Marine Transportation System Technology Revolution

Digitalization

Achieving a maritime security advantage

by Luke Ritter
Senior Vice President, Maritime
ARES Security Corporation

Mark DuPont
Executive Director
National Maritime Law Enforcement Academy

The term "smart port," a label with many definitions that can be used to describe a variety of different maritime initiatives, is appearing regularly in trade journals and other industry news. One of the most compelling examples of putting "smart" into the maritime domain has to do with going digital, and digitalization has the potential to provide any port enterprise with a maritime security advantage.

For the purposes of this discussion, we will use a definition that supports security management and anchors any approach to becoming more secure and resilient. Published in a 2021 *Port Technology*[1] article, a smart port was defined as one "that uses automation and innovative technologies including artificial intelligence (AI), big data, Internet of Things (IoT) … to improve its performance." Those last four words are important, and are what sophisticated, mature enterprises tend to pursue—continual, incremental improvement.

Opportunities to improve performance, in maritime security, exist through the application of digitalization, modeling, and simulation. Digitization, "the process of converting information into a digital, or computer-readable, format."[2] is a fundamental pre-requisite—a building block—for establishing a technology baseline that supports and fosters innovation.

Digitalizing security functions follows as the next logical step up from digitization, and is defined by research and advisory firm Gartner as "the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business."[3] To simplify, owners of maritime critical infrastructure that digitalize their enterprise create an opportunity to use advanced technology in a way that optimizes security requirements, while lowering specific operational costs.

The return on investment associated with becoming a smart port is compelling. Security threats in the maritime domain are persistent, and pervasive, and geopolitical issues are creating new security challenges for ports around the world. There is no better time than the present to digitalize to achieve a maritime security advantage. But as an industry, the maritime sector has some catching up to do, as stated in a report published by Deloitte titled *Smart Port—Point of View.*[4]

> *Seaports are playing catch-up with the large transport & logistics players when it comes to developing insight driven solutions and IoT applications…. Even though some ports today are starting to come to terms with the importance and need for digitalization and IoT, there is still a long road ahead to get to relatively mature smart port concepts.*

This comment is echoed in the *Port Technology* article, "Although the maritime industry is often criticized for being too conservative and resistant to change, there are digital technologies, systems and solutions emerging in the maritime that will alter this perception."

The Internet of Things (IoT) is a term used to describe devices, other than computers and smart phones, that connect to the internet.

