October 2017

Marine Design & the Vibrant Adventure Cruise Sector

Marine Propulsion
MAN D&T Debuts the “Game Changer”

Interview
John Haeflinger, Carnival Corp.

Thought Leadership
Class Sounds Off on Future Tech
Cyber Shoal Waters:
Understanding and Meeting Emerging Cyber Threats to the Marine Transportation System
Over the past two months the world has been rocked by three major hacking events that have garnered international notice. These included the EQIFAX event in which 140 million individuals were reported to be possibly compromised, the WannaCry attack and the NotPetya event. In the past two years the emphasis on the cyber security of the Marine Transportation System, a vital economic cog to the world has come under increasing scrutiny.

In August, trade journals and major international publications such as the UK’s Register newspaper highlighted the NotPetya ransomware which resulted in reported impacts across many elements of the Marine Transportation System, including the shipping giant Maersk. The attack shut down operations completely at some facility locations for short periods, and disrupted normal operations for two weeks. Company statements indicated losses in excess of $200 million.

If a nine-figure bill isn’t enough to get your attention, consider that the marine industry can expect more of this in the future. It has certainly gotten the attention of the insurance field as cyber experts look for ways to address the spiral development of this issue. Increasing automation including the Internet of Things increases our vulnerability, and we have every reason to believe that the threat, be they state actors, terrorists, criminal organizations, or insiders, will grow. An analysis of this event and some emerging cyber governance systems for the marine industry can help us understand and prepare for the next event.

At first glance, NotPetya appears to have been a fairly standard ransomware attack – a form of cyber attack where the perpetrator gains access to and locks the owner out of their own files, demanding a ransom (typically paid in bitcoin) for the return of the files.

A ransomware attack on a home computer is, at the least, a significant inconvenience, but not necessarily a disaster. For any sufficiently complex business or organization, a ransomware event can halt nearly all operations – even if IT, rather than OT, systems are impacted. The marine industry – international, mobile, dispersed, contractor dependent, and with status updates demanded 24/7 by global customers – has all the right ingredients for high vulnerability and high consequences to this type of attack.

While ransomware attacks have become increasingly common, the NotPetya attack had some unusual aspects that suggest disruption, rather than the ransom itself, may have been the motive. If so, this has some troubling implications for the marine industry and other aspects of critical infrastructure.

Why should the Maritime Industry Worry About the NotPetya ransomware?

NotPetya employed many common exploit techniques; however, it is the way that NotPetya employed those techniques that moves it into a dangerous arena. NotPetya used automation to move throughout an organization’s network, compromising endpoints and rendering the organization operationally defunct. Another concerning issue is the infiltration of the automatic MeDoc software updates. According to Talos intelligence, a forged digital signature for the MeDoc software update contained the initial payload (Fox-Brewster, 2017). Since software updates typically have admin access, it gives attackers an easy route into the system. This technique bypasses firewalls and other security controls, typically found in components of the MTS, due to the ability to make outgoing connections that are typically encrypted. This type of attack was used in the Flame malware in 2012 and is often associated with nation states. In essence, the attackers were able to weaponize software updates.

Additionally, many researchers have noted that the back-end of the ransomware associated with NotPetya is extremely crude. Given the complexity of the weaponization of the MeDoc software update and the multiple attack vectors of NotPetya, one would assume that if the purpose was to collect money, more effort would have gone into designing the backend payment method. Thus, we are left to wonder if it was ransomware scheme or something entirely different. There is also the symbolism factor involved in this maritime cyber attack. Ukraine established a partnership through the NATO Ukraine Charter, which was signed in 1997, much to Russia’s displeasure. A cyber attack on Ukrainian infrastructure could be seen as a low risk form of retaliation by Russia, given that the Ukrainian partnership status with NATO would not invoke Article 5. Since NATO is a collective defense organization, an attack on one is an attack on all. Article 5 of the NATO Charter is the seminal document that dictates this collective defense. Since Article 5 was written in 1949 when NATO was formed, it addressed only physical attacks. In 2013, NATO published the Tallinn Manual, which was designed to delineate legally justifiable responses to cyber attacks. The Tallinn Manual 2.0 was published in early 2017 and attempted to expand on the first edition and define the new cyber world in legal terms. Although it attempts to provide a secondary source of law for cyber conflict, it did not explicitly answer the question of employing Article 5 in the event of a cyber attack. Since NATO has not determined the appropriate level of response to cyber attacks against its members covered under Article 5, Russia’s risk of NATO retaliation would be minimal given Ukraine’s partner status.

Mitigation Strategies and the Maritime Transportation Security Act

While it may not be possible to objectively determine the motivation behind the NotPetya attack, the incident shows that the consequences of cyber attacks go beyond credit card and financial fraud. While the attackers may have gained little in bitcoin, the event was a significant economic and marine transportation system disruption.

In the United States, one of the objectives of the Maritime Transportation Security Act (MTSA) is to prevent and prepare...
for a Transportation Security Incident (TSI), which is “a security incident resulting in a significant loss of life, environmental damage, transportation system or economic disruption”. The ISPS Code serves a similar function for the IMO. Despite obvious benefits for overall security, both regimes are focused on terrorism and similar threat actors rather than routine criminal activity, which has dominated cyber attacks up to this point.

