Maritime Hybrid Risks and Threats:

Consequences for Harbours, Navies and Maritime Services – A European View

Lutz Feldt

January 2019

Abstract

Ports play a pivotal role in international maritime trade and passenger. The global shipping industry – much like air, road and rail transportation – is undergoing a technological revolution. Automation has made incredible advances in recent years and will continue to do so. Software programs are the dominating instrument to achieve efficiency.

The protection of harbours against hybrid threats is an ongoing task for all civilian harbours, be they sea ports or river ports and naval bases. It is a civilian and military task.

Hybrid warfare is essentially asymmetric in its way of taking action exploiting such differences, attacking vulnerabilities and weaknesses rather than fortresses.

A lot of different aspects have to be considered when developing protective and preventive measures for harbours, as commercial, cyber, energy, communication, territorial, maritime security , disinformation and military and civilian aspects.

Major conclusions are the demand for "Good Governance at Sea", the "Whole of Government" and the "Whole of Society" approach.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is an objective, task-oriented and politically non-partisan institute.

In the increasingly complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, which occasions both major opportunities and risks, decision-makers in the economic and political arena depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, the economy, international relations, and security/ defense. ISPSW network experts have held – in some cases for decades – executive positions and dispose over a wide range of experience in their respective fields of expertise.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Analysis

"People only accept change in necessity and see necessity only in crisis."
Jean Monnet

"The international consensus on 'hybrid warfare' is clear: no one understands it, but everyone, including NATO and the EU, agrees it is a problem".

Introduction

The raison d'être of ports is interconnection. Ports play a pivotal role in international maritime trade and passenger transport. Some ports act as specialized nodes for international container traffic, while others are terminals for the transfer of goods or passengers between the hinterland and other ports, switching transport modes. Oil and gas terminals are in a different category often more distant from built-up areas. Pipelines provide the interlinkages.

Ports often occupy a wide sea area including anchorages, pilot stations and waiting areas which are all potentially open to attack, with the ships clearly visible, stationary and without obvious protection.

The global shipping industry – much like air, road and rail transportation – is undergoing a technological revolution. Automation has made incredible advances in recent years and will continue to do so.

"Ships are an opening to the outside world," wrote Chris South, a senior underwriter for West of England Protection and Indemnity (P&I) Club.

"Four factors are at play in the maritime industry", said South. The first is automation itself, as machinery on vessels is increasingly controlled by software. The second is integration. On any given vessel, there may be multiple systems connected together. The third is the ability of ship-to-shore systems that communicate via remote monitoring. "Ships are now talking to head offices continuously," says South. The fourth factor is that all these systems are connected through the internet.

All these factors apply to harbours and maritime infrastructure as well and must be considered.

Myanmar: The Situation

In Myanmar, we should consider the actual situation, which has been presented during a Capacity Building Workshop on Strengthening Transport Connectivity among CLMV-T, 9-10 October 2018, Yangon, Myanmar.

Myanmar´s total coastline is 2,228 km, the continental shelf 228,000 km and territorial waters 486,000 km, including the EEZ.

Myanmar also possesses the five major rivers for inland water transport:

1. Ayeyarwady River,
2. Chindwin River,
3. Thanlwin River,
4. Sittaung River and
5. Kalardan River.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

The total length of these rivers is approx. 8,000 miles, navigable waterways about 2,000 miles with more than 400 river ports.

Myanmar has a total of nine ports catering mainly for its seaborne and coastal trade spread over the whole coastline

Yangon is the main port city of Myanmar (and former capital city).

Part one, Protection of Harbours

The protection of harbours against hybrid threats is an ongoing task for all civilian harbours, be they sea ports or river ports and naval bases. They constitute a vital part of the whole logistic chain for goods, and they are also resources for navies and military transport. Harbours are part of the global critical maritime infrastructure and they constitute the gateway between sea and land.

Protection, like security and resilience, is a multi-faceted term, particularly in a maritime context. Traditionally, to the military it implies the allocation of men and equipment to specific tasks in response to threat intelligence by active surveillance, detection and monitoring of the environs and defensive perimeter measures. Civilians have been more likely to adopt a risk-based approach taking account of their responsibilities and authorities as limited by law, geography and ownership. As hybrid threats pose a combination of threats, risks and challenges, that are neither purely military nor civilian, they require an integrated response spanning both approaches. Workshops to gather and share views between civilian and military – two communities which have rare opportunities to meet, but which hybrid threats require to meet more often.

