Final Assignment

[Writers’ Name]

[Institution]

Final Assignment

1) What are 4 published official resources (strategies, International Codes, etc) available to the port FSO in assessing domestic and international risks associated with terrorism and other criminal activity threats posed to port maritime operations? Provide a critical analysis of each…strengths, weaknesses areas that need further development/ Remember an FSO is a private citizen!

It was not quite a time ago when on 1st October 2003, a new career field is opened officially by the U.S. government for a large number of fast-growing ranks people that belongs to the homeland-security professionals. Final rules on that date relates to the maritime security of the nation were published, and previously many of the men and women who were in the possession of jobs such as human resource specialist, terminal manager, or operators/owners took these new responsibilities that include duties in the facility of security officers at maritime and port facilities all over the United States(Domesticpreparedness.com, 2019).

The Maritime Transportation Security Act that is passed in 2002 expanded the safety effort bars at land and on the offices just as on the above water vessels. Previous to the events of 9/11, the U.S. was facing the security problems in the port security domain. President Clinton in the year 1999 approved the Interagency Commission on Security and Crime in U.S. Seaports.. The findings of the commission are that American ports vulnerability is very high to be attacked by the terrorists and in the near future might be higher.

The Goals of the MTSA is to prevent a sea TSI from occurring, or any transportation episode breaking the security characterized by the subsequent occurrence that caused significant damages to the life, transportation disruption, environmental change, and particular area affected by the economic disruptions.

To codify the requirements related to security, a parallel movement was started all over the world which includes nations that hold main trading nations that took place in the United Nation. The International Maritime Organization (IMO) on December 2002 adopted the code-named as (ISPS) International Ship and Port Facility Security Code. According to this code, the risk considered port facilities should appoint their own officers related to the security of the port facility, and also appropriate preparation of the security plan should be undertaken.

Regrettably, facilities in the large numbers that are in the vicinity or are adjacent to the U.S. waters are at higher risk relatively of a TSI and therefore it comes under the umbrella of these regulations. Among the tasks, are the facilities which include handling of particular cargoes and/ or subjects related to the services of vessels which come under the International Convention of the Safety of Life at Sea (SOLAS), and vessels related to the foreign-flag.

Intelligence also plays a prominent role in maintaining and assessing the security as well as combating posed risks of the maritime port operations. Like other risk management system, this system also analyzes different information sources like library sources and newspaper reports that are composed by the concerning specialists identified with port-related psychological warfare and other concerning criminal dangers. Surveys that are related to security issues are also used in evaluating and accessing different risk factors.

FSOs also rely on the tools of the surveillance as a resource of criticality in order to monitor tasks that are carried out in the domain of the port authorities' considerations. For example, reconnaissance on the waterside makes the likelihood of recognizing dangers that could result from vessels or swimmers submerged who could utilize explosives and could be furnished (Christopher, 2014).

At long last, another secret weapon is the sonar innovation that helps the FSOs in port security upkeep. This innovation is an incredible one and it has the capacity in physical properties testing of transmission of sound through the water (Taylor & Kaufman, 2009). Objects can be located using the sonar technology in underwater as well as variables can be calculated that are associated with the objects such as speed, distance, size, and object direction that is posing the threat. Sonar is a very useful and powerful resource having the ability to keep safety at the ports. Several uses can be attributed to this resource such as depth determination of the water and any underwater object that can pose a catastrophic event if not checked otherwise.

**References**

(2019). *Domesticpreparedness.com*. Retrieved 30 May 2019, from <https://www.domesticpreparedness.com/journals/t.i.p.s.--total-integrated-preparedness-solutions--volume-i--issue-17/>

Christopher, K. (2014). Port Security Management, 2nd ed. Boca Raton, FL: CRC Press

Taylor & Francis GroupTaylor, B., & Kaufman, P. (2009). Protecting America's ports. National Institute of Justice Journal, 262.

2) What is the role of MTSA 2002 required Area Maritime Security Committee or AMSC? Why is this organization critical to the secure operation of a port? Be specific. Are there areas within the security regime that committee members can work more closely?

