Sohaib
0312-6905384

Day: _____ Date: _____

Topic: Hybrid Warfare: the Way Forward

Keep practicing on different themes/topics

Outline

1. Introduction

Thesis statement:

The use of hybrid warfare presents significant number of challenges including socio-economic and political threats. These challenges require immediate redressal to impede the growth of hybrid tactics.

2. Understanding Hybrid Warfare

3. Challenges and Threats of Hybrid Warfare

a) Attribution challenges due to covert nature

b) Enhances unrest in political landscape

c) Fear of Economic consequences

d) Psychological impacts due to disinformation

e) Threat to Global Interconnectivity

Scanned with CamScanner

f) Cyber attacks with the evolution of technology

4. Countering challenges of Hybrid Warfare: the Way Forward

a) Technological advancement to counter such threats

b) Cyber Deterrence: a tool to resist hybrid attacks

c) Widening the scope of International laws

d) Regulations on AI and Technology

e) Diplomatic engagement with adversary

f) Fostering Alliances and Defense Mechanism

g) Creating positive economic interdependency

Mature your arguments further

5. Conclusion

The Essay

"Every age has its own kind of war" — Carl von Clausewitz

Scanned with CamScanner

Day: _____ Date: _____

With the advent of modern technology, the sphere of warfare is transforming. This advancement has resulted in emergence of fifth generation warfare in the 21st century. The use of cyber tactics and disinformation is a significant part of this warfare. This covert use of tactics to impede the capacity of adversary results in challenges like political destabilization and economic instability. Moreover, the country affected is mostly unaware and cannot counter the threat by being aggressive. Some other challenges include cyber attacks which can also result in global interconnectivity issues. However, for all problems there are solutions available. By advancement in technology, countries can create Cyber deterrence and strengthen their defense mechanism. International laws and diplomatic engagement

on the regulation of technology can also help in curbing such threats. Therefore, the use of hybrid warfare presents significant number of challenges including socio-economic and political threats. These challenges require immediate redressal to impede the growth of hybrid tactics.

Hybrid warfare is the use of conventional military tactics combined with non-traditional tactics including proxy, cyber attacks and disinformation to carry covert operations against the adversary. This category falls under the umbrella of fifth generation warfare which is known for its non-traditional battle grounds. States and non-state actors use it by heavily relying on Artificial Intelligence, Social engineering and propaganda. It presents severe challenges for

Day: Date:

the victim state which finds it difficult to counter such measures effectively.

The most significant and difficult challenge that victim state faces is of attribution. The state is unable to understand and confirm that who initiated the attack due to its covert nature. State or non-state actors use technological capacity to destroy the capability of an adversary without letting them know who was behind the attack. For example, the stuxnet worm, widely attributed to the joint U.S-Israel military operation to destroy the nuclear facility of Iran in 2010 is an attack where it is not confirmed with proof who was behind the attack. Thus, attribution of cyber and hybrid attacks is one of the

Scanned with CamScanner

imperative challenge faced by the victim state.

Another challenge besides attribution is of political destabilization in the country. Political destabilization can cause further severe damages to the state which then becomes difficult to handle resulting in divide and political polarisation within the society. The adversary state might use misinformation to spread the wrong news which further deteriorates the political stability in the country. For instance, it is alleged that Russia used social media campaigns to spread misinformation during 2016 presidential election in the USA. This attack was clear demonstration to destabilize the political landscape. Hence, one of the challenge and threat of hybrid warfare is to

Day: _____ Date: _____

create ~~sec~~ unrest in political arena.

Moreover, political destabilization is not the only tool to create hostility, economic consequences created by such tactics also present a danger to the country. Economic instability puts pressure on the country which can also result in accepting harsh terms. The aggressive country uses its influence on media to put economic pressures which can be through misinformation. Such economic damages can also result from direct damage with the help of proxies to the economic infrastructure. According to CISS report, India has used disinformation campaign against Pakistan to influence Financial Action Task Force (FATF). Moreover, India is funding Balochistan liberation Army to carry attacks

Day: _____ Date: _____

on economic infrastructure mainly CPEC inside Pakistan. Therefore, fear of economic consequences is a challenge and threat created by hybrid warfare.

Furthermore, hybrid warfare also results in psychological impact on the life of human beings. The sensitivity of misinformation can cause severe harm to the social sphere of life. Non-state or state actors use it to create distrust among society further deteriorating the psychological thinking of the people. For instance, a report by EUDisinfo lab indicates the use of social media accounts by the US military to spread false news against Chinese Vaccine for Covid-19. Thus, hybrid warfare involving misinformation creates significant psychological impacts.

