# Game Changer – Cyber Security in the Naval Domain

**Ralph D. Thiele**

**January 2018**

## Summary

The systems and networks naval forces must protect are complex and large in size. Ships are increasingly using systems that rely on digitization, integration, and automation. Offensive actors understand the naval reliance on communications, ISR, and visualization technologies, and perceive them as vulnerable to disruption and exploitation. Cyber has been moving from a supportive to a rather active role within an operational force. 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 warfighting capabilities as these will be particularly valuable when they can be delivered reliably and in concert with other capabilities.

## 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. Disruptive Times

NATO is a Maritime Alliance.[1] So is the European Union. The seas and oceans connect member states and allow for trade and communications on global scale thus providing for prosperity and security. This includes - via underwater cables - even the cyber space. Madeleine Moon's November 2016 report to the Defence and Security Committee of NATO's Parliamentary Assembly highlighted impressively: *„The transatlantic link is, in its most concrete manifestation, a deep blue ocean serving as a vital medium of exchange between Europe and North America. … The role of maritime in NATO, however, often takes a back seat in Allies' immediate thinking about near and long-term threats as well as opportunities for the Alliance."*[2]

Europe's security environment has deteriorated in the past years. New, hybrid threats have emerged to include cyber threats from hostile governments and non-state actors causing instability in Eastern Europe, the Middle East, and Africa. In the altered security environment, the maritime domains around Europe have become potential friction zones. While the Russian navy is growing its capabilities, it is challenging NATO at sea and beyond with the build-up of Anti-Access/Area Denial (A2/AD) networks from the High North to the Mediterranean. This is coupled with a significant increase in the size, quality, capabilities, and operational activities of Russian maritime forces.

Russia is not alone. Other rising powers such as China or Iran have boosted their maritime engagement, not only through commercial activities but also through the increasing reach of their maritime forces. For example, in the South China Sea, China has been building artificial islands and extending the land mass of reefs and installing air and maritime facilities as well as A2/AD components on them. China also has demonstrated an emerging interest in the High North, both as a source of energy and future conduit of trade between Europe and Asia. Additionally, there are serious non-state maritime threats and challenges such as terrorism at sea.

Several actors are eager to combining innovative methods and domains with traditional approaches to deny Western nations and organisations areas of competitive advantage. New security challenges include sophisticated means such as military, economic, information, infrastructure, social, and political instruments of power. Yet, there is also the broad spectrum of opportunities offered in and through cyberspace - the global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.

At present NATO is not well prepared to meet the complex mixes of hybrid challenge in the maritime domain. Until today, NATO cyber operations are still in their infancy. As NATO looks to bring its cyber operations online valid strategies and doctrine are missing. The current Alliance Maritime Strategy, approved in 2011, does not reflect the altered security environment.[3] In particular, NATO has not figured out what cyber operations need to accomplish. What precisely is cyberspace as an operational domain? What are the rules of engagement in

[1] Vice Admiral Clive Johnstone, Commander Allied Maritime Command. Presentation during the Defence and Security Committee Meeting at the NATO Parliamentary Assembly in Istanbul, Turkey. The Role of Allied Naval Forces and Allied Maritime Command after Warsaw 2016. https://www.mc.nato.int/media-centre/news/2016/the-role-of-allied-naval-forces-and-allied-maritime-command-after-warsaw-2016.aspx
[2] Madeleine Moon. Report to the Defence and Security Committee of NATO's Parliamentary Assembly. November 2016.
[3] Steven Teven Horrel, Magnus Nordemann, Walter B. Slocombe. Updating NATO's Maritime Strategy. Issue Brief Atlantic Council. July 5, 2016. 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


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

cyberspace? What type of cyber challenge would trigger the alliance's collective self-defence provision? The European Union is in no different position.[4]

In contrast, naval forces are facing complex maritime challenges following an era of broadly declining maritime investment in line with the general trend of defence budget cuts. Naval budgets were devastated by the cuts started after the Cold War as part of the 'peace dividend', and accelerated in the wake of the 2008 global financial crisis. Ships built today, though far more capable than their predecessors, are proving much more expensive thus increasing the existing financial pressures.

Consequently, equipment inventories have been reduced to critical levels across most weapons categories. Many systems are outdated. Austerity and an increase in missions abroad have further reduced the readiness of Europe's forces to include navies. In many countries, considerable military equipment is not available. At the same time, United States is sending mixed signals about continuing the high level of military support it has provided for Europe in the past decades.

Russia´s engagement in the Ukraine has been a wakeup call to the West. It came by complete surprise, in particular its hybrid design. This development has led to a situation in Europe, where defence budgets are rising again. Consensus is that countries should cooperate more closely and maximize the value of their investments.