Part two: Maritime Trade

The maritime trade world is multi-dimensional with many stakeholders and few clear boundaries. It is the backbone of globalization facilitating long, complex supply chains through fragmented regulatory frameworks. It is also highly competitive and thus reluctant to absorb additional costs. Individual or associations of stakeholders are limited in their ability to enforce security standards outside their own particular place in the supply chain, thus opening opportunities for risk arbitrage by hostile or criminal groups. Shipping companies and harbour authorities have responded by developing sophisticated communication and intelligence networks to facilitate their understanding of routine markets and risks. But commercial entities have a finite capacity and limited resources and can be overwhelmed by terrorism, cyber-attacks, environmental challenges, financial, social or other catastrophic events beyond their control. In a crisis situation when the limits of resilience have been reached external assistance may be required to withstand further threats or to enable recovery.

Part three: Definition of Hybrid Warfare

Definition of hybrid warfare

Hybrid warfare is essentially asymmetric in its way of taking action exploiting such differences, attacking vulnerabilities and weaknesses rather than fortresses. Weaknesses in this context must be understood as the absence of a coordinated plan between civilian and military authorities and the lack of common vulnerability assessments.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Countering hybrid threats requires an agreed definition or at least a common understanding between all actors responsible for protecting harbours against this threat. Several attempts have been made at defining a complex and cross-cutting concept:

"*While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalize, recruit and direct proxy actors can be vehicles for hybrid threats.*"[1]

"*The fundamental idea of hybrid-warfare is to find the space short of clear-cut military action with direct and recognizable tactical, operational, and strategic impact and compress it into a zone where insufficient ambiguity is created to allow an offensive actor a better chance of accomplishing an objective without full-blown, overt offensive action*."[2]

Finally, in this list of attempts, the document "*Understanding Hybrid Warfare*" includes a very concise definition of hybrid warfare (because of lack of consensus it is presented as a description, but formally it is a definition): "*The synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects*."[3]

While none of them has reached universal acceptance, the combination of these three attempted definitions encapsulates the concept very well and demonstrates the civilian and military components of the challenge posed.

The diversity of options available to an invader are manifold and to safeguard ships, harbours, anchorages and maritime infrastructure as a whole must be understood as requiring a comprehensive approach, involving all maritime services and governmental and private authorities.

"To safeguard harbours and ships from cyber threats, companies should follow International Maritime Organization approved guidelines on cyber risk management, which focus on identifying the systems, data and capabilities that pose a risk to operations, when they are disrupted. To do that, companies must implement risk control processes and have the ability to detect cyber events in a timely manner. They must also be able to back-up and restore systems necessary for shipping operations or services impaired following a cyber event."

Part four: General Setting

Seaports are generally built near or inside a town, or alongside a river and are connected to the hinterland by road and rail. There are often no continuous walls to separate the port area from the town, only particular critical installations are protected. With ports open to the town and sensitive locations not far from built up areas, the surroundings of the port area must be under surveillance.

[1] Quotation from the Joint Communication to the European Parliament and the Council, April 2016
[2] ADM Stavridis in the Proceedings of the US Naval Institute, 2016
[3] Multinational Capability Development Campaign "*Understanding Hybrid Warfare*" January 2017

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Every day, thousands of people go to work inside the port area, hundreds of cars and trucks have to enter and leave, numerous industrial sites or terminals operate within the area, thousands of passengers have to transit through and maritime traffic is permanently moving on the water or alongside the quays.

Different aspects have to be considered in order to achieve a better and real awareness of the situation.

The challenge are increased security requirements and the harbour manager has to consider: how to optimize the movement of cargo—ensuring that containers, personnel, ships, trucks, and rail traffic move in and out of port as efficiently as possible.

What could be done:

Maximize the mobility and productivity of personnel by enabling them to access data and communicate with each other from any point in the facility.

Monitor security throughout the port by screening the port and its perimeter, as well as containers, ships, trucks, rail, cars and personnel that enter or leave the facility.

