Seminar

Report

Good Practices in Countering Terrorism in

MARITIME DOMAIN

4-5 October, 2023

Ankara, TÜRKİYE

DISCLAIMER

This Seminar report is a product of the Centre of Excellence Defence Against Terrorism (COE-DAT), and is produced for NATO, NATO member countries, NATO partners and related private and public institutions. The information and views expressed in this report are solely those of the authors and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the authors are affiliated.

CONTENT

DISCLAIMER 1

CONTENT 2

Seminar Team 4

Good Practices in Countering Terrorism in Maritime Domain Seminar 5

Introduction 5

DAY I 7

Contemporary Approaches on Maritime Counter-Terrorism as a part of Maritime Security 7

Lt.Jr. H.Engin CANTEKİN (TUR A, MARSEC COE) 7

Discussion 11

Implications of the new NATO strategic Concept for Countering Maritime Terrorism at the Black Sea and other Seas of Recent Conflict 12

Ret. Col. Dr. Marten MEIJER, Director Meijer Innovation Partners Ltd. Blaricum, The Netherlands 12

Terrorist Use of Emerging and Disruptive Technologies (EDT) in the Maritime Domain (Online) 14

Prof. Dr. Arnold DUPUY (Naval Postgraduate School, Atlantic Council, US) 14

Ship Cyber Security Management (Online) 16

Prof. Dr. Arnold DUPUY (Naval Postgraduate School, Atlantic Council, US) 16

Discussion 18

Secure Data and Communications at Sea 20

Mrs. Kristen KUHN, PhD (Coventry University, Researcher, UK) 20

Discussion 22

Indo Pasific Legal Aspects-the Law of Armed Conflict in Maritime Security, ... 23

Dr. Joanna SIEKIERA (Faculty of Law, University of Bergen, Norway) 23

Discussion 24

DAY II 25

Usage of Maritime Unmanned Systems in Maritime Counter Terrorism 25

CDR Francisco CAVACO (PRT N, MARSEC COE) 25

Discussion 27

South China Sea Hybrid Threats on Maritime Security/Undersea communication cables to hybrid threats 28

Mrs. Diren DOĞAN (Alanya Alaaddin Keykubat University, Türkiye) 28

Discussion 30

The Importance of Bilateral and Multinational Cooperation in Maritime Terrorism 31

Mr. Kenneth YEO (S. Rajaratnam School of International Studies, Singapore) 31

Cognitive Aspects of Cyber Threats 40

Dr. Vira RATSIBORYNSKA (Vrije Universiteit Brussel, NATO, Belgium) 40

Conclusion 44

Seminar Team

Seminar Director

Mrs. Müge MEMİŞOĞLU AKAR (TUR Civ.)

Activity Assistant

Mrs. Aslıhan AKYOL KEMER (TUR Civ.)

Speaker & Organizations

Lt. Jr. H.Engin CANTEKİN (TUR A, MARSEC COE)

Ret. Col. Dr. Marten MEIJER (Senior Maritime Specialist, Director Meijer Innovation Partners Ltd. Blaricum, The Netherlands)

Prof. Dr. Arnold DUPUY (Naval Postgraduate School, Atlantic Council, USA)

Mrs. Kristen KUHN, PhD (Coventry University, Researcher, UK)

Dr. Joanna SIEKIERA (Faculty of Law, University of Bergen, Norway)

Cdr. Francisco CAVACO (PRT N, MARSEC COE)

Mrs. Diren DOĞAN (Alanya Alaaddin Keykubat University, Türkiye)

Mr. Kenneth YEO (S. Rajaratnam School of International Studies, Singapore)

Dr. Vira RATSIBORYNSKA (Vrije Universiteit Brussel, NATO, Belgium)

Rapporteur

Ms. Elif Merve DUMANKAYA (TUR)

Good Practices in Countering Terrorism in Maritime Domain Seminar

Introduction

Hosted by COE-DAT in Ankara, Türkiye, from October 04th to 05th, 2023, the “Good Practices in Countering Terrorism in Maritime Domain Seminar” convened a distinguished panel of experts. The seminar aimed to address the emerging challenges in maritime security, with a specific focus on countering terrorism in the dynamic and evolving maritime domain.

Lt. Jr. H. Engin CANTEKİN set the stage by acknowledging that the field of maritime terrorism is still in its nascent stages, despite debates within academic circles. He emphasized the imperative for security and counter-terrorism professionals to comprehend and combat the diverse ways terrorists exploit the maritime domain. Recognizing the disparity in defining terrorism, he stressed the importance of understanding maritime terrorism’s modalities. The escalating threat in the maritime domain has garnered significant attention due to its potential to disrupt global trade, endanger lives, and compromise national security. Lt. Jr. CANTEKİN highlighted the growing role of advanced technologies in maritime security operations to counter this evolving threat.

Dr. Marten MEIJER delved into the NATO Strategic Concept, emphasizing the commitment to defending the rules-based international order. He underlined the importance of enhancing dialogue and cooperation to address shared security threats, with a specific mention of the menace posed by terrorist organizations. Dr. MEIJER’s analysis shed light on NATO’s role in defending against maritime terrorist attacks and the need for a comprehensive approach.

Prof. Arnold C. Dupuy presented on Emerging and Disruptive Technologies (EDTs), emphasizing their potential benefits and risks in the maritime domain. He explored the unique challenges these technologies pose to security forces, especially in detecting, defeating, and recovering from attacks. Prof. Dupuy addressed the application of EDTs by terrorist organizations and proposed mitigating strategies.

In his second presentation, Prof. Dupuy focused on Ship Cyber Security Management, highlighting the vulnerability of the global maritime sector to cyber threats. He discussed the threats in maritime cyber security and recommended international guidelines and security standards to mitigate risks.

Mrs. Kristen Kuhn underscored the urgent need to strengthen maritime cyber resilience against escalating threats and potential terrorism. She explored how geopolitical interests and terrorist motives could amplify cyber threats, emphasizing collaborative efforts between governments, international organizations, and the private sector. Mrs. Kuhn proposed strategic methodologies for maritime stakeholders to adopt proactive cybersecurity measures.

Dr. Joanna Siekiera provided a comprehensive overview of the legal aspects in maritime security, stressing the evolving challenges and opportunities. She highlighted the unpredictable nature of terrorism, its impact on the rules-based international order, and the need for NATO to proactively address existing and emerging threats in the Indo-Pacific.

CDR Francisco CAVACO focused on the usage of Maritime Unmanned Systems (MUS) in support of Maritime Security Operations. He highlighted the advantages of MUS, including enhanced situational awareness and reduced risk to human life, proposing a seamless partnership between autonomous systems and human operators.

Mrs. Diren DOĞAN provided a comprehensive understanding of the South China Sea disputes, emphasizing their reflection on the international system. She delved into China’s three distinct warfare doctrines and underscored the global significance of the South China Sea, urging a nuanced approach to navigate its complexities.

Mr. Kenneth YEO’s presentations unveiled the complex nexus between maritime activities and regional terrorism, emphasizing the need for multilateral cooperation. He analyzed the Philippines’ dual maritime challenges and provided insights into the threat landscape presented by terrorist groups in Indonesia and the Philippines.

Dr. Vira Ratsiborynska’s presentation explored the cognitive dimension of war in the context of changes in the security environment and evolving cyber threats. She critically reflected on the question of a cognitive dimension of war, outlining different perspectives on cognitive aspects of cyber threats and the need for NATO’s engagement.

The seminar provided a platform for in-depth discussions, critical analyses, and recommendations, fostering a collective effort towards countering terrorism in the maritime domain. The diverse expertise of the speakers contributed to a holistic understanding of the challenges and opportunities in maritime security.

DAY I

Contemporary Approaches on Maritime Counter-Terrorism as a part of Maritime Security

Lt.Jr. H.Engin CANTEKİN (TUR A, MARSEC COE)

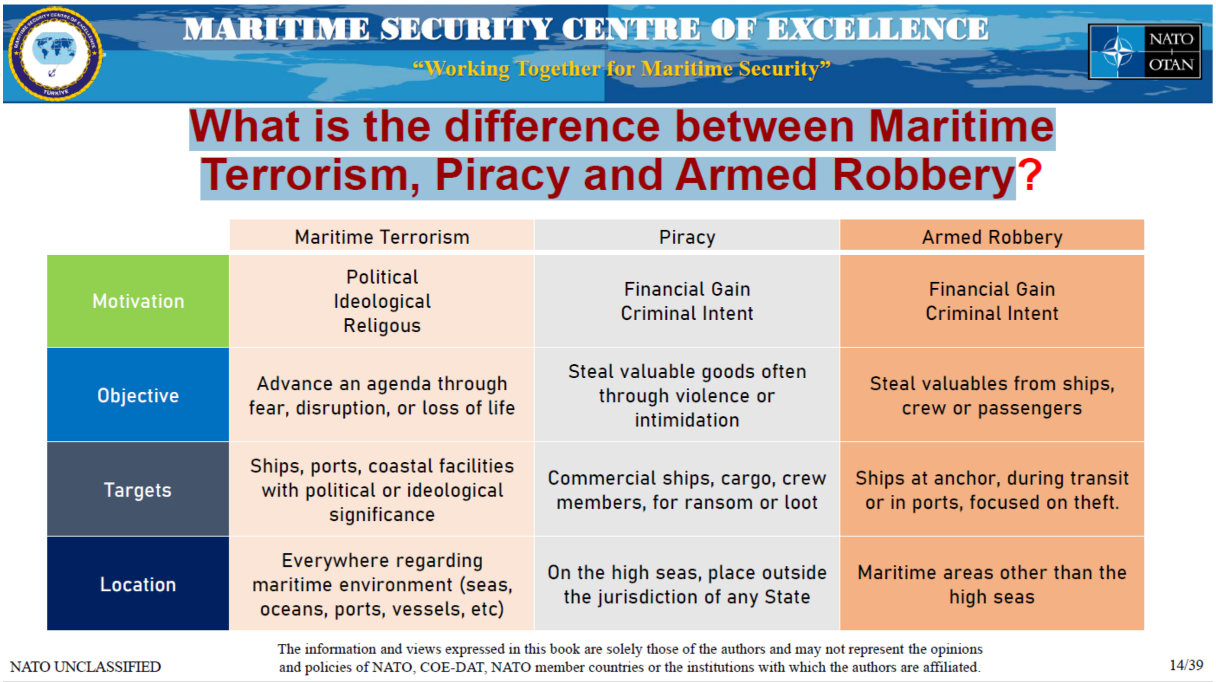
Lt. Jr. H. Engin CANTEKİN presented on NATO's maritime counter-terrorism efforts, which are primarily focused on enhancing security and preventing potential attacks. The initiative gained momentum, particularly after the events of 9/11. In 2011, NATO approved the Maritime Security Concept (MC 0588), consisting of seven Maritime Security Operations (MSO) tasks. Subsequently, an overarching Maritime Strategy was adopted by the Alliance, a framework also embraced by MARSEC COE.

The key areas covered by this strategy include:

1. Supporting Maritime Situational Awareness
2. Contributing to Maritime Security Capacity Building
3. Supporting Maritime Counter-Terrorism
4. Upholding Freedom of Navigation
5. Fighting Against Proliferation of Weapons of Mass Destruction
6. Protection of Critical Infrastructure
7. Maritime Interdiction Operations

Maritime terrorism, as defined in the speech, involves "*terrorist acts within the maritime environment, targeting vessels, fixed platforms, passengers, personnel, coastal facilities, settlements, tourist resorts, port areas, and port towns or cities*". The Maritime Security Concept outlines maritime counter-terrorism as the "*deterrence, defense, disruption, and protection against terrorist activities, involving planning and conducting operations to deny access to designated areas and apply forceful containment of maritime-based threats*."

While explaining the differences between Maritime Terrorism, Piracy, and Armed Robbery, he has presented the distinctions through motivation, objective targets, and location in his presentation. The table illustrating these differences, as included in Lt. Jr. H. Engin CANTEKİN's presentation, is provided below.



MARITIME SECURITY CENTRE OF EXCELLENCE

“Working Together for Maritime Security”

NATO OTAN

What is the difference between Maritime Terrorism, Piracy and Armed Robbery?

