Hybrid Warfare: Countering the Impending Threats

Brigadier Mohammad Yasin (Retired)∗

∗ Brigadier Mohammad Yasin (Retired) is Senior Advisor, Sustainable Development Policy Institute (SDPI) for Capacity Building in Islamabad, Pakistan. He has been with SDPI for over 26 years. He has previously worked in the Prime Minister’s Committee for Research and Analysis where he coordinated a number of research projects on district administration, police systems, dispensation of justice, Information Technology, and education. He also served in National Institute of Electronics. He has a number of publications to his credit.
Abstract

Hybrid warfare is not a new concept. What is new is the emergence of high Information and Communication Technologies (ICTs). It is the expansion of cyberspace and the availability of the Internet for all. This has made it very economical and easy to launch anti-state movements in target countries through propaganda, fake news, espionage, and terrorism. Besides, the hybrid actors can remain below the threshold of detection till the movement is well underway. Hybrid war is planned and executed in three phases: first the Color Revolution which is anti-state movement indigenously organized but influenced through external acts; second phase is cyber war which employs ICTs to disrupt critical functions of the state by attacking infrastructures, websites, command and control systems and economic and financial institutions’; third, the Unconventional Warfare that is, activities and actions of the hybrid actor to take advantage of the ongoing color revolution to add to the momentum by organizing guerrillas and auxiliary forces to overthrow the government. The momentum built through phases is then carried forward by the culminating phase, the Hybrid Warfare. The final phase is the synchronized use of multiple instruments of power to exploit vulnerabilities of the target state. The whole is greater than the sum of its parts.

This policy brief, in addition to explaining how the above phases evolve and roll out, will also cover the exploitable vulnerabilities and how the hovering threats of hybrid warfare can be mitigated. It also briefly covers challenges that Pakistan faces. Finally, some portent recommendations are offered.

Keywords: Hybrid Warfare, Color revolution, Unconventional Warfare, Cyber Warfare, Vulnerabilities, Instruments of Power.
# Table of Contents

1. Introduction ................................................................................................................................. 1
2. Color Revolutions ......................................................................................................................... 1
3. Cyber Warfare ............................................................................................................................... 2  
   3.1. Denial of Service (DoS) ........................................................................................................... 3
   3.2. Espionage ............................................................................................................................... 3
   3.3. Propaganda ........................................................................................................................... 3
   3.4. Infrastructure Manipulation ................................................................................................. 3
4. Unconventional Warfare ................................................................................................................. 4
5. Hybrid Warfare .............................................................................................................................. 5
6. Weaknesses, Challenges, and Vulnerabilities of Target States .................................................... 6
7. Countering Hybrid Threats .......................................................................................................... 6
8. Challenges for Pakistan ............................................................................................................... 8
9. Conclusion .................................................................................................................................... 8
References ......................................................................................................................................... 10
1. **Introduction**

Over the last decade or so, the conduct of warfare has undergone a gradual paradigm shift. Although the concept of hybrid warfare is not new, the high technologies realm has changed the military threat environment (an environment in which militaries operate). Adversaries now use non-military means to achieve their objectives. Through the synchronized escalation of external acts, the political, economic, social, military and infrastructure elements of the target state are weakened before resorting to unconventional or conventional warfare. Attackers’ actions are ambiguous, asymmetrical and non-linear so as to remain below the threshold of detection. The goal of hybrid war is to achieve the objective through targeting societies not the military. The high technologies now provide the necessary tools which facilitate the implementation of attackers’ plans. Achieving the objectives through propaganda, fake news, espionage, proxies and economic pressures is far more economical than engaging by military means. With the changing military environment, the countries (especially with huge military establishments) may be planning reductions in combat elements. The defense against hybrid threats would make it essential for nations to remain prepared for any eventuality. That means a continuing self-assessment of critical functions and vulnerabilities across all sectors and taking quick actions against possible threats.

This policy brief will look at factors like, cyber warfare, unconventional warfare, hybrid warfare and vulnerabilities of target states. It will then cover how to mitigate the evolving dangers. Finally, some pertinent recommendations to counter hybrid threats will be made.

2. **Color Revolutions**

Anti-government indigenous movements against dictatorial regimes or rulers non-compliant to the interests/dictates of adversarial powers have been normal occurrences. Such movements have been called Color Revolutions. Simply stated, a color revolution comprises externally induced acts that adversely affect internal affairs of the target nation. The goal of any color revolution is to seize power by over-throwing the government through creating internal turmoil. This is done by engaging the opposition parties, non-state actors, and proxies to give it an appearance that a sizeable population has revolted against the government.