Comply with government regulations. Monitor security throughout the port. Unify and upgrade the facility's communication systems for greater operational efficiency.

The following text is a modified quotation from „Countering Hybrid Threats in the Maritime Environment":

Commercial aspects

Vessels of all kind and sea and river ports, are vulnerable to hybrid threats.

Sabotage, navigational spoofing, and cyber-attacks on supply chain information systems. At the same time, foreign ownership and control of commercial port facilities can lead to the disruption of their use when these same facilities are required in times of crisis. This is already a major concern.

Cyber aspects

Commercial and military maritime activities are more reliant on cyber-enabling capabilities than ever, with everything from navigation systems to port information systems all being vulnerable to cyber-attack by hybrid actors and criminal organizations. The Maersk incident of 2017 illustrates the challenge well. A cyber-attack on the government of Ukraine inadvertently impacted Danish global shipping giant Maersk when they went to pay their Ukrainian taxes online.

As a result, Maersk's global operations came to a halt as they temporarily lost the ability to govern their fleet. Numerous other industries were also impacted as the global supply chain was disrupted.[5] If this attack was actually aimed at commercial ports and logistics companies, the damage and disruption could have been much worse.

Information held by a port such as the financial and business transactions of its many stakeholders, attracts cyber-attackers to target ports and port facilities whose computer systems and databases may include the control of safety infrastructure such as pumps, storm and flood barrages.

As a general rule, while individual ports are important, the number of ports and competition provides redundancy. Practical experience has proven that common sense and practical measures are required as well as sophisticated solutions. The central role of the State in protecting harbours is obvious, but the capabilities used to enforce protection vary widely due to geography, function, culture and tradition creating a complex environment for enforcing protection.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Cyberattack is a key element in current hybrid attacks, occurring in almost all spheres of life on a daily basis. Cyberattacks are disrupting digital services in harbours, reducing the effectiveness of logistic chains and personnel security. There is a need to discuss how to improve the resilience of communication and information systems. Cyber threats to maritime security have been addressed in the EU Maritime Security Strategy and its Action Plan. The threats caused by manned and unmanned systems, in all three dimensions, air, surface and subsurface must also be assessed. These systems have a cyber dimension that could be exploited to cause physical and organizational damage. Cyber threats are a growing menace, spreading to all sectors of industry that progressively rely on Information and Communication Technology (ICT) systems. Recent examples of deliberate disruption of critical automation systems prove that cyber-attacks can have a significant impact on critical infrastructure. Disruption or unavailability of these ICT capabilities may have disastrous consequences for all governments and social stability. The need to ensure reliability and ICT's robustness against cyber-attacks is thus a key challenge at national and international level.

Critical information infrastructure supports vital services and goods such as energy, transport, telecommunications, financial services, etc., that are so essential that their unavailability may adversely affect the well-being of a nation. Maritime transport is no exception. Whether it is the logistics chain or the ships themselves, global maritime trade can no longer ignore this risk. Navigation systems, telecommunications, energy management systems, and possible entry points must not only be considered upstream, during the design of ships and harbour control systems, but also subsequently as electronic and computer systems need to be updated continuously to meet emergent risks.

Due to their significant importance, the protection of critical information infrastructure is required to sustain and further enhance the well-being of societies, the global and national economy. The subject has therefore drawn the attention of the policy makers in national governments and regional and global fora.

Energy aspects

Diversification of energy supplies has led to an increase in the importance of liquefied natural gas (LNG), to include the transport vessels and onshore offloading facilities. In addition, gas and oil exploration in many maritime domains and the trans-shipment of petroleum and LNG at sea makes the energy supply chain more vulnerable to hybrid threats against the commercial entities which explore, extract, and ship these commodities.

Communications aspects

Today's economies are very reliant on the global information technology infrastructure with 97 percent of intercontinental communications moving through undersea cables, most of which lack even basic defences. These cables are not owned by states, but rather by private entities which cannot afford to harden them and still make a profit.

The potential impacts are apparent when considering that in December 2008, accidental cable cutting in the Mediterranean and Persian Gulf resulted in widespread internet outages in the Middle East and India.