Digitalization: The Importance and the First Steps

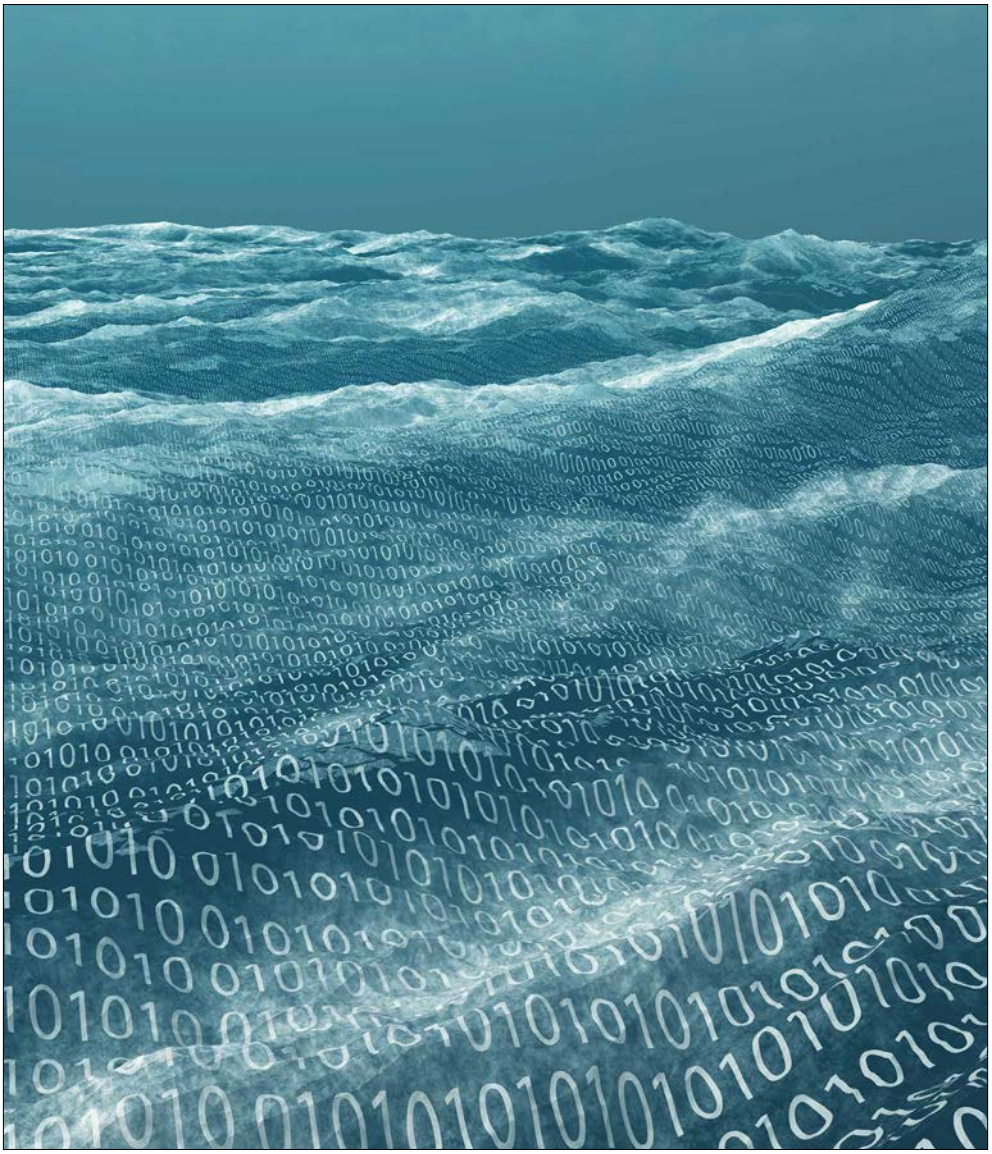
In the United States, port security can digitalize to achieve a higher level of security competency, preparedness, and resilience. By driving maritime critical infrastructure into the digital age, maritime security leaders have an opportunity to facilitate change that can achieve multiple advantages, including:

- increased productivity
- lower operational costs
- enhanced decision making
- improved information security
- process automation
- increased agility and mobility

Creating a digital twin is one of the first and most fundamental investments a port can make in pursuing a digital security advantage. By creating a digital twin, port security professionals establish a virtual representation

of the port. This three-dimensional model shows the terrain features and major physical elements, including structures, capital equipment, and other objects, like critical infrastructure that are being protected. The twin then serves as a digital foundation for security improvement by allowing for accurate modeling of different security scenarios.

Digital twin models for security can be incredibly accurate, and ultimately include details about a site's guard force; security concept of operations (CONOPS); and installed security technology—cameras, radar, perimeter structures, and barriers. Once a site's security posture is accurately modeled, maritime security professionals can use software to identify, monitor, analyze, and optimize both operational and security requirements. Digital decision support tools can be used to support various requirements such as vulnerability assessments, training, and exercises that directly impact maritime security preparedness, readiness, responsiveness, and resiliency.



Tryaging | iStock/Getty Images

Security Cost Savings

The process of addressing complex security questions can be facilitated using digital decision support tools. In the hands of a qualified subject matter expert, security software can be a force multiplier and rapidly process comprehensive answers to complex security questions. Advanced algorithms and digital security libraries can be applied to compliance-related tasks like the Maritime Transportation Security Act of 2002 Facility Security Assessments. Digital tools can make future assessments and related security analyses more efficient by eliminating the need to re-baseline with each iteration. Digital twins are typically refreshed annually meaning vulnerability assessments do not need to start with a site survey. Additionally, maritime security teams can use their digital twin to continually perform rapid cost/benefit

Digital Tools and Security

Digital tools provide security teams with a way to easily and cost-effectively address important questions that can have a significant impact on overall security effectiveness. Questions like:

- Are there any gaps in coverage that could impact security readiness?
- How will the current security strategy work against different threats?
- What improvements can be made to optimize security posture?
- What are the costs versus the benefits of various security solutions?

analyses to thoroughly analyze new threats or proposed security design changes. This results in reduced costs for future security analyses and assessments.