	Maritime Terrorism	Piracy	Armed Robbery
Motivation	Political Ideological Religous	Financial Gain Criminal Intent	Financial Gain Criminal Intent
Objective	Advance an agenda through fear, disruption, or loss of life	Steal valuable goods often through violence or intimidation	Steal valuables from ships, crew or passengers
Targets	Ships, ports, coastal facilities with political or ideological significance	Commercial ships, cargo, crew members, for ransom or loot	Ships at anchor, during transit or in ports, focused on theft.
Location	Everywhere regarding maritime environment (seas, oceans, ports, vessels, etc)	On the high seas, place outside the jurisdiction of any State	Maritime areas other than the high seas

NATO UNCLASSIFIED

The information and views expressed in this book are solely those of the authors and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the authors are affiliated.

14/39

After providing an overview of contemporary approaches to Maritime Counter-Terrorism, Lt. Jr. H. Engin CANTEKİN delves into the threats posed by maritime terrorism. These threats encompass a wide range of consequences, including loss of life, economic disruption, environmental damage, fear and panic, trade disruption, infrastructure disruption, political and social instability, insecurity, insurance and legal challenges, and tensions in international relations. Notably, maritime terrorism can serve as a precursor to attacks or be linked to money laundering and drug trafficking.

Lt. Jr. H. Engin CANTEKİN emphasizes that these attacks can manifest through various means, such as direct assaults from the sea, attacks on coastal regions, employing classic terrorist attack strategies, or even through cyber attacks.

Furthermore, he proceeds to define different types of maritime terrorism incidents, starting with the type involving attacks on the water from the water. As an illustrative example, he refers to the USS Cole Attack in the year 2000. The second type of attack is the attack on the water from the land. The drone strikes on the Mercer Street Vessel in 2021 was raised as an example of this type of attack. The attack was conducted in the Gulf of Oman and let to the loss of lives of two crew member. Lt. Jr. CANTEKİN stressed that these attacks are becoming more common nowadays due to the use of unmanned systems by different groups easily. As a third category, attacks *from the air* could be considered. These attacks are also heavily conducted by the use of unmanned systems which terrorist organizations have been highly exploiting. *Precursors attacks* in the maritime domain were also mentioned in the presentation. In this context, attacks in India in 2008 were given. During these attacks, the terrorists hijacked the Kuber, which was simply a fishing vessel, claiming the lives of all crew members but the captain. The captain was compelled to steer the ship to Mumbai. This attack was considered as an important example of precursor attack, which lead to the death of approximately 200 people. As a fifth category, Lt. Jr. CANTEKİN touched upon the attacks on the land from the water. In 2008, a number of coordinated attacks occurred in Mumbai, India. One of the significant characteristics of the attack is its simultaneous targeting of different coastal locations. Terrorist used small boats to reach their targets. Depending on several incidents such as this one, Lt. Jr. CANTEKİN stressed that countries should not underestimate the threats that could be directed from the sea to the lands. As an instance of classical terrorist attack strategy. Lt. Jr. CANTEKİN examined the attack by the Abu Sayyaf Group (ASG) on the Philippines ships. Terrorists attacked these ships by placing bombs in a television set and claimed over one hundred lives. Finally, Lt. Jr. CANTEKİN talked about the *attacks on the coastal regions* by shedding the light on the Sri Lanka Easter Sunday Bombings in 2019. In addition to these, Lt. Jr. CANTEKİN emphasized that the maritime domain serves as an area for Money Laundering and Drug Trafficking for terrorists. He stated that, from this perspective, monitoring maritime security and combating terrorism at sea are essential. Lt. Jr. CANTEKİN, emphasizing the need to enhance cyber resilience and capacity for the protection of maritime forces, recalled the example of the Port of Antwerp. He highlighted that the port had been subjected to cyber attacks by drug traffickers over a two-year period. Lt. Jr. CANTEKİN stated that MARSEC COE is working to develop the concept of cyber intelligence and maritime security operations to effectively combat cyber threats in this area.

In the context of utilizing technology in maritime counter-terrorism, Lt. Jr. CANTEKİN specified four different categories as follow:

- Surveillance and Reconnaissance,
- Unmanned Systems,
- Artificial Intelligence,
- Biometric Identification.

Surveillance and Reconnaissance: Over the past two decades, terrorists have increasingly utilized small boats to carry out attacks in the maritime domain. Additionally, they have sought to exploit security vulnerabilities by acquiring cost-effective unmanned systems. Consequently, the significance of reconnaissance and surveillance systems has never been more crucial.

Synthetic Aperture Radar (SAR) Systems are discussed as a means to combat these threats. These systems are capable of detecting small boats, offering a range of advantages:

- They can operate day or night; are effective in any weather conditions;
- have the ability to collect data at different wavelengths and polarizations; can penetrate subsurface elements such as vegetation and soil to a varied extent;
- can provide very detailed, high-resolution images; have the capability to collect data that can be processed, examined, and combined with other types of data, including optical satellite data, in unique ways.

In essence, SAR systems offer a comprehensive solution for identifying and addressing the challenges posed by terrorists utilizing small boats and unmanned systems in the maritime domain.

Unmanned Systems: Unmanned systems play a crucial role in bolstering maritime counter-terrorism initiatives, particularly in safeguarding vulnerable targets. Unmanned Aerial Vehicles (UAVs) and Unmanned Surface and Underwater Vehicles, equipped with advanced sensors, contribute significantly to enhancing maritime situational awareness. Their deployment enables swift response and efficient data collection in remote or hazardous areas. By leveraging the capabilities of these unmanned systems, authorities can proactively address maritime security challenges, ensuring a more robust defense against potential threats.

Artificial Intelligence: Big data analytics and artificial intelligence play a pivotal role in analyzing vast amounts of information. These technologies excel at identifying patterns and anomalies, enabling the detection of potential threats. By harnessing the power of artificial intelligence, security efforts are strengthened, providing a proactive approach to mitigating online terrorism risks.

Biometric Identification: Biometric systems, including facial recognition and fingerprint scanning, are employed for personnel identification and access control at ports and critical infrastructure.

In conclusion, Lt. Jr. CANTEKİN emphasized that maritime security could be implications over various fields including security, economy, technology, safety. Terrorist organizations could target the maritime vehichles, coasts, ports and other critical infrastructures of maritime domain to cause casualties and political and economic harms. In this sense, maritime security operations can help preserve these critical components as well as maintain the secutiry in the maritime domain. On the other hand, Lt. Jr. CANTEKİN underlines the fact that tecnology's impact has been twofold. On the one hand, it enables the authorities to effectively address current challenges in a shorter but powerful manner. On the other hand, the terrorists have learned how to make use of these new technologies and further challenge the states and. Lt. Jr. CANTEKİN stated that a comprehensive maritime counter-terrorism strategy requires a proactive approach to address these threats.

Discussion

The discussion session commenced with a question about the impact of counter-terrorism activities, particularly in economic domains. In a hypothetical scenario where a port is closed due to the perceived risk of an explosion, the challenging economic repercussions for the state were highlighted.The query about the real-time operation of SAR systems was raised, to which Lt. Jr. Cantekin responded affirmatively, stating that they are currently in use and can be integrated into both aircraft and unmanned systems.

Lt. Jr. Cantekin addressed inquiries about the possibility of attacks originating from underwater sources, clarifying that unmanned systems have been involved in such incidents. Anticipating an increase in these types of attacks, particularly those directed by submarines, Lt. Jr. Cantekin emphasized the need for analysts capable of understanding both past and future developments.

Highlighting the importance of manpower, he underscored the necessity for well-educated and experienced individuals, particularly in intelligence and naval operations. While technology is advancing rapidly, the importance of a skilled workforce is paramount.

Regarding data usage, the discussion emphasized the need for well-organized fusion centers that bring together data and intelligence. Lt. Jr. Cantekin stressed the importance of staying ahead of technological waves, calling for technical assistance in maritime operations and the establishment of proficient fusion centers.

Implications of the new NATO strategic Concept for Countering Maritime Terrorism at the Black Sea and other Seas of Recent Conflict

Ret. Col. Dr. Marten MEIJER, Director Meijer Innovation Partners Ltd. Blaricum, The Netherlands

Dr. Marten MEIJER started his presentation by reminding that there was once was a perception that maritime terrorism was not a significant concern, but this perception has been changing recently. Ret. Col. Dr. Marten MEIJER, while discussing NATO's new strategic concept, highlighted the persistent perception of "*Keeping Russia out of Europe, Germany down in Europe, USA in Europe*," noting that this is not a new agenda item. Especially after Russia's intervention in Ukraine, he emphasized the increased importance for NATO to adhere to international law. Dr. MEIJER argued that this emphasis should extend to maritime security, an area NATO has been closely monitoring in recent times.

Regarding terrorism, Dr. MEIJER noted that its intention is to spread fear and anxiety. However, he pointed out that this impact is limited at sea due to the low number of people present. He emphasized that attacks on land leave a lasting imprint on people's minds, contrasting this with the fact that high seas lack constant surveillance cameras, being monitored by satellites from space. He expressed that the power of witness in the seas is not as intense as on land.

Dr. MEIJER raised the challenge of addressing the concepts of "fear" and "anxiety" in NATO's definition of terrorism in the context of the sea since he believes these notions are not very influential if the incidents are taking place on the seas. In terms of the negative effects of the terrorism in the maritime domain, Dr. MEIJER touched upon the attacks of sea lines of communication. He underlined that these attacks affect millions of people due to their impact on global logistics, data cables, and gas pipelines. However, he clarified that the impact is more financial than psychological.

In terms of the instances of maritime terrorist attacks, Dr. MEIJER provided for different cases:

1. Sinking wooden Iranian Fishing Vessel Mosin 24 October 2012 in Somalia Territorial Waters,

2. Polluting Somalia Territorial Waters by North Korean Dae San Cement Cargo Carrier in November 2012,
3. Chasing Ultra Large Crude Carrier Grace 1 at Gibraltar Straits 4 July 2019,
4. Destroying Gas Pipeline Nord Stream 2 in Baltic Sea 26 September 2022.

In conclusion, Ret. Col. Dr. Marten MEIJER offers a thought-provoking perspective on maritime terrorism. He challenges the conventional understanding by stating that “Maritime Terrorism is Contradictio in Terminis.” In the context of the threats posed by maritime terrorism, it is conveyed that the fear and anxiety generated by such incidents impact individuals living in coastal areas, aligning with NATO’s definition of terrorism. However, the speaker notes that when incidents that could be considered as terrorism occur in high seas, they do not evoke the same level of impact. The distinction lies in the geographical context, suggesting that the psychological effects of maritime terrorism are more pronounced when closer to populated coastal regions. In this sense, terrorist attacks at high seas primarily yield financial results rather than psychological impacts, according to Dr. MEIJER.

Dr. MEIJER advocates for an increased focus on surveillance at sea, emphasizing the need for enhanced maritime patrolling and satellite surveillance. He suggests employing automated identification systems, monitoring ships at sea, and deploying unmanned surveillance systems afloat or on the sea bed. This nuanced perspective prompts a reassessment of the traditional notions surrounding maritime security and terrorism, urging a more comprehensive and technology-driven approach to safeguarding the seas.

Finally, NATO’s way forward was discussed, emphasizing the importance of adhering to the rule of law, being transparent, and acknowledging the role of truth in the battlefield by stressing that NATO’s strength as an alliance. Overall, the presentation highlighted the evolving perception of maritime terrorism and the need for vigilance and cooperation in addressing potential threats at sea.

Terrorist Use of Emerging and Disruptive Technologies (EDT) in the Maritime Domain (Online)

Prof. Dr. Arnold DUPUY (Naval Postgraduate School, Atlantic Council, US)

Prof. Dr. Arnold Dupuy provided the definitions of emerging and disruptive technologies, with a focus on how disruptive technologies can change the perception and practices of organizations. Emerging and disruptive technologies (EDTs) are new innovations, which are recently developed, are under development, or are likely to be developed, that can drastically change how organizations and industries' function. These can range from Artificial Intelligence (AI)—deepfakes, video manipulations, autonomous systems (drones, airborne and/or maritime), quantum computing, biotechnologies, hypersonics, space-based applications (GPS/GNSS), novel materials and manufacturing, energy and propulsion and next-generation communications networks.

