Updating Naval Cyber

Ralph D. Thiele

December 2018

Summary

The maritime economy is of outstanding importance for the prosperity and security of nations. A great opportunity for shipping lies in the networking of ships and ports. Yet, as ships, harbours and related infrastructures become more sophisticated and connected cyber risks increase. Cyber has emerged as the major enabler of hybrid threats posed by government agencies and non-state actors. Perhaps one of the most challenging of potential scenarios is an opponent's ability to establish Anti-Access/Area Denial (A2/AD) postures, weapons and methods to counter own power projection from accessing and achieving freedom of manoeuvre in key areas. NATO and European Union nations - to include the U.S. - have fallen behind their competitors in the cyber domain, both conceptually and operationally. It is recommended

- Naval forces should embrace cyber effects as an integral component of naval power.
- Develop policy guidance to ensure effective use of cyber capabilities.
- Enhance resilience as a necessary foundation for an effective offensive cyber capability.

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

1. Context

The oceans connect nations globally through an interdependent network of economic, financial, social, political and security related relationships. The maritime economy is of outstanding importance for the competitiveness of nations as a business location. Around 90 percent of the intercontinental exchange of goods takes place by sea. The enduring prosperity of the world's industrialised democracies as well as the steady rise of new economic powers owes much to the fact that the world's maritime spaces have been, by and large, a secure and safe domain. Yet, the emerging maritime environment in this second decade of the 21st century appears to become different from the past. Disruptive innovation and globalization have been driving this development.

A great opportunity for shipping lies in the networking of ships and ports. This requires the retrofitting of powerful digital infrastructure on both sides and concerns the supply of fiber optic cables and the 5G mobile radio standard, as well as the nationwide use of sensors and satellites. Logistics chains could thus be managed and organized much better in real time, waiting times could be reduced and ship arrivals could be predicted more reliably. Overall, the increased connectivity offers the prospect of unmanned shipping. Consequently, the global maritime industry has become increasingly dependent on advancing technology.[1]

As ships, harbours and related infrastructures become more sophisticated and connected cyber risks increase.[2] In many cases threats in cyberspace develop faster than the capabilities to protect. Last year's Global Risks Report highlighted that threats to cybersecurity are rapidly increasing, both in their frequency and in their damage potential. The number of attacks on businesses has nearly doubled in five years, and incidents that were previously considered exceptional are becoming common risks. Cyber-attacks on critical infrastructure and strategic industries are becoming more common. The financial impact of cyber attacks is likewise increasing.

In the cyber domain offense has the advantage. The domain is constantly evolving. New systems, platforms, and tools come up at a rapid pace. The arrival of remote-controlled and autonomous ships in the near future, is likely to intensify the effect of cyber attacks going forward.[3]

The transmission of information such as command and logistical data, orders and inventories, and the tracking of assets utilizes a vast network of both intercontinental undersea cables and space-based satellite links and is a critical enabler of *time sensitive* operations or *on demand* business models. Globalisation has reduced barriers particularly for transnational criminal and terrorist activities. Issues of jurisdiction of merchant vessels using Flags of Convenience but crewed by nationals of many different states complicate the security tapestry.

New hybrid threats have blurred the traditionally known conventional or unconventional threats, combining mixtures of high-tech and low-tech weaponry, new strategy and tactics, and a wide and confusing array of state and non-state combatants with overlapping political, criminal, informational, economic and terroristic methods and agendas. The Russian use of *little green men* has impressively visualized the term hybrid warfare

[1] See for example Martyn Wingrove, *Top 10 disruptive technologies to impact fleet management, "*Maritime Digitalization & Communications", 30 May 2018, https://www.marinemec.com/news/view,top-10-disruptive-technologies-to-impact-fleet-management_51958.htm (Access: 06-11-2018)
[2] ENISA, Analysis of cyber security Aspects in the Maritime Sector, Heraklion 2011. *Cyber Security Aspects in the Maritime Sector*, pg. 1 https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1.
[3] Kimberly Tam & Kevin D. Jones, *Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping*, "Journal of Cyber Policy" Volume 3, 2018 - Issue 2 , pg. 149, Published online: 29 Aug 2018). https://doi.org/10.1080/23738871.2018.1513053 (Access: 06-11-2018).