A digital twin can also be used to facilitate virtual security exercises, thereby removing the guesswork and wildcards associated with traditional exercises while providing a realistic training opportunity in a virtual environment. Users can be prompted to make decisions based on computer-generated analysis, and then view and evaluate the outcome of those decisions in real time. Additionally, recordings and files can be archived and reused, as desired. Expenses associated with a traditional physical exercise—travel, lodging, labor, and logistics—are reduced or eliminated.

Security software that uses simulations to evaluate security vulnerabilities is available to the industry, and its algorithms and digital libraries of security characteristics can reliably determine various potential vulnerabilities in any maritime facility with a digital twin. These tools provide security professionals with a complete understanding of their existing security posture, the predicted success of threat mitigation strategies, and options to optimize the security solution for both effectiveness and costs.

Security Efficiency/Effectiveness

Analysis parameters can be easily changed within digital models to address a wide range of security system configurations, threats profiles, and risk elements. Once the vulnerabilities and pathways have been identified and analyzed, users can adjust, test, and evaluate various notional security solutions—sensors, systems, and procedures—by testing their effectiveness using software. An unlimited number of iterations can be considered using this process, at a very low cost. Output from these digital tools provides port security experts with a detailed analysis of security effectiveness and thorough cost/benefit analysis.

Using a quantitative approach to maritime security management also offers operators a cost-effective means to continually assess risks and optimize security effectiveness. Rather than assessing facility security requirements once every 3 to 5 years, digital solutions can analyze continually, and on a case-by-case basis, as security upgrades are made and threat profiles change, and at no additional cost.

Savings through cost-reduction examples like those shown above represent "hard savings," and are often the easiest to identify. Using digital tools can also result in savings and improved effectiveness in less obvious ways. Digital security simulations can be used to evaluate a security CONOPS and can lead to operational changes that highlight areas where costs can be reduced, such as headcount. Additionally, planned security upgrades, like sensor additions and perimeter detection systems, can be digitally evaluated before a commitment is made to procure. And finally, digital tools can be used to cost-effectively evaluate plans for future capital improvements, changes in threat or regulatory requirements, and new or modified design basis threats.

Return on Investment

Vulnerability assessments provide the foundation for the effective implementation of maritime security measures at ports and port facilities. Every one of America's more than 300 ports have different security infrastructure and risk profiles. Vulnerability assessments can be both expensive and subjective, based on how they are performed. Using a digital twin, and applying software tools, can reduce cost, eliminate variability in analysis and output, and optimize results.

Digital security tools enable experts to visualize, quantify, assess, and optimize the security posture at a designated site. Digitalizing maritime security processes delivers accurate, measurable, and repeatable results to optimize the physical security analysis process. Potential benefits derived from using digital security tools include:

- quantifiable, systematic, automated process to evaluate facility security posture
- data-driven input regarding security risks,

bestdesigns | iStock/Getty Images

expenditures, and benefits
- evaluations of security designs permutations to verify desired performance outcomes
- ability to evaluate alternative security detection and deterrence strategies/technologies
- virtual testing and validation of vulnerabilities and changes to security plans and procedures
- processing of thousands of threat scenarios and responses to determine security effectiveness
- identification of security cost savings through quantified risk assessments and cost benefit analysis

All Hands on Deck

Effective maritime security requires attention to a unique set of capabilities and often demands expertise in an array of specific disciplines from law enforcement to infrastructure protection to security technology. Sensitivity to the nuanced nature of the individual missions, capabilities, and cultures of many federal, state, and local law enforcement agencies can be critical. The ability to build bridges among maritime security stakeholders, and to remain current in relevant best practices—public, private, domestic, and international—is a critical component of an effective maritime security solution.

Finally, reliable analysis of emerging issues and industry trends, and the ability to adapt and respond rapidly to complex challenges to business continuity, are the characteristics differentiating maritime organizations with successful security solutions from the rest of the marketplace. Security leaders need as many tools at their fingertips as possible to manage this complex environment, and digital security solutions are exceptional tools. Digital twins, and associated digital tools, are critical components in a comprehensive security strategy.