The NotPetya attack shows that routine cyber crime can have MTS-wide consequences, and that cyber crime can mask attacks whose actual purpose is to disrupt the MTS or otherwise weaken our trade patterns and infrastructure. In other words, cause a TSI.

The MTSA achieves its goals by addressing security risks at the individual vessel and port facility level, and at port-wide risks. Individual vessel and facility operators conduct a security assessment and develop a security plan for Coast Guard approval. These guidelines will take time to finalize and implement, but in the meantime, class societies and industry groups have already begun to establish their own programs.

At the port level, Area Maritime Security Committees serve as risk assessment, information sharing, and communication forums. In 2013 they began to consider cyber attacks a potential TSI to the port, and 22 of 43 have since established cyber sub-committees whose primary role has been to share best practices and educate members on cyber security issues. Many committees have included cyber security threats in exercises and training events. Like the individual vessel and facility plans, the cyber aspects of Area Maritime Security Committees are far from mature, but their multi-agency and public-private membership brings strengths that will be useful in cyber, physical security, and mixed attacks in the future. Information sharing is a vital element to cyber security, and it is here that an AMSC can really shine. While a cyber attack on any given entity may occur at the speed of an electron, organizations may become aware of looming attacks as they creep across the world, or by monitoring social media and other platforms. Some members

Captain Drew Tucci is the USCG Captain of The Port for Sector Long Island Sound.

Professor Scott Blough is a faculty member at Tiffin University, directing Center for Cyber Defense & Forensics.

Dr. Joe DiRenzo is the Director of Research Partnerships for the U.S. Coast Guard R&D Center.

EVENT Maritime Risk Symposium

Tiffin University, a member of the Department of Homeland Security Coastal Resilience Center of Excellence, in collaboration with American Military University, other local, state, and federal authorities, along with industry, will host the 8th Annual Maritime Risk Symposium (MRS 2017) on November 13-14, 2017 at Tiffin University. This event will focus on maritime cyber security and the maritime transportation system. MRS 2017 will bring together local, state, and federal authorities, academics, and industry to discuss the threats and challenges to maritime cyber security and the marine transportation system. With a focus on the articulation of current and future maritime cyber challenges and threats, the symposium will outline the implementation and operationalization of a sound maritime cyber strategy.

The symposium will assess threats, vulnerabilities, and recent advancements in both attack vectors and maritime cyber security research to inspire ideas for innovative research that will define the next generation of maritime cyber space. The event will also include a student poster contest to encourage additional academic research in this growing area of cyber security.

Maritime Risk Symposium Panels
Panel 1: Threats in Maritime Cyber (Case Studies)
Panel 2: Afloat Cyber Vulnerabilities
Panel 3: Legal & Insurance Issues in Maritime Cyber
Panel 4: Advancing Maritime Cyber Security Education & Research
Panel 5: Maritime Cyber: An Industry Perspective
Panel 6: Maritime Cyber Risk: The Holistic View
Panel 7: Maritime Cyber Risk: The National Labs Panel

www.tiffin.edu/criminaljustice/maritime-risk-symposium-2017
of an AMSC will also be members of ISAOs and ISACs, others will have internal resources that enable them to identify these threats as early as possible, and to determine effective mitigation strategies. Without any need to expose specific vulnerabilities and impacts, private sector AMSC members can help one another discern the nature of an attack, confirm or dispel rumors, and provide general advice on protection and response actions. Government agency members can provide access to reliable sources of information to the incident, and advise on techniques that will preserve evidence to support forensic analysis and prosecution. The cooperation and information sharing activities of an AMSC can thereby reduce vulnerabilities to and accelerate the recovery from a cyber attack impacting a port community or Marine Transportation System.

### Cyber-Physical Attacks

The NotPetya attack was not accompanied by any maritime physical attacks on people or infrastructure, but what if it had been? With cargo stacking up and communications systems impaired, port areas might have presented target rich environments with reduced response and recovery capabilities. The sinister synergy between cyber and physical threats becomes more apparent when one considers cyber attacks targeting safety critical IoT devices or physical security systems, such as cameras and sensors.

The potential for a combined cyber-physical attack is a warning to organizations who stove-pipe their cyber and physical security personnel – a not uncommon scenario since cyber security is often managed at the corporate level, while physical security is managed at individual vessels and facilities. AMSC’s, whose membership usually includes physical as well as cyber security experts, can help bridge this gap in steady-state environments by conducting exercises and sharing best practices, and through information sharing during actual attacks or periods of heightened threat. Individual vessel and facility security plans should also address cooperation between the cyber and physical security managers.

### The Way Ahead

At the very least, the NotPetya attack shows that the sophistication of cyber threats is growing along with the marine industry’s reliance on cyber technology. Existing government institutions, regulatory regimes, business practices, technical protocols, and research efforts may be adequate to address this threat, but only if we integrate these efforts and approach this challenge with tenacity and creative thought. The patriotic spirit and hard work that the industry embraced after the attacks of 9-11 have vastly improved the physical security and resilience of our marine transportation system.

That same approach will enable us to develop effective approaches to cyber security.