HYBRID WARFARE: A CHALLENGE TO NATIONAL SECURITY

RABBIA HAYAT[Φ]

[Φ]Rabbia Hayat is a graduate of the LLB (Hons) Programme of The University of Lahore.

ABSTRACT

The social, political and economic developments in the modern world have emerged due to advanced technology and extensive communication. However, such advancement is elusive and prone to grave threats. It is pertinent to mention here that due to the vast globalisation network, civil society, human rights law and bolstering geopolitical environment, the initiation of traditional war by a state is not achievable and impracticable. Nevertheless, this has given a concept of "Hybrid warfare." States engage in hybrid war to curtail the economy of another state and muddle in internal matters by using clandestine military means such as cyber-attacks, diplomatic and geopolitical strategies, controlling of media networks and backing of small opposition parties.[1] Hybrid warfare faces severe legal challenges since the term needs to be further defined or to be recognised by law. Apart from legal challenges, the consequences of Hybrid warfare had been seen in the annexation of Crimea by Russia thus, highlighting the issues of Human rights law and use of force. Hybrid warfare faces severe legal challenges since it is not yet identified that whether it operates under armed conflict or non-armed conflict. Currently, hybrid warfare represents a threat to Pakistan's national security and to its citizens' human right as a consequence of hybrid warfare's tactics.

[1] Raashid Wali Janjua, 'The Looming Challenge of Hybrid Warfare' (2018) 2(12) World Times < http://jworldtimes.com/pakistan-affairs/the-looming-challenge-of-hybrid/> accessed 18 March 2021.

INTRODUCTION

In 1625, the father of modern international law, Hugo Grotius, stated that there is no intermediate state between peace and war.[2] However, Professor Aurel Sari, in a 2018 Strategic Analysis paper prepared for the European Center of Excellence in Hybrid Warfare, reminds us that declaring peace and war as 'mutually exclusive conditions with no middle ground between them'[3] was concerned with war and peace as formal concepts, rather than with the presence or absence of actual hostilities per se.[4] Grotius' approach was technical: the term 'war' referred to a specific legal condition characterised by certain formalities, including a declaration of war.[5] However, it may safely be maintained that nation-states and empires have always competed for power and influence. This led them to use a various range of hostile and warlike acts against each other, which, although they may have fallen short of war proper, were nevertheless aimed at disrupting the functioning of the enemy state or empire and securing strategic advantages in case of was proper.[6]

This state of affairs continues in today's world, in the midst of a renewed cold-war scenario, where the United States has launched a geopolitical contest against China, perceived as the current major threat to America's hegemony.[7] This happens at a time when, after sixty years of nuclear armaments, nuclear powers are reluctant to engage in direct warfare due to international legal challenges, legitimacy and reputational costs and especially to avoid nuclear escalation of the conflict when it involves a nuclear power [8]. In this

---

[2] Hugo Grotius, *De Jure Belli ac Pacis* (first published 1625) Book III, Chapter XXI, (citing Marcus Tullius Cicero, Philippics, VIII, 4: '*Inter bellum et pacem nihil medium*').
[3] Aurel Sari, *Blurred Lines: Hybrid Threats and the Politics of International Law*, Hybrid Centre of Excellence Publications, (January 2018) 3.
[4] ibid.
[5] ibid.
[6] ibid.
[7] Kishore Mahbubani, 'Has China Won? The Chinese Challenge to American Primacy' (2020) 1-2.
[8] Treaty on the Non-Proliferation of Nuclear Weapons, Article 1 (1970).

scenario, the so-called 'hybrid warfare[9] is a valuable tool for states to safeguard and advance their strategic interests.

This article will first define hybrid warfare, showing how historically, states have used often mixed warfare techniques, including recent examples where Pakistan was involved. It will then provide an assessment of hybrid warfare under current international legal rules on the use of force and on human rights. It will conclude by looking at the recent use of hybrid warfare by non-state actors, with specific reference to Pakistan.

I. HYBRID WARFARE: HISTORY AND DEFINITION

The American Revolution serves as an early example whereby both conventional and irregular strategies were used by 'guerrilla' fighters to defeat British forces between the years 1775–1783. These guerrilla tactics proved to be effective when the British surrendered, leading to America achieving independence.[10]

Historian Vision-Alonzo claims that Rafael Carrera of Guatemala, a rebel leader, used hybrid warfare during his struggle against the establishment in Central America.[11] Another example of hybrid warfare in more recent times is the invasion of Georgia by Russia in 2008, which resulted in the takeover of South Ossetia and Abkhazia in 2013. [12] Additionally, the Ukrainian conflict (where

[9] In this paper the expression 'hybrid warfare' is used. Other commonly used alternatives are: fifth-generation warfare, hybrid threats, hybrid conflicts and hybrid wars.

[10]Stuart Salmon, 'The Loyalist Regiments of the American Revolutionary War', 1775-1783, (PhD Thesis, The University of Stirling 2009).