While these technologies have the potential to benefit broader society, in the hands of terrorists, they could prove devastating. Moreover, terrorist activities in the maritime domain, present unique challenges to security forces when trying to detect, defeat and recover from such attacks. As most global trade is dependent on maritime activity, any serious disruption to this sector could negatively economic viability, particularly emerging nations. This is particularly so with nations that are already being destabilized or under threat by terrorist groups operating on their territory. This presentation addresses the specific EDTs in the maritime domain context, their potential applications by terrorist organizations and mitigating strategies.

NATO's innovation priorities were outlined, including AI, autonomous systems, quantum computing, biotechnologies, hypersonics, and more. Prof. Dupuy made a definition of terrorism as a political attack aimed at undermining legal authorities' credibility, emphasizing how such attacks enable radicalization, recruitment, and planning through technology like social media and gaming platforms. The ODNI's 2022 Annual Threat Assessment was mentioned during the presentation, which highlighted the expectation that terrorist organizations would leverage emerging technologies such as AI, robotics, automation, and smart materials. Examples from Ukraine and Syria showcased innovations by not only terrorist organizations but also intelligence agencies and security bureaucracies.

The use of drones for ISR (Intelligence, Surveillance, and Reconnaissance) activities, including weaponized drones, was discussed. The significance of the maritime domain in counter-terrorism, especially due to its critical role in global trade, was highlighted. Threats in this domain could have significant economic and supply chain implications. Various maritime threats, including MIEDs (Maritime Improvised Explosive Devices), surface/sub-surface attacks, small boat attacks, and the vulnerability of undersea fiber-optic cable networks, were addressed.

Countering maritime terrorism requires a multifaceted approach that incorporates various strategies and collaborative efforts. First and foremost, establishing threat awareness is critical. This involves staying abreast of emerging technologies and understanding potential terror groups and their capabilities. Enhancing technological literacy at all organizational levels is imperative, necessitating the recruitment and hiring of competent staff with the necessary expertise. Legal changes may also be required to adapt to evolving threats.

Organization-wide threat and technology training should be implemented to ensure that every member is equipped to recognize and respond effectively to potential risks. Stakeholder collaboration plays a pivotal role in countering maritime terrorism. This involves the development and study of best practices and lessons learned, fostering relationships with international, federal, state, and local partners. Sharing best practices and lessons learned is essential for building a collective knowledge base.

Joint counter-terrorism drills and training exercises enhance coordination and preparedness. Continuous assessment of resource requirements is crucial, involving proactive evaluations of resource allocation and investments. The utilization of cutting-edge technologies is also essential in countering maritime terrorism. This includes information collection, decision-support tools for data analysis, and the use of biometric, data mining, video, and metadata analysis. The integration of AI technology for threat monitoring is recommended, with a focus on restrained and judicious use within the framework of the law. Through a comprehensive and collaborative approach, countering maritime terrorism becomes more effective and adaptive to evolving threats.

In short, the presentation underscored the evolving landscape of terrorism involving emerging and disruptive technologies in the maritime domain and the importance of proactive countermeasures and collaboration to address these challenges effectively.

Ship Cyber Security Management (Online)

Prof. Dr. Arnold DUPUY (Naval Postgraduate School, Atlantic Council, US)

In his second presentation, **Prof. Dupuy** touched upon the increasing use of new technologies, automation, and digitalization in the maritime sector, which have both benefits and risks. There is a need for greater awareness of cyber threats. A rise in cyber incidents has been observed, impacting shipping and offshore operations.

Commercial cyber requirements and associated risks were discussed. The recent incident at the Suez Canal served as an illustration of how disruptions in maritime activities can have far-reaching consequences, highlighting real and tangible threats to the maritime domain. A timeline of non-kinetic attacks on critical infrastructure was presented, with a question raised about whether June 2017 could be considered a turning point in cyber attacks.

The Maersk Not Petya cyber attack was highlighted as an example of how cyber attacks could have high-impact consequences. Shipboard systems' vulnerabilities were discussed, emphasizing similarities to onshore threats, and distinguishing between IT (Information Technology) and OT (Operational Technology) networks. Prof. Dr. Arnold Dupuy discussed the cybersecurity themes and initiatives at the Naval Postgraduate School, including five pillars, cyber threat awareness, collaboration tools, incident reporting, and legal responsibilities. The presentation emphasized the importance of defining and declaring cyber security incidents, clarifying attacks, and developing incident reporting procedures.

Other areas of concern included the need for a shared cybersecurity incident response communication strategy, documenting and sharing lessons learned from cyber security incidents, and the importance of a testing environment for threat detection. The presentation addressed the critical need for cybersecurity measures in the maritime sector, emphasizing awareness, preparedness, and collaboration to mitigate cyber threats effectively.

Modern ships heavily rely on sophisticated shipboard systems to navigate, control propulsion, manage cargo, ensure safety, and facilitate communication. The integration of advanced technologies, while enhancing efficiency and safety, also introduces vulnerabilities that need careful consideration:

1. **Bridge Control:** Shipboard systems like Voyage Data Recorders (VDR) and Automatic Radar Plotting Aids (ARPA) on the bridge are crucial for navigation. Vulnerabilities in these systems could compromise the ship’s ability to navigate safely.
2. **Propulsion and Power:** Systems controlling engines, steering, fuel, and machinery are vital for propulsion and power management. Any compromise in these systems could lead to propulsion failure or other critical issues.
3. **Navigation:** Navigation systems such as GPS/GNSS, Electronic Chart Display and Information System (ECDIS), radar, and weather systems are essential for safe passage. Cybersecurity threats to these systems may jeopardize the ship’s navigation accuracy.
4. **Loading and Stability:** Ballast systems, hull stress monitoring, and stability control systems play a crucial role in maintaining the ship’s stability. Vulnerabilities in these systems could lead to accidents or instability.
5. **Safety Systems:** Fire and flood control systems, tracking, shipboard security, Closed-Circuit Television (CCTV), and emergency shutdown systems are critical for the safety of the crew and the vessel. Cyber threats to these systems pose severe risks.
6. **Communications:** Shipboard communication systems, including satellite internet, ship-to-shore, ship-to-ship, and Voice-over-IP (VoIP), are essential for operational and emergency communication. Cyberattacks on these systems may disrupt communication.
7. **Operations Security:** Human-machine interfaces (HMIs), logic controllers (PLCs), and digital/analog sensors are integral to ship operations. Cyber vulnerabilities in these interfaces could compromise overall operational security.
8. **Network Security:** Firewalls, segmentation devices, antivirus software, and regular software updates are critical for protecting shipboard networks from cyber threats. Breaches in network security could expose sensitive information.
9. **Physical Security:** Ensuring the physical security of server rooms, access control systems, and network infrastructure is crucial to prevent unauthorized access or tampering.
10. **Ship Networks:** Email systems, personnel administration, and maintenance and spares management networks are vulnerable to cyber threats that could disrupt shipboard operations.
11. **Crew Network:** Crew networks, including email and Wi-Fi, are susceptible to cyber intrusions that may compromise crew communication and privacy.

12. **Supply Chain:** Remote or on-shore vendor updates, maintenance procedures, and administration processes are potential targets for cyber threats, impacting the ship's overall supply chain.

Understanding and addressing these vulnerabilities are essential to ensure the resilience and cybersecurity of modern shipboard systems, safeguarding both the vessel and its crew from potential cyber risks. Regular assessments, updates, and adherence to cybersecurity best practices are crucial in mitigating these threats.

Discussion

One of the participants asked, "*We can consider maritime infrastructure as critical infrastructure, and an attack could result in severe damage. If a cyber-attack leads to such consequences, and we can identify its source, can we provide a collective defense response*?" In response, Prof. Dupuy mentioned that an evaluation could be discussed further under Article 5 in such a scenario. Discussions are ongoing regarding the scope and evaluation of non-kinetic attacks.

Another participant commented that the technology is advancing at an unstoppable pace, but efforts to combat the threats it creates are not keeping up. This also applies to legal efforts. Worldwide implementation requires a culture shift, but traditional law lacks such norms. An assessment from international law is needed; however, the participant disgreed that the law can catch up with this problem in the medium to long term. Prof. Dupuy acknowledged the challenges, mentioning that no one from institutions is keeping up or developing preemptive measures, especially from a legal standpoint. He emphasized the need for leaders knowledgeable in this area to take responsibility and act, recognizing that legal regulations often lag behind.

During the discussion, a participant remarked that resilience is a national responsibility and added that cyber security is a different dimension, and states cannot mobilize ground forces for it.. Preventing a cyber-attack is extremely challenging, as you only learn of the attack after it's completed. Participant stated that information sharing is crucial in tackling such threats and must be encouraged. Prof. Dupuy weighed in on the difficulty of preventing cyber-attacks and the challenges in information sharing due to varying national agendas within the Alliance. He emphasized the importance of sharing for mutual benefit and acknowledged the challenging nature of this aspect for the alliance.

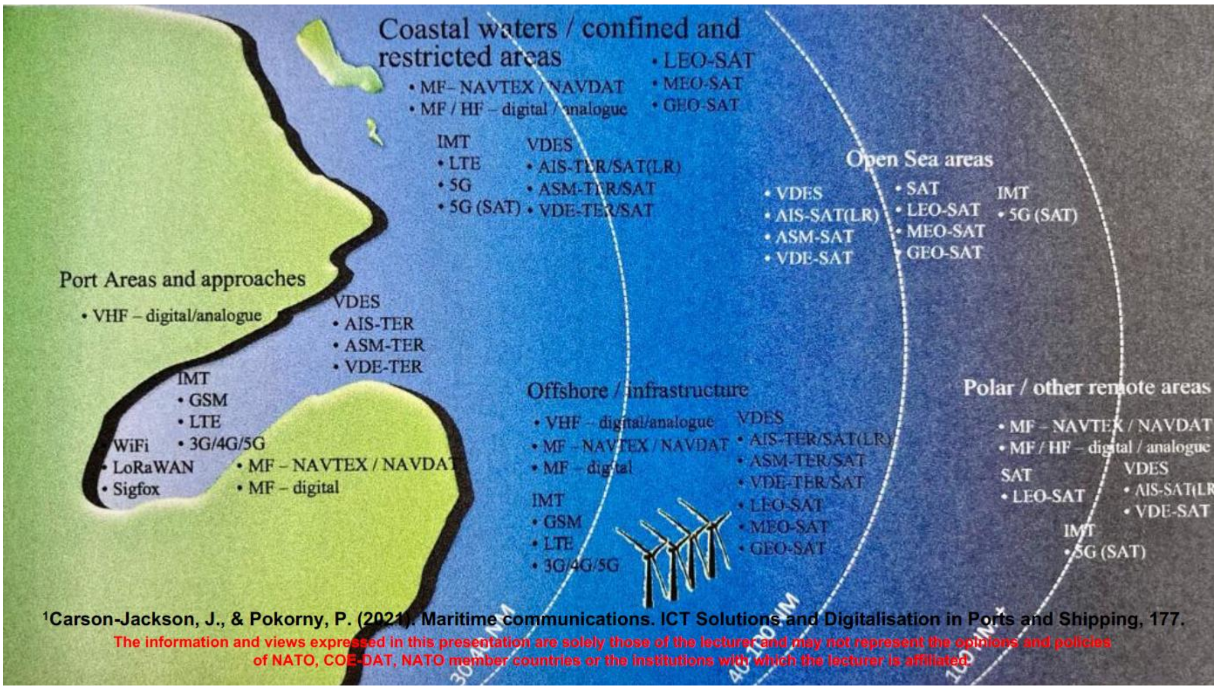
Secure Data and Communications at Sea

Mrs. Kristen KUHN, PhD (Coventry University, Researcher, UK)

During her presentation on “Secure Data and Communications at Sea”, **Mrs. Kristen Kuhn** talked about the importance of communications systems in the maritime domain. She stated communication systems in terms of this issue has been investigated in the context of critical infrastructure protection. Mrs. Kuhn underlined the fact that there is a continuous evolution of communications at sea and recalled that communications systems play a crucial role in different sectors such as the economy, serving as a fundamental component for businesses, public safety organizations, and governments. They enable various infrastructure sectors to function efficiently, making the communications sector a critical component.

