WEEKLY FOCUS
#73 | AUG 2022

VISIONIAS
INSPIRING INNOVATION
www.visionias.in

HYBRID WARFARE

NEW AGE WAR WARRANTS A NEW AGE RESPONSE

INTRODUCTION

> Subterfuge and surprise are as old as warfare itself.
>
> - Art of War, Sun Tzu (5th century BC)

One can argue that the nature of international security and conflicts remains the same. States are—as always—embroiled in zero-sum military and economic competitions, armed conflicts still seem inevitable, security dilemmas take place unremittingly. However, the modus operandi is no longer the same.

In 2014, mysterious "little green men" without military insignia emerged in Crimea and wrested the peninsula from Ukraine with hardly a shot being fired. Soon after, in eastern Ukraine, a motley collection of armed thugs and Russian forces took over enclaves in the region of Donbas, claiming to seek independence. These events, and many of the murky actions attributed to Russia since then—from cyber-attacks to assassinations abroad, meddling in elections in the West, and now the invasion—have been labelled as forms of "hybrid war".

But what exactly is hybrid warfare? Why state and non-state actors are resorting to Hybrid Warfare? How Hybrid Warfare and Hybrid Threats are potential issues for India? And what can be done to combat these issues? In this edition, we will attempt to answer these questions.

WHAT IS HYBRID WARFARE?

Hybrid warfare is an emerging, but ill-defined notion. It generally refers to the use of unconventional methods as part of a **multi-domain warfighting approach.** These methods aim to **disrupt and disable an opponent's** actions **with or without engaging in open hostilities.**

The methods adopted by it are a combination of activities, including **disinformation, economic manipulation, use of proxies and insurgencies, diplomatic pressure,** and **military actions.** For example, Russia's use of gas and lending instruments in the Ukrainian conflict.

Following can be cited as key domains of Hybrid Warfare:

Political Warfare: Interference in the political activities of the countries to the detriment of the country. This includes fueling protests by spreading disinformation or fake news items, efforts at subversion of democratic institutions etc. E.g., the 2016 US election and UK Brexit vote are suspected to have been influenced by Russia.

Technological warfare: Using technological capabilities to inflict harm on entities like citizens, enterprises, institutions etc. E.g., targeting software systems of a nuclear power plant via cyberattacks.