[11]Gilmar E. Visoni-Alonzo, 'The Carrera Revolt and "Hybrid Warfare" in Nineteenth Century Central America' (Palgrave Macmillan London, 2017).

[12] Sari (n. 3) 5.

Russia used non-military tactics to ensure the annexation of Crimea), which resulted in Eastern Ukraine leaving NATO,[13] as well as the distribution of the 'little green men' in Eastern Ukraine, are also important examples of hybrid warfare.[14] Russia employed the use of narrative control, anonymous militias, diplomatic support, cyber-attacks, and clandestine supplies to this end.[15]

DEFINITION AND PRINCIPAL COMPONENTS

The term hybrid warfare is used to refer to various actions and means that states adopt to target the perceived weaknesses of their enemies.[16] These involve a number of strategies whereby states engage in unpredictable warfare using non-military acts ranging from cyber-attacks to economic coercion, from media propaganda to deployment of anonymous militias. Thus, hybrid warfare may be understood as a form of 'non-conventional, 'grey zone' type of conflict', which is on the rise around the world.[17]

States are increasingly aware of the threat of hybrid warfare: in 2014, the leaders of the North Atlantic Treaty Organization (NATO) raised security concerns due to hybrid warfare in the Wales Summit Declaration:

> We will ensure that NATO is able to effectively address the specific challenges posed by hybrid warfare threats, where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design.

---

[13]Taras Kuzio and Paul D'Anieri, 'Annexation and Hybrid Warfare in Crimea and Eastern Ukraine' E-International Relation (June 2018) https://www.e-ir.info/2018/06/25/annexation-and-hybrid-warfare-in-crimea-and-eastern-ukraine/ accessed March 2021.

[14] Douglas Cantwell, 'Hybrid Warfare: Aggression and Coercion in the Gray Zone' American Society of International Law (2017).

[15] Ibid.

[16] Erik Reichborn-Kjennerud and Patrick, *'Understanding hybrid warfare; MCDC countering hybrid warfare'* Information note (January 2018).

[17] Joshua Stowell,*'What is Hybrid Warfare?'* Global Security Review (August, 2018).

> It is essential that the Alliance possesses the necessary tools and procedures required to deter and respond effectively to hybrid warfare threats and the capabilities to reinforce national forces.[18]

According to NATO, hybrid warfare includes espionage activities to influence key players in an enemy state while avoiding direct conflict. It also includes both conventional and unconventional means, media propaganda and psychological operations in a targeted state.[19] The European Centre of Excellence for Countering Hybrid Threats defined it as:[20]

Action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronised and deliberately target democratic states' and institutions' vulnerabilities. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution.

The notion of hybrid warfare has attracted academic attention too. John J. McCuen defines hybrid warfare as "spectrum wars with both physical and conceptual dimensions: the former, a struggle against an armed enemy and the latter, a wider struggle for control and support of the combat zone's indigenous population, the support of the home fronts of the intervening nations, and the support of the international community."[21]. Another writer, Frank Hoffman, identified different

---

[18] Wales Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council, Wales. Art. 13(September, 2014).

[19]Waseem Ahmad Qureshi, *'The Rise of Hybrid Warfare'* Notre Dame Journal of International and Comparative law (2020).

[20] Hybrid COE, 'Hybrid Threats as a concept' The European Centre for Excellence for countering Hybrid Threats, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon Accessed 14 March 2021.

[21] McCuen, John J., *'Hybrid wars'* Military Review, Vol. 88, No. 2, (2008).

modes of hybrid warfare like conventional capabilities, terrorist activities, including violence and criminal disorder[22].

For the purpose of this paper, hybrid warfare will be defined as: Threats and strategies used by hybrid actors using non-military actions like cyber-attacks, economic warfare, espionage, media propaganda, and terrorists' activities aimed at influencing different forms of decision-making at the local, state, or institutional level, or undermining or hurting the target indirectly.

Having defined hybrid warfare, its two most important components will be separately analysed next.

ECONOMIC WARFARE

The key aim of economic warfare is to decrease economic productivity and diminish the resources of the enemy state[23]. Sometimes, economic policies are mapped out by intelligence agencies and the military to take control over supply lines and assets that directly cause impediments to the economic progress of the enemy state and their ability to fight a war.[24]

Additionally, corruption by the ruling elite, the government, or the military during these forms of conflict allows the country perpetrating the hostilities to continue their underground operations. Countries like Ukraine, Syria, Libya, Yemen, Venezuela and Iraq faced various instances of hybrid warfare with a major component of economic warfare, particularly increasing the class gap therein. Consequently, these countries suffered from grave security breaches

---

[22] Frank g. Hoffman, *'Conflict in 21st century: the rise of hybrid wars'* Potomac inst. for policy studies. (2007).

[23] Adeela Naureen, 'Hybrid Warfare and Economy' *The Nation* (17 October, 2017) < https://nation.com.pk/17-Oct-2017/hybrid-war-and-economy> accessed 10 May 2021.