Mrs. Kuhn emphasized that when one thinks about how communication systems at sea are evolving, sub-sea sensors, surface vehicles, and linking all of these to a satellite communication should pop one’s mind. Additionally, satellites, particularly their positions, navigation capabilities, and precise timing, are becoming increasingly essential. In the maritime domain, the evolution of communications systems aims to address user requirements and support safe, efficient, and environmentally friendly shipping. However, this evolution is not without challenges, including considerations related to latency, bandwidth, channel capacity, and the overall life cycle costs of implementing these systems.

Mrs. Kuhn stated that the digital communication systems in the maritime sector displays a practical application of various critical systems and an envisioned interdependencies between these systems. She provided a graphic that illustrates a maritime communications options for IMO areas.



[1]Carson-Jackson, J., & Pokorny, P. (2021). Maritime communications. ICT Solutions and Digitalisation in Ports and Shipping, 177.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Mrs. Kuhn mentioned the six areas of operation defined by IMO and stressed that with multiple systems available, the flow of data communication continues, allowing the system to operate seamlessly and continuously.

Furthermore, the communications sector has significant interdependencies with other sectors, including the maritime industry. Maritime critical infrastructure is experiencing shifts in importance. By referring to the report entitled "Ocean's Future to 2050" and recalling thei increasing significance of coastal waters, Mrs. Kuhn stated that energy and food production are gaining prominence in this matter and added that overfishing is underscoring the significance of territorial waters. The increasing population along shorelines is creating crowded conditions, contributing to cascading risks.

In the realm of maritime communications, the focus is on evolving systems that align with specific goals. These goals include addressing user requirements and fostering safe, efficient, and environmentally friendly shipping practices. However, these advancements come with challenges that necessitate careful considerations. Challenges such as latency, bandwidth, and channel capacity, along with the overarching concern of life cycle costs, highlight the complexities involved in enhancing communication systems at sea. Striking a balance between meeting user needs and overcoming these challenges is crucial for the development of effective and sustainable maritime communication solutions

With the interconnected nature of operations in the maritime sector, a breach in one company's data or communications assets can have severe repercussions for other organizations in the supply chain. These interdependencies introduce new threats, resulting in cascading risks that can lead to catastrophic consequences if not adequately addressed and secured.

In summary, Mrs. Kuhn emphasized the critical role of communications systems in the maritime industry, the shifting importance of maritime critical infrastructure, challenges in evolving communications systems, and the importance of securing data and communications assets to mitigate cascading risks and ensure the safe and efficient operation of maritime activities.

Discussion

In the question and answer session, the discussion turned to communication cables placed on the seafloor. Specifically, there was a query about whether certain countries could create a backdoor through these cables to conduct intelligence gathering activities. Mrs. Kuhn responded by acknowledging the existence of numerous vulnerabilities, emphasizing the intensive risks associated with such cables. However, she also highlighted the opportunities presented by these cables and the technology integrated into them. Mrs. Kuhn mentioned that sensors integrated into these cables enable the detection of natural disasters such as tsunamis. Furthermore, she noted that this technology allows for the timely detection of such disasters, enabling the provision of warnings to people to take precautionary measures against these events.

Indo Pasific Legal Aspects-the Law of Armed Conflict in Maritime Security,

Dr. Joanna SIEKIERA (Faculty of Law, University of Bergen, Norway)

In a presentation by **Dr. Joanna Siekiera** stated that terrorism is characterized as being difficult to predict, cost-effective, and able to achieve the fear that perpetrators seek. Addressing the impact of the unpredictability of terrorist attacks, it is emphasized that the unexpected nature of such actions amplifies their effects. Terrorism at sea remains a neglected area, with limited resources allocated and a lack of attention from decision-making centers. Dr. Siekiera asserted that future wars will likely occur at sea or sub-sea areas. She attributed the increasing likelihood of this scenario to the expanding battlefield facilitated by technological advancements.

Dr. Siekiera warned that the sources of threats managed by states are rapidly evolving, outpacing the comparatively slower pace of legal frameworks. Developing the necessary measures and sanctions to combat these evolving threats is a time-consuming process. When it comes to national interests, the definitions of threat, risk, and terrorism by a state can change. This dynamic nature highlights the difficulty in establishing international norms in this context

However, the presentation highlighted that these maritime threats will have a growing influence in the future, with the Indo-Pacific region gaining significant attention. Criminals involved in maritime security issues are not underestimated; they understand how to navigate the international system effectively. Dr. Siekiera stated that international law is shaped by countries' interests and perceptions, and the presence of raw materials on the seabed presents both opportunities and threats. Countries are developing technologies not only to extract resources but also to enhance their military capabilities, making the protection of these areas essential.

The Indo-Pacific region becomes increasingly important for the security and geopolitics of not only the United States and Canada, but also other Alliance members with its civilization based on democratic values of the rule of law, transparency, and human right. Dr. Siekiera recalled that the 2022 NATO summit in Madrid was crucial and innovative as for the first time in its history 4 non-member states, all from the Indo-Pacific region, were invited as the key guests: Australia, New Zealand, Japan, and the Republic of Korea.

The vital reputation of this region for Euro-Atlantic peace and stability was highlighted at the 2022 NATO Strategic Concept. The second document which needs to be shed light on is the

2022 NATO Strategic Foresight Analysis: Regional Perspectives Report on the Indo-Pacific, where the rise of China along with all its illegal and inhumane activities was finally recognized. Firstly, the political, economic, and legal consequences of Beijing's policy affect not only states in South-East Asia. Secondly, sea-level rise is the biggest threat for the Oceania and Asian nations, who risk losing their territory and thus statehood, which might not only result in local instability but also the global struggle for spheres of influence. Finally, Dr. Siekiera reminded the audience that the experts predict that the future of warfare will be wars for raw materials, while the most valuable raw materials lie at the bottom of the Pacific Ocean. Thus, it is essential to make aware the NATO Member States why the geopolitical center of gravity has shifted towards the Indo-Pacific, as the 21st century is indeed the Pacific century.

With the rise of aggressive interference in domestic relations of the Indo-Pacific nations by different power, Russia's aggressive policies, terrorism in general and lonely wolves using terror across the world in particular, Dr. Siekiera stressed that the Alliance must be able, ready, and well-equipped to protect its values regardless of where a threat comes from – either from its territory, outside of it, or through the non-state actors. What cannot be forgotten either is the political-military power to counter terrorism and all its forms at sea and on land. That is as the Indo-Pacific region which has and will continue to lead to demographic instability, mass migration, legal questions of sovereignty and territorial integrity, and thus uncertainty of the world order. Therefore, there is a place for NATO to play a crucial, that is proactive, role in this region reducing the already existing threats to the Alliance and its system of values at times of great power competition, she concluded.

Discussion

In the Q&A section, there was a suggestion that new regulations are needed for the Indo-Pacific region, emphasizing the importance of closely monitoring China's construction of artificial islands to assert dominance. However, alongside this view, it was cautioned that new regulations could potentially exacerbate the situation. Dr. Siekiera was then asked about his thoughts on this matter. Dr. Siekiera expressed agreement with the second perspective, stating that an excessive number of regulations and institutions do not necessarily contribute to problem-solving.

DAY II

Usage of Maritime Unmanned Systems in Maritime Counter Terrorism

CDR Francisco CAVACO (PRT N, MARSEC COE)

CDR Francisco CAVACO reflected on his insights on "Usage of Maritime Unmanned Systems in Maritime Counter Terrorism". He started his presentation by defining ***maritime security as*** "*the ongoing condition in the maritime environment where international and national laws are adhered to, the right of navigation is preserved, and citizens, vessels, infrastructure, and resources are safe*." He then added that Maritime Security Operations are "*those operations conducted in cooperation with national authorities and International Organizations as appropriate, or by the Alliance alone when directed, to counter the threats, and mitigate the risks, of illegal or threatening activities, in order to help safeguard Allies' strategic interests, security and stability by contributing to mitigating gaps in current national civilian and/or military law enforcement capacity*."

CDR CAVACO highlighted the concept of **governance**, defining it as the way organizations or countries are managed at the highest level and the systems involved in this process. He further explained it as the activity of governing a country or controlling a company or organization, delineating how a country or institution is governed or controlled. Continuing with the discussion, he introduced the concept of **Maritime Governance**, describing it as a dynamic process involving interdependent areas of legal regulations, the blue economy, security, and environmental elements. Additionally, he emphasized the government's ability, through direct actions and partnerships with private, non-governmental, and international entities, to exercise effective control over its maritime domain.

Then CDR CAVACO turned to explain the mission and vision of Maritime Security Centre of Excellence (MARSEC SOE), followed by focus areas of MARSEC COE Concept. The mission of MARSEC COE is "*to expand the capabilities of NATO and Partner Nations by providing comprehensive innovative and timely expertise in the field of Maritime Security Operations*." The vision of the Centre is "*to become an internationally recognized focal point as well as comprehensive expertise and knowledge provider in the area of Maritime Security, thus expanding capabilities of NATO and Partner Nations*."

MARSEC COE Concept depends on seven different focus areas as follow:

1. Supporting Maritime Counter-Terrorism (MCT),
2. Supporting Maritime Situational Awareness (MSA),
3. Contributing to the Maritime Security Capacity Building (MSCB),
4. Upholding Freedom of Navigation (FoN),
5. Maritime Interdiction Operations (MIO),
6. Fighting Against Proliferation of Weapons of Mass Destruction (WMD),
7. Protection of Critical Infrastructure (CI).

In its commitment to enhancing maritime security from diverse perspectives, MARSEC COE engages in the implementation of projects and courses, alongside the formulation of concepts and the orchestration of significant events. At present, MARSEC COE is actively involved in formulating a concept regarding the utilization of Unmanned Aerial Systems and Unmanned Maritime Systems to bolster Maritime Security Operations (MSO). The use of unmanned systems in the maritime domain has rapidly expanded in recent years due to their many advantages over legacy systems. These systems have proven to enhance situational awareness, reduce human workload, and provide persistence, versatility and prolonged endurance while reducing risk to human life and diminishing the costs to nations. The integration of maritime unmanned systems (MUS) into maritime security operations (MSO) has allowed for a more efficient and effective approach. The vision for this integration is to create a seamless partnership between the autonomous system and the human system, allowing the MUS to take on dangerous and difficult tasks while maximizing the unique skills of human operators. By developing the Usage of MUS in Support of MSO Concept, MARSEC COE aims to provide a comprehensive approach to integrating MUS in MSO, enabling NATO forces to effectively leverage the capabilities of all types of MUS across all seven MSO tasks.

In conclusion, CDR Francisco CAVACO’s presentation underscored the critical importance of maritime security. Beginning with a comprehensive definition of maritime security and Maritime Security Operations (MSO), CDR CAVACO emphasized the role of governance and introduced the concept of Maritime Governance, emphasizing effective control over maritime domains. The mission and vision of the Maritime Security Centre of Excellence (MARSEC COE) were elucidated, with a focus on expanding capabilities and becoming a recognized expert in maritime security. MARSEC COE’s concept centers on seven crucial areas, ranging from Supporting Maritime Counter-Terrorism to Protection of Critical Infrastructure. The commitment to enhancing maritime security involves engaging in projects, courses, and concept development, with a current emphasis on formulating a concept for the utilization of Unmanned Aerial Systems and Unmanned Maritime Systems in MSO. The integration of unmanned systems into maritime security operations brings about increased efficiency, reduced risk, and optimized capabilities. MARSEC COE's vision is to create a seamless partnership between autonomous and human systems, enabling effective utilization across all MSO tasks. In summary, MARSEC COE plays a pivotal role in shaping the future of maritime security by leveraging technological advancements and comprehensive expertise.

Discussion

An inquiry was directed to CDR CAVACO regarding the effectiveness of unmanned maritime systems in long-term threat mitigation. In response, CDR CAVACO conveyed that these systems could play a crucial role in eliminating threats through their capabilities in reconnaissance and surveillance activities. He emphasized that in the event of a maritime attack, terrorists would inevitably need to disembark on land, and these unmanned systems would be instrumental in facilitating their apprehension. Drawing parallels with past incidents of a similar nature, CDR CAVACO highlighted instances where these systems demonstrated their promising potential. The discussion underscored the significant contribution unmanned maritime systems could make in long-term threat mitigation, particularly in scenarios involving maritime security and counter-terrorism efforts.