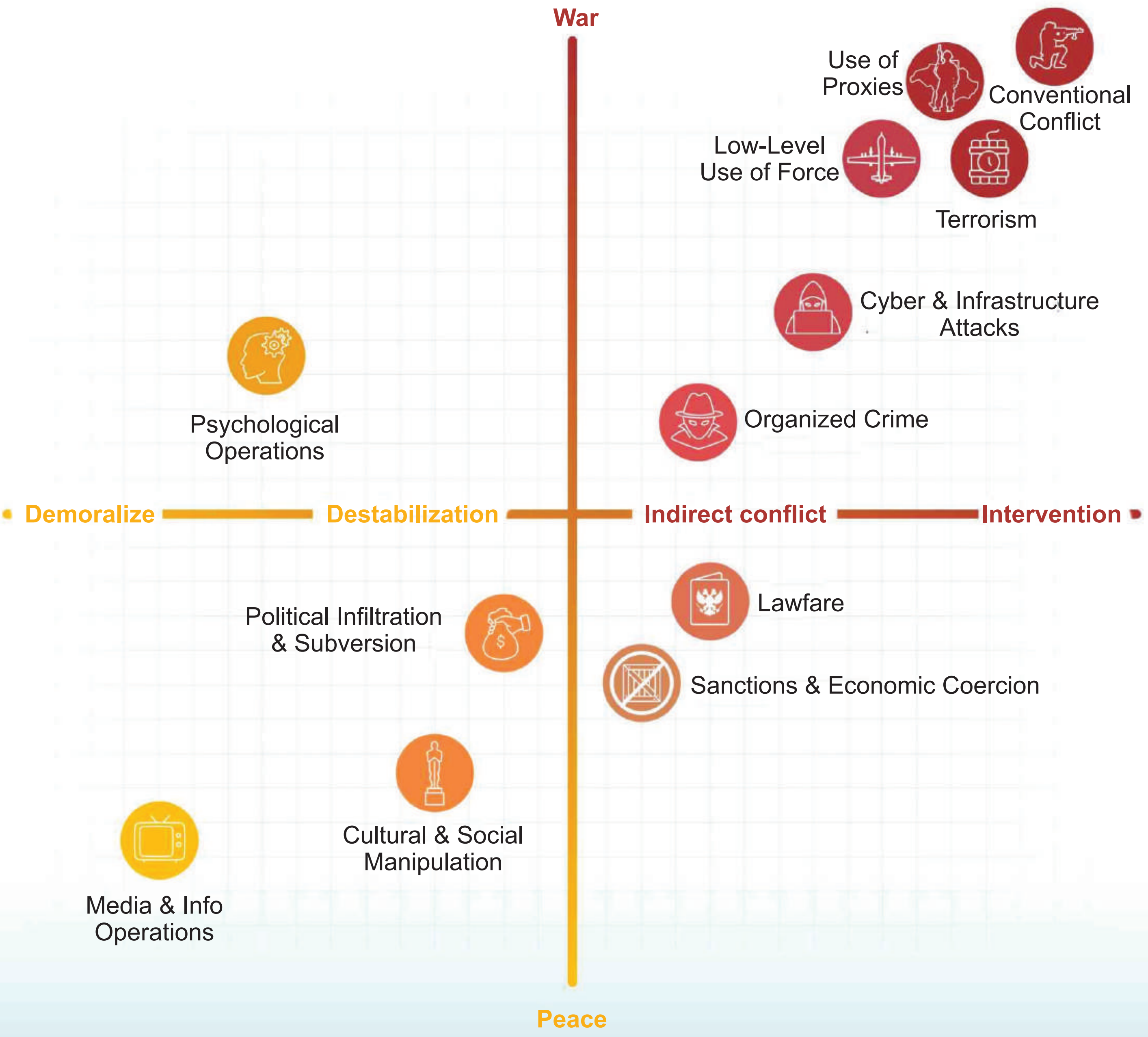
Military warfare: Hybrid warfare includes military actions such as use of improvised explosives, targeted commando operations, guerrilla warfare along with traditional techniques. E.g. in the Israel–Hezbollah War of 2006, Israel used cluster bombs.

Economic warfare: It is used by the state and non-state actors to weaken the economy by disrupting the supply chains, introduction of counterfeit currency etc.

Social warfare: This involves exploiting already prevalent social issues and vulnerabilities via propaganda, provocative messaging etc. E.g., The deep sectarian, ethnic and economic divisions in Syrian society were exploited by both Iran and Islamic State of Iraq and the Levant (ISIL) with a view to achieving their strategic objectives.

But all these facets do not operate in isolation. They generally happen in conjunction with each other. For instance, Russia achieved its political goals in Ukraine by employing hybrid warfare which included cyber-attacks, propaganda, disinformation, economic coercion, and diplomatic pressure, and military methods such as conducting covert operations and empowering proxy warriors.

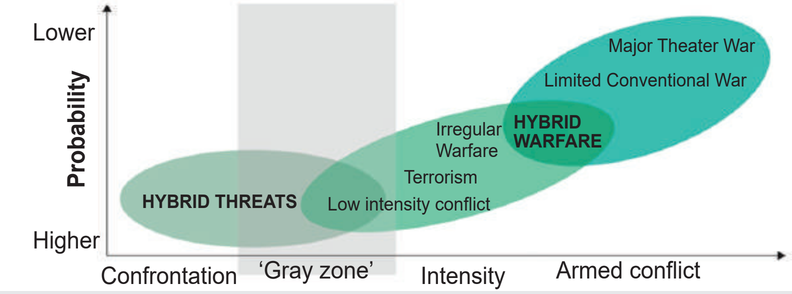
MEANS OF HYBRID WARFARE



IS HYBRID WARFARE AND HYBRID THREAT SAME?

