Maritime Hybrid Threat

by Türkay KOTMAN
Navy Captain
Support Branch Head

Abstract

Notwithstanding the fact that the term ‘Hybrid’, as associated with ‘Warfare’ made its first appearance a decade ago, the reconceptualization of ‘hybrid warfare’ became the main topic of conversation on the heels of Russian’s invasion of Ukraine and annexation of Crimea on 21st of March, 2014. From that day forward, North Atlantic Treaty Organization (NATO) has put utmost emphasis on hybrid warfare. Having been underscored in the NATO Summits between 2014 and 2018, the significance of hybrid threats was declared in the summit of the North Atlantic Council in London on 3-4 December 2019. Hybrid warfare, methods of which are propaganda, deception, sabotage and other non-military tactics etc., has long been used to destabilise adversaries. What are new about attacks is their speed, scale and intensity, facilitated by rapid technological change and global interconnectivity. Taking into account that 90% of world transportation has been seaborne, we may infer that it is imperative for the states to develop instruments to prepare, deter, and defend against hybrid threats in maritime domain such as maritime cyber-attacks, piracy, maritime terrorism, weapons of mass destruction (WMD) proliferation, transnational organized crime, irregular migration, big scale maritime pollution, psychological operations, economic pressure, disinformation, deployment of irregular armed groups and use of regular forces, attacks against offshore oil and gas installations, huge hydrocarbon installations, shipping terminals or pipelines, underwater cables and deep seabed mining rig. Now it is time for states to embark on entertaining ideas for scenarios and how to counter them, both for their own forces and on behalf of allies, partners, and friends in the global maritime coalition.

Keywords: Hybrid threat, Hybrid Warfare, Maritime Hybrid Warfare, Maritime Hybrid Threat, Maritime Safety and Security

Introduction

“Supreme excellence consists in breaking the enemy’s resistance without fighting.” (TZU, 500 BC).

The legendary Chinese military leader Sun Tzu discovered that the indirect conflict is one of the most powerful ways to fight against the enemy about two thousand years ago. This helps an adversary to beat the rival without directly addressing them, hence preserving the money that can be invested on full-scale war. An indirect assault on an opponent will weigh them down and put them on the guard, leaving them exposed to alternative ways to attack. This also provides a certain amount of opportunity on the defending side, since they can potentially make more use of the time and resources to cope with the indirect attack. There are also political gains, in addition to the tactical advantages. Many prohibitions and relations prohibit one individual from starting warfare against another directly. The only way to disrupt the other is to engage in indirect tactics. (KORYBKÖ, 2015)
In an age of hybrid threats, both state and non-state entities are targeting countries and organizations which they view as a danger to their interests or as an agitation against them. There is a wide range of methods and practices in their fingertips, like influencing information; technological vulnerabilities such as pipelines for energy supply; economic and commercial related bribery; weakening international institutions through inadequate and open-ended rules; and terrorism or reducing stability. Methods and activities targeting the adversary's vulnerabilities are hybrid threats. Many things, including collective memory, laws, aged practices, geopolitical variables, a heavily polarized society, technological downsides and differences of opinion, can create vulnerabilities. When hybrid methods and actions are not accomplished in the interests and goals of the user, then the scenario may develop into hybrid warfare and the presence of the military and brutality can rise considerably. (The Europen Hybrid Centre Of Excellence for Countering Hybrid Threats, 2019)

**Hybrid Warfare and Hybrid Threats**

A decade ago, the word "hybrid" was first used by American military experts, correlated with "warfare." In fact, it was Frank Hoffman who invented it first. He recognized that other concepts, such as "unrestricted", "compound" or "4th generation", had already identified the changing features of combat of the 21st century as practiced by both state and non-state actors. Both focused solely on tactical, "directed and co-ordinated strategic operations within the main battlefield for adaptive purposes." (MISSIROL, 2019)

Hybrid influence can be split into two stages essentially, priming and operational phases, based on experience. In the first step, the opponent observes the condition continuously by using relatively subtle means to influence as well as progressively develop its assets. When agreed, in the second step, a more severe hybrid project can be introduced in which the impact of actions will become heavier, decreasing the basis for more aggressive and logical denial. (The Europen Hybrid Centre Of Excellence for Countering Hybrid Threats, 2019)

The Wales Summit of NATO in 2014 emphasized that the particular complexities presented by hybrid war threats, in which a large number of overt and covert military, paramilitary and civilian action are taken in the context of a deeply integrated way. (North Atlantic Treaty Organization, 2014).