[24] Robert duke Leakin, *'Economic Information Warfare'* (June 2003) <http://eprints.qut.edu.au/15900/1/Robert_Deakin_Thesis.pdf> accessed 11 May 2021.

and financial losses due to the excess outflow of money by way of corruption and embezzlement.

This type of economic warfare poses a looming threat to the economies of various states, depending on their geopolitical position, due to the hostile environment created by the existing economic war between China and the USA. To Trump, China represents a major challenge to employment and economic prosperity in America. Trump initiated economic warfare against China to create an anomaly in Chinese economic practices like affecting technology and the digital market (threat to ban Tiktok and other social apps). The US has also announced its intentions to impose tariffs of around $550 bn on China-made products. While China also had retaliated with the imposition of tariffs of $185 billion on US products. [25]

II. TECHNOLOGY AND CYBER-ATTACK

In most developing countries, progress in technology is a driving force and has often been used to supplement military strategies. These technologies bolster the cyber-security of states and may range from secret technical tools to advanced information data systems and centres that allow these states to gain an advantageous position during the conflict. However, even states with advanced technology are vulnerable to attacks at times. [26]

The European Centre for Excellence for countering Hybrid Threats identifies the hybrid threat as ambiguity created by hybrid actors by combining "disinformation, propaganda and interference through

[25] Rayas Hass and Abraham Denmark, '*More pain than gain:How the US-China trade war hurt America' (2020)* https://www.brookings.edu/blog/order-from-zamerica/#:~:text=President%20Trump%20launched%20the%20trade,subsidies%20to%20state%2Downed%20enterprises> accessed 29 September 2020.

[26] YuriyDanyk, Tamara Maliarchuk and Chad Briggs, *'Hybrid War: High-Tech, Information and Cyber Conflicts'* Partnership for peace consortium of defense academies and security studies institutes stable, (2017) 16 <Https://Www.Jstor.Org/Stable/10.2307/26326478> accessed 28 June 2020.

different activities and cyber operations and attacks are one of them.[27]

This can be observed in the case of the annexation of Crimea; the key aides were the use of multidimensional technologies and the commissioning of information through both psychological and cyber-active sources. Technical weapons and military hardware were supplied in order to supplement military combat. The weapons supplied included advance electronic systems and centres, including electronic warfare countermeasures, robotic systems, weapon regulator systems, and innovative automotive software. However, Russia did not use these weapons. They were part of military strategy. They created an impression on their opponent of the power of their military might. This tactic made the opponent state more vulnerable psychologically. These weapons were a part of a larger information warfare campaign in order to further add to the social and political destabilisation of Ukraine by undermining faith in government authorities among the public.[28]

An interesting challenge presented by these technological advancements is the rise of network-centric warfare (NCW), controlled warfare, and global warfighting amongst developing countries. These strategies are used by militaries or intelligence agencies from a distance on potential enemies, which may cause a future challenge in maintaining global peace and security. Generally, the military component in hybrid cyber warfare includes warfighting in both cyber and airspace environments. This involves robotisation, automated surveillance complexes, non-lethal weapons, and the use of irregular paramilitary forces.[29]

---

[27] Hybrid CoE, 'Hybrid Threats as a concept,' The European Centre for Excellence for countering Hybrid Threats, <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon> accessed 14 March 2021.

[28] Janiz Berzinz, *'Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy'* Center for Security and Strategic Research (April 2014).

[29] Frank G. Hoffman, *'Complex Irregular Warfare: The Next Revolution in Military Affairs,*' Orbis 50 (2006) 395-411.

Other forms of cyber warfare include politically motivated hacking, the collection of civilian data through internet service providers, industrial espionage, viruses, malware, the dark web, spam emails used to hack passwords or other personal data that allows attackers to access networks.[30] In 2010, the Stuxnet worm was developed to target the Iranian nuclear uranium enrichment program, which attacked the systems that controlled the centrifuges in the Iranian nuclear project. States like Israel and the USA were accused of developing the worm, but they denied the allegations. [31]

World powers are now relying on digital networks for critical services and are now resorting to a cyber-arms race that is akin to the nuclear arms race.[32] According to McAfee Strategic Intelligence researchers,[33] a series of cyber-attacks targeted energy firms located in Qatar and Saudi Arabia. These attacks destroyed the data of 30,000 computer systems. North Korea also clandestinely disrupted the national identification system of South Korea, which cost more than one billion US dollars to repair.[34]

In 2007, the digital infrastructure of Estonia was almost destroyed when the government made the decision to move the Bronze Soldier to a military cemetery on the outskirts of the city. Russian-language media spread outrage and led to numerous protests by false Russian reports claiming that the statue was being destroyed. Numerous people died, many were detained, and the Estonian digital

---

[30] Lily Hay Newman, 'Menacing malware shows the dangers of industrial system sabotage' (*Wired*, 18 January, 2018).

[31] Steve Ranger, 'What is cyberwar? Everything you need to know about the frightening future of digital conflict' (*ZDnet*, 2018) <https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/> accessed 28 March 2021.