- Hybrid warfare describes a **change in the character of warfare** (that is, against violent adversaries during armed conflict).
- On the other hand, hybrid threats emanate from **nonviolent** strategies that seek gains while avoiding reprisal by **exploiting the gray zone.** E.g., threat of economic sanctions, piracy etc.

Hybrid Threats and Hybrid Warfare Shown on a Continuum of Conflict

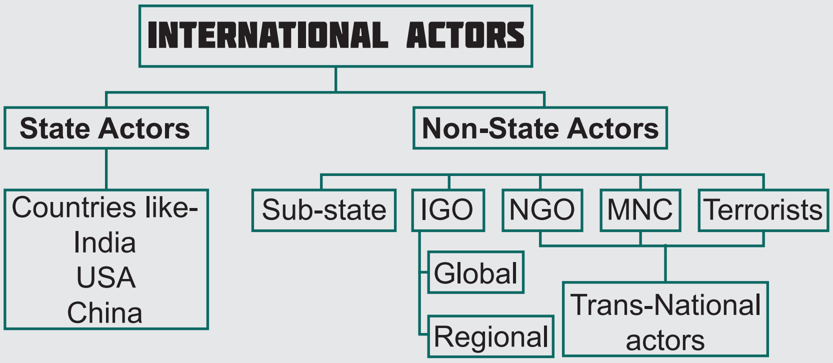


▶ 'Gray Zone' is a related terminology referring to a situation of conflict which is not peace but does **not cross the threshold of war.**

WHY STATE AND NON-STATE ACTORS ARE RESORTING TO HYBRID WARFARE?

The combination of global military proliferation (like growth in military technology), increasing presence of non-state military actors (such as ISIL, Jaish-e-Mohammad etc.) and specific geopolitical objectives have made conventional warfare a 'lose-lose' scenario. In this context, Hybrid Warfare provides following advantages over conventional warfare:

- **Asymmetric nature of activities – gets overlooked in threat assessment:** Hybrid warfare uses a wider set of military, political, economic, civilian and informational instruments which are usually **overlooked in traditional threat assessments.**



IGO: International Governmental Organization

NGO: Non-Governmental Organization

MNC: Multi-National Company

- **Targets highly vulnerable areas:** It tends to **target areas which are highly vulnerable** and where maximum damage can be caused with minimum effort.
- **Synchronized and multi-actor: It can involve state actors, non-state actors or both** indulging in different roles but in a synchronized manner, with an agenda to afflict maximum damage.
  - For example, an urban gathering can experience a simultaneous cyber-attack and a 'lone-wolf' attack, which if synchronized could cause large scale damage to life and property.
- **Scale and target of the attack can be precisely controlled:** It can be tailored according to the circumstances to **stay below detection and response thresholds, including international legal thresholds,** thus hampering the decision- making process and **making it harder to react to such attacks.**
  - The actor in hybrid warfare generally denies involvement in the attack and thus creates a **scenario of plausible deniability.** This enables the entity to avoid any response to its actions at international level. For example, Russia systemically denied its involvement in Ukraine.

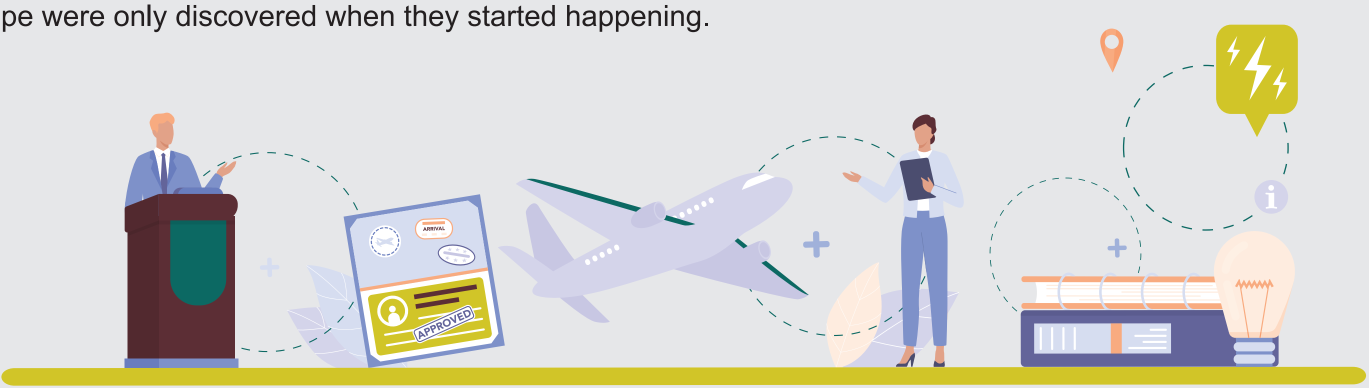
HYBRID TARGET: WHY HYBRID WARFARE TARGET THE URBAN SPACES?