The Allies agreed in November 2015 on a devoted 'NATO Role Strategy to Combat Hybrid Warfare' while openly debating their practical and geographical range. For the first time, the Warsaw Summit Communiqué of the Alliance spoke of 'terrorist, cyber or hybrid attacks, possibly coming from all tactical angles, indicating that NATO could react to hybrid warfare by recalling Article 5 of the Washington Treaty.(North Atlantic Treaty Organization, 2016)

The Brussels Summit declaration in July 2018 noted that 'hybrid threats, including campaigns for disinformation or for disruptive cyber attacks' and 'hybrid activities that aim to create ambiguities and blur the lines between peace, crisis and conflict' were reported and NATO was prepared to invoke Article 5 in the case of hybrid warfare. (North Atlantic Treaty Organization, 2018)
Having been underscored in the NATO Summits between 2014 and 2018, the significance of hybrid threats was declared in the summit of the North Atlantic Council in London on 3-4 December 2019. Hybrid warfare techniques, such as deception, frustration, disruption as well as other non-military tactics, have been used for decades to weaken opponents. The recent attacks are unique in speed, size and severity, motivated by rapid change in the technology and global interconnection. NATO has a hybrid war-fighting policy and is prepared to stand up against any potential danger, traditional or hybrid, by defending the Alliance and all Alliance members. (North Atlantic Treaty Organization, 2019)

Hybrid threat is the potential and evident preparation for hybrid strategies of a State or non-State actor. A hybrid threat exists in behaviours not subject to immediate conventional military intervention which can be conducted for a long time. (North Atlantic Treaty Organization Standardization Office, 2019).

A variety of combat styles including conventional powers, unconventional strategies and preparation, insurgency, indiscriminate violence and intimidation, and criminal disorder have been integrated in hybrid threats. Both states and a variety of non-state actors may conduct hybrid wars. This multimodal activity can be carried on by individual units or even by the same unit, but is usually guided and organized operationally and tactically inside the primary battlefield in order to have synergistic effects in the physical and mental aspect of war. At all combat stages the results can be achieved. (HOFFMAN, 2007)

Hybrid threats are mainly including the intentional "blur and blend" of opponent organizational structures with the application of tactics and weaponry ranging from modern military assets to improvised explosive devices and with the intention of using these against various targets whether a legal authority or civil in the global environment. (MURPHY, HOFFMAN, & SCHAUB, 2016)

The potential challenges from hybrid threats include military and non-military, clandestine and/or covert methods, like information theft, cyber warfare, financial strain, recruiting and deploying armed mercenary groups and usual combat force operations. If the boundaries between war and peace have to be crossed and if doubts are to be seeded in the minds of the intended groups, hybrid methods are proven to be efficient. Hybrid menaces have developed shoulder to shoulder with technology in recent years in size, scale and severity.
Hybrid threats rose to the top of NATO’s agenda following the appearance of "little green men" in Crimea in 2014, which created an acute awareness of how military force could be used in the Euro-Atlantic area below the legal threshold of war. NATO was quick to adopt a strategy to counter hybrid threats based on a horizontal "all-of-NATO" approach. NATO has created a capability to monitor and analyze hybrid threats, based in the intelligence community and cooperating with other NATO authorities. Furthermore, NATO has established counter hybrid support teams that can be sent in support of the authorities of a stricken nation.

NATO assembles strategic resources, knowledge and intelligence sharing, military-civilian preparations and other security initiatives. NATO has developed ways to be prepared for hybrid attacks and deterrent and defensive methods against a possible attack.

NATO has been implementing a strategy to combat hybrid warfare since 2015. The Alliance and Allies are capable enough to counter hybrid attacks regardless of form, while NATO is prepared to deter hybrid attacks on the Alliance and protects the allies involved if required. NATO collects information and analyses the data actively to lay the foundation to identify and assign any emerging hybrid action.

The NATO Headquarters Joint Intelligence and Security Division helps the Allies to understand and evaluate emerging threats. The hybrid analysis branch provides better awareness of the potential hybrid attacks to decision-makers. On request, the Alliance helps the efforts of the Allies to detect national security issues and reinforce the member’s defences. NATO is also a centre with experts in different essential fields such as Civil Preparation, chemical, biological, radiological and nuclear (CBRN) matters to provide competence to Allies. These include critical infrastructure security; strategic information systems; cyber defence; counter-terror; protection of energy supplies and public security. In the battle against these new hybrid threats; planning, preparation and research still play an important role. In collaboration with other players this means conducting decision-making scenarios and collective military and non-military reaction. NATO is prepared to act swiftly and wherever possible to combat hybrid threats as part of its disincentive and defence strategy, it is constantly improving its preparation and readiness and has improved the decision-making process and its command structure. This shows that the Alliance is strengthening its political and military approaches and its capacity to deliver the necessary assets at or before the correct time. If dissuasions fail, NATO fully intends to "protect" each and every Ally from every threat. NATO forces must be prepared to respond rapidly and nimbly, wherever and whenever necessary.