Color revolutions are well-planned. First, data about the target demographics is collected, vulnerabilities of the target regime are carefully assessed and then the movement is launched. John Warden (a Colonel retired from the US Air Force) identifies five primary centers of gravity that hold an opposing force together. Beginning from the core (the most important) and expanding outwards, these are: leadership; system essentials; infrastructure; population; and fighting mechanisms. Warden (2014) is the originator of the five-ring strategic concept as shown in Figure 1.
Figure 1: 5-ring strategic concept

Source: Hybrid Wars: The Indirect Adaptive Approach to Regime Change, Moscow, Peoples’ Friendship University of Russia, 2015 (pp: 20)

For a color to succeed, the above centers of gravity should be compromised, starting from the core, through internal uprising. The aim is to win over a critical mass of the population and then deploy it against the target regime.

In the modern era of high technologies, it has become easy to mobilize a critical mass of the target state’s population through propaganda, fake news, espionage and the social media. However, these tools have to be well-planned so that it appears an internal uprising and that these acts appeal to the internal population. The entire exercise is so planned that the acts of the adversarial power remain below the threshold of detection and international condemnation.

Sometimes, a question is asked as to why such movements initiated by the external powers to destabilize the target regimes are called color revolutions? This term has been widely used by the worldwide social media to describe various anti-state movements, especially in the former Soviet Union states, for example, Bulldozer Revolution in Serbia 2000, Rose Revolution in Georgia 2003, Orange Revolution in Ukraine 2004, Purple Revolution in Iraq 2005. In Ukraine, the election symbol of one of the candidates was Orange (Thein 2009). Perhaps the names given to the color revolutions were, “hopes of the movement”.

3. Cyber Warfare

In cyber warfare, the Information and Communication Technologies (ICTs) are used to disrupt the activities of a state or an organization by attacking its information systems devised for strategic or military purposes. Such attacks would disable websites, channels of communication, weapon systems, economic and financial institutions and command and control capability (Yasin 2017). The United States’ Air Force describe cyber war as the ability to “destroy, deny, degrade, disrupt, [and] deceive, while at the same time defending against the enemy’s use of cyberspace for the very same purpose” (Singer 2014).
The cyberspace is an uncharted territory and with its expansion, the prevalence and severity of cyber-attacks has been exponentially increasing. This poses serious threats to countries’ economy and national security. During the last decade or so, there have been a large number of cyber-attacks where the infrastructure and services were targeted. The ambiguity, asymmetry and anonymity of such attacks have made attributions very difficult.

Cyber-attacks come in many ways. One, these compromise confidentiality of information. Civil and military organizations stand to suffer serious consequences if the confidential information is accessed by unauthorized persons or organizations. Two, Integrity of the information is at stake. This means the information can be altered or modified. In military, wrong information can be passed vertically and horizontally creating confusion and uncertainty. Weapon systems can receive wrong commands. Third, the essential information can be withheld or denied to rightful users.

In recent years, there have been a significant number and types of cyber threats. According to Geers (2011), the cyber-attackers and hackers attempt to achieve the following objectives through such attacks:

3.1. **Denial of Service (DoS)**
Essential services like, electric power grids, banking services, transport systems, etc. are targeted. This can very adversely affect daily life of the victims.

3.2. **Espionage**
Sensitive information and data is stolen, which can be remotely done. In fact, espionage is a continuing process used by the adversaries to gain intelligence to destabilize the victim’s economy. For example, the US often suspects that its military computer systems have been targeted by the Chinese hackers to steal information on unit deployment schedules, readiness assessment, maritime positioning plans, air trafficking and logistic status of US forces (Singer 2014)

3.3. **Propaganda**
High technologies now facilitate the spread of weaponized information to influence the leadership of the target countries. A website of the TechTarget (1999) weaponized information is a message or content piece that is designed to affect the perception about something or someone in a way that is not warranted.] Both domestic and foreign media can be used for this purpose. Employing artificial intelligence even the voices can be faked. Imagine the consequences, if in a battle, voice of the commander is faked to order ‘retreat’ like it was done in Ukraine by the Russians. In any future conflict, cyberspace will be used as an effective platform for propaganda by the adversaries. Even internally, terrorists and extremists have been spreading false rumors to influence the population to achieve their objectives.