[32] Khalid Chandia, *'Cyber Security/Warfare in Pakistan*' Islamabad Research Policy Institute (13 August, 2015) <https://www.ipripak.org/cyber-securitywarfare-and-pakistan/> accessed 28 March 2021.

[33] McAfee Strategic Intelligence/Shamoon2 https://www.mcafee.com/enterprise/en-us/assets/faqs/faq-mcafee-strategic-intelligence.pdf >accessed 20 March 2021.

[34] Ibid.

infrastructure was almost ruined.[35] Social media platforms like Twitter, WhatsApp, Facebook and YouTube have become a medium of spreading misinformation propaganda by certain groups.[36]

III. HYBRID WARFARE IN INTERNATIONAL LAW

HYBRID WARFARE AND THE PROHIBITION ON THE USE OF FORCE

In International Law, the use of force under international law counters hybrid warfare same as the ban on aggressive war. Under Article 2(4) of the United Nations Charter, states exercise the right to prevent any threat of or use of force against their territorial integrity or political independence.[37] In order to activate this provision, the opponent state must engage in any military activity, having either state or non-state actors involved in waging war against that specific state. Additionally, the Rome statute of the International Criminal Court also reaffirms the general principle that international law is violated by aggression.[38]

The question comes whether hybrid warfare involves the use of force. This issue will be considered by way of an example. When a state is involved in cyber activities that effectively initiate a hybrid war in order to damage the infrastructure of another state (in a way that resembles the use of force and weapons), it is arguable that it becomes akin to traditional war. The treatise on cyberspace, known

[35] Damien McGuinness, 'How a cyber-attack transformed Estonia' *BBC News* (April 2017) <https://www.bbc.com/news/39655415> accessed 20 March 2021.
[36]Ikram Sehgal, 'Hybrid warfare strategic coercion against Pakistan' (*The Daily Times*, 15 February 2019) <https://dailytimes.com.pk/354690/hybrid-warfare-strategic-coercion-against-pakistan/> accessed 15 February 2021.
[37] U.N. Charter art. 2 (4), General Assembly (1974).
[38]General Treaty for the Renunciation of War (Kellogg-Briand Pact, 1928)

as the Tallinn *Manual*, describes unlawful uses of force through cyber operations and declares them to be unlawful if it leads to similar outcomes as traditional war would.[39]

A major legal challenge that allows states to perpetrate hybrid war is covert actions because Article 2(4) cannot be activated in such a case. Covert operations undermine the enforcement of international law. However, actions which do not constitute the use of force can still be unlawful due to the interference in another state's affairs by attacking the sovereignty of another state. Article 2(1) of the UN Charter states that all states have equal sovereignty, and therefore the law binds states to respect the sovereignty of other nation-states. The 1970 Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States highlighted that "all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural element" must be banned to protect intervention in the internal or external affairs of any other state.[40]

A landmark opinion of the ICJ (International Court of Justice) in the 1986 Nicaragua case reflects this view. The Court opined that all states exercise the right to decide matters and issues related to state sovereignty, political, economic, social and cultural systems and foreign policy on their own terms. If such choices are affected by coercion, indirect force or any form of subversion, it constitutes unlawful interference. Therefore, it can be concluded that if a state is the victim of any hybrid warfare activities (such as false news stories, strategic leaks of information, and cyber-attacks), the actions of the perpetrator state will constitute unlawful interference. For this to be possible, the specific coercive acts need to be recognised, and a measured response must be decided by the victim states, as well as

[39]Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare (2013).

[40] Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States, G.A. Res. 25/2625, (24 October, 1970).

international and non-governmental institutions that are willing to ensure the protection of political independence and state sovereignty enshrined in the Charter.[41]

Moreover, Article 51 of the UN Charter also enshrines the right to self-defence. In fact, Article 5 of the NATO Charter states that an armed attack against "one or more of them in Europe or North America shall be considered an attack against them all." This gives member states the right to collective self-defence against any aggression, use of force and any alarming situation of threat to national security. As hybrid warfare is likely to constitute a threat to national security, in 2014, the member states of NATO raised the concern of hybrid warfare at the Wales Summit[42]. 'Armed attack' is a critical word because for a military operation to be undertaken, hybrid warfare must come under the ambit of an armed attack. However, the right of self-defence generally can be exercised even if there is a non-armed conflict[43].

HYBRID WARFARE, HUMANITARIAN LAW AND INTERNATIONAL HUMAN RIGHTS LAW

Both international humanitarian law and international human rights law are applicable to hybrid warfare. When states violate international humanitarian law, they have an obligation to prosecute the offenders under domestic law. Also, such violations can also be prosecuted by various international criminal tribunals[44]. While countering Hybrid Warfare, states those are Parties to the European Convention on Human Rights can refer to Article 15.1 of the

---

[41] *Nicaragua. v. U.S* (1986) I.C.J. Rep, 202

[42] NATO Wales Summit Guide Newport, 4-5 September 2014 <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20141008_140108-SummitGuideWales2014-eng.pdf > accessed May 2, 2021.