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

– i.e. soldiers without insignia, irregular militias and other proxy forces, its combination of high-end and low-end weapons systems and tactics, and its intentional blurring of the state/non-state and conventional/ unconven-tional divide'. A *new* type of battle space has emerged with different, possibly shifting centres of gravity. All of this does not fit well into the traditional Western analytical categories.

Cyber has emerged as the major enabler of hybrid threats posed by government agencies and non-state actors.[4] Perhaps one of the most challenging of potential scenarios – actually one currently confronting NATO – is an opponent's ability to establish Anti-Access/Area Denial (A2/AD) postures, weapons and methods to counter own power projection from accessing and achieving freedom of manoeuvre in key areas. In an A2/AD scenario it is of increasing importance for a Naval Commander to request cyberspace effects to exploit a vulnerability in the enemy's Air Defence or C2 System and create opportunities in time and space to, along with conventional forces as part of a joint effort, sufficiently degrade the adversary's A2/AD posture. Impacting adversaries' systems in such a manner is not a trivial task in particular as it includes the employment of Electronic Warfare measures.

The days have gone, when cyber was simply an emerging capability that needed to be exploited. It has rather evolved into a global domain consisting of the interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. Future naval missions will likely require delivering warfighting effects in and through cyberspace, to provide tailored signals intelligence, and to assure critical naval networks. Unfortunately, it appears NATO and European Union nations - to include the U.S. - have fallen behind their competitors in the cyber domain, both conceptually and operationally.[5]

2. Vast Surface

The utility of the *maritime domain* depends on ships, harbour, related infrastructure and cyberspace.[6] Given the degree to which civilian and military infrastructure and naval operations depend on cyber-enabled technologies, risks in the cyber domain present a serious and growing challenge to national and international stability and security.[7]

Naval Cyber is special.[8] Unlike most onshore systems, ship builds and ship life cycles last much longer. Due to this, the certification of systems often supports technology that is well-known but obsolete. Many ships cannot upgrade software because of outdated hardware. Yet this hardware often is indispensable for critical systems. For example, the Royal and US Navies, have continued employing Windows XP for considerable time after Microsoft discontinued it.[9] While upgrades have been made in between, other ships are still vulnerable

[4] NATO, *Cyber Defence*, Brussels, July 2018, https://www.nato.int/cps/en/natohq/topics_78170.htm (Access: 06-11-2018)
[5] See the cover letter: MEMORANDUM FOR THE UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING in Defense Science Board, Department of Defense, *Cyber as a Strategic Capability. – Executive Summary*, Washington June 2018, https://www.acq.osd.mil/dsb/reports/2010s/DSB_CSC_Report_ExecSumm_Final_Web.pdf (Access 06-11-2018)
[6] Basil Germond, *The Geopolitical Dimension of Maritime Security,* "Marine Policy" 54, pg. 139, 2015, https://www.sciencedirect.com/science/article/pii/S0308597X14003509 (Access: 06-11-2018)
[7] Kate Belmont, *Maritime Cybersecurity: Cyber Cases in the Maritime Environment.* AAPA, Ney York 2016, pg. 8ff, https://www.ahcusa.org/uploads/2/1/9/8/21985670/k._belmont_-_aapa_maritime_cybersecurity_final.pdf (Accessed: 06-11-2018)
[8] ENISA ... pg.10
[9] David Goldman, *Navy Pays Microsoft $9 million a Year for Windows XP*, "CNN tech. CNN Business", June 2015, http://money.cnn.com/2015/06/26/technology/microsoft-windows-xp-navy-contract/index.html (Access: 06-11-2018)

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

through legacy hardware. With view to the design cycle of newer ships it can be expected that this problem will likely continue.

A further aspect, ships are increasingly using systems that rely on digitization, integration, and automation.[10] Practically all major systems on ships, aircraft, submarines, and unmanned vehicles are networked – and frequently connected to the internet. This includes ships' hull, mechanical and electrical systems, weapons and navigation systems, aviation systems, and not at least control systems. The continual reliance on position, navigation, and timing systems, such as the Global Positioning System (GPS) satellite constellation for navigation and precision weapons constitutes a considerable technical vulnerability.[11]

New generations of sensors in radar, sonar, optronics and electronic warfare are connected in a network to send the signals they detect for real-time processing and analysis by artificial intelligence and big data. Those technologies transform the data into actionable information supporting naval commanders and crews in their decision-making. This development also applies to commercial ships as these are increasingly using systems that rely on digitization, integration, and automation. In a nutshell, the systems and networks naval forces must protect are complex and large in size. Naval platforms have become floating platforms of data. That data empowers all of vital warship functions, be it navigation, surveillance, interception, or defensive measures.