Allies with Counter Hybrid support teams, NATO Special Operations Forces and other strategic support teams (Cyber, Electronic Warfare and Chemical Biological, Radiological and Nuclear Power) are funded by NATO. The very first NATO counter-hybrid support team was assigned to Montenegro in 2019, with the intention of aiding in improving the capacity of the nation to dissuade and react to hybrid threats. Hybrid threat scenarios include training and drills by NATO in particular in disaster control, where NATO works with allied nations as well. (North Atlantic Treaty Organization, 2019)
Maritime Hybrid Warfare

There has been a great deal of discussion in the world of hybrid warfare, especially in the Russian invasion of Ukraine and occupation of Crimea. There are numerous reports of this. To this date, hybrid warfare has been largely confined to land warfare, in practical and theoretical sense. This might change soon and maybe even in the coming decades we shall see the appearance of “maritime hybrid combats.” It is time for governments to start thinking about and how to address threats. For the sake of their own armies and alliances, as well as partners and members they have in the maritime world. (STAVRIDIS, 2016)

Given its need to appear somewhat ambiguous to outside observers, maritime hybrid warfare generally will be conducted in the coastal waters of the littorals. Instead of using force directly from identifiable “gray hull” navy platforms, hybrid warfare will feature the use of both civilian vessels (tramp steamers, large fishing vessels, light coastal tankers, small fast craft, and even “low slow” skiffs with outboard engines). It also will be conducted and likely command-and-controlled from so-called white hulls assigned to the coast guards of given nations. Both the Chinese and the Iranians are using their coast guards (and revolutionary guards in the case of Iran) in this fashion in the South China Sea and Arabian Gulf, respectively.

The vessels being used for maritime hybrid warfare will be manned by a collection of what might be termed “little blue sailors,” individuals who are not exactly uniformed personnel. To give the appearance of non-state action, they may be categorized as nationalists, rogue actors, terrorists, or even “vacationing” sailors acting on their own volition. This technique was harnessed very capably by Russia during the invasions of Ukraine and the subsequent annexation of Crimea and allowed the Kremlin to spend weeks denying there were any Russian “troops” present on Ukrainian soil. The little blue sailors will not have any markings on their clothing, will not carry passports, and, if captured, will deny being part of any organized military.

“On board maritime hybrid warfare platforms, a variety of weapons will be available, from light arms to heavier calibre but temporarily mounted machine guns, hand-held surface-to-surface missiles, and light surface-to-air missiles. The sailors also will have access to high-intensity laser dazzlers, sound emitters, tear gas dispensers, water cannons, and other nonlethal weapons. Their command and control will be compact, civilianized, and largely composed of off-the-shelf systems, but it will have the ability to deploy overhead, unmanned sensors (light, smart, cheap, and disposable). Over time, they will have the ability to deploy sonobuoys and underwater and surface unmanned sensors and to emplace permanent sensor nodes on the seabed. All this technology will be maintained ashore by Special Forces assigned in units to a nation’s coast guard and irregular maritime force.
At the most sophisticated level, it is conceivable for a nation to build a small force of “Q Ships,” specially designed to look like coastal steamers or other small-to-mid sized commercial vessels but that have concealed ports built into their sides for weapons, can launch speedboats from internal bays, and can function as mother ships for even smaller and less sophisticated vessels conducting maritime hybrid warfare. Such vessels also could surreptitiously discharge mines made in a crude and untraceable fashion to approach maritime improvised explosive devices.

A particularly concerning element of maritime hybrid warfare could be attacks against:

- Offshore oil and gas installations,
- Huge hydrocarbon installations,
- Shipping terminals or pipelines,
- Underwater cables and
- Eventually deep seabed mining rigs. This could have a chilling effect on further investment in a country or a region given the liability of environmental effects.