3.4. **Infrastructure Manipulation**
There can be serious fallouts if critical infrastructures are manipulated. For example, if electric grids, transport systems, hospitals and other civil and military infrastructures are degraded, the effects will be devastating. According to ASC (2016), not all attacks are about theft or destruction. A more sinister course is the manipulation of data in places so that machines can be controlled or wrong information reported to human operators without their knowledge. The US and Israeli cyber-attack on Iranian nuclear centrifuges by using “Stuxnet” in 2010 is well-known. The revolving machines went out of control and became erratic.
Every year, there are numerous incidents of cyber-attacks which are widely covered by the print and electronic media. Cyber warfare seems to be unending. However, some strategists say that the aim of cyber-attacks is purely espionage, sabotage and subversion. These acts do not constitute a war because a war is a formal fight between the adversaries where lives are lost. However, here it is pertinent to recap Sun Tzu’s military doctrine:

“To fight and conquer in all our battles is not supreme excellence. Supreme excellence consists in breaking the enemy resistance without fighting. The supreme art of war is to subdue the enemy without fighting.”

The tools and techniques used in cyber warfare can so weaken the target state that the attacking forces can move in without a formal fight.

4. Unconventional Warfare

Anti-state movements and other acts of destabilization and regime change in the target states are initiated through the color revolutions and cyber warfare. If such attempts fail, then the adversarial powers resort to unconventional warfare (UW). What is unconventional warfare? “Activities conducted to enable a resistance movement or insurgency to coerce, disrupt or overthrow a government or [an] occupying power by operating through an underground, auxiliary and guerrilla force in a denied area. Unconventional warfare is not a mechanism for creating revolutionary conditions—rather, it seizes on and supports existing political, military and social infrastructure to accelerate, stimulate and support a decisive action-based, calculated political gain” (Petit 2012).

According to Horybho (2015), the success of unconventional warfare is determined by seven key variables which are: leadership; ideology; objectives; environment and geography (including social); external support; phasing and timing; and organizing and operating patterns. He emphasizes that everything must be well-planned and in order. The time is most important otherwise the endeavour will be a failure.

Headquarters, Department of the Army (2010) had prepared a well-written comprehensive confidential field manual which was published in 2012. It provided guidelines for planning and conducting unconventional warfare. It laid down when the US will directly participate and when it will indirectly participate in an unconventional war to destabilize or overthrow the targeted government. This plan was implemented in Syria, Iraq and Afghanistan. The Russians did the same in Ukraine.

The color revolution and cyber warfare, explained above, lay down the ground work for the unconventional war and both are the essential component of Hybrid Warfare explained below.

The important difference between the color revolution and unconventional warfare (although they are complementary) is that guerrillas, special forces or regular armed forces are not an essential part of color revolutions. But such elements can be a part of an unconventional war. However, this is done after the incipient phase of the unconventional war. A greater degree of flexibility is adopted in unconventional warfare. In the event of a setback, the activities may be temporarily suspended to revitalize the color revolution and cyber war and further training of the insurgents, guerrillas and mobilizing the population against the targeted regime.
5. **Hybrid Warfare**

Fairclough (2017) quotes Hoffman to define hybrid war as being the incorporation of a range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion and criminal disorder. Hoffman (2007) later expanded this definition to reflect hybrid war as being, sophisticated campaigns that combine low-level conventional and special operations; offensive cyberspace and psychological actions that use social and traditional media to influence popular perceptions and international opinion.

Monaghan, Cullen, and Wegge (2017) describe hybrid warfare as: the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergetic effects. The instruments of power are the: military; political; economic; civil; and information. Depending on the situation, any one or more of these instruments can be used for vertical escalation or all of them synchronized for horizontal escalation. The use of instruments will depend on the capabilities and goals of the hybrid actor and on the vulnerabilities of the victim regime (see Figure 2).

**Figure 2**: synchronized vertical and horizontal escalation characteristic to hybrid warfare

![Diagram of vertical and horizontal escalation](https://example.com/diagram.png)

**Source**: Multinational Capacity Development Campaign (MCDC 2017 pp 9)

The concept of hybrid warfare is not new. It has been used in Vietnam, by Hezbollah, by Israel, by the US in Iran and Afghanistan and by India against Pakistan. What has changed the scenario is the emergence of high information and communication technologies (ICTs). As a result, the cyberspace has expanded which facilitates the hybrid actors to remain below the threshold of detection and avoid international legal complications. Besides, the cost of conventional war has increased to such an extent that even the super powers like the USA finds it uneconomical to commit their regular armed forces in future armed conflicts. They are planning to effect significant reductions in their armed forces and instead enhance their capabilities in hybrid warfare. This is like adopting Sun Tzu’s military doctrine propounded by him in about 1000 B.C. and that is:

“The supreme art of war is to subdue the enemy without fighting. If you are far from the enemy make him believe you are near. When you are weak make him believe you are strong. Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win.”