Whether one is charged with managing the security of a small facility, with a limited security profile, or a large enterprise that must address complex hazards, digital tools help protect critical infrastructure from threats that suspend operations, interrupt business, and compromise the well-being of personnel. Smart ports put software to work to evaluate "what if" scenarios and assess security options in a virtual environment to prioritize future investments and operational procedures.

Knowledge is Power

Ex Scientia Tridens. From Knowledge, Seapower.

The U.S. Naval Academy motto, reminds us that knowledge and information can, and should be, at the root of our security initiatives. The National Maritime Law Enforcement Academy's motto, *Per Scientiam Vires*,

or Strength Through Knowledge, conveys the same message. These are certainly true in the case of maritime security, as well.

Mitigating natural and man-made threats in the maritime domain using digital solutions is becoming increasingly more important. These tools put the power of data-driven optimization, and knowledge, in the hands of maritime security leaders.

Asking "Why?" can be an essential first step in the pursuit of security excellence. By focusing on an end result that is designed to create both operational and security benefits, end users can do more than simply check boxes toward compliance. The power of machine learning and artificial intelligence offers the maritime security industry an opportunity to gauge the effectiveness of its overall security or response plans, as well as the individual systems, staff, and procedures. A knowledge-based approach to security management is critically important to ensure that security information does not become just another cumbersome stockpile of data.

The maritime industry continues rapidly evolving, and connectivity is a key component of success in security operations, threat intelligence, and incident response. Driving operational efficiencies and lowering costs, while maintaining or improving security effectiveness, is a realistic goal—particularly when digital tools are employed.

The most important part of any organization is its people. And as the world around us has demonstrated, today's workforce is dynamic. As retention, recruitment, retirement, and diversity challenges continue, it is more critical than ever to adapt to preferred learning styles. Adult-learning research tells us that providing on-demand, readily accessible training through a learning management system is critical to achieving an organization's goals. Digital training tools can ensure that maritime security professionals will have what they need, when and where they need it. Digital tools also allow for opportunities to optimize training by creating a more accessible, affordable, and adaptable training environment that maximizes the people part of the equation.

Conclusion

So, what is the 'secret sauce' with regard to achieving a maritime security advantage? It includes, but is not limited to:

- investing in a digital twin to serve as the baseline for digital growth
- applying digital decision support tools, and quantitative analysis, to enhance security readiness
- employing software solutions to essential security tasks, including vulnerability assessments and exercises

Fundamental Aspects of Maritime Security Connectivity

There are some fundamental aspects of connectivity that apply to maritime security:

- connectivity enhances readiness and resiliency
- access to information enhances opportunities to succeed
- remaining current with events, threats, and dynamic changes in the maritime environment is an essential element of a comprehensive security strategy

It is hard to argue with the reasoning that a more secure and resilient port is a more valuable one. Mitigating risks and optimizing security posture creates value. Digitalization represents a clear path toward reduced cost, optimized security, and the ability to continually verify and validate that proposed security investments have been optimized to achieve the desired results. Using data analytics to support risk-informed, cost-effective, and quantifiable improvements in security will become the hallmarks of a smart port. Data-based decision making has always driven continual, incremental improvement, and security initiatives are no exception.

America's ports can get "smarter," in how they conduct security operations, train their people, do vulnerability assessments, and conduct exercises through digitalization and the application of machine learning. It is time to consider pursuing digital initiatives that impact the fence line, as well as the bottom line.

About the authors:

Luke Ritter is senior vice president for maritime solutions at ARES Security Corporation. He is a graduate of the U.S. Naval Academy, a former surface warfare officer, and the co-author of Securing Global Transportation Networks *(McGrawHill).*

Mark DuPont (USCG ret) is the executive director of the National Maritime Law Enforcement Academy (NMLEA), and formerly Florida FWC's chief intelligence and domestic security officer. NMLEA hosts the Maritime Security Digitalization & Accreditation Program.

Endnotes:

1. www.porttechnology.org/news/what-is-a-smart-port/
2. Collins Dictionary. (n.d.). Definition of 'digitize'. Retrieved December 15, 2021, from www.collinsdictionary.com/dictionary/english/digitize
3. www.gartner.com/en/information-technology/glossary/digitalization#:~:text=Digitalization%20is%20the%20use%20of,Scale%20and%20Lead%20Digital%20Initiatives
4. https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/energy-resources/deloitte-nl-er-port-services-smart-ports.pdf