To European NATO partners suddenly there is a unique opportunity to build forces to meet 21st-century challenges. With smart choices, European leaders can build the basis for more connected, and more capable armed forces. The 2-percent goal by 2024, as agreed to in NATO's Wales Summit, has highlighted the ambition. Rising defence budgets will facilitate some of the transformative processes needed. It will be of particular importance to increase funding to fight cyber-attacks. Just bolstering the Armed Forces the traditional way may not help at all. European nations will need to upgrade equipment with a special focus on closing today's 'interoperability and digitization' gap. Political and military leaders will need to make choices to enable existing platforms to communicate with each other, allow forces and other security stakeholders to process and analyse data jointly, and build effective cyber forces to defend and better employ the networked forces and critical infrastructures.

Naval forces have an important role in this. 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. Cyberspace enables robust command and control, situational and maritime domain awareness, intelligence gathering, and precision targeting, which are at the core of mission success. Yet, opponents will likely seek to destroy or degrade those capabilities in crisis and conflict. Soon cyberspace may become a game changer.

## 2. Threats and Vulnerabilities

The systems and networks naval forces must protect are complex and large in size. Ships are increasingly using systems that rely on digitization, integration, and automation. 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

[4] Council of the European Union. European Union Maritime Security Strategy. Brussels, 24 June 2014. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT


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

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.[5] This clearly has magnified the risk of unauthorized access or malicious attacks to ships' systems and networks.

The rising tide of information technology driving unpredictable events on global scale constitutes a threat area of its own. The volume of data and the speed can be overwhelming. Data compromise and information loss threaten naval performances. In all senses, information disruption is crippling. Whether caused by malfunction or malevolence doesn´t make a big difference. The results are the same: loss of freedom of action, higher operational risks, damage, injury and even death.

The cyber threats that naval forces continue to face, are stemming from individuals, crime, NGOs, intelligence, national and international actors seeking to probe naval networks for vulnerabilities that can be exploited to their own ends. In the new security environment, opponents and even crazy kids can harm naval forces in nanoseconds, often with scant exposure of attribution. To exploit given vulnerabilities takes only little financial investment, thus making them potentially cheap attack vectors.

Theft, disruption, and destruction are all happening, and getting worse. On daily basis, new vulnerabilities are discovered and published, these publications expand attack surfaces and ease it for malicious actors to penetrate own networks. Risks may even occur from personnel accessing systems on board, for example by introducing malware via removable media.

While the crime space for the defence forces is limited, it still needs to be addressed as given actors use it to commit crimes via hacking against defence organizations and the defence industrial base. On the intelligence space, virtually all aspects of intelligence will eventually be cyber-enabled. While traditional intelligence operations such as terrorist network analysis would be done the old-fashioned way, the big-data analysis of the intelligence would be the cyber-enabled portion.

Also, information operations – i.e. the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent – are becoming cyber-enabled. Cyber will mostly be the means of choice to extracting the data. Actors and nations such as Russia have developed high professional skills to conduct information operations below the threshold of triggering a military response.

Espionage is looking for operational information and technical data, and counter info operations. Nations such as Russia, China, Iran, and North Korea, have been developing quite impressive capabilities. In various stages of competency, they show interest in exploiting naval networks to conduct espionage operations, either by stealing information and technical data on fleet operations or preventing the Navy from taking advantage of information capabilities. All of these threats follow a "cyber kill chain" from discovery to probing, penetrating then escalating user privileges, expanding their attack, persisting through defences, finally executing their exploit.

[5] BIMCO et. alt. The guidelines on cyber security onboard ships. June 2017. Bagsvaerd, Denmark. Pg. 1. http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16


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

One particular closely-watched threat source is the insider threat – i.e. an insider's action that puts an organization or its resources at risk.[6] By virtue of their position within the organization, insiders have already bypassed many of the technical controls and cyber defences that are designed to defeat external threats. These insiders can cause irreparable harm to national security and the Navy's interests in cyberspace - malicious or unintentional.

Attackers in the cyber domain exploit technologies at an accelerating rate. They seek for attack surfaces – i.e. the sum of an organization's security risk exposure. This is the aggregate of all known, unknown and potential vulnerabilities and controls across all software, hardware, firmware and networks - on four given layers:

The physical layer provides the physical infrastructure of the cyberspace, e.g. the hardware. Fibre optic cables including undersea cables, and satellites comprise some of the more prominent features of the physical layers of cyberspace.

The logic layer constitutes the central nervous system of cyberspace. On the logic layer occurs the routing to send and receive messages and to retrieve files. Here are decisions taken. Key elements of the logic layer are Domain Name Servers and Internet Protocols.

The information layer comprises everything that entertains the internet: websites, chats, emails, photos, documents, apps etc. The information layer is reliant on the previous two levels in order to function.

At the user layer people are interacting with cyberspace. As cyberspace is a man-made entity its topography can be changed by people.