5
Apart from gaining the advantage of remaining below the response level, including the international legal threshold, the hybrid actors enjoy various other advantages. They can exploit ambiguity, asymmetry, non-linearity and flexibility. The entire operation can remain below the level of detection till the hybrid war is well under way. When the victim detects the danger, the damage has already been done. Because of the cyber realm, the use of other hybrid tools is now economical and more effective. Weaponized information directed at the target population through the domestic and foreign media can influence the leadership and the opposition parties. The social media is another effective tool at almost zero cost. The world has seen the outcome of fake news used by Russia to defeat Hilary Clinton in the US 2016 elections and in Ukraine. As they say, the lies spread very fast. The hybrid tools are varied and diverse like, proxies, cyber-attacks, Non-Government Organizations (NGOs), etc. The Ambiguity of hybrid wars enhances speed and flexibility. Vertical and horizontal synchronization of various instruments of power, as discussed above, can turn the tides against the victim state.

6. Weaknesses, Challenges, and Vulnerabilities of Target States

Weaknesses and vulnerabilities of target states make it easier for hybrid actors to exploit them to achieve their objectives. Ethnic and religious divide, polarization among the political parties, weak macroeconomic functioning and dependencies on foreign aids are some of the vulnerabilities that make it difficult to face hybrid challenges. If the opponent state is contiguous to the victim state then again it makes it harder for the latter. The most serious vulnerability is the emergence of ICTs which now enable cyber actors to misuse the extended cyberspace and go on the offensive. Non-hardened and non-resilient ICT infrastructures are very vulnerable. Cashing in on these vulnerabilities determined hybrid opponents will tailor their use of power instruments to exploit the relevant vulnerabilities of the victim state. In summary, the following are exploitable vulnerabilities:

- Weak national cohesion
- Weak macroeconomic functioning
- Domestic and foreign debts
- Dependencies on foreign aid
- Ethnic and religious divide
- Polarization among political parties
- Authoritarian/undemocratic regime
- Politics without principles
- A significant part of the population below poverty line
- Irresponsible use of social media
- Delay in responding to propaganda and fake news
- Non-hardened and non-resilient ICT infrastructure (critical vulnerability)
- Absence of continuing risk assessment

7. Countering Hybrid Threats

The future wars will combine color revolution, cyber war, and unconventional war which is termed as hybrid warfare; the whole being greater than the sum of its parts. “Countering hybrid warfare demands an assessment of critical functions, the interdependencies of these functions and their vulnerabilities. This ‘look at ourselves’ requires a risk assessment process that is sensitive to
vulnerabilities across civil society and not just within the military or security sector” (Monaghan, Cullen, and Wegge 2017).

An ideal course to mitigate/counter hybrid threats would be a continuous and constant endeavor to work on the vulnerabilities and weaknesses covered in paragraph 6 above. A standing national setup comprising military, the private sector, in fact the whole government and whole society and working on permanent basis will be an effective defense mechanism against hybrid threats. A number of countries now have this mechanism. There should be continuous monitoring of critical functions and infrastructures. Any threat to these must be quickly and effectively responded. Weaponized information should be countered through awareness, assessing indicators and with quick responses.

As mentioned earlier, in order to respond to hybrid threats, quick decisions are required. Some strategists recommend using OODA’s loop to make timely and good decisions. OODA’s loop has been defined as the cycle to observe-orient-decide-act. It was developed by military strategist and United states Air Force Colonel John Boyd. He applied the concept to air combat operations. He used it to train Air Force pilots in air to air combats (Schwandt 2018). Air to air combats require very innovative and quick decisions by the pilots because even a second’s delay can mean being shot down. The process is shown in Figure 3.

**Figure 3. OODA’s loop**

The objective is to shorten the cycle/process and decide before your opponent can make the decision. Whichever adversary completes the cycle faster is the winner. The OODA’s loop encourages decision makers to think critically, anticipate threats and neutralize them before they become outdated or critical. It is a military methodology and is used in deciding the H-hour for attacks and counter
attacks. The 2016 US elections were seriously interfered with by Russians because timely decision to neutralize the threat was not taken by America. In comparison, France took a quick decision in its 2018 election to thwart the threat.