South China Sea Hybrid Threats on Maritime Security/Undersea communication cables to hybrid threats

Mrs. Diren DOĞAN (Alanya Alaaddin Keykubat University, Türkiye)

Mrs. Diren Doğan discussed various aspects related to the South China Sea and hybrid threats in maritime security. The South China Sea (SCS) is a region with diverse names and definitions by different countries, although it is officially recognized as the South China Sea. These contradictory approaches towards the naming of the area are considered a reflection of great power competition in the region. The dispute in the South China Sea involves the participation of six countries—China, Brunei, Indonesia Philippines, Taiwan and Vietnam—each with different claims. Multiple actors are involved in the SCS issue, including China, which asserts historical background and geographical boundaries, leading to legal arguments versus historical claims. Some regional countries refrain from commenting on the SCS issue due to China’s economic influence and dependence on their economic cycles.

Mrs. Doğan emphasized that this dispute in the South China Sea is a reflection of the international system. This conflict not only involves regional complexities but also signifies a broader impact within the global arena. The diverse claims and interests of the countries in the South China Sea underscore the geopolitical and diplomatic challenges in the region, making it a complex issue with implications beyond the immediate vicinity.

The SCS holds significant importance due to its role in global shipping, rich fishing reserves, hydrocarbon resources, and the geopolitical rivalry overshadowed by the rise of Asia. She noted that, considering the increasing population in Asia, there is heightened attention, particularly on fishing activities in the region.

In the context of power competition in the region, while there is talk of a balance among major powers, the countries in the region, especially when feeling a sense of insecurity in their bilateral relations with China, tend to seek refuge under the security umbrella of the United States. Despite the notion of a broader equilibrium involving major powers, the regional dynamics reveal that countries, driven by a lack of trust in their interactions with China, often turn to the security protection offered by the United States. This dynamic underscores the nuanced relationships and strategic considerations that shape the geopolitical landscape in the region.

Mrs. Doğan emphasizes that the complexity of legal uncertainty and struggle has turned this region into a gray zone. By this, she means that neither war nor peace entirely prevails in the region, highlighting the intricate and ambiguous nature of the situation. The term "gray zone" denotes a state of uncertainty where traditional distinctions between war and peace become blurred, making it challenging to categorize the ongoing dynamics definitively. Mrs. Doğan recalled that the international system has been under a great change and this has some repercussions over the security environment. This new security environment also introduces new types of threats along with it. In this sense, she touched upon the notion of "hybrid threats" which are considered to encompass all types of new threats.

At this point, Mrs. Diren introduced three different warfare doctrines of China. **Media Warfare** (also known as public warfare) is a continuous, ongoing activity aimed at the long-term impact of perceptions and attitudes. It uses all means of informing and influencing the public, including movies, television shows, books, the internet and the global media network (especially Xinhua and CCTV), and is owned and administered by the PLA nationally and locally by the People's Armed Police. **Psychological Warfare** attempts to influence or distort an opponent's decision-making ability, create doubts, fuel anti-leadership sentiment, deceive opponents, and reduce the will to fight among competitors. It uses diplomatic pressure, rumors, false narratives, and harassment to express dissatisfaction, establish hegemony, and convey threats. **Legal Warfare** (or "law") uses the legal system to achieve political or business goals. It plays an important role in the war trilogy. Lawfare has several applications. These range from enacting laws to inform claims about territory and resources to using fake maps to 'justify' claims.

China has engaged in reclamation efforts in the South China Sea. Starting in 2014, China has proceeded with extensive and swift land reclamation activities. By late 2015, when most of the reclamation work was finished, the reclaimed area measured approximately 12.9 square kilometers. Following the completion of reclamation, China further militarized the features, consistently enhancing various infrastructures and deploying military assets. Despite efforts by the United States to generate public perception that China's artificial islands will be used for military purposes, China claims that these islands were constructed for scientific research purposes in the maritime domain.

Undersea communication cables are of paramount importance, as they facilitate 98% of global communication. They are costly to lay and are vulnerable to backdoor strategies for collecting intelligence. China's control of undersea cables is a concern, as three Chinese companies both own and produce these cables, potentially posing risks to global communications. Some countries are changing and improving their cable installation strategies to mitigate risks and challenges, such as those posed by Vietnamese fishermen attempting to profit from cables in their waters.

In conclusion, Mrs. Diren Doğan’s comprehensive discussion on the South China Sea sheds light on the complex and multifaceted nature of the disputes in the region. The varying claims and interests of the countries involved, coupled with the geopolitical importance of the South China Sea, make it a focal point of global attention. The intricate power dynamics, particularly in relation to China, reveal a nuanced balance, with regional countries seeking security assurances from the United States in the face of uncertainties. The term “gray zone” aptly describes the ambiguity in the region, where neither war nor peace prevails definitively. Moreover, the emergence of hybrid threats and China’s unique warfare doctrines, including Media Warfare, Psychological Warfare, and Legal Warfare, further complicates the security landscape. China’s reclamation activities and militarization of features in the South China Sea have added to the tensions, with the United States attempting to shape public perception of China’s intentions. Additionally, the strategic importance of undersea communication cables, dominated by Chinese companies, introduces concerns regarding global communication security. Overall, Mrs. Doğan’s insights highlight the evolving challenges in the South China Sea, impacting not only the region but also global security dynamics.

Discussion

Mrs. Doğan was asked whether she had come across an example in the South China Sea that could be considered as maritime terrorism. She mentioned that she had not encountered a direct incident that could be classified as terrorism in the SCS; instead, incidents were more along the lines of robbery. She pointed out the definitional challenge.

The issue of sovereignty and ownership of the islands was raised, questioning whether they constitute a no man’s land or belong to one of the countries in the region. The response emphasized the uncertainty surrounding this matter, underscoring the need for new international legal regulations to address such complexities. Concerns related to Exclusive Economic Zones (MEB) were highlighted, indicating attempts to make territorial claims based on the challenges arising in these zones. This discussion points to the pressing need for a clearer legal framework to navigate the maritime disputes in the South China Sea.

The Importance of Bilateral and Multinational Cooperation in Maritime Terrorism

Mr. Kenneth YEO (S. Rajaratnam School of International Studies, Singapore)

In his first presentation, Mr. Kenneth YEO unraveled the complex nexus between maritime activities and regional terrorism. He delved into the transboundary nature of terrorism, exploring how the vast and often under-policed maritime domain has inadvertently enhanced the survivability and operational capacities of terrorist groups. The presentation sheds light on the limitations individual states face due to geographical constraints in combating this issue single-handedly. Emphasizing the critical need for multilateral cooperation, the speaker aims to underscore the importance of a unified, data-driven, strategic response among NATO members to effectively counter maritime terrorism. This conversation invites a deeper understanding of the challenges at hand and promotes collaborative action for enhanced security in the maritime domain. Additionally, the cases Mr. YEO put forward exemplified the Philippines' dual maritime challenges directed to the west of the archipelago. The primary focus was on managing the great power rivalry in the South China Sea or the North Philippines Sea, and the concurrent importance of maintaining vigilance over the Sulu-Celebes Seas. The recent third Philippines-Australia Maritime Dialogue, hosted by the Philippines on July 5, 2023, was examined. Mr. YEO discussed and analyze the proceedings of this dialogue, emphasizing the outcomes, decisions made, and their implications on the counterterrorism strategies of both countries. The presentation provided insights into this complex balancing act between power rivalry and maritime security cooperation.

Mr. Kenneth YEO delved into the intricate relationship between maritime activities and regional terrorism. Highlighting the transboundary nature of terrorism, Mr. YEO examined how the expansive and often under-policed maritime domain has inadvertently bolstered the survivability and operational capacities of terrorist groups.

The presentation underscored the inherent limitations individual states face when addressing maritime terrorism on their own due to geographical constraints. Mr. YEO emphasized the urgent need for multilateral cooperation, advocating for a unified, data-driven, and strategic response among NATO members. Such collaboration, he argued, is essential for effectively countering the complex challenges posed by maritime terrorism.

The modus operandi of maritime militants often involves the utilization of wooden pump boats, which presents several distinctive characteristics and implications for security forces:

1. **Travel in Wooden Pump Boats →** Implication: Undetectability with radar or satellites due to the material's composition, enabling covert movements.
2. **Pump Boats Fitted with 2 x 60 Horsepower Engines→** Implication: High maneuverability, allowing militants to navigate through diverse maritime environments with agility.
3. **Multiple Pump Boats, 2-6 Pirates Each→** Implication: Highly coordinated operations involving multiple vessels, indicating a sophisticated and organized approach to maritime activities.
4. **Armed with Machetes and Assault Rifles→** Implication: Militants are adequately armed, posing a serious threat to maritime security and potentially engaging in both close-quarters combat and long-range engagements.

Understanding these asymmetric maritime capabilities is crucial for devising effective counterterrorism strategies. The combination of stealth, coordination, and armament highlights the need for comprehensive security measures to mitigate the risks posed by such adept and adaptable adversaries on the open seas.

Additionally, Mr. YEO presented compelling cases, focusing on the Philippines' dual maritime challenges. The presentation shed light on the great power rivalry in the South China Sea and the concurrent importance of vigilance over the Sulu-Celebes Seas. A case in point was the third Philippines-Australia Maritime Dialogue, offering insights into its proceedings, decisions, and implications for the counterterrorism strategies of both countries.

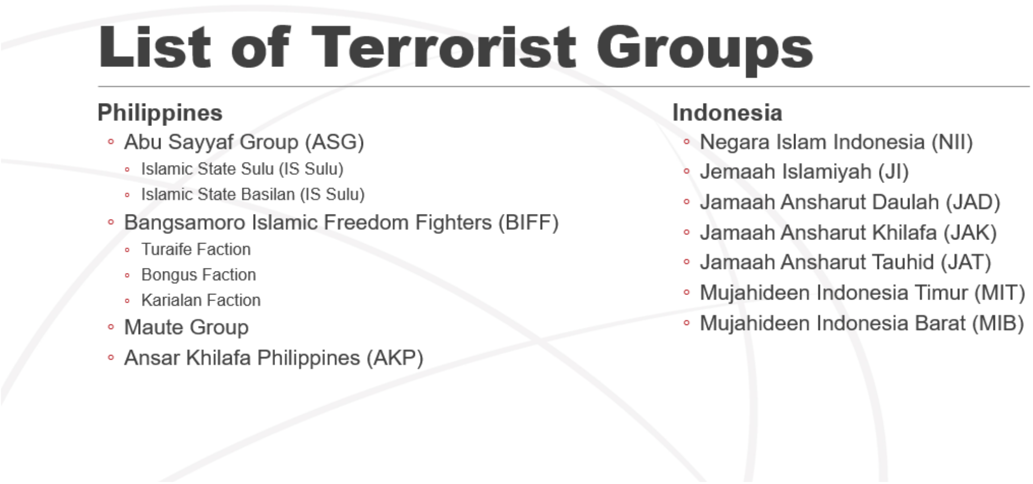
One striking observation made by Mr. YEO was the concentration of terrorist strongholds around the Sulu-Celebes Seas, particularly in the Southern Philippines. He attributed this phenomenon to a combination of historical factors, geography, and ethnic ties, introducing the concept of the "T3 Nexus" — the intricate relationship between terrorist groups, territory, and tribes. According to Mr. YEO, the Southern Philippines has traditionally served as an operational hub for terrorist groups due to its geographical features, dense forests, and the availability of guns. However, the strong ethnic character of insurgencies in Southeast Asia plays a pivotal role. Terrorists tend to operate within their ethnolinguistic boundaries, exploiting common ancestorial identities to gain local support, forming the backbone of the T3 Nexus.

Moreover, Mr. YEO emphasized the critical role of maritime trade in the context of terrorism. With statistics revealing that sea transport handles a significant portion of global trade volume and value, the vulnerability of these sea routes becomes evident. The Sulu-Celebes Seas, in particular, witness the trade of goods worth billions, making them a focal point for security concerns.

In sum, the countering maritime terrorism demands a nuanced and cooperative approach that addresses the specific challenges posed by the sea. The outlined insights underscore the need for international collaboration, technological advancements, and public awareness to effectively mitigate the diverse threats emanating from the maritime domain. Implementing these key takeaways will contribute to a more resilient and secure maritime environment in the face of evolving terrorist tactics.