Day: Date:

Besides socio-economic impacts, hybrid warfare can cause severe distress by disrupting global interconnectivity. Global supply chains use Internet of Things and technology to communicate around the world. This interconnection can be destroyed by an aggressor country for personal gains to destabilise the multi-national companies. For example, in 2020, the SolarWind attacks, attributed to Russia disrupted global software supply chains mainly affecting the US technological companies. Hence, Hybrid warfare poses a severe threat to global interconnectivity in the form of disrupting supply chains.

Additionally, cybex attacks with the ongoing evolution of technology poses severe challenge in the form of hybrid warfare. The attacks in

the form of malware, virus or hacking are considered as cyber attacks. These attacks are usually aimed to destroy the important data or steal an important details about the opponent party. States use such threat to steal secret details of the country or non-state actors use such attacks for financial gain. In 2023, for instance, financial institutions experienced a 38% increase in cyber attacks. Therefore, cyber attacks are used as a tool for hybrid warfare challenging state writ.

However, with these challenges, there are also some solutions that can prevent such tactics and avoiding the nature of warfare.

First of all, hybrid warfare uses

Day: Date:

technology to carry on attacks; therefore, such attacks can be countered with the advancement in technology. The use of technology in modern warfare can significantly help a country to strengthen their defense. For example, the use of artificial intelligence by cyber security companies to protect their clients from a cyber attack showcase the use of technology to counter threats. Hence, advancement in technology is an important way forward to counter the challenges of Hybrid warfare.

Secondly, countries should strengthen their cyber capabilities to create a deterrance between themselves and the adversary. For this, one needs to be aware of who the is behind the attack. This attribution requires

Scanned with CamScanner

Day: _____ Date: _____

proof to blame the opponent which can be enhanced with the help of machine-learning devices that process data within seconds. This can help a country to create cyber deterrence where the cost of the attack carried by the adversary will be higher than the benefits of it. For example, nuclear deterrence where the the parties are aware of each other capabilities, avoid large-scale conflict. Pakistan can built cyber deterrence capacity to counter the threat from India in the form of disinformation and funding of ~~proxy~~proxies like BLA. Therefore, to counter challenges of Hybrid Warfare, Cyber deterrence can be used as an effective measure.

Besides national measures like

Cyber Deterrence, countries can raise this issue in international court or United Nation General Assembly. International laws require fresh interpretation in the time of new warfare tactics. United Nation can pass respective resolution that prevents countries to engage in such tactics against each other. Therefore, there is a need of widening the scope of international laws to counter challenges of hybrid warfare.

Moreover, the threat of evolution in technology like AI can be regulated with the help of regulations. AI can be the most dangerous tool in the time of warfare if given freehand. The use of AI should be regulated by watch dogs and strict

Scanned with CamScanner

Day: _____ Date: _____

adherence to the laws should be maintained. For instance, use of deepfake technology to spread disinformation should be regulated and institutions like EUDisinfo Lab can be created which can help verify such information.

Furthermore, a traditional but the effective measure to counter such threats can be a diplomatic engagement with the adversary. In the age of nuclear weapons, diplomatic engagement holds imperative value. States can engage with each other to eradicate their reservations. Subsequently, Pakistan and India need to engage in constructive dialogue to remove such threats and dampen the hostility. Hence, diplomatic engagement can be a way forward to counter

Day: Date:

challenges and threats by adversary with respect to hybrid warfare.

Besides diplomatic engagements, victim country needs to foster alliance with a offshore balancing state to strengthen its defense mechanism. Such alliances enhances the technological capacity of the country to counter any hybrid threats. Alliances also help in balancing of power in the region resulting in minimizing the intervention of foreign country. Nato intelligence chief recently said to invoke Article 5 should also include in the time of cyber attacks faced by any NATO ally. Hence, alliances can create stable balance between two adversaries to avoid such attacks.

Lastly, hybrid warfare is a

Day:_____ Date:_____

tool to damage the political, economic and technological capacity of the opponent. However, it can be countered by creating positive interdependency which results in stable environment. The countries can use this measure by providing other countries to engage with them economically or technologically. According to Moeed Yusufzai, former National security advisor of Pakistan, projects like CPEC and TAPI can help Pakistan in creating a positive economic interdependency for other countries including India. This can foster good relation between both countries. Hence, creating such interdependency can be used as an effective measure to counter hybrid warfare.

In conclusion, the number of

challenges by hybrid warfare paints a grim picture. In contrast, these challenges can be effectively countered using adequate measures. Hybrid warfare, due to hidden nature of its attacks make it difficult for the victim country which threatens political, economic, social and technological landscape of the country. Therefore, countries need to advance their technological capacity to strengthen their defense ability. With the evolution of new technologies like quantum computing and artificial intelligence, deterrence can be maintained and the hidden operations of the aggressor can be exposed. The regulations on the national and global level foster a promising future where the peace can be maintained and states can collectively work on the prosperity of poor people.