Nations also will think more coherently about how to use maritime forces to support hybrid operations ashore. This type of operation could consist of unmarked vessels, perhaps appearing to be fishing craft or even mixed in with legitimate fishermen, to provide surveillance, logistics, command and control, or shore fires against an antagonist. In addition, it would afford the means to attack inland installations from the sea in support of operations ashore. This is similar to traditional sea basing operations (as used in the initial invasion of Afghanistan in 2001-2002), except it would be done from unmarked vessels to prevent attribution.” (STAVRDIS, 2016)

**Maritime Hybrid Threats**

Maritime threats continue to be increasingly composite in design and difficult to predict due to their diverse behaviour and for their consecutive occurrence. Such occurrences and their effects can pose extremely important threats, as their simultaneous availability of exploiting the flaws of various systems and/or spheres interdependently. In fact, the impacts appear to be amplified quite rapidly across global markets. Societal structures are therefore highly linked and interdependent to secure the Sea Lines of Communication and to maintain a high degree of maritime security and awareness. These are some of the several variables that play a significant role in the marine environment and in possible maritime hybrid threats. (The Europan Hybrid Centre Of Excellence for Countering Hybrid Threats, 2019)
Vulnerabilities to Maritime Hybrid Threats

“Commercial: Commercial vessels and ports are vulnerable to hybrid threats in the form of sabotage, navigational spoofing, and cyber-attacks on supply chain information systems, resulting in lost or disrupted cargo, denial of access to critical port facilities, and environmental damage. At the same time, foreign ownership and control of commercial port facilities can lead to the disruption of their use when these same facilities are required in times of crisis.

Cyber: Commercial and military maritime activities are more reliant on cyber-enabling capabilities than ever, with everything from navigation systems to port information systems all being vulnerable to cyber-attacks by hybrid actors and criminal organizations. The Maersk incident of 2017 illustrates the challenge well. A cyber-attack on the government of Ukraine inadvertently impacted Danish global shipping giant Maersk when they went to pay their Ukrainian taxes online. As a result, Maersk’s global operations came to a halt as they temporarily lost the ability to govern their fleet. Numerous other industries were also impacted as the global supply chain was disrupted. If this attack was actually aimed at commercial ports and logistics companies, the damage and disruption could have been much worse. Under this same category, some commercial shipping companies are currently testing technologies to enable the use of cyber-controlled unmanned container ships to move commodities across the world’s seaways. Obviously, the risks associated with this potential development are self-evident when looked at through the lens of maritime hybrid threats, with a potential scenario of a cyber-hacked unmanned vessel being turned into a weapon.

Energy: Diversification of energy supplies has led to an increase in the importance of liquefied natural gas (LNG), to include the transport vessels and onshore offloading facilities. In addition, gas and oil exploration in the eastern Mediterranean and the trans-shipment of petroleum and LNG at sea makes the energy supply chain more vulnerable to hybrid threats against the commercial entities which explore, extract, and ship these commodities.
Communications: Today’s economies are very reliant on the global information technology infrastructure with 97 percent of intercontinental communications moving through undersea cables, most of which lack even basic defences. Approximately $10 trillion in financial transactions is carried over these 213 cable systems every day, illustrating the global economy’s reliance on them. These cables are not owned by states, but rather by private entities which cannot afford to harden them and still make a profit. The potential impacts are apparent when considering that in December 2008, accidental cable cuts in the Mediter ranean and Persian Gulf resulted in widespread internet outages in the Middle East and India. For example, during that accident, Egypt lost 70 percent of internet connectivity, while India lost 50 percent.

Territorial Vulnerabilities: The borders and exclusive economic zones (EEZ) of coastal nations can be disrupted and contested by hybrid actors acting on behalf of a state in order to contest the governance of their sovereign territory. In the South China Sea, China seeks to expand its claims, often interfering with the territorial waters and exclusive economic zones (EEZ) of countries like Vietnam and the Philippines, using methods such as armed fisherman to challenge the authorities of these nations and their commercial entities operating in their own EEZ. Since the ability to control, maintain, and protect sovereign territory is a key aspect of governance, these are among the central tasks of coast guards and naval forces. In some cases, governments find it necessary to modify the rules of engagement for coast guards to be authorized to use deadly force, as Finland did in 2017.

Threats to Maritime Security Forces: Clandestine hybrid actors using armed frogmen or unmarked vessels disguised as commercial or fishing craft can surprise and swarm military vessels, disabling or disrupting them to keep them from being able to respond to other elements of a hybrid attack. The ability to detect, attribute, and respond to these threats is among the greatest challenges presented to security forces. In addition, the availability of increasingly sophisticated commercial off-the-shelf (COTS) technology to hybrid actors means that maritime security forces must constantly adapt in order to mitigate these emerging risks.
Disinformation: Alongside the previously mentioned maritime hybrid threats is the vulnerability to adversary disinformation campaigns aimed at eroding internal and regional trust by creating a false counter narrative. These disinformation campaigns across the media spectrum can bring into question the intentions and activities of friendly maritime security forces and their governments, not just in other countries but at home among their own people.” (Centre for International Maritime Security, 2018)