As the second part of his presentation, Mr. Kenneth YEO examined Philippines-Indonesia and Philippines-Australia case studies and to conceive the threat of terrorism in Southeast Asia. Mr. YEO stated that the main focus is on Philippines and Indonesia in talking about terrorism in the Southeast Asia.

In both these countries, there are a number of terrorist groups and these are displayed below by Mr. YEO:



List of Terrorist Groups

Philippines

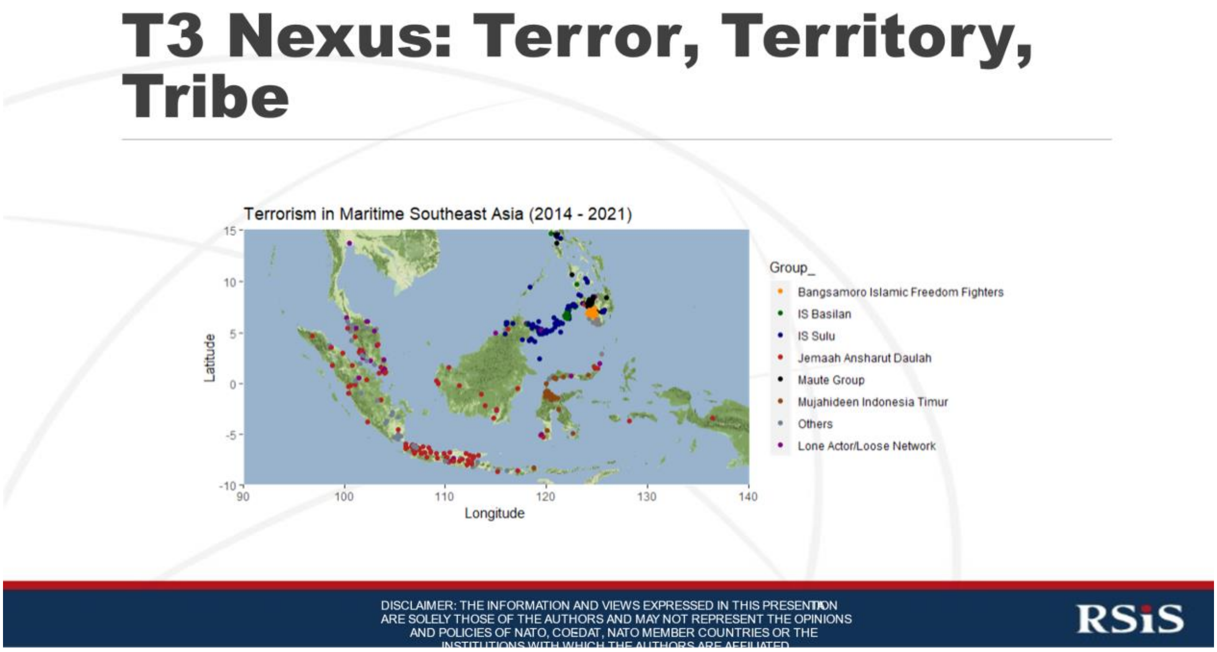
- Abu Sayyaf Group (ASG)
  - Islamic State Sulu (IS Sulu)
  - Islamic State Basilan (IS Sulu)
- Bangsamoro Islamic Freedom Fighters (BIFF)
  - Turaife Faction
  - Bongus Faction
  - Karialan Faction
- Maute Group
- Ansar Khilafa Philippines (AKP)

Indonesia

- Negara Islam Indonesia (NII)
- Jemaah Islamiyah (JI)
- Jamaah Ansharut Daulah (JAD)
- Jamaah Ansharut Khilafa (JAK)
- Jamaah Ansharut Tauhid (JAT)
- Mujahideen Indonesia Timur (MIT)
- Mujahideen Indonesia Barat (MIB)

Over the years, some groups have been decommissioned or co-opted by the government. This includes the Moro Islamic Liberation Front (MILF). Scholars have debated the status of the MILF before they were co-opted to form the Bangsamoro Government. Regardless the conclusions of these debates, the fact was that the BIFF, Maute Group, and Ansar Khilafa Philippines are splinters of the MILF.

The simplest way to understand terrorism in the region is that Southern Philippines is the operational center of terrorism, while Indonesia is the ideological center of terrorism. Mr. YEO argues that he raw information does not provide us with a clear picture of the terrorist landscape in Southeast Asia. It may seem that terrorist incidents are scattered across Indonesia, Malaysia, and the Philippines with no significant conclusion to be drawn. However, if the heat density analysis is applied, interesting trends could be observed as it is shown in the graphic below.



T3 Nexus: Terror, Territory, Tribe

DISCLAIMER: THE INFORMATION AND VIEWS EXPRESSED IN THIS PRESENTATION ARE SOLELY THOSE OF THE AUTHORS AND MAY NOT REPRESENT THE OPINIONS AND POLICIES OF NATO, COEDAT, NATO MEMBER COUNTRIES OR THE INSTITUTIONS WITH WHICH THE AUTHORS ARE AFFILIATED

Mr. YEO stated that it is easily noticeable that most of the terrorist strongholds are located around the Sulu-Celebes Seas. Firstly, the Philippines has traditionally been the operational center for terrorist groups. In the pre-Islamic State era of terrorism, Southern Philippines is covered under the Jemaah Islamiyah's (JI's) Mantiqi 3. This is where JI sends aspiring terrorists from Indonesia, Malaysia, and Singapore to Southern Philippines for training. This is due to the access to guns in the Philippines and their mountainous and densely forested terrain. Geography and access to Guns have allowed insurgencies to thrive in Southern Philippines for a long time.

But beyond geography and guns, there is a strong ethnic character of insurgencies in Southeast Asia. Mr. YEO stated that it is easy to notice that terrorists from particular groups rarely operate beyond their arbitrary geographical boundaries. These geographical boundaries correlate with the ethnolinguistic ancestorial territories. For example, the Islamic State Sulu Faction which mainly comprised ethnic Tausug tend to operate along the Sulu Island chains. On the other hand, the Islamic State Basilan Faction, which also splintered from the Abu Sayyaf, comprised mainly ethnic Yakans and operates almost exclusively on Basilan Island. This trend is observed by the Maute Group, comprising ethnic Maranaos and primarily operates in the Lanao region, while the BIFF's ethnic Maguindanao solely operate in the Maguindaanao region.

The relationship between terrorist groups, territory, and tribes is what Mr. YEO called the T3 Nexus. Terrorist groups recruit from within their ethnolinguistic tribe because of a common ancestorial identity which grants them greater perceived legitimacy as compared to the government. By exploiting the common ethnolinguistic heritage, terrorist groups win the hearts and minds of the local population. Hence, the stronger the T3 Nexus, the stronger the insurgency.

Additionally, there is an outlier on the map. That is the presence of the Mujahideen Indonesia Timur (MIT) at Poso, Central Sulawesi, Indonesia. Poso represents a unique case study for Southeast Asia. While there is no clear ethnic identity attached to Poso, religiously-motivated terrorist organizations have exploited the Poso riots in 1998 – 2001 to exacerbate the Muslim-Christian conflict. Originally, JI attempted to establish a stronghold by supporting local Muslims in the area. However, the Islamist movement became MIT, and they pledged allegiance to the DAESH. This space continues to hold narrative significance for Islamists in Indonesia because it is the only territory they hold. However, due to the absence of the historical ethnic dimension, MIT is unable to garner popular support from the locals and has thereby been a weak insurgency that relies on "imported" religiously-motivated terrorists from other parts of Indonesia.

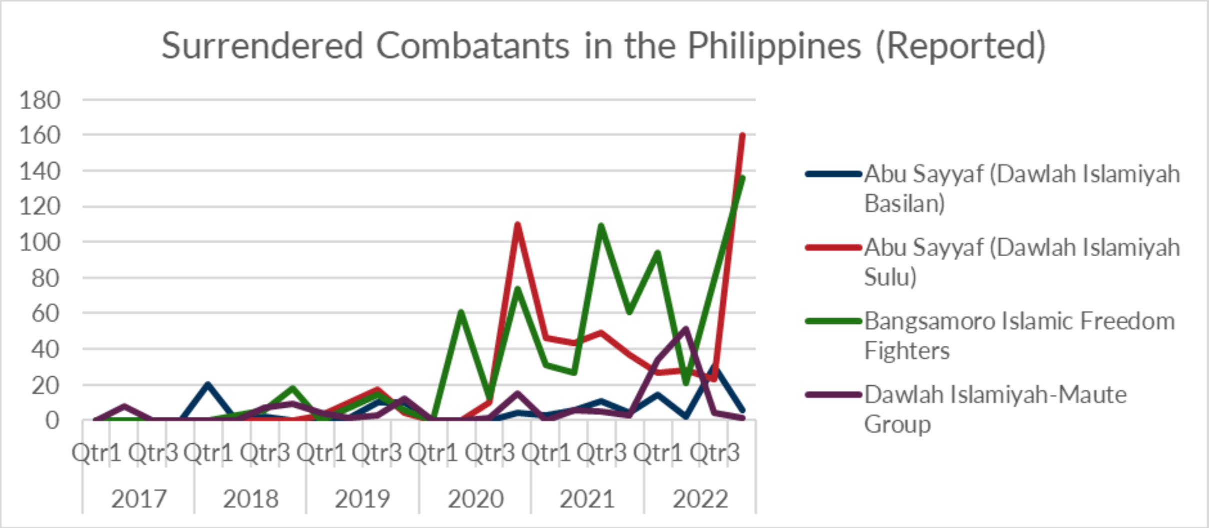
During the COVID-19 pandemic, there has been a dramatic reduction in the number of violent plots in Southeast Asia. While the causal relation between COVID-19 and the reduction of terrorist incidents in Southeast Asia is unclear, we can make some speculations. Firstly, travel restrictions might have reduced the terrorists' ability to travel between countries to participate in foreign conflicts, exchange knowledge, and coordinate attacks.

"However, the borders between Malaysia, Indonesia, and the Philippines are too porous, and it is likely for aspiring fighters to migrate between countries even if the authorities tighten border controls. Moreover, as travel restrictions have relaxed, we do not observe increased terrorism.", Mr. YEO added.

Secondly, internal movement restrictions might have crippled the terrorists' abilities to launch attacks. Lockdowns and curfews may hamper their ability to procure weapons, meet to coordinate plans and select high-casualty targets.

Similarly, this explanation does not address the low rates of attack and foiled plots after movement restrictions are lifted. Moreover, the presence of attacks in low-density areas indicates that the absence of high-density targets did not deter terrorists from launching attacks. Overall, while the reduction of terrorism in Southeast Asia coincided with the COVID-19 pandemic, it is unclear how the COVID-19 pandemic has resulted in the reduction in terrorism in the region.

The Philippines has also experienced significantly lower rates of terrorism. Through both military and non-military interventions, many combatants have surrendered to the authorities. Based on what we know, there are three explanations for why combatants surrender. Firstly, there is a credible opportunity to surrender. Upon surrender, the military works with the local governments and civil society organisations to reintegrate them into society. Various mechanisms were explored. Ex-combatants are provided with vocational training. There are psychological counselling sessions to address the trauma they faced in battle. Housing and financial support were also provided. Secondly, combatants are disillusioned from battle. They are hungry, fatigued, and penniless. Some reports also indicated that they ran out of ammunition. If the graphic below is carefully examined, one would notice that almost 120 members surrendered to the government in Q3 of 2020. That is because their leader died at the end of Q2 of 2020. We observed a similar trend with the BIFF when Salahuddin Hassan was hunted and subsequently died in Q4 2021. Thirdly, there are accounts that the friendlier and more approachable military encouraged some to surrender.



