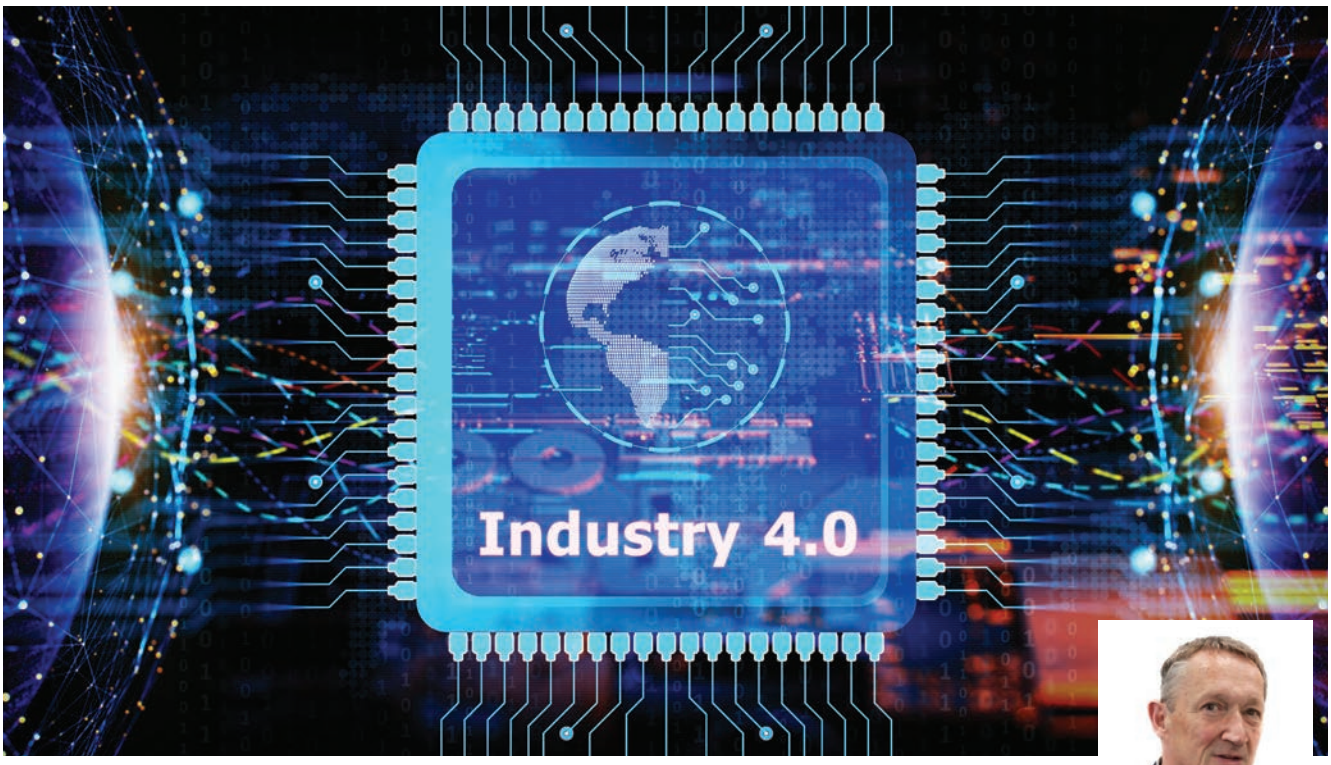

THE FOURTH INDUSTRIAL REVOLUTION

PORT SECURITY IN THE 21ST CENTURY

Richard Westgarth, Head of Campaigns, BMT

As we enter the third decade of the 21st Century, our ports and terminal are facing a dynamic if not turbulent future. They are being assailed on all fronts by transformational changes in technology, business models, the advent of autonomous systems, decarbonisation, the changing nature of trade and trade patterns including a rapidly diversifying workforce, all resulting from the Fourth Industrial Revolution.

We are seeing ever closer integration throughout supply chains alongside the rise of the digital and data economies enabled by high speed interconnectivity. With this transformation, we are faced with ever evolving and challenging issues around security and resilience, driven by the pace of this change. As a transitioning sector we now need to adopt highly agile and progressive approaches to security in a collaborative manner working with our colleagues in other areas of the transport sector.

The UK Department for Transport's (DfT) Maritime 2050 strategy recognises this change with clear recommendations across the sector including around our ports and infrastructure. Looking in more detail at Maritime 2050, it contains a wealth of recommendations and provides the UK with a real opportunity to regain a position as a leading low-carbons' innovator in the global maritime sector. The UK Government has estimated the value of the global ocean economy to be $3 trillion by 2030.

CHANGING THE BALANCE

The new multi-role technologies and their deployment, whether in the air, on land, at sea or in space are being developed rapidly and are changing the balance between their operational domains. This innovation is being driven by global demand in consumer markets and other civilian applications. Let's speculate for a moment about just how our maritime world will look in this new advanced technology future, driven by the Fourth Industrial Revolution.

We will see smart ships, exploiting advanced navigation and communications technologies such as 5G, with on-board sensors and intelligent systems, using lightly manned semi-autonomous, and in time, unmanned and fully autonomous capabilities. They will operate seamlessly with digital, inter-connected ports and trading systems, which use autonomous vehicles and remotely operated loading/unloading facilities to drive up efficiency and productivity. Logistic and asset data from disparate sources is handled using technologies such as block chain to quickly, securely, and accurately, connect owners, operators, hauliers, traders, insurers and supply chains, with real time information about their products or assets.