The cyber threats that naval forces continue to face, are stemming from individuals, crime, NGOs, governmental and international actors seeking to probe naval networks for vulnerabilities that can be exploited to their own ends. The threat itself is multi-faceted and diffuse. It may come from a developer who has accidentally or otherwise introduced a malware into a system or an item of equipment, or from the integrator, the maintenance supervisor or the user, propagating a malware via tools or simply by connecting a standard medium such as a USB key. It may also take the form of an intentional external attack. The vectors of such attacks may be deliberate and malevolent, or simply negligent and ill-informed.

Offensive actors mostly follow a *cyber kill chain* from discovery to probing, penetrating then escalating user privileges, expanding their attack, persisting through defences, finally executing their exploit. They fully understand the naval reliance on communications, ISR, and visualization technologies, and perceive them as vulnerable to disruption and exploitation. For them it is possible to render a component of an enemy ship defective, to steal data, to take control of the ship, of its information system, of its weapon system or one of the many monitoring and control programmable logic controllers used both for managing the ship's power supplies and for its steering.[12]

On daily basis, new vulnerabilities are discovered and published, these publications expand attack surfaces and ease it for malicious actors to penetrate own networks. To exploit given vulnerabilities takes only little financial investment, thus making them potentially cheap attack vectors. Risks may even occur from personnel accessing systems on board, for example by introducing malware via removable media.

[10] Siraj A. Shaikh, 2017, *Future of the Sea: Cyber Security*. Foresight: Government Office for Science, London 2017, pg. 4, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/671824/Future_of_the_Sea_-_Cyber_Security_Final.pdf (Access:01-11-2018)
[11] BIMCO et. alt., *The guidelines on cyber security onboard ships. Version 2*, Bagsvaerd, Denmark June 2017, pg. 1. http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16 (Access: 06-11-2018)
[12] Travis Howard and José de Arimatéia da Cruz, A Cyber Vulnerability Assessment of the U.S. Navy in the 21st Century, Center for International Maritime Security, 2017, http://cimsec.org/cyber-vulnerability-assessment-u-s-navy-21st-century/30405 (Access: 06-11-2018)

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

Cyber attacks on ships may aim at

- Course manipulation by falsified GPS signal, course change by 3 degrees, attack by the ship not to detect. Yet, attackers must be close to the ship. Even pirates use hacker know-how
- Burglary into the CMS of the shipowner
- Ship and cargo are specifically selected
- Sabotage through falsification/deletion of data
- Spying on confidential data to support crime (theft, smuggling, terrorism)

Such attacks have been quite successful in the recent past. Maersk's computer network almost completely shut down.

Attackers are particularly interested to finding unlocked doors and eagerly study their target's weaknesses. They collect information about the target's networks, systems and their defensive measures. They interact with potential victims online as the easiest method to gather information. The volume of accessible information posted on social networking sites is immense. Consequently, particular successful techniques to gain network or system access include:

- **Social Engineering**[13] **–** attackers search for personal or critical information and use this information to access sensitive data. Cyber criminals are excellent at tricking victims into visiting a webpage, downloading an app or connecting an unauthorized device containing malicious code.
- **Phishing -** attackers send apparently trustworthy e-mails containing a website link or an attachment. By clicking on the link or opening the attachment, victims may be directed to a website that prompts them to provide personal information or that uploads malware onto their computer.
- **Watering Hole –** attackers go after websites frequented by specific interest groups or organizations. As they profile victims and observe online behaviour such as most visited websites or social media circles. They identify a flaw in the system on one of those sites, compromise it and wait for a target. Users visiting a watering hole site are stealthily redirected to another site and exploited by the adversary through implanted malware.

Particular threats and vulnerabilities include malware, jamming, denial of service and spoofing.