[43] Ibid.

[44] Council of Europe, Legal challenges related to hybrid war and human rights obligations Report | Doc. 14523 | 06 April 2018 https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24547&lang=en#:~:text=The%20right%20of%20self%2Ddefence,self%2Ddefence%20cannot%20be%20invoked. accessed 15 March 2021.

convention, which allows *"States Parties to derogate from their obligations under the Convention in time of war or "other public emergency threatening the life of the nation*"[45]. But, the states are not allowed to derogate from rights like the right to life (except in lawful acts of war), freedom from torture or degrading treatment or punishment, freedom from slavery and forced labour, and prohibition of double jeopardy. [46]

In the context of a hybrid war and human rights obligations, the Assembly of the Council of Europe stated that when a state uses forces against the sovereignty of another state, then it has a right to self-defence under Article 51 of the UN Charter, provided that its dimension is parallel to those of a conventional armed attack.[47]

As far as human rights are concerned, it is not always necessary that the method used to violate the specific right was military in nature. In the case of *Tagayeva and vs Russia,* 330 people (including children) were killed due to the deployment of military units by Russia. Although these military units did not breach the European Convention on Human Rights, the European Court decided that the use of weapons and strategies by those military units contravened the provisions of the convention.[48]

The European Union's legal instruments have also discussed the legal challenges posed by hybrid warfare in Resolution 2217 presented in the Parliamentary Assembly on March 26, 2018. Certain recommendations were made to provide information regarding hybrid

---

[45] European Convention on Human Rights, 1950, Article 15.1 < https://www.echr.coe.int/documents/convention_eng.pdf > accessed 15 March 2021.

[46] Council of Europe, Legal challenges related to hybrid war and human rights obligations Report | Doc. 14523 | 06 April 2018 accessed 15 March 2021.

[47]Aurel Sari, 'Blurred Lines: Hybrid Threats and the Politics of International Law' Strategic Analysis(January 2018) 3-4 <https://www.hybridcoe.fi/wp-content/uploads/2018/01/Strategic-Analysis-2018-1-January-Sari.pdf> accessed 20 March 2021.

[48]*Tagayeva and Others V. Russia* (2017) Application no. 26562/07.

violence in Europe and to take measures to keep the public aware of hybrid threats. Also, the EU aimed to take steps towards international cooperation for recognising hybrid war and drafting legal regulations for the implementation of these rules by the Council of Europe's Convention on Cybercrime.[49]

Although some areas in the Resolution are ambiguous as the definition of hybrid warfare and the need to distinguish between lawful use of force for national security and illegal annexation of territory. The recommendations made by the Committee to the Assembly while passing the Resolution were to enhance the cooperation mechanism among the states of the Union to fight against cyber terrorism and to improve user information and ensure security in cyberspace. These recommendations were passed in Resolution 1565 in 2007. All the European Union member states encouraged NATO to counter hybrid war with other states in line with human rights necessary for the protection of national security.[50]

IV. HYBRID WARFARE: THE ROLE OF NON-STATE ACTORS AND STATE RESPONSES

Under the threat of Hybrid Warfare, a state first needs to detect that hybrid warfare had been initiated against it. Second, it needs to deter hybrid warfare; third, it must react to the threats caused by hybrid warfare. Despite the gaps in international law, NATO had

[49] Council of Europe, Committee On Legal Affairs and Human Rights, Report (06 April 2018).
[50] Ibid.

included these three measures to detect, deter, and defend as a possible solution to eliminate the threats to national security.[51]

Firstly, detecting can help victim states to identify the threat of Hybrid warfare. States should examine all the major aspects of their systems like legal, social, political, defence, technology, media, vulnerable classes of the population (likely to be exploited by aggressors), and any other sensitive areas where hybrid warfare can be initiated. For this purpose, states must employ intelligence (composed of both military and agencies) to gather information regarding perceived hybrid warfare attacks, especially media. The U.S. has already started to collect data of its citizens through the internet and social media for the purpose of detecting hybrid warfare[52].

Secondly, deterrence strategies like cost analysis of government resources and the assessment of the system's capabilities[53]. On the other hand, deterrence can also be achieved by undermining the capabilities of the enemy state, causing a psychological effect on them or making the enemy aware of the possible consequences as a reply to a hybrid war attack. For these purposes, states can employ economic, legal, political, intelligence, military, social media, digital infrastructural means to deter threats.[54]

Thirdly, defence is an effective measure to counter hybrid warfare. Few defensive strategies like imposing heavy fines against targeted group can prevent hybrid attacks when any threat is detected. However, a state should not exceed the limits of international law. Moreover, a defensive response can be achieved by strengthening its

---

[51]Jan Jakub Uziębło, '*United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats,'* Diplomacy Paper *(*2017)

[52] Cynthia M. Grabo, *A handbook of warning intelligence* (1972).

[53] A. T. Mahan, 'The influence of sea power upon history-1660-1783 (2007). < http://www.gutenberg.org/files/13529/13529-h/13529-h.htm> accessed 20 March 2021.