Emerging Requirements to Counter Maritime Hybrid Threats

“As recent history has shown us, the vulnerabilities to Maritime Hybrid Threats point to a new list of emerging requirements in order to deter and counter maritime hybrid threats:

- A review of national legal frameworks and the rules of engagement for maritime security forces to ensure they are sufficient and appropriate to the task of deterring and countering maritime hybrid threats.
- A national and global foreign investment screening process for critical infrastructure and sensitive technologies.
- The ability to operate in and regain control of contested commercial spaces.
- The ability to differentiate clandestine hybrid threat vessels from other commercial and privately owned vessels.
- The ability to operate in and regain control of contested cyberspace.
- The ability to detect and attribute hybrid threats on shore and at sea.
- The ability to operate quickly and decisively in a contested public information environment.
- The need for whole-of-government, whole-of society, and comprehensive approach table-top exercises and scenario-based discussions to develop deeper cooperation and information sharing between public and private entities.

Through meeting these new requirements, strengthening public and private governance, and seeking deeper and broader cooperation among institutions, nations, and civil society, we can turn globalization and our greater interconnectedness from vulnerability into an advantage.” (Centre for International Maritime Security, 2018)

What More Can be Done in the Fight Against Hybrid Maritime Threats?

The danger must be reduced before a major attack happens by an efficient plan to counter possible maritime hybrid warfare. Innovations in technology would contribute to smaller operational units which could significantly expand their effect by the use of drones, smaller bombs, cyber-attacks and acts of deception. One of the effective ways to challenge the actions of smaller boats is to deploy forces which are able to overcome them when they strike. The goal is to confront, discourage and prevent these acts while on a low level. This pressures the adversary to choose to acknowledge their forces and wage war or at least admit a brief tactical defeat. Nonetheless; this can only be accomplished if enough forces can be deployed immediately. (HAWKEN, 2017)
To facilitate this, naval forces, port authorities, and coastguards must have good intelligence gathering and surveillance assets as well as the ability to share information in a timely manner. A key to gathering intelligence will be surveillance drones, which could operate over a wide area. These drones need not just be airborne but instead can help identify incursions in a timely manner by operating in various domains.

In the future, however, the supply of defensive weaponry such as laser weapon systems may be augmented in the commercial sector, and although much more work is needed, feedbacks against rogue drones have been reported as promising. (KUZMA, 2017) Other options for defensive weaponry could be jamming systems or an electro-magnetic pulse as a last ditch defence against a major swarming attack.

The communications systems, as described before, will have to be very efficient so that information is shared in a reasonable time frame. If a cyber-attack compromises even a portion of this infrastructure, it would open way for a hybrid attack to achieve immediate dominance in a region, preventing a prompt reaction. It will certainly be important to work with government, state and military organizations, and to consider very carefully how they can plan and prepare themselves for maritime hybrid threats.

In this context, it is important to think like that of a possible oppressive force and military and non-military entities, should work both in collaboration with national and international partners to create cross-functional committees to identify and establish strategies and techniques to address the possible weaknesses. Although these approaches may not eliminate all instances of modern maritime warfare, they may reduce their output and perhaps prevent or counter major attacks. (HAWKEN, 2017)
Conclusion

Having witnessed several maritime hybrid activities during the past few years, the world needs to embark on improving its preparedness at all levels so as to be able to meet, counter and recover from maritime hybrid threats. Notwithstanding the fact that the methods of Maritime Hybrid Warfare will be hard to counter, their effects can be reduced. As such, by means of developing defensive measures against drones, non-military vessels and civilian installations can achieve the capability to defend themselves against attacks which may come about out of the blue. That being said, by developing offensive drone systems and creating an effective communications system, military patrol vessels can quickly and effectively respond to attacks in a timely manner, enabling responses to the whole spectrum of conflict that maritime hybrid warfare consists of. Military and non-military authorities, both with national and international partners, should work together to identify the weaknesses in maritime domain regarding hybrid threats before they are exploited, formulate doctrine to prevent threats, conduct table-top exercises and scenario-based discussions to develop deeper cooperation and information sharing between public and private entities. In case of any dispute in maritime domain, nations should resort to proactive means of peaceful dispute settlement rather than reactive measures for the sake of global peace. Nations should be aware of the fact that maritime hybrid threat will continue to be a significant issue in the future and it can be overcome provided that action is taken at nation’s earliest convenience.
Bibliography


