 77).

Presidential Proclamation 7219 (64 F. R. 48701).

Seger, Karl A., Ph.D, **"Utility Security: The New Paradigm",** Pennwell Corporation, Tulsa, OK, 2003.

Security Guidelines for Oil and Natural Gas Production, 1st Ed., American Petroleum Institute, March 2002

Testimony of Paul Shorb, Vice-President, North American Cable Association, before the U.S. Ocean Policy Commission, Boston, Mass, July 24, 2002.

United Nations Law of the Sea Convention (1982).

Vestgard, K., K.A. Johansen, R.A. Klepacker and N. Storkersen, **"Kongsberg-Simrad HUGIN Untethered Underwater Vehicle (UUV/AUV)"**, Underwater, July/August 2002.

Westwood, John, **"What the Future Holds for ROVs and AUVs"**, *Underwater*, May/June 2001.

Wilson, Thomas J. RDML., Oceanographer U.S. Navy, **"A Sea Change for the United States Navy",** *Sea Technology Magazine*, March, 2003.

Biographies

Robert T. Bannon, President, BANNON INTERNATIONAL CONSULTING LLC and S4 Intelligence LLC, IEEE Fellow, Secretary / Treasurer IEEE Sensor Council, IEEE Oceanic Engineering Society - AdCom Member, Chairman- Submarine Cables Technology Committee, Advisory Committee Member to Japan Marine Science and Technology Center (JAMSTEC) and IEEE- Japan Committee on Submarine Scientific Cables Use and Related Technologies, Retired District Manager- AT&T International (Submarine Systems), DMTS Supervisor and Senior Engineer-Bell Labs, Delegate to International Cable Protection Committee (ICPC), Pennsylvania State University -BSEE , George Washington University - MSEE, PSU - MBA-Global Business, GW MBA-International Business, Wharton School, University of Pennsylvania - MBA. bannon_intl@earthlink.net.

Douglas R. Burnett, Partner, Holland & Knight LLP, International Law Adviser, International Cable Protection Committee (ICPC) 1998-present, Chairman, Committee on International Law of the Sea, Maritime Law Association of the United States, 1994-2000, Instituto de Derecho Maritimo, Captain, USNR, DOD Level II Anti-Terrorism Instructor-Military Sealift Command 2002, Commanding Officer, NAVCENT NCAPS DET C, 2000-2002, U.S. Naval Academy, B.S. 1972, Defense Language Institute (Portuguese and Spanish), 1976, University of Denver, J.D. 1980. dburnett@hklaw.com.