- **Malware** can be easily installed physically by a variety of devices, via any port capable of reading data. As a universal technology, the widely used USB is often the prime choice for physical malware infection[14]
- **Signal jamming** devices are relatively small and inexpensive to make or obtain, thus it would not be difficult to introduce a satellite or radio signal jammer to a ship heading to a dangerous hotspot like the Malacca Straits. As it is easy to prevent signals from reaching their destinations by concentrating noise near the targeted receiver or emitter and cause signal congestion, jamming is particularly effective on ships, as they are often very far from other signal sources, making those signals very weak and easy to jam.

[13] For definitions compare: Cooperative Cyber Defence Centre of Excellence, *Cyber Definitions*, https://ccdcoe.org/cyber-definitions.html, (Accessed: 06-11-2018).
[14] Jacob Maskiewicz et alt., *Mouse Trap: Exploiting Firmware Updates in USB Peripherals*, pg. 2, 2014. https://www.usenix.org/system/files/conference/woot14/woot14-maskiewicz.pdf (Access: 06-11-2018)

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

- **Denial of service vulnerabilities** attacks have become a problem as ships get larger, more advanced, and saturated with devices, many connect transmitters, repeaters, and sensors via network packet transmission. Generally speaking, today's ships are installing increasing numbers of sensors for monitoring cargo and ship functions to increase safety and efficiency. In addition to that, future ships are more reliant on sensor data for computer-based decisions.
- **Spoofing** - i.e. providing false data - is typically more sophisticated than jamming as it requires an understanding of the transmission protocols. However, the pay-off of spoofing instead of jamming is that the absence of a GPS signal often results in ship-wide alarms, whereas misdirection is less noticeable and can cause more subtle outcomes.

3. NATO and EU approaches

NATO is a Maritime Alliance.[15] So is the European Union. At present both organisations are not well prepared to meet the complex mixes of cyber challenges in the maritime domain. Until today, cyber operations are still in their infancy. Valid strategies and doctrine are missing. The current Alliance Maritime Strategy, approved in 2011, does not reflect the altered security environment.[16] The slightly younger European Union Maritime Security Strategy hardly mentions the word cyber.[17] Clearly there is a need for strategies that identify the required policies, capabilities and operational concepts in the maritime domain within the context of current and foreseeable operational and strategic realities vis-a-vis the (re-)emergence of capable potential opponents. Cyber will be among the top issues addressed by the upcoming strategy updates. In particular, NATO needs to figure out what cyber operations need to accomplish. What precisely is cyberspace as an operational domain? What are the rules of engagement in cyberspace? What type of cyber challenge would trigger the alliance's collective self-defence provision?

Vice Admiral Clive Johnstone, Commander Allied Maritime Command set the right tone when addressing in late 2016 the NATO Parliamentary Assembly in Istanbul, Turkey:

„Time is critical. We need to recognise this as threats work around our traditional thinking and society. We need to be ready to respond with what we have, and to assume we will suffer from strategic surprise."[18]

The defence of its CIS/IT has always been one of NATO's principle responsibilities in order to protect its ability to connect the Alliance, support projects. The overall responsibility to protect NATO's CIS /IT was shared for decades among several agencies until in 2012 the NATO Communication and Information Agency (NCIA) was formed from the amalgamation of several agencies. From the early days of CIS/IT with features such as basic e-mail and web page capabilities, through to today's complex C4I technology for Ballistic Missile Defence, Joint Intelligence Surveillance and Reconnaissance (ISR) and the Federated Mission Network (FMN), CIS/IT has rapidly evolved from being a simple data communications system, to an enabler, and today being critical for mission assurance.

[15] Vice Admiral Clive Johnstone, Commander Allied Maritime Command, *The Role of Allied Naval Forces and Allied Maritime Command after Warsaw 2016*, Presentation during the Defence and Security Committee Meeting at the NATO Parliamentary Assembly in Istanbul, Turkey. https://mc.nato.int/media-centre/news/2016/the-role-of-allied-naval-forces-and-allied-maritime-command-after-warsaw-2016.aspx (Accessed: 06-11-2018
[16] Steven Horrel, Magnus Nordemann, Walter B. Slocombe, *Updating NATO's Maritime Strategy*, Issue Brief Atlantic Council. July 5, 2016, pg. 1. http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/Updating_NATO_Maritime_Strategy_0705_web.pdf (Accessed: 06-11-2018)
[17] Council of the European Union. *European Union Maritime Security Strategy*, Brussels 2014, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT (Accessed: 06-11-2018)
[18] Vice Admiral Clive Johnstone a.a.O.