Territorial Vulnerability aspects

The borders and exclusive economic zones (EEZ) of coastal nations can be disrupted and contested by hybrid actors acting on behalf of a state in order to contest the governance of their sovereign territory. In the South China Sea, China seeks to expand its claims, often interfering with the territorial waters and exclusive economic zones (EEZ) of countries like Vietnam and the Philippines, using methods such as armed fishermen to challenge the authorities of these nations and their commercial entities operating in their own EEZ.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Since the ability to control, maintain, and protect sovereign territory is a key aspect of governance, these are among the central tasks of coast guards and naval forces. In some cases, governments find it necessary to modify the rules of engagement for coast guards to be authorized to use deadly force, as Finland did in 2017.

Maritime Security Forces aspects

Clandestine hybrid actors using armed frogmen or unmarked vessels disguised as commercial or fishing craft can surprise and swarm military vessels, disabling or disrupting them to keep them from being able to respond to other elements of a hybrid attack. The ability to detect, attribute, and respond to these threats is among the greatest challenges presented to security forces. In addition, the availability of increasingly sophisticated commercial off-the-shelf technology (COTS) to hybrid actors means that maritime security forces must constantly adapt in order to mitigate these emerging risks.

Disinformation aspects

Alongside the previously mentioned maritime hybrid threats is the vulnerability to adversary disinformation campaigns aimed at eroding internal and regional trust by creating a false counter narrative. These disinformation campaigns across the media spectrum can bring into question the intentions and activities of friendly maritime security forces and their governments, not just in other countries but at home among their own people.

Military and civilian aspects

When talking about the necessity to improve the awareness for these vulnerabilities, risks and threats it became very obvious that there is a gap between civilian and military threat assessments and a notable lack of common understanding in thinking, planning and acting. How far this lack of common understanding and planning is relevant for the development of common capabilities deserves further investigation but depends on the willingness of all stakeholders to come together in an open and transparent way. The special role of Naval Bases and Stations and how far their security measures and experiences can be of general value is relevant for protection against hybrid threats to civilian harbours, depending on the country concerned.

Conclusions

Hybrid risks and threats are more than cyber, but cyber offers the best and a most efficient option for an attack which does not need people on the ground and which is difficult to detect. Sometimes it will never be discovered. For a long time, governmental and private stakeholders assessed cyber as purely an information technology issue and were the responsibility of the IT department. There is no doubt that a technical knowledge is essential but the technical aspect is only one of several other aspects and the best way to approach the situation is by a comprehensive approach. People who are responsible for security must have an understanding of all three levels of possible impacts: the strategic level, the operational and management level and the tactical level which means people on the ground. And all experience indicates that people are the weakest link in the chain of all security plans. People on all three levels could be targets, but the people on the ground could easily be hacked when using the Information technology to do their job efficiently and professionally. Cyber security is a leadership responsibility and people at all levels have a responsibility to share concerns and anomalies with their superiors who must have a direct access to the leadership/management people whether in government organisations or private companies.

The aspect of “good governance” is closely linked with the demand for better and deeper coordination and cooperation between the public and the private sectors. Good governance is also based on international

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

cooperation when it comes to finding appropriate solutions and coordinating actions against hybrid attacks and specific cyber threats.

A whole-of-government approach is required in which all agencies and ministries from national to local level cooperate and share information to reduce any gaps, seams, and vulnerabilities which can be exploited by hybrid and transnational threats.

A whole-of-society approach is needed, which is similar to the whole-of-government approach, but also includes engagement with the private sector, academia, and civil society stakeholders.

Placing the focus on governance, instead of looking at hybrid and transnational threats primarily through a military lens, does not exclude a role for military capabilities.

Naval stations have their own security standards which are based on national rules. They have their internal alert systems which do not necessarily correspond with the standards of civilian ports. These alert systems are based on a broader security assessment which takes the hinterland of a Naval Station into consideration as well.

The European Union´s and NATO´s harbour protection activities for example, are based on four principles: they are multinational, deployable, modular and executed on the “plug and play” principle. The task includes protecting ships at anchor/berths as well as port infrastructure in expeditionary operations where host nation’s harbour protection capabilities are limited or non-existent. The activities should provide deployable harbour-protection against tri-dimensional threats and integrate/execute Command and Control functions.