The way through which we secure the ports of the USA changed significantly with the 2002 Maritime Transportation Security Act (MTSA) implementation. The authorization through this act specifically established Area Maritime Security Committees (AMSCs). Currently, the established AMSCs are 43 all around the United States. Each AMSC is run by the U.S. local (COTP) port coast guard captain or FMSC federal security maritime coordinator who addresses the issues of the security at the level of the ports(Crownell, 2018).

The role of the AMSCs is to form the collaborative forum for industry partners and the government to enhance security by working together in the maritime environment. This task is accomplished by the means of conducting meetings, building partnerships, establishing networks, gathering and sharing information, giving training, assessing vulnerabilities, and strategies and plans development. Annual reports of the local AMSC are the vital tool used to share and compile the information relating to issues of the AMSC such as training events, committee organization, accomplishments, challenges, recommendations, and the best practices. Such endeavors guarantee the sea and the coast watch networks in arrangement keeping up with the national goal of preparedness, strategies, requirement reporting, and mainly to serve in improving the effectiveness of the AMSC nationwide.

We know that the AMSCs are the coordination forum of issues related to the security and are the partner in U.S. ports. It is due to their effort that strengthens cooperation between the stakeholders. In the year 2017, AMSCs and all its subcommittees facilitated collectively 1,857 events. From this total, 950 are the included meetings of AMSC administration and 624 are the event specific training. These opportunities of the coordination resulted in the prevention of real-world issues of security, responses, effective, and efforts of recovery(AMSC Accomplishments Report, 2017). Some of the areas where the AMSC is engaging is as follow:

**Cyber**

AMSCs engage continuously in several activities related to cybersecurity. Recently in 2017, 29 AMSCs have cybersecurity subcommittees established to support in cyber risk addressing, sharing of the information, and ways of enhancing resilience and the preparedness of incidents related to the cybersecurity issues.

**Active Shooter:**

To mitigate the threats physically, AMSCs addressed several ways in the marine environment. One such example is the New Jersey and the New York subcommittee of AMSC's Recovery and Response which determines the incident of a waterborne active shooter that has to be addressed by them. As a consequence, the subcommittee of the small passenger vessel of the AMSC's assisted with the risk analysis collection data that is related to such an incident in order to develop protocols of the response and drafting Active Threat Plans of Passenger Ferry.

**PRND:**

The focal point of the AMSCs is the PRND (Preventive Radiological and Nuclear Detection) initiatives that are sponsored by the DNDO. The AMSC of the Charleston responded to "dirty bomb" real world report which involves an inbound flagged foreign container ship. The AMSC of the Charleston implemented the AMSP Radiological/Nuclear response and detection annex that makes the way for information sharing and the joint operational planning amongst members of the AMSC. It helps the AMSC members in quick fostering and effective assets deployment in order to resolve the issues and public safety protection.

Other such areas include where AMSC resolves the challenges includes RAD/NUC CONOPS, call center provision, and course development of the training for Ferry Boat Security.

Although the AMSCs are working efficiently there are certain areas where it is necessary to counter challenges by working more closely. Some of these areas are discussed as follow:

1. **Marine Transportation System and the Cyber Security**

It has been noted in the year 2016 report that cybersecurity and the MTS are going to be the main challenge in the year 2017. Cybersecurity dynamic nature threats and the subject matter shortage experts make the response and preparedness of cyber security a continuing challenge(AMSC Challenges Report, 2017).

1. **Up gradation to Homeport 2.0**

Homeport is the internet portal of the enterprise of the Coast Guard of United States. It was built to secure and support the requirements of information sharing that was described in MTSA 2002. The upgrade from Homeport to Homeport 2.0 was a challenge identified by the AMSC community(Parfomak & Frittelli, 2007).

Other areas where it is necessary to counter the challenges include UAS access to MTS, expansive PSS responsibilities and the security and safety of public access facilities.

References

Crowell, B. (2018). *Area Maritime Security Committees and the Maritime Transportation System*. Naval Postgraduate School Monterey United States.

Guard, U. C. Enclosure 1: AMSC Challenges.”. *Area Maritime Security Committees 2017 Annual Report: Challenges, Suggestions, Accomplishments, and Best Practices*.

Guard, U. C. Enclosure 3: AMSC Accomplishments.” *Area Maritime Security Committees 2017 Annual Report: Challenges, Suggestions, Accomplishments, and Best Practices*.