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

This evolution has seen steady transformation at the unit and organizational levels, but also increasing prominence within the Alliance's political agenda. First mentioned at the 2002 Prague Summit where the Alliance committed modestly to 'strengthen our capabilities to defend against cyber-attacks', the Alliance has steadily increased the role of cyberspace.[19]

The increase in prominence of cyberspace on NATO's political agenda was inspired primarily by two seminal events – the cyber-attacks on Estonia in April 2007 and the conflict between Russia and Georgia in the summer of 2008, in which cyber was a significant component to Russia's *Hybrid Warfare* tactics. The attacks on Estonia prompted NATO to develop a policy on cyber defence in January of 2008. After the conflict in Georgia, when it became clear that cyberspace had 'the potential to become a major component of conventional warfare' and that 'most crises and conflicts today have a cyber dimension', there was a succession of responses undertaken by NATO, the more significant of which included the adoption of a Strategic Concept (November 2010), the integration of cyber defence into the NATO Defence Planning Process (April 2012), the establishment of NCIA (July 2012), the endorsement of the current Cyber Defence Policy (June 2014), the approval of the new Cyber Defence Action Plan (September 2014) and the Technical Arrangement on Cyber Defence between the NATO Computer Incident Response Capability and the Computer Emergency Response Team of the European Union. All these activities were developed within the framework of NATO's mission and core tasks of collective defence, crisis management and cooperative security.

At the Warsaw Summit in July 2016, Allied Heads of State and Government reaffirmed NATO's defensive mandate and recognised cyberspace as a domain of operations to improve NATO's ability to protect and conduct its missions and operations.[20] Allies also pledged to enhance the cyber defences of their national networks and infrastructures, as a matter of priority. In December 2016, NATO and the EU agreed on a series of more than 40 measures to advance how the two organisations work together – including on countering hybrid threats, cyber defence, and making their common neighbourhood more stable and secure. In December 2017, NATO and EU Ministers agreed to step up cooperation between the two organisations in a number of areas, including cyber security and defence.

At the Brussels Summit in 2018, Allied leaders agreed to set up a new Cyberspace Operations Centre (CYOC) as part of NATO's strengthened Command Structure. Created on August 31, 2018, in Mons, Belgium, the CYOC should be fully operative by 2023. It is supposed to provide situational awareness and coordination of NATO operational activity within cyberspace. Allies also agreed at the Summit that NATO can draw on national cyber capabilities for its missions and operations. Finally, Allies took stock of their progress to enhance national resilience through the Cyber Defence Pledge.

Of notably operational benefit has been the expansion of NATO's Joint Intelligence, Surveillance & Reconnaissance capabilities into the maritime domain. Even small, targeted efforts have already disproportionately improved NATO's maritime situational awareness. NATO has been helping member countries by sharing information and best practices, and by conducting cyber defence exercises to help develop national expertise. It aims to integrate cyber defence elements and considerations into the entire range of Alliance exercises, including the annual Crisis Management Exercise. NATO is also enhancing its capabilities for cyber education, training and exercises, including the NATO Cyber Range in Estonia.

[19] NATO, *Prague Summit Declaration*, North Atlantic Treaty Organization, http://www.nato.int/cps/en/natohq/official_texts_19552.htm, para. f, (Accessed 06-11-2018).
[20] NATO, *Warsaw Summit Communiqué*, North Atlantic Treaty Organization, http://www.nato.int/cps/en/natohq/topics_78170.htm, para 70, (Accessed 06-11-2018)

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

Already at the Wales Summit in September 2014 NATO has adopted an enhanced policy and action plan to keep pace with the rapidly changing threat landscape. Yet, to this point this has not become a truly comprehensive approach as it focused predominantly on building and maintaining a robust cyber defence - i.e. activities seeking via the use of cyberspace to detect, analyse, mitigate and prevent vulnerabilities in order to protect computers, electronic information and/or digital networks.