Offensive actors understand the naval reliance on communications, ISR, and visualization technologies, and perceive them as vulnerable to disruption and exploitation. They are particularly interested to finding unlocked doors. To this end, they are eager to learn about 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.

Particular successful techniques to gain network or system access include:

- Social Engineering – 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.

In order to degrade or disrupt network activity attackers may attempt to penetrate in-depth across the network and wait until needed. They may also implant software to capture passwords to access privileged

[6] Travis Howard, Jose Arimateia da Cruz The Cyber vulnerabilities of the U.S. Navy. The Maritime Executive. h. Jan 31, 2017.h ttps://maritime-executive.com/article/the-cyber-vulnerability-of-the-us-navy


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

accounts, critical information, sensitive data, state secrets, intellectual property, or C4I systems. Once reliable network access has been established, attackers can move sensitive information to an outside location where encryption can be cracked outside of the compromised environment. Then they would target the victim again or use the information obtained to identify another victim. Once the system or network is compromised, the attacker will blend in with normal traffic, making their detection difficult. In this stage, attackers begin identifying existing security flaws within the network's lifelines and will secretly deploy their cyber tools to probe deeper to identify additional vulnerabilities.

Skilled attackers make an intrusion appear like a computer glitch. They will attempt to get rid of any evidence, such as over-writing data or cleaning up event logs, to make sure they are undetected. Some adversaries plan only one cyber-attack and will disconnect from the system while others may work to establish a backdoor entry so that they can revisit at any time.

## 3. Towards an active Cyber Role

Naval forces must not only ensure the own access to cyberspace, but also increasingly conduct operations in and through cyberspace to ensure naval and joint freedom of action and decision superiority while denying the same to opponents. The days have gone, when cyber was simply an emerging capability that needed to be exploited. Cyber has been moving from a supportive to a rather active role within an operational force. Future missions require to deliver warfighting effects in and through cyberspace, to provide tailored signals intelligence, and to assure critical naval networks.

Operational commanders increasingly build on an active cyber role in every phase of conflict and crisis. Yet, providing cyber capabilities comes on top of the classical shallow water and blue water role. To keep pace with the dynamic mission space and rapidly growing operational needs, naval forces need to mature their effects-delivery capability and capacity. They 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 need to be integrated alongside kinetic action. This would enable integrated fires as cyberspace can increase the effectiveness of traditional kinetic fires through improved intelligence and targeting.

Excellence in defensive and offensive cyber operations is a precondition for operational success. In order to detecting and monitoring opponent´s activities, blocking attacks, manoeuvring to defeat opponents, and defending naval information networks and critical infrastructure[7] 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.

[7] GAO. 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

Defensive cyberspace operations are intended to defend national or allied cyberspace systems or infrastructure. Defensive cyber operations must keep up with constantly incoming attacks. 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.

Offensive cyberspace operations are designed to project power through the application of force in or through cyberspace. Offense has the advantage. Threats in cyberspace develop faster than forces can protect against in many cases. The domain is constantly evolving. New systems, platforms, and tools come up at a rapid pace. Yet, new applications bring along new vulnerabilities.

To keep pace with view to a highly dynamic mission space and rapidly growing operational needs, the naval effects-delivery capability and capacity needs to mature. Increasingly sophisticated capabilities become available to operational commanders and these get in a position to leverage both cyberspace and electromagnetic effects. Effects-delivery capabilities need to be advanced to support a full spectrum of operations. Assured command and control requires key ingredients such as resilient capabilities and networks, diverse architecture, efficient data transfer, and operational knowledge and risk management. This is especially important for key terrains. 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.

Signals intelligence operations can take increasingly full advantage of big data analytic technologies to meet the time sensitive operational demands of operating forces. As signals intelligence derives from electronic signals and systems used by opponents targets, such as communications systems, radars, and weapons systems, it provides a vital window into their capabilities. It furnishes decision makers with vital information about opponents, including their capabilities, actions and intentions. Warfighting effects must be delivered across a full spectrum of operations to include the capabilities to achieve those effects. Through these effects naval forces broaden the range of kinetic and non-kinetic options.

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. Operational commanders, depend on naval networks for command and control, maritime situational awareness, and integrated fires in all phases of conflict or crisis. The availability, integrity, and confidentiality of naval networks and communications systems need to be well protected. A malicious intrusion into naval networks may prove disastrous for own operations. On top networks are required for the logistics, administrative, medical, and training functions. Yet, securely operating and defending naval networks is a particular challenge.

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 cybersecurity 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 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


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

denied operational conditions. Clearly, there is a need to take precautions to ensure continuity of operations in a degraded cyber environment.[8]

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?[9] 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.[10] To enable shared cyber situational awareness will require that a data-driven analysis can be transformed into visualized situational awareness.