[54] Colin S. Gray, *'Deterrence in the 21st century',* Comparative Strategy (2007).

digital infrastructure, national media, or controlling misinformation on media, or similar means like developing platforms to identify political agendas[55].

LATEST DEVELOPMENT: FROM STATE TO NON-STATE HYBRID WARFARE

Both states and non-state actors can initiate hybrid warfare. This can be carried out strategically and operationally to achieve a combined effect of both physical and psychological aspects of the conflict. It is important to understand the difference between state hybrid warfare and non-state hybrid warfare. State hybrid warfare includes the engagement of both military and non-military means by a nation-state in order to use force and threat to gain political advantages and to avoid conventional war at a strategic level. Particularly, state hybrid warfare exploits the stratification system in western democracies that lack strong and decisive leadership. By using non-military operations and tactics in certain geopolitical 'grey zones', states attempt to weaken enemy states by depleting their military and security resources. The term hybrid warfare, when used in the context of non-state actors, usually refers to groups such as ISIS (The Islamic State of Iraq and the Levant), Hamas, Hezbollah and the Taliban, who have developed several non-military means of maneuvers to advance their objectives.[56]

ISIS in Iraq and Syria model these attributes through traditional means and through information warfare. By controlling online propaganda, they have been able to carry out mass ideological mobilisation in favour of their regime. Other non-actors include LTTE (Liberation Tigers of Tamil Eelam) in Sri Lanka, FARC in Colombia (Revolutionary Armed Forces of Colombia), and

[55] Waseem Ahmad Qureshi, "The Rise of Hybrid Warfare" (2020) Notre Dame Journal of International and comparative law.

[56] Ahmed Salah Hashim,'State and Non-State Hybrid Warfare' Oxford Research Group (2017) <https://www.oxfordresearchgroup.org.uk/blog/state-and-non-state-hybrid-warfare> accessed 20 March 2021.

Hezbollah in Lebanon. These non-state actors have also deployed several terrorist hit and run strategies for destroying small enemy units. Non-state actors have seemed to encourage hybrid warfare to a great extent by conducting both offensive and defensive actions against conventional forces[57].

An important attribute of non-state hybrid warfare is that the ambit of combat is enlarged beyond the scope of the armed realm. Although these non-state actors employ advanced weapons systems, UAVs (unarmed aerial vehicles) and combined arms, they also make use of non-military tools such as hidden cyber activities and secure command and control servers. The combination of these two means of warfare means that these non-state actors are often able to go far beyond the approach and methods of their opponents.

V. HYBRID WARFARE AND PAKISTAN

Pakistan is currently facing hybrid threats challenges which include border terrorism, cyber-attacks, media propaganda and threatening claims by both external and internal. A study by Comparitech ranked that Pakistan 7th in terms of the countries with the least cybersecurity.[58] According to National Cyber Security Index, Pakistan is ranked 69th out of 160 countries in preventing cyber threats[59].

In April 2013, The Intercept revealed that US National Security Agency (NSA) used Malware to spy on civil-military leadership in

[57] Ibid.

[58] Paul Bischoff, "which countries have the worst (and best) cybersecurity?" Comparitech <Https://www.comparitech.com/blog/-privacy/vpncybersecurity-by-country/ > accessed 13 March 2021.

[59] National Cyber Security Index 2020 , < https://ncsi.ega.ee/ncsi-index/?order=name > accessed 20 March 2021.

Pakistan.[60]A group of Indian hackers targeted more than 150 individuals in Pakistan, Kazakhstan, and India through malware. It included individuals having links to the Pakistan Atomic Energy Commission, and election officials in Kashmir, the Pakistan Air Force. [61]

After 9/11, Pakistan had suffered from terrorism, sectarianism and ethnic conflicts. The hybrid actors incorporate some ethnic and religious groups to gain their motives. Examples such as funding by foreign or external actors to Baluchistan Liberation Army and the Tehreek-i-Taliban Pakistan in Pakistan is one such example. The blasts in Quetta, security threats to the CPEC project, and ethnic cleansing of minor sects are the consequences of foreign sponsorship[62]

Pakistan had also been facing media propaganda since 200 through the Indian Chronicles Operation. This had been revealed by EU Disinfo Lab's investigation. About 750 websites backed by India have been operating across 119 countries to undermine Pakistan. The report indicates that the objectives were to promote propaganda against Pakistan and China at forums like the UN and EU.[63]

RESPONSES AND THE NEED FOR STRATEGIC MEASURES IN PAKISTAN

Pakistan should strengthen its capacity to deal with this issue by adapting itself to the conflict to protect the national interests of Pakistan. Pakistan should move UN security resolutions under

---

[60] Sam Biddle, "The Nsa Leak Is Real, Snowden Documents Confirm" (*The Intercept 2016*) <https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/> accessed 13 March 2021.

[61] Centre for Strategic & International studies, "Significant Cyber Incidents" < https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents > accessed 14 March 2021.