DRIVING PRODUCTIVITY

This will lead to greatly enhanced speed and productivity of shipping and port operations driving a change to the types and volumes of goods and services which are traded internationally by sea. The adoption of technology-enabled security enhancements, and as defined by the International Maritime Organisation's

(IMO) Code of Practice for global sea trade, will increasingly influence customer and supply-chain choice as to where trade takes place in a world where cyber and piracy threats may also disrupt established commercial trade routes and practices.

We are already seeing the increasing rise in alternative transport models, moving from road-based solutions to adopt short sea and coastal shipping solutions removing congestion and emissions from the roads of the UK. These will be autonomous ships, operated and supervised remotely, capable of entering smaller ports, driving regulatory change, introducing potential new operating paradigms and alongside this, the need for new operating practices and procedures. A key element will be the ability to maintain and safeguard the required high levels of physical, cyber, personnel and information security.

DIGITAL TRANSFORMATION

Many ports are now undertaking digital transformation modernisation programmes, often integrating existing legacy systems with new technologies to deliver enhanced operational solutions and reduce 'outside' threats. This gives rise to several interdependent challenges for maintaining the security and resilience of our ports and harbours and through into the enterprise:

- The fast-paced technological changes will require us to adopt highly agile and robust mechanisms to maintain security at all levels throughout the enterprise and its supply/value chain, collaboration will be essential if we are to avoid security weak links.
- There will be a need for continuous investment in maintaining and updating security systems both physical and cyber, to stay ahead of emerging threats, security and resilience will need to be a central part in operational technology development and selection.
- As technologies such as the Internet of Things, 5G and cloud-based systems continuously evolve and generate colossal amounts of data, new methods, controls and governance will be required to safeguard critical data, whilst also maintaining compliance with emerging regulations and requirements, for example General Data Protection Regulation (GDPR), as well as the protection of mission critical commercial information.
- The digitalization of the operating methods, will require us to move away from traditional perimeter type methods of protection such as firewalls, etc, we will need to build in safeguards within our systems to compartmentalise any compromised systems rapidly, in particular solutions with links to publicly accessible networks
- Sub-contractors and other third parties will need to be carefully assessed and their compliance with security and resilience required assured before they are contracted to work in our ports.
- The development of enterprise wide regulatory standards needs to be addressed and appropriate measures for enforcement adopted.
- The human element will become critical, the design of the systems, their operating practices and the training of the individuals needs to be a key element. Solutions which focus on technology solutions to drive economic/ business benefits may fail to address the people aspects could lead to security weaknesses, disaffected staff and ultimately to the enemy within, where deliberate acts of sabotage take place (insider threats). If we are to benefit from the technology and reduce security risks, we will need highly trained, motivated and committed personnel or we simply will not achieve competitive edge. A key element will be sourcing and training future talents, and developing transferrable skill sets across existing workforces, that are able to take full advantage of future technologies and much leaner organisations.

We need to think hard about how the maritime sector can afford to make all these changes. It is a capital-intensive business – ports and port infrastructure is expensive to build, and they are built to last a long time, meaning margins are often low. Given the extent of changes the industry is under pressure to implement – new physical infrastructure, new technologies, expanded trainings for personnel – there are significant concerns around whether businesses can make the transformation a financially secure one. Failure to adopt new technologies carries the risk of becoming obsolete, yet the process of transitioning is a risk, security must not be seen as a bolt on.

As an enterprise we now need to consider:

- Dependencies: how reliant will our business be on a future highly connected data and information ecosystem to drive operations and how will this change over the coming decade?
- Risks and vulnerabilities: what are the areas of our business where disruption will have significant and unintended consequences and how can we build in resilience?
- Governance and decision making: have the leaders of our businesses validated, understood and have evidence of how they made, and monitor, decisions relating to investment in security and cyber?

BMT sees a future in which many local and multinational consumer companies not only thrive within sectors, but go deep into one country and then proliferate across its business environment, thus appreciating the need for collabora¬tion and local relationships which are critical for the growth of your business in a data-driven world. No one company can have a complete set of skills and capabilities to take a view of the sector, we need to blend experts in shipping with experts in port and harbours, experts in data and analytics and experts in security and cyber. To deliver this as a unified, connected system and to get all the necessary economic benefits, we need to work together to bridge these different silos and encourage cross-interest collaboration.

ABOUT THE AUTHOR

As Head of Campaigns for BMT, Richard Westgarth is responsible for the shaping of campaigns which align to the BMT strategy ensuring that the campaigns are focused on delivering the future growth aspirations of the organisation. A co-author of the Global Marine Technology Trends (GMTT) 2030, GMTT 2030: Autonomous Systems and a regular contributor and commentator about Smart Ships for the IET, RINA and Chartered Institute of Ergonomics and Human Factors institutions, Richard is currently looking at the impact the fourth industrial revolution will have on the maritime sector. His expertise in maritime projects is extensive and he has played a progressive role in advancing issues about autonomy in transport, digital transformation, intelligent and autonomous systems, quantum technology and as well the fourth industrial revolution. He is a Chartered Electronics Engineer, a Fellow of the IET, a Fellow of the Royal Institute of Naval Architects and a Fellow of the Royal Society for Arts, Manufacture and Commerce.

ABOUT THE ORGANIZATION

BMT is a leading international design, engineering, science and risk management consultancy with a reputation for engineering excellence. BMT is driven by a belief that things can always be better, safer, faster and more efficient.

The organisation invests significantly in research and its customers are served through a network of international offices. Its assets are held in beneficial ownership for its staff.