## 4. Delivering Cyber Capabilities

Today navies acknowledge the importance of cyberspace as a critical enabler. Yet, with view to delivering appropriate cyber capabilities, NATO nations in Europe still have a long way to go. Up to now guiding doctrine is missing. Naval strategies are in a period of transition. NATO is planning to revise its outdated 2011 Alliance Maritime Strategy, which no longer reflects the present geostrategic reality. It needs a strategy that identifies the 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 strategy update.[11] The same is true for the slightly younger European Union Maritime Security Strategy that hardly mentions the word cyber.[12]

NATO's initial top cyber priority has been the protection of the communications systems owned and operated by the Alliance. To facilitate an Alliance-wide and common approach to cyber defence capability development, NATO has defined targets for Allied countries' implementation of national cyber defence capabilities via the NATO Defense Planning Process. Cyber defence has also been integrated into NATO's Smart Defense initiative that enables countries to work together to develop and maintain capabilities they could not afford to develop or procure alone, and to free resources for developing other capabilities.

[8] GAO. Report to Congressional Committees. Defense Cybersecurity. DOD's monitoring of progress in implementing cyber strategies can be strengthened. Washington. August 2017. Pg. 30. https://www.gao.gov/assets/690/686347.pdf
[9] Vice Admiral Clive Johnstone …
[10] U.S. Fleet Cyber Command/Tenth Fleet. Strategic Plan 2015-2020. Pg. 18http://www.navy.mil/strategic/FCC-C10F%20Strategic%20Plan%202015-2020.pdf
[11] Violetta Rusheva. Deputy Assistant Secretary General for Emerging Security Challenges at NATO Jamie Shea said that present maritime policy does not lift a number of threats to its members. New Europe. October 27, 2017. https://www.neweurope.eu/article/nato-current-maritime-environment-poses-threats-us/
[12] Council of the European Union. European Union Maritime Security Strategy …


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

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.

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. 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.

NATO has started working closely with the European Union. The nature of this cyber cooperation is complementary. 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.

NATO has recently announced the establishment of a cyber operations centre. Defense ministers strive to integrate cyber into all NATO planning and operations to become just as effective in the cyber domain, as NATO is in air, on land and at sea.[13] The cyber operations centre could take on a role of a NATO special operations headquarters, include NATO-owned offensive capability, become a clearinghouse for coordination of nationally-owned offensive capabilities and serve as a pool of operational and tactical cyber expertise.

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 warfighting capabilities as these will be particularly valuable when they can be delivered reliably and in concert with other capabilities. Interoperability across joint weapon delivery platforms will essential to make tools and methods easy to employ.

As globalization expands and opponents become increasingly sophisticated cyber strategists and planners need to focus on flexibility at tactical levels. 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

[13] NATO. Defence Ministers agree to upgrade NATO Command Structure. Brussels 08 Nov. 2017. https://www.nato.int/cps/en/natohq/news_148419.htm?selectedLocale=en


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

operate from a contested cyber space environment needs to be a top priority. Naval forces need to embrace cyber effects as an integral component of naval power.

To this end, maritime strategy and subsequent operational concepts should focus on generating interoperable naval forces capable of establishing and maintaining all-domain access.[14] 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. For lesser technologically advanced navies, cyber capabilities will still play an important role in augmenting other capabilities by providing command and control and acting as a force multiplier in certain situations.

Staying ahead in this rapidly altering domain requires tempo and agility in the planning, budgeting and acquisition of cyberspace capabilities. To this end 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.

A sense of urgency is needed to address ongoing naval cyber security challenges. Vice Admiral Clive Johnstone, Commander Allied Maritime Command, has 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."* [15]

***

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

This paper was presented under the title "Cyber Security in the Naval Domain" at the NATO Allied Maritime Command in Northwood, UK on December 6, 2017.

[14] Steven Teven Horrel …
[15] Vice Admiral Clive Johnstone …


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 D. Thiele is President of EuroDefense Germany, Chairman of the Political-Military Society (pmg), Berlin, Germany and CEO at StratByrd Consulting. In 40 years of politico-military service, Colonel (ret.) Thiele has gained broad political, technological, academic and military expertise. He has been directly involved in numerous national and NATO strategic issues while serving as executive officer to the Bundeswehr Vice Chief of Defence Staff, Military Assistant to the Supreme Allied Commander Europe, in the Planning and Policy Staff of the German Minister of Defence, as Chief of Staff of the NATO Defense College, as Commander of the Bundeswehr Transformation Centre and as Director of Faculty at the German General Staff and Command College in Hamburg.

He has published numerous books and articles and is lecturing widely in Europe, Asia (Beijing, Seoul, Tokyo, and Ulaanbaatar) in the U.S. and Brazil on current comprehensive security affairs, cyber security, border security, maritime domain security, protection of critical infrastructure and defence and also historical issues.

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