In between, NATO has learned that also offensive capabilities are required. Up to now NATO lacks the capabilities to exploit offensive cyberspace effects. It also lacks the processes and the procedures to obtain these effects from its member nations. There is a general lack of knowledge of how offensive capabilities might benefit NATO during operations. To successfully implement a mechanism to request cyber effects, NATO planners should have at least a general understanding of the offensive cyber capabilities of contributing nations. Equally, the nations contributing personnel skilled in OCO should be familiar with NATO doctrine, operational planning and ideally, the specific mission. Since the cyber capabilities are highly classified, it may mean that both the requests for effects and the corresponding responses must be filtered through an interface to ensure highly classified information is safeguarded.

Principal focus needs to be on demystifying cyber and developing requirements to help operational commanders

- integrate cyber into their joint and maritime operations centres;
- provide cyber effects in the context of crafting operational plans.

Clearly, NATO should focus energies on bridging the gap in the cyberspace domain as maritime operations need to cope with denied environment, like operational or tactical limitations that are caused by Electronic Warfare or Cyber Attacks.

NATO has started working closely with the European Union. The nature of this cyber cooperation is complementary. As NATO the EU has taken a number of steps to improve its performance in cyber space. It has

- drafted a cooperation blueprint to handle large-scale cyber incidents on EU level;
- facilitated the establishment of an 'information hub' to support the exchange of information between EU bodies and Member States;
- created a high-level advisory group on cyber security;
- extended the mandate of the European Union Agency for Network and Information Security Agency (ENISA).

Both organisations have developed a shared interest in becoming more cyber resilient. Consequently, they have started sharing information between cyber crisis response teams, exchanging best practices, policy updates and working together on training, education and exercises. NATO's Cyber Defence Pledge and the implementation of the EU's Network and Information Security Directive have been reflecting this already. This increasingly coordinated effort is helping both organizations to better defend against cyber-attacks and enhance their resilience, which is critical to counter hybrid threats.

4. The Challenge

The rise of cyber capabilities means that navies will be simultaneously more connected and more vulnerable at sea than ever before. New opportunities and new vulnerabilities have developed. To keep pace with the

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

dynamic mission space and rapidly growing operational needs, naval forces need to mature their effects-delivery capabilities and capacity. Naval commanders and their staffs need to develop a holistic, full spectrum understanding of the role cyberspace plays from tactics to operations to grand strategy.

Defensive and offensive cyber capabilities[21] need to be integrated alongside kinetic action. This enables integrated fires as cyberspace can increase the effectiveness of traditional kinetic fires through improved intelligence and targeting. Assured command and control require key ingredients such as resilient capabilities and networks, diverse architecture, efficient data transfer, and operational knowledge and risk management. Cyber key terrain needs to be defined for each network, including communication and satellite networks, and for each mission to include operational availability for each terrain.

Defensive cyber operations must keep up with constantly incoming attacks as they operations are intended to defend national or allied cyberspace systems or infrastructure. Advanced persistent threats - stealthy persistent attacks on a targeted computer system in order to continuously monitor and extract data - have turned out to be particular challenging. They are difficult to detect and could render significant damage.

In order to detecting and monitoring opponent´s activities, blocking attacks, manoeuvring to defeat opponents, and defending naval information networks and critical infrastructure[22] mission areas will likely include

- Operations and defence of the naval networks and operating shore-to-ship communications systems;
- Relevant and actionable intelligence and surveillance data based on the analysis of adversary communications and radars;
- Signals Intelligence and associated threat warnings to provide naval forces with location and intent of opponents;
- Provision of context to other intelligence sources;
- Provision of the maritime domain and a common operational picture;
- Warfare in the electromagnetic spectrum;
- Interrelated and complementary missions.

Network operations design, build, configure, secure, operate, and maintain information networks and the communications systems vis-à-vis adversaries who are constantly seeking new ways of attack or penetration of networks. A key issue has become to reduce 'attack surfaces' – i.e. the opportunities for malicious actors to get into naval networks. To this end, network controls include network firewalls, intrusion detection and prevention systems, security information and event management, continuous monitoring, boundary protection, and defence-in-depth functional implementation architecture, anti-virus protection on all host systems, robust vulnerability scanning, and cyber risk management. Technical cyber security applies across the naval network, afloat and ashore, including host level protection with software designed specifically for naval requirements.