Parfomak, P. W., & Frittelli, J. (2007, January). Maritime security: Potential terrorist attacks and protection priorities. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

3) Define and give specific examples of maritime Cyber terrorism. How does it threaten port security operations now and in the future? Place your response in a way that highlights this growing threat. Be specific.

Although the community of maritime is still had to establish the proper maritime cyber security definition according to the definition from the Merriam-Webster, cybersecurity can be defined as "measures that are taken in order to protect a computer or system of computers against unauthorized attack or access." Therefore the maritime cybersecurity can be defined as the measures that are taken in order to protect computer and the network assets on terminals, ships, ports, and all the equipment that are computerized, assisting the maritime processes. Any endeavor to upset, harm, or getting to unapproved increase to a computer or electronic system of correspondence falls under the classification of a digital assault. Cyber-attacks refer to the similar assets of a computer on the ships, ports, terminals, and all equipment that are computerized and supports the operations of maritime. All things and areas relating to or falling under the category of or adjacent to the sea, navigable waterways, oceans, and all maritime-related processes, infrastructure, cargo, people and vessels fall under the Maritime domain.

The question that needs to be answered is why do states or individuals carry out the cyber-attacks on maritime? Lars Jensen, who is an expert in the maritime cyber security gives a reply to this query as that the motivation of an attacker ranges from financial benefits to smuggling in order to steal secrets of the company from different industries working in maritime affairs. Ashore or afloat, the operation of maritime industries includes the working on the sensitive equipment that can be accessed easily through the Internet.

Different cyber terrorism types exist in our time in the maritime environment which includes ship systems hacking that includes jamming and spoofing. Jamming and spoofing are the two different hacking terrorism forms that can cause ships on route to diverge on to different destinations. For example, when it is decided by the terrorist groups to jam GPS and the radio signal on the ship, they can then prevent the ship from navigation and finding its proper destination making the ship susceptible to the sea itself or the attack in the near future(Jacq et al., 2018).

This thing also goes for the spamming. False coordinates are given to the ship when it is susceptible to the spammed onboard navigation system. This is used in luring the ships to intentional terrorize the crew and the ship. It also then can lead to the bigger physical attack of terrorism such as leading the ship into an uncharted area where the ambush becomes easy. Sometimes the combination of these two processes also can be used in order to ambush causing the charge of the ship to be taken over and making the captivation of the crew or killing them and if there are some resources that are in ship vicinity, it also helps the cyber terrorists to take them as well.

Most of the groups of the pirates that do this type of activities use the type of technologies funded by the group of terrorists. These groups of terrorists use such pirate raiding parties so that they can gain ships and supplies as well and thus can cripple the country's economy. Since most cybersecurity and the ship techs are well behind the security of the office by at least 20 years, therefore it can be a major problem.

Best way to combat these sort of attacks is to increase the security of cyber technologies that are placed on to the ships. Portable jammers of radar can help in jamming the frequencies that are incoming used to stop the ship from navigation and crippling the radio signals(Jacq et al., 2018). Along with this, individuals' expert in the cyber security domain can boost the security from any incoming cyber-attacks. These individuals can also help in spoof prevention by detecting different radio waves forms using the scanners preventing the attack on the ship.

References

Boske, L. B. (2006). *Port and Supply-Chain Security Initiatives in the United States and Abroad Prepared for the Congressional Research Service*(pp. 1-239, Rep. No. 150). Austin, TX: Lyndon B. Johnson School of Public Affairs.

Jacq, O., Boudvin, X., Brosset, D., Kermarrec, Y., & Simonin, J. (2018). Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre. *2018 2nd Cyber Security in Networking Conference (CSNet)*. doi:10.1109/csnet.2018.8602669

Security Since 9/11: Creating the Maritime Transportation Security Act. (2018, February 09). Retrieved from <https://www.hstoday.us/subject-matter-areas/maritime-security/security-since-9-11-creating-maritime-transportation-security-act-isps-code/>

The International Ship and Port Facility (ISPS) Code. (n.d.). *Maritime Work Law Fundamentals: Responsible Shipowners, Reliable Seafarers,*665-706. doi:10.1007/978-3-540-72751-4\_6

United States Coast Guard. (2017). *Area Maritime Security Committees (AMSC)*[Brochure]. Washington, DC: Author.