Rather, it puts military capabilities into a perspective which more closely matches each nation’s own legal authorities and frameworks. Given the nature of these threats, the first to detect and respond are most likely to be civilian entities (both public and private), which may nevertheless require varying degrees of military capabilities to provide support. This is especially important since no government can afford to provide different sets of capabilities and this would undermine the responsibility to share information and knowledge. If risks become threats close civil-military cooperation is vital and this includes interoperability. This is another argument for “dual use” capabilities to counter hybrid and cyber threats.

Cyber-attacks are reported to the national cybersecurity agencies in the countries where they exist. Tools could be developed to facilitate and accelerate information exchange between the appropriate communities (port authorities, ship-owners, companies, military commands).

Only a comprehensive range of sensors operating in different environmental domains, with the information they provide being collated and processed in real time, can provide a reliable picture of the situation. Vulnerable single sensors like AIS should be only one of several sources of information.

Unmanned systems are a future core element of harbour’s security systems, especially for very long-lasting, monotonous activities for persistent monitoring of the harbour waters or providing means of identification/classification and countermeasures.

New technologies (Artificial Intelligence, swarm intelligence,) can be used to counter threats. Resilience of systems should be very carefully studied and updated with technological progress. Weaknesses should be addressed. Capabilities to interfere with system functions are constantly increasing. In this field, artificial intelligence plays a very important role and a very interesting idea - swarm intelligence - that can and must be used in autonomous systems.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

The lack of coordination between stakeholders in information exchange and coordination between national and international agencies creates major discrepancies in tackling maritime security risks and threats. It would be helpful if governments could provide a lead in developing a platform for further consultation and coordination on maritime cyber security. The European Union has established two Centres of Excellence dealing with cyber risks and threats.

A last but not least aspect should be mentioned. Training and exercises are crucial in any kind of security and defence related activity, but even more so in countering hybrid warfare, where recognising the existence of an attack from a set of apparently random events is a particular difficulty faced by those responsible. Frequent table top and communications exercises presenting scenarios as variable as the imagination can go are vital. These exercises must involve all three levels, strategic, operational and tactical very importantly, port authorities and harbours security directors.

***

Remarks: Opinions expressed in this contribution are those of the author.

This paper was presented at the joint conference *Security Threats in the 21st Century* of the Myanmar Institute of Strategic and International Studies (MISIS) and the Konrad Adenauer Foundation (KAS) on November 26, 2018 in Yangon, Myanmar.

References

References used and benefitted from:

1. Hybrid Warfare Protection of Harbours, A report by Wise Pens International, June 2018, not published
2. MCDC Understanding Hybrid Warfare, January 2017
3. Cyber security in the maritime industry
   http://www.mondaq.com/canada/x/667590/Marine+Shipping/Cybersecurity+In+The+Maritime+Industry
4. Joint Communication to the European Parliament and the Council, April 2016
   https://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vkhn74f29mz1
5. Hybrid threats in the maritime environment
   http://cimsec.org/coutering -hybrid threats in the maritime environment/36553
6. Maritime Hybrid Warfare Is Coming by ADM James Stavridis
   https://www.usni.org/magazines/proceedings/2016-12-0/maritime-hybrid-warfare-coming

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

About the Author of this Issue

Vice Admiral (rtd) Feldt served in the German Navy for 41 years and retired in 2006 as Chief of the German Naval Staff in Bonn and Berlin. He was engaged in sea duty assignments for 13 years, which included leadership functions on all command levels and duty assignments in different naval staffs, national and in NATO.

Since retirement, he has occupied several posts of honor. Vice Admiral Feldt was president of the German Maritime Institute until June 2012 and is now a member of its board. From 2008 until 2009 he was working for the European Commission as advisor for the "Instrument for Stability". From July 2009 to December 2010 he served the European Defence Agency as member of the Wise Pen Team, working on topics of maritime surveillance and maritime security. From November 2013 until March 2017 Vice Admiral Feldt was President of EuroDefense Deutschland e.V.

Since August 2011, Vice Admiral Feldt, in his function as a Director of the Wise Pens International, is working on studies dealing with future maritime safety, security and defence, for example "On the Future of EU Maritime Operations Requirements and planned Capabilities" together with his fellow Directors. Recently they have finalized a study about "Naval Challenges in the Arctic Region".

Lutz Feldt

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de