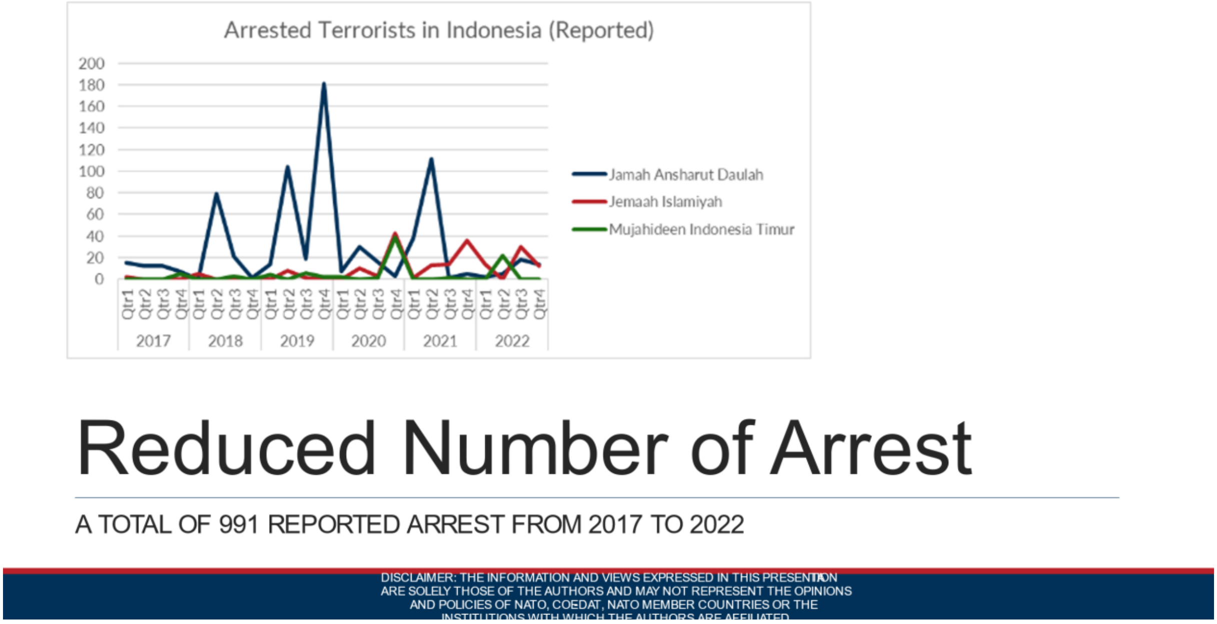
Here, Mr. YEO came up with possible explanations to answer why terrorist surrender as such:

- Credible Opportunity to Surrender
- Disillusionment from Leadership/Ideology
- Perception of Defeat
- Socialization (Family/Friends)

Mr. YEO also talks about eliminating the terrorist leaders to tackle the terrorist threat, which is coined as "*decapitation*" in the Terrorism Studies Literature. Firstly, Mr. YEO stated that the authorities' leadership decapitation strategy works in the context of Southeast Asia. Since the emergence of the affiliates of DAESH in Southeast Asia, the authorities have actively pursued to neutralize the leadership of terrorist groups and their team. There are two general effects of leadership decapitation in the context of Southeast Asia. Firstly, leadership decapitation has a temporary demoralizing effect on the terrorist group. Mr. YEO acknowledged that he observed a higher rate of terrorist surrender after the leader of the terrorist group is taken out. Secondly, leadership decapitation has a temporary radicalizing effect on the terrorist group. There is also an observable increase in the number of plots by the terrorist group whose leader was killed. These attacks seemed to be motivated by revenge. Overall, leadership decapitation has mixed impacts on the terrorist organization. However, there is net benefit from leadership decapitation and this remains a key strategy against terrorist groups in Southeast Asia.

In the context of Indonesia, the number of terrorist plots decreased significantly. There were only two attacks in 2021 and 2022. Of which, the suicide bombing at the police station was conducted by an inmate recently released for terrorism charges. This shows that there are gaps in the rehabilitation process in Indonesia. It is also important to note the number of arrests in

Indonesia. Most of them were arrested after the implementation of Indonesia’s Anti-Terrorism Law in 2018. However, the sentences for individuals with terrorism charges range between 3-5 years. The recidivism rate of terrorism is reported to be at 11%. Therefore, while the threat of terrorism in Indonesia is comparatively lower than it was during the pre-pandemic period, we are unsure about the statuses of detained individuals that are expected to be released between 2024 and 2025.



Reduced Number of Arrest

A TOTAL OF 991 REPORTED ARREST FROM 2017 TO 2022

DISCLAIMER: THE INFORMATION AND VIEWS EXPRESSED IN THIS PRESENTATION ARE SOLELY THOSE OF THE AUTHORS AND MAY NOT REPRESENT THE OPINIONS AND POLICIES OF NATO, COEDAT, NATO MEMBER COUNTRIES OR THE INSTITUTIONS WITH WHICH THE AUTHORS ARE AFFILIATED

The challenge of terrorism persists, with the looming specter of a potential resurgence fuelled by various factors. Two key elements in this equation are the returning foreign terrorist fighters and the release of incarcerated terrorists. The reintegration of individuals who had previously engaged in extremist activities abroad poses a complex and dynamic threat. The phenomenon of returnee recidivism, where individuals relapse into terrorism after their release or return, further compounds the intricacy of counterterrorism efforts. Understanding and effectively addressing these dynamics are crucial components in the ongoing endeavor to mitigate the risks associated with the resurgence of terrorism.

Due to the borderless nature of terrorism, regional cooperation is necessary. The state of terrorism is in the hands of the government. With great military, policing, and social initiatives, Southeast Asia can keep the threat of terrorism low. Mr. YEO Stressed that more must be done upstream in the Preventing and Countering Violent Extremism (P/CVE) space.

During the presentation, Mr. Kenneth YEO highlighted the significant role of Australia in supporting counterterrorism efforts in the Philippines, particularly through maritime cooperation. The assistance extended by Australia encompasses a broad spectrum of initiatives aimed at fostering stability and resilience in the region.

One pivotal aspect is the enhancement of access to basic services, contributing to the overall well-being of the affected communities. This multifaceted approach includes initiatives to promote community peace, security, and resilience. Furthermore, Australia has been actively involved in facilitating the transition of combatants to civilian life, recognizing the importance of reintegration in the broader counterterrorism strategy.

The impact of Australia's commitment is evident in the tangible outcomes of reconstruction programs, benefitting over 600,000 people. Notably, the Accelerate Sulu initiative has played a crucial role in empowering 288 women entrepreneurs through training and capacity-building efforts.

Beyond economic empowerment, Australia's involvement has played a vital role in resolving 54 local conflicts, emphasizing the holistic nature of their engagement. Psychosocial support and livelihood assistance for 325 Abu Sayyaf returnees underscore the comprehensive approach adopted by Australia in addressing the complex challenges associated with counterterrorism.

Australia's commitment is further demonstrated through its support for 14 Local Government Units (LGUs) in efforts related to Preventing and Countering Violent Extremism (PCVE). Engaging with communities, particularly 500 youths and 200 mothers involved in PCVE dialogues, reflects Australia's dedication to fostering sustainable peace.

The financial commitment of AU$92.4 million spanning the period from 2014 to 2023 underscores the long-term vision and sustained effort of Australia in collaboration with the Philippines. This partnership serves as a testament to the shared commitment to regional security and the importance of international cooperation in addressing the multifaceted challenges posed by terrorism.

Cognitive Aspects of Cyber Threats

Dr. Vira RATSIBORYNSKA (Vrije Universiteit Brussel, NATO, Belgium)

In the presentation by Vira Ratsiborynska, the focus on the cognitive domain within the realm of cyber threats brought to light the paramount importance of understanding the intricate interplay between the human mind and the evolving cyber landscape. At the heart of this discourse lies the acknowledgment of the complexities inherent in the information environment. The strategic security landscape is undergoing rapid transformations, and the role of cognitive aspects emerges as a pivotal factor in comprehending the nuances of cyber threats. Dr. Ratsiborynska delved into the realm of cognitive warfare, emphasizing the significance of cognitive superiority and, perhaps more crucially, how adversaries perceive and exploit these cognitive dimensions.

The evolving character of warfare, as outlined in the presentation, is marked by its constant and unending nature. This perpetual state of conflict is intricately linked with the increased interconnectivity across various domains, including air, land, sea, cyber, space, and information/knowledge. The augmentation of knowledge accessibility further complicates matters, providing adversaries with opportunities to exploit the weaponization of information activities. The ensuing challenges to international law and norms in this dynamic landscape create a complex web that demands meticulous navigation.

A noteworthy aspect illuminated by Dr. Ratsiborynska is the changing nature of armed conflicts, ushering in the era of gray zones that blur the traditional lines between military and non-military facets of conflict. This paradigm shift requires a nuanced understanding of cognitive dimensions, where the perception of threat and response is as crucial as the technical fortifications against cyber adversaries.

At the core of NATO’s understanding, cognitive warfare encompasses activities synchronized with other instruments of power, aiming to influence, protect, or disrupt individual, group, or population-level cognition to gain a strategic advantage over adversaries.

<u>Objectives:</u>

1. **Break the Will of the Enemy**: Undermining the determination and resolve of adversaries.

2. **Modify and Manipulate Perception of Reality**: Altering how individuals or groups perceive the world around them.
3. **Degrade Rationality**: Disrupting logical and analytical thinking processes.
4. **Influence Public Opinion**: Shaping the perspectives of the general populace.
5. **Decay Public Trust**: Eroding confidence and reliance on established institutions.
6. **Impede Decision-Making Process**: Hindering the ability to make informed and strategic choices.

The fusion of social sciences and cutting-edge technologies across all domains characterizes cognitive warfare, aiming to directly manipulate the mechanisms of understanding and decision-making. For China, this form of warfare is viewed as the “ultimate domain of military confrontation between major powers.”

Cognitive warfare involves operations of simulation, dissimulation, deception, and information manipulation or subversion, with the ultimate objective of manipulating the adversary’s brain to influence, paralyze, or confuse. The means employed include information and psychological operations, offensive cyber warfare, and the utilization of technology as enablers.

Unlike traditional information or psychological operations, cognitive warfare extends beyond the dissemination of false information. It encompasses the strategic dissemination of accurate information to create controversy and conflicting narratives within a society. Exploiting cognitive biases, shaping perceptions, building distrust, and weakening alliances are key strategies. The goal is to alter or impact the interpretation of a situation, fostering an environment conducive to the aggressor’s objectives.

Cognitive warfare, as detailed by Ratsiborynska, integrates cyber, information, psychological, and social engineering capabilities to achieve its objectives. The multidimensional nature of this warfare underscores its complexity and the need for comprehensive approaches to mitigate its impact on individual and collective cognitive domains.

In the ever-evolving landscape of cyberspace, a myriad of challenges and threats presents itself, necessitating a vigilant and adaptive approach to cybersecurity. The contested environment is rife with a diverse array of threat actors, ranging from nation-states to hackers and criminals. The rapid escalation of tensions among governments, the private sector, and commerce further complicates this multifaceted domain.

Multifaceted Threat Landscape: Cyber attacks, executed by various actors, are multi-purpose, swift, and often anonymous. The potential for causing physical damage and inducing confusion is vast.

Stakes for National Security: Understanding the stakes involved is paramount, especially considering the multi-sectoral nature of cyber attacks. Critical infrastructure and all economic sectors are potential targets.

Dynamic Nature of Cyber Threats: Cyber threats evolve with technological advancements, becoming more sophisticated over time.

In the complex realm of cyberspace, countering cognitive warfare demands a comprehensive and integrated approach. The following imperatives outline strategic measures crucial for bolstering defenses and ensuring a resilient posture against cognitive threats.

Effectively addressing cognitive warfare necessitates a holistic strategy that transcends individual departments. A whole-of-government approach ensures seamless coordination, fostering integration between cyber and information domains. By breaking down silos, governments can respond cohesively to the nuanced challenges posed by cognitive threats.

A pivotal aspect of countering cognitive threats lies in prioritizing information security and fortifying the resilience of command and control structures (C2). Strengthening the defense mechanisms in these critical areas is essential to thwarting the impact of cognitive warfare, ensuring the integrity and functionality of vital systems.

The implementation of effective monitoring and alert systems stands as a frontline defense against cognitive warfare campaigns. Swift identification and tracking of emerging threats are imperative for proactive responses. Real-time monitoring enhances situational awareness, allowing for timely interventions and mitigations.

A foundational pillar in the fight against cognitive threats involves building strategic awareness. Understanding the sources of instability, risks, and vulnerabilities is paramount. Intelligence gathering, coupled with the anticipation of potential crises, provides decision-makers with the insights needed to formulate effective responses and adaptive strategies.