Information assurance is a top priority in highly networked environments. It requires the coordinated use of multiple security countermeasures to protect the integrity of the information assets. Obviously, it would be more difficult for an opponent to defeat a complex and multi-layered defence system than to penetrate a

[21] For definitions compare: Cooperative Cyber Defence Centre of Excellence, *Cyber Definitions*, https://ccdcoe.org/cyber-definitions.html, (Accessed: 06-11-2018).
[22] United States Government Accountability Office. *Cybersecurity. Actions needed to strengthen U.S. capabilities,* Washington. February 2017. Pg. 18. https://www.gao.gov/assets/690/682756.pdf

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

single barrier. Also, the naval ability to exercise command and control in the presence of a protracted "information blockade" employed by adversaries needs to be assured, especially under heavily contested or denied operational conditions. Clearly, there is a need to take precautions to ensure continuity of operations in a degraded cyber environment.[23]

Offensive cyber operations refer to computer activities to disrupt, deny, degrade, and/or destroy. These include reconnaissance, intrusion, privilege escalation, and payload dropping and would strike military, government and perhaps civilian targets such as critical infrastructure in the opponent homeland used to support war efforts. Such attacks would disrupt data and services, sow confusion, damage networks and computers - including software and computers embedded in weapons systems - machinery.

"Tactical" operations would be undertaken to support combat forces and to shape the battlefield by degrading command networks and weapons software. Cyber actions at the tactical or operational level will be used against deployed forces and their support. The most likely form of attack will be against command and control systems - including sensors and computer networks - and against the software that runs advanced weapons such as surface-to-air missiles or fighter aircraft.

Operations on the operational and strategic level can be used in long-range "strikes" against rear areas or the opponent's homeland, including against civilian targets. The intention would be to disrupt services and degrade morale.

To bring available maritime power to bear when necessary, naval forces need be able to build a new kind of situational awareness of the collective 'fleet' wherever they sail, of own maritime activity and readiness as well as of commercial ships and assets at sea. Many questions need to be answered such as: What naval capabilities are out there? Who is deployed and who is ready to deploy. What is the readiness of the assets and their level of training?[24] Cyber situational awareness has to deliver inputs based on a sharable cyber common operational picture.

This cyber common operating picture needs to synthesize current performance of cyber systems, operations, and threats into an integrated picture. It informs network and defensive operations, in addition to supporting other mission operations. It reports – tailorable by missions and by region - status, vulnerability, threats, suspicious activity, and mission impact. It provides real-time information to tactical, operational and strategic decision-makers. It evolves to full, immediate awareness of the naval network, i.e. of what is happening on naval networks, of blue network status, posture and capability as well as of adversary activity on own networks, satellites, and communication systems.

Dedicated predictive and prescriptive analysis tools should feed cyber situational awareness and support data-driven network manoeuvre decisions.[25] To enable shared cyber situational awareness will require that a data-driven analysis can be transformed into visualized situational awareness.

[23] United States Government Accountability Office. *Defense Cybersecurity. DOD's monitoring of progress in implementing cyber strategies can be strengthened,* Report to Congressional Committees, Washington. August 2017, pg. 30. https://www.gao.gov/assets/690/686347.pdf
[24] Vice Admiral Clive Johnstone a.a.O.
[25] U.S. Fleet Cyber Command/Tenth Fleet, *Strategic Plan 2015-2020.* pg. 18, http://www.navy.mil/strategic/FCC-C10F%20Strategic%20Plan%202015-2020.pdf (Accessed: 06-11-2018)

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

5. Towards Implementation

While physical defences are well understood, in contrast, modern cyber and cyber-physical attacks aimed at ships and harbour infrastructures are significantly less understood and, therefore, less preventable with current codes and practices. Particularly modern ship technology is significantly different from both typical computing systems and traditional maritime tools. As ships grow increasingly automated, perhaps even achieving full automation within the next couple of years[26] threats must be better understood and defined.

Policy needs to be shaped to prevent future incidences. For historical reasons existing policies have primarily been designed for physical safety and efficient operations, not for addressing cyber or cyber-physical security. Recent internationally standardized systems increase the cyber attack surface of ships across the globe. As these systems are already known to have vulnerabilities.