[62] Dawn < https://www.dawn.com/news/1578769/army-chief-stresses-importance-of-protecting-countrys-interests-against-5th-generation-warfare> accessed 14 March 2021.

[63] Eu DisInfo LAB, "Indian Chronicles" <https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests/ > accessed 13 March 2021.

International law at international forums to address the Hybrid Threats along with other nations. The military should design special operation forces by giving them proper training to be prepared for any grey zone conflict. These Special Forces must be experts in designing cyber weapons and the establishment of alliance networks. There is a serious need to make laws and policies to address cybersecurity challenges from external threats. Pakistani social media and journalism are very active, but policies should be made to protect the fundamental rights and the national security of Pakistan.

CONCLUSION

Initiating a war against a country is costly and may not necessarily be effective. Military strategists have started to engage in battles that are inexpensive and comparatively effective. Hybrid warfare is a major threat against the national security of states, and international law needs to develop a strong mechanism against it. States need to strengthen their legal framework in this regard. Above all, states should recognise the threats that hybrid warfare poses. Although taking countermeasures sometimes involves a human rights trade-off, it creates deterrence for other states by setting a precedent.

Bibliography

Primary Sources

Case Laws

1. Nicaragua. v. U.S., 1986 I.C.J. Rep. at 202
2. Agayeva and Others V. Russia, Strasbourg 13 April 2017

Statutes and Statutory Instruments

3. U.N. Charter
4. General Treaty for the Renunciation of War (Kellogg-Briand Pact, 1928)
5. Rome Statute of International Criminal Court
6. The North Atlantic Treaty, Article 5
7. Treaty on the Non-Proliferation of Nuclear Weapons, Article 1 (1970)
8. European Convention on Human Rights, 1950, Article 15.1 <https://www.echr.coe.int/documents/convention_eng.pdf> accessed 20 March 2021

European Union Legislation and Directives

9. Wales Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council, Wales. Art. 13(September 2014)
10. Nuremberg Trial Proceedings, 1946, 426 <http://avalon.law.yale.edu/imt/09-30-46.asp.>
11. Council of Europe, Committee On Legal Affairs and Human Rights, Report (April 06 2018)
12. Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare (2013)

13. Council of Europe, Legal challenges related to hybrid war and human rights obligations Report | Doc. 14523 | April 06, 2018, <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24547&lang=en#:~:text=The%20right%20of%20self%2Ddefence,self%2Ddefence%20cannot%20be%20invoked>. accessed 20 March 2021
14. Hybrid CoE, 'Hybrid Threats as a concept,' The European Centre for Excellence for countering Hybrid Threats, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon accessed 20 March 2021

Secondary Sources

Books and Articles

15. Raashid Wali Janjua, 'The Looming Challenge of Hybrid Warfare' (2018) 2(12) World Times < http://jworldtimes.com/pakistan-affairs/the-looming-challenge-of-hybrid/> accessed 18 March 2021.
16. Aurel Sari, '*Blurred Lines: Hybrid Threats and the Politics of International Law*' Strategic Analysis(January 2018) 3-4 <https://www.hybridcoe.fi/wp-content/uploads/2018/01/Strategic-Analysis-2018-1-January-Sari.pdf> accessed December 2019
17. Joshua Stowell, *'What is Hybrid Warfare?'* Global Security Review (August 2018)
18. Ahmed Salah Hashim, 'State and Non-State Hybrid Warfare' Oxford Research Group (2017) <https://www.oxfordresearchgroup.org.uk/blog/state-and-non-state-hybrid-warfare> accessed 20 March 2021
19. Douglas Cantwell, 'Hybrid Warfare: Aggression and Coercion in the Gray Zone' American Society of International Law (2017)
20. Yuriy Danyk, Tamara Maliarchuk and Chad Briggs, *'Hybrid War: High-Tech, Information and Cyber Conflicts'* Partnership

for peace consortium of defence academies and security studies institutes stable, (2017) 16 <Https://Www.Jstor.Org/Stable/10.2307/26326478> accessed 20 March 2021

21. JanizBerzinz, *'Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy'* Center for Security and Strategic Research (April 2014)
22. Frank G. Hoffman, *'Complex Irregular Warfare: The Next Revolution in Military Affairs,*' Orbis 50 (2006) 395-411
23. Khalid Chandia, *'Cyber Security/Warfare in Pakistan*' Islamabad Research Policy Institute (August 13, 2015) <https://www.ipripak.org/cyber-securitywarfare-and-pakistan/> accessed 20 March 2021.
24. Vikrant Deshpande, *'HYBRID WARFARE The Changing Character of Conflict'* Institute for Defense Studies and Analyses, (2018) < https://idsa.in/system/files/book/book-hybrid-warfare-vdeshpande.pdf> accessed 20 March 2021
25. Waseem Ahmad Qureshi, *"The Rise of Hybrid Warfare"*, Notre Dame Journal of International and comparative law (2020)
26. McCuen, John J., *"Hybrid wars"* Military Review, Vol. 88, No. 2, (2008)
27. Frank g. Hoffman, *"Conflict in 21st century: the rise of hybrid wars,"* Potomac inst. for policy studies. (2007)
28. Jan Jakub Uziębło, '*United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats'* Diplomacy Paper *(*2017)
29. A. T. Mahan, The influence of sea power upon history 1660-1783 (2007) (ebook). <http://www.gutenberg.org/files/13529/13529-h/13529-h.htm> accessed 20 March 2021
30. Colin S. Gray, *'Deterrence in the 21st century'*, Comparative Strategy (2007)