Early identification of evolving challenges is a critical imperative. Timely risk assessment allows for a proactive alignment of military planning with political decision-making. By staying ahead of emerging threats, nations can craft informed responses and allocate resources efficiently, ensuring a robust defense against cognitive warfare.

Bolstering societal resilience is a cornerstone of effective defense. Defined as the ability to adapt and recover from stresses and shocks, societal resilience is foundational for rebuilding national capacity. By cultivating a populace that is resilient to cognitive threats, nations enhance their ability to deter and defend against a broad spectrum of security challenges.

To sum, these strategic imperatives form a comprehensive framework for navigating the intricacies of cognitive warfare in cyberspace. Through a whole-of-government approach, emphasis on information security, robust monitoring systems, strategic awareness, early recognition, and societal resilience, nations can fortify their defenses and effectively counter the evolving landscape of cognitive threats in the digital age.

Conclusion

Lt. Jr. H. Engin CANTEKİN stated that field of maritime terrorism is still in its early stages, and some have even argued that it is not a field at all. Terrorists have and are using the maritime domain in different ways, regardless of any academic squabbles. It is crucial for security and counter-terrorism professionals to not only be aware of how terrorists use the maritime domain, but also be prepared to combat them. The maritime domain is the site of different modalities of terrorist behavior, all of which could be considered maritime terrorism. Due to the disparity in the definitions of terrorism by states, organizations, and instruments, it may be beneficial to emphasize what maritime terrorism entails. The threat of terrorism in the maritime domain has gained significant attention in recent years due to its potential to disrupt global trade, endanger lives, and compromise national security. As a part of Maritime Security Operations to counter this evolving threat, maritime security agencies and organizations are increasingly turning to advanced technologies as integral components of their counter-terrorism strategies. The usage of technologies in maritime counter-terrorism is pivotal in enhancing the capabilities of security agencies and organizations to detect, deter, and respond to threats effectively. As terrorist tactics evolve, the continuous development and integration of advanced technologies will be essential to safeguarding the world's maritime interests and ensuring global security.

Dr. Marten MEIJER touched upon the June 2022 declaration of the Heads of Governments and Heads of States of the North Atlantic Treaty Organisation (NATO) the New NATO Strategic Concept will strengthen their ties with NATO partners that share the Alliance's values and interest in upholding the rules-based international order. Dr. MEIJER acknowledged that they will enhance dialogue and cooperation to defend that order, uphold our values and protect the systems, standards and technologies on which they depend as well as work with partners to tackle shared security threats and challenges in regions of strategic interest to the Alliance, including the Western Balkans, the Black Sea region, the Middle East, North Africa and the Sahel regions. Additionally, they also stated: terrorism, in all its forms and manifestations, is the most direct asymmetric threat to the security of our citizens and to international peace and prosperity. Terrorist organizations seek to attack or inspire attacks against Allies. These organizations have expanded their networks, enhanced their capabilities and invested in new technologies to improve their reach and lethality. Non-state armed groups, including transnational terrorist networks and state supported actors, continue to exploit conflict and weak governance to recruit, mobilize and expand their foothold. These statements were reiterated at the NATO Summit in Vilnius, Lithuania in July 2023. Dr. MEIJER’s presentation examined the question how NATO defends itself in various regions against maritime terrorist attacks. Upon analysis of critical terrorist attacks in the NATO maritime domain it is concluded that NATO needs to improve the understanding of the rules-based international order. Therefore, it is recommended to facilitate dialogue and cooperation within NATO nations and between NATO and non-NATO nations, which appears to be an essential part of the NATO comprehensive approach.

Prof. Arnold C. Dupuy’s first presentation focused on emerging and disruptive technologies (EDTs). EDTs are new innovations, which are recently developed, are under development, or are likely to be developed, that can drastically change how organizations and industries’ function. These can range from Artificial Intelligence (AI)—deepfakes, video manipulations, autonomous systems (drones, airborne and/or maritime), quantum computing, biotechnologies, hypersonics, space-based applications (GPS/GNSS), novel materials and manufacturing, energy and propulsion and next-generation communications networks. While these technologies have the potential to benefit broader society, in the hands of terrorists, they could prove devastating. Furthermore, terrorist activities in the maritime domain, present unique challenges to security forces when trying to detect, defeat and recover from such attacks. As most global trade is dependent on maritime activity, any serious disruption to this sector could negatively economic viability, particularly emerging nations. This is particularly so with nations that are already being destabilized or under threat by terrorist groups operating on their territory. Prof. Dupuy’s presentation addresseed the specific EDTs in the maritime domain context, their potential applications by terrorist organizations and mitigating strategies.

Prof. Arnold C. Dupuy’s second presentation elaborated upon “*Ship Cyber Security Management*.” The global maritime sector is vital to worldwide economic viability and a functioning civil society. Yet, increasingly dependent on information communications technologies (ICT) for a range of tasks, such as ship propulsion and power, navigation, Global Positioning Systems/Global Navigation Satellite Systems (GPS/GNSS), radar, weather systems, loading and stability, safety systems and communications and ship operations security. Moreover, shipboard systems are often comprised of legacy infrastructures, which present inherent vulnerabilities to a ship’s information technology (IT) and operational technology (OT) environments. Through the malicious use of industrial control systems (ICS), these vulnerabilities create innumerable attack vectors from which hostile actors can gain access to a ship’s network and jeopardize its safety and efficient operation. While efforts are underway to standardize best practices and security guidelines, their implementation is years away from being a reality. Prof. Dupuy's presentation considered the threats in the maritime cyber security field, as well as some general mitigation strategies, to include the various international guidelines and security standards.

Mrs. Kristen Kuhn reflected on the fact that there is an urgent need to strengthen maritime cyber resilience against escalating cyber threats and potential acts of terrorism. As the maritime industry embraces interconnected systems, the risk of attacks targeting critical infrastructure, sensitive data, communication networks, and undersea data cables increases significantly due to both increased attack surfaces and advanced technological integration. Mrs. Kuhn's presentation explored how power and politics impact maritime communications, with nations leveraging space-based assets, potentially amplifying the risks associated with cyber-terrorism. Collaborative efforts between governments, international organizations, and the private sector are essential to establish a cohesive defense against cyber threats driven by geopolitical interests and terrorist motives, with NATO playing a crucial role in fostering multilateral cooperation and sharing best practices in addressing future maritime cybersecurity challenges. Strategic methodologies such as risk assessment frameworks, robust encryption protocols, secure communication channels, data cable protection, and the integration of space-based technologies empower maritime stakeholders to adopt proactive cybersecurity measures. Cultivating a cyber-conscious culture onboard is vital, with well-trained personnel capable of recognizing and responding effectively to cyber threats and potential terrorist acts, preserving data and overall maritime security. Embracing cutting-edge technologies while mitigating risks ensures uninterrupted global trade, safeguarding critical communication pathways, and preserving the stability of the blue economy.

Dr. Joanna Siekiera's presentation on "*Indo-Pacific Legal Aspects-The Law of Armed Conflict in Maritime Security"* provided a comprehensive overview of the evolving challenges and opportunities in maritime security. She underlined the unpredictable and cost-effective nature of terrorism, emphasizing its heightened impact due to its unpredictability. Despite terrorism at sea being a neglected area with limited resources, Dr. Siekiera forewarned that future wars are likely to occur in maritime or sub-sea areas, attributed to technological advancements expanding the battlefield. The presentation acknowledged the rapid evolution of threats managed by states, outpacing the development of legal frameworks. The complex nature of defining threats, risks, and terrorism at the national level further complicates the establishment of international norms. Dr. Siekiera underscored the growing influence of maritime threats in the future, particularly in the Indo-Pacific region, highlighting the importance of this region for Euro-Atlantic peace and stability. The presentation stressed the need for NATO to proactively address the existing and emerging threats in the Indo-Pacific, offering a crucial role in times of great power competition.

CDR Francisco CAVACO's presentation focused on "Usage of Maritime Unmanned Systems in support of Maritime Security Operations." The use of unmanned systems in the maritime domain has rapidly expanded in recent years due to their many advantages over legacy systems. These systems have proven to enhance situational awareness, reduce human workload, and provide persistence, versatility and prolonged endurance while reducing risk to human life and diminishing the costs to nations. The integration of maritime unmanned systems (MUS) into maritime security operations (MSO) has allowed for a more efficient and effective approach. The vision for this integration is to create a seamless partnership between the autonomous system and the human system, allowing the MUS to take on dangerous and difficult tasks while maximizing the unique skills of human operators. By developing the Usage of MUS in Support of MSO Concept, MARSEC COE aims to provide a comprehensive approach to integrating MUS in MSO, enabling NATO forces to effectively leverage the capabilities of all types of MUS across all seven MSO tasks.

Mrs. Diren DOĞAN illuminated the multifaceted nature of disputes within the region, providing a comprehensive understanding of the geopolitical intricacies involved. Central to Mrs. Doğan's analysis is the reflection of the international system in the SCS conflict, transcending regional complexities to reverberate on the global stage. The area's significance in global shipping, abundant fishing reserves, hydrocarbon resources, and the overarching geopolitical rivalry in Asia underscores its pivotal role. In the context of power competition, Mrs. Doğan highlighted the nuanced relationships and strategic considerations of regional countries, especially their inclination to seek security assurances from the United States amid uncertainties in their dealings with China. Furthermore, Mrs. Doğan elucidated China's three distinct warfare doctrines—Media Warfare, Psychological Warfare, and Legal Warfare—each playing a role in influencing perceptions, distorting decision-making, and utilizing legal systems for strategic goals. In summary, Mrs. Diren Doğan's comprehensive examination of the South China Sea provides profound insights into the intricate power dynamics, geopolitical challenges, and evolving security threats in the region. Her analysis underscores the global significance of the SCS and emphasizes the need for a nuanced approach to navigate the complexities it presents.

Mr. Kenneth YEO's presentation unraveled the complex nexus between maritime activities and regional terrorism. He delved into the transboundary nature of terrorism, exploring how the vast and often under-policed maritime domain has inadvertently enhanced the survivability and operational capacities of terrorist groups. The presentation shed light on the limitations individual states face due to geographical constraints in combating this issue single-handedly. Emphasizing the critical need for multilateral cooperation, Mr. YEO underscored the importance of a unified, data-driven, strategic response among NATO members to effectively counter maritime terrorism. He invited a deeper understanding of the challenges at hand and promotes collaborative action for enhanced security in the maritime domain

Mr. YEO's first presentation elaborated upon the Philippines' dual maritime challenges directed to the west of the archipelago. The primary focus was on managing the great power rivalry in the South China Sea or the North Philippines Sea, and the concurrent importance of maintaining vigilance over the Sulu-Celebes Seas. The recent third Philippines-Australia Maritime Dialogue, hosted by the Philippines on July 5, 2023, will be examined. He discussed and analyze the proceedings of this dialogue, emphasizing the outcomes, decisions made, and their implications on the counterterrorism strategies of both countries. The presentation provided insights into this complex balancing act between power rivalry and maritime security cooperation.

During his second presentation, Mr. YEO provided an in-depth analysis of the threat landscape presented by terrorist groups operating within and between Indonesia and the Philippines. Central to the discussion placed the importance on adopting a data-driven approach to better understand these threats, track patterns, and formulate strategic countermeasures. The presenter will also provide updates on the Trilateral Cooperative Arrangement, a crucial tool in the cooperative efforts of these nations. The presentation candidly discussed its strengths and weaknesses, shedding light on the areas of success and those that require further enhancement. The presentation shed the light on indicators of threat escalation in the region and how states can take proactive steps to address these challenges. This discourse encouraged a holistic understanding of the bilateral counterterrorism efforts between Indonesia and the Philippines.

Dr. Vira Ratsiborynska's presentation gave an overview of what it means to constitute a cognitive dimension of war, especially in view of changes in the security environment and the exposure of different cyber and information threats resulting from the complex information and strategic environment. Dr. Ratsiborynska explored different approaches to a cognitive dimension of war as developed by adversaries and competitors and outlines different perspectives on cognitive aspects of cyber threats. The presentation also offered a critical reflection on the question of a cognitive dimension of war and whether NATO needs a new, cognitive domain.

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM

2004

TÜRKİYE

2023