With today's rapidly evolving threats, naval forces are well advised to develop a sense of urgency not only to develop cyber resilience capabilities that will enable them to "fight through", but also cyber war fighting capabilities as these will be particularly valuable when they can be delivered reliably and in concert with other capabilities. As a principal policy approach should

- treat cyberspace as an operational domain to organize, train, and equip in order to take full advantage of cyberspace potential;
- employ dedicated operational concepts to protect own networks and systems and to engage alongside other operational capabilities;
- partner with other government departments and agencies and the private sector to enable whole-of-government cybersecurity strategies;
- build robust relationships with allies and national/ international partners to strengthen collective cybersecurity;
- leverage existing capabilities through an exceptional cyber workforce and
- invest in Innovation to keep pace with the challenges.

Already in 2013, the U.S. DoD Defense Science Board highlighted the requirement for technology to provide for automated intrusion detection, automated patch management, status data from each network, and regular network audits, for operational systems to be able to tell senior leadership authorities

- when they were compromised,
- whether the system is still usable in full or degraded mode,
- identify alternatives to aid the commander in completing the mission, and
- provide the ability to restore the system to a known, trusted state.[27]

It is time to get there. A sense of urgency is needed to address ongoing naval cybersecurity challenges.

I would like to conclude with eleven recommendations:

- Naval forces need to embrace cyber effects as an integral component of naval power.

[26] Simon de Bruxelles, *Robotic Ship Leaves Humans in its Wake.* The Times. December 29, 2016, https://www.thetimes.co.uk/article/robotic-ship-leaves-humans-in-its-wake-hsqnsszg0.
[27] U.S. DoD Defense Science Board TASK FORCE REPORT : Resilient Military Systems and the Advanced Cyber Threat, pg. 64, Access: https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf (06-11-2018)

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

- Develop policy guidance to ensure effective use of cyber capabilities.
- Naval strategy and subsequent operational concepts should focus on generating interoperable naval forces capable of establishing and maintaining all-domain access.
- Naval cyber capabilities must be integrated into a joint and additionally into a whole-of-government approach and integrated with private sector and coalition efforts to most effectively defend collective security interests.
- Interoperability across joint weapon delivery platforms will essential to make tools and methods easy to employ.
- Focus at tactical levels needs to be on flexibility. This includes adversarial anti-access and area denial operations, improved targeting capabilities, and cyber-attacks.
- As naval forces adopt next technologies to leverage the unique capabilities of cyberspace, reliable access to cyberspace is a necessity. Assuring access to cyberspace and reliable command & control for deployed forces regardless of the threat environment, the ability to operate from a contested cyberspace environment needs to be a top priority.
- Resilience is a necessary foundation for offense. Effective offensive capability depends on defensive assurance and resilience of key military and homeland systems.
- Ensure experience and readiness of cyber forces, to include leadership. Sustained experience in operations is essential to readiness of own cyber capability.
- Staying ahead in this rapidly altering domain requires tempo and agility in the planning, budgeting and acquisition of cyberspace capabilities.
- Naval forces must come up with clear and valid requirements to deliver the full capabilities required for success. This impacts on traditional ways how to acquire, field, modernize, and govern systems and new technology and asks for a dramatically accelerated acquisition process.
- Rapid technological advancement will prompt the need to upgrade or replace technology, including communications equipment, at a much faster rate. Particularly, technologically advanced navies need cyber capabilities that are fully integrated into weapon systems and platforms.

***

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

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

Ralph Thiele, born in 1953, retired Colonel, held in his 40-year military career in the German Armed Forces key national and international positions. He

- Commanded troops up to the battalion level;
- Developed concepts and capability requirements in the Ministry of Defence;
- Drafted speeches and policy papers for Federal Presidents, Ministers of Defence, Major NATO Commanders and Service Chiefs;
- Drove educational innovation at the German Armed Forces Command and Staff College (Director Faculty) and at the NATO Defense College (Chief of Staff);
- Shaped the Bundeswehr's path towards network enabled capabilities (Commander Bundeswehr Transformation Command).

In his honorary and business functions he advices on Defence Innovation and Cyber issues in times of digital transformation. He has been frequently consulting, publishing and lecturing in Europe, America and Asia.

Ralph D. Thiele is also a member of the ISPSW Speaker Management Team. Further information at ISPSW website: http://www.ispsw.com/en/speaker-management/


Ralph D. Thiele

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