31. Jason Daley, 'New Excavation Will Examine Germany's Legendary' Founding Battle' *(Smart News*, July 28 2017*)* <https://www.smithsonianmag.com/smart-news/> accessed 20 Match 2021
32. Franz-Stefan Gady, 'What Napoleon can teach western land forces winning about Hybrid wars' (*The National Interest*, November 27, 2018) <https://nationalinterest.org/blog/buzz/what-napoleon-can-teach-western-land-forces-about-winning-hybrid-wars-37217> accessed 20 March 2021
33. MunirAkram, 'Hybrid Warfare' (*Dawn*, December 09, 2018) <https://www.dawn.com/news/1450346> accessed 20 March 2021
34. Adeela Naureen, 'Hybrid Warfare and Economy' (*The Nation*, October 17, 2017) <https://nation.com.pk/17-Oct-2017/hybrid-war-and-economy> accessed 20 March 2021
35. Ikram Sehgal, 'Hybrid warfare strategic coercion against Pakistan' (*The Daily Times,* 15 February 2019) <https://dailytimes.com.pk/354690/hybrid-warfare-strategic-coercion-against-pakistan/> accessed 20 March 2021
36. Lily Hay Newman, 'Menacing malware shows the dangers of industrial system sabotage' (*Wired*, January 18, 2018)
37. Roy Allison, 'Russian "Deniable" Intervention in Ukraine: How and Why Russia Broke the Rules' (*International Affairs*, 2014)
38. Aurel Sari, 'Legal Aspects of Hybrid Warfare' (*Law Fare*, October 02 2015) <https://www.lawfareblog.com/legal-aspects-hybrid-warfare> accessed July 01 2019
39. John Vandiver, 'Saucer: Allies Must Prepare For Russia' Hybrid War' (*Stars And Stripes,* September 2014)<http://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464> accessed 20 March 2021

40. Damien McGuinness, 'How a cyber-attack transformed Estonia" *BBC News* (2017) <https://www.bbc.com/news/39655415> assessed 20 March 2021
41. Taras Kuzio and Paul D'Anieri, 'Annexation and Hybrid Warfare in Crimea and Eastern Ukraine' E-International Relation (June 2018) < https://www.e-ir.info/2018/06/25/annexation-and-hybrid-warfare-in-crimea-and-eastern-ukraine/ > accessed 20 March 2021
42. Stuart Salmon, 'The Loyalist Regiments of the American Revolutionary War, 1775-1783' (PhD theses, The University of Stirling 2009)
43. Robert duke Leakin' *Economic Information Warfare'* (June 2003) <http://eprints.qut.edu.au/15900/1/Robert_Deakin_Thesis.pdf > accessed 20 March 2021
44. Steve Ranger, 'What is cyberwar? Everything you need to know about the frightening future of digital conflict' (*ZDnet*, 2018) <https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/> accessed June 28, 2019
45. Gilmar E. Vision-Alonzo, 'The Carrera Revolt and "Hybrid Warfare" in Nineteenth-Century Central America' (Palgrave Macmillan London,2017)
46. Erik Reichborn-Kjennerud and Patrick, *'Understanding hybrid warfare; MCDC countering hybrid warfare'* information note (January 2018)
47. Saeed Wazir, 'Hybrid Warfare; Fifth Generation Warfare' (*CSS Times*, February 2019) <https://www.csstimes.pk/css-essay-on-hybrid-warfare-fifth-generation-warfare/> accessed 12 March 2021
48. Cynthia M. Grabo, *A handbook of warning intelligence* (1972)

49. Paul Bischoff, 'Which countries have the worst (and best) cybersecurity?' Comparitech <Https://www.comparitech.com/blog/-privacy/vpncybersecurity-by-country/ >accessed 13 March 2021
50. National Cyber Security Index 2020 <https://ncsi.ega.ee/ncsi-index/?order=name > accessed 12 March 2021
51. Sam Biddle, 'The NSA Leak Is Real, Snowden Documents Confirm' (2016) <https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/> accessed 14 March 2021
52. Centre for Strategic & International Studies, 'Significant Cyber Incidents' < https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents > accessed 14 March 2021
53. Dawn < https://www.dawn.com/news/1578769/army-chief-stresses-importance-of-protecting-countrys-interests-against-5th-generation-warfare> accessed 14 March 2021
54. Eu DisInfo LAB, 'Indian Chronicles' <https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests/> accessed 20 March 2021