8. **Challenges for Pakistan**

- Because of ethnic and religious divide, national cohesion is weak.
- We suffer from political polarization because of politics without principles.
- Our macroeconomic functioning is weak. A significant part of the population lives below the poverty line. Successive governments constantly blame the preceding governments for causing weak economy, corruption and nepotism.
- Because of weak economy, we are dependent on foreign aid/loans. Lending organizations, like International Monetary Fund (IMF) thrust their own agenda on us resulting in inflation and price hikes and causing hardships to the poor and middle classes.
- Our ICT infrastructure is non-hardened and non-resilient. Pakistan is significantly behind in ensuring robust cyber security posture of public and private organizations. Our approach in this sector is reactive, superficial, box-oriented, and contentious and documentation focused (Mahmood 2019). Because of lack of good processes and practices we are vulnerable to cyber-attacks.
- We have a hostile neighbor who remains ever ready to destabilize Pakistan. General Rawat, the former Indian Army Chief and presently the Chief of Defense Staff India, has repeatedly been threatening Pakistan of hybrid war. This remains a critical challenge for Pakistan.

9. **Conclusion**

Hybrid Warfare is diffused, ambiguous and non-linear which allows the hybrid actors to remain below the threshold of detection and response till the operation is well under way and significant damage has already been done. It uses synchronized - means of military and non-military instruments of power to subdue the adversary. The emergence of high information and communication technologies has made this type of warfare flexible and economical. The target states will have to undertake risk assessment of their critical functions and act to minimize exploitable vulnerabilities. This would mean establishing an effective intelligence and counter-intelligence infrastructure and awareness program for timely detection of the impending threats. The OODA’s loop (observe-orient-decide-act) must be completed before the adversary can do it. Let’s accept that this form of warfare is there to stay and evolve and that we must remain ready to face it.

Pakistan cannot lower its guard, especially when the adversary has repeatedly and openly threatened us. Pakistan must take the needed consequential decisions so as not to be surprised.
10. **Policy Recommendations**

Hybrid wars will target one or more of the instruments of power, namely military, political, economic, civil society and information depending on the requirements and capabilities of hybrid actors. Hybrid attacks will be well-planned and systematic. The attacker will indulge in vertical or horizontal escalation. Therefore, the response will also have to be well-planned and systematic. Victim’s vulnerabilities will be an open invitation to the attacker to act. The following recommendations, if implemented, can be a result-oriented strategy against the hybrid threats/attacks:

- Although, it’s difficult for a truly representative and democratic government to forcibly suppress ethnic and religious divide, there is no worthwhile alternative to such a regime. Only, statesmen like Nelson Mandela could bring about national cohesion and harmony. Such a leadership at the helm of affairs would be able to neutralize anti-state movements and color revolutions.

- What are the critical functions of the state? These must be identified and risk assessment of these functions should be carried out on a regular basis. Exploitable vulnerabilities across the military, public and private sectors should be assessed and threshold levels that would indicate hybrid threats should be laid down. Once there is even the slightest indication that any such level is likely to be crossed by the hybrid actor, action to counter it should be initiated.

- Effective coordination among the military and civil should be strengthened. Responsibility to counter hybrid attack should not be left to the military alone. The whole government and civil society should be the real defenders.

- Countering hybrid threats requires timely and sound decisions. Any delay in taking counter action will have disastrous consequences. OODA’s loop (observe-orient-decide-act) should be shortened to defeat the hybrid actors.

- A well-planned and comprehensive awareness programme should be an ongoing exercise. Propaganda, fake news and espionage must be countered as soon as these are detected. Any action when the damage has been done will be of little use. The country must have a strong intelligence and counter intelligence infrastructure.

- A dedicated agency at the national level should ensure close coordination among the stakeholders. It should formulate a national action plan with policies, laws and regulations and other actions required for effective defense against hybrid dangers.

- Hybrid warfare is now an international issue and will remain so in the future. To counter hovering cyber threats necessitates close international cooperation for a coordinated multinational approach. The United Nations should lay down necessary framework and make it mandatory for all countries.

- Pakistan cannot afford to be indifferent to hybrid warfare threats from its hostile neighbour. It must always complete the “OODA’s loop” faster than the possible hybrid actor.
References


Horybho, A 2015, Hybrid Wars: The Indirect Adaptive Approach to Regime Change, Peoples’ University of Russia, Moscow (pp. 20)


Singer, P and Friedman, A 2014, Cyber Security and Cyber War, Oxford University Press, New York, NY 10016, USA (pp. 28)