Urban spaces due to their **large populations and economic vibrancy** provide **ample opportunity for terrorists and non-state actors** to sneak in and inflict large scale damage to terrorize populations through **"shock and awe" tactics.**

Traditional armed forces are ill-trained and equipped **to fight in crowded urban areas** with large civilian populations.

Conventional warfare demands direct and complete engagement with the adversary. Hybrid Warfare **uses proxies as indirect tools** creating a **scenario of limited warfare.**

- **Difficult to identify through intelligence systems:** A hybrid warfare campaign **may not be discovered until it is already well underway,** with damaging effects having already begun manifesting themselves and degrading a target's capability to defend itself. For example, the 2008 Mumbai attacks and a series of 'lone wolf' attacks in Europe were only discovered when they started happening.



WARS HAVE BECOME "PROTRACTED SLOW-BURNING CONFLICTS OF ATTRITION."

In case of conventional war, both the entities endure considerable loss to life and property after the war, irrespective of the entity that wins the war. Consequently, both state and non-state actors have started adopting techniques of hybrid warfare.

These techniques **change the nature of the war by bringing down its scale and intensity,** but at the same time, **makes it a long-drawn-out conflict.** For example-

- The insurgency in Guatemala lasted for over thirty years.
- The current war in Columbia began in the 1960s.
- All of the African insurgencies lasted for more than a decade.
- Israel fought Hizbullah in southern Lebanon for eighteen years.

Such a scenario blurs the **distinction between war and peace,** normalizing the acts of hybrid warfare like cyberattacks, terrorism, political interference etc.

HOW HYBRID WARFARE AND HYBRID THREATS ARE POTENTIAL ISSUES FOR INDIA?

India has been at the receiving end of variants of Hybrid Warfare. Firstly, **terrorism,** whose motivations and roots can be traced to Pakistan and the other through **cybersecurity-threats.** Increasing inclination towards Hybrid Warfare from both state and non-state actors can lead to following issues:

- **New forms of terrorist attacks:** The idea of Hybrid Warfare encourages new forms of terrorist attacks such as **'lone-wolf' attacks,** creation of **'sleeper cells' and emergence of hybrid militants.** These attacks are extremely difficult to detect, and, in most cases, the financial and ideological source remains anonymous.
  - Adversary could also act on the lines of **radicalization of the population,** which leads to issues like **Communalism, Naxalism and Separatism** in the long run.
- **Cyber-attacks:** An adversary can pressure the government to concede to its demands by threatening devastating cyber-attacks aimed at the civilian population. Examples include attacks on networks governing hospitals or electricity and water supplies.
  - For instance, post the abrogation of Article 370, cyberattacks on Indian institutions have increased, with many of the attackers openly acknowledging their allegiance to Pakistan based organizations.
- **Interference in electoral processes:** It involves use of techniques like campaigning through the media and social networks and securing financial resources for a political group. This may indirectly influence the outcome of an election in a direction that favors the adversary's political interests.
- **Disinformation and fake news:** An adversary can create a parallel reality and use falsehoods to **fuel social fragmentation.** The idea behind this is to disorient the public and make it difficult for a government to seek public approval for a given policy or operation.
- **Financial influence:** An adversary can make investments, conclude unfavorable energy-supply deals, or offer loans that make a country vulnerable to political pressure in the long-run . For example, the recent steps by Chinese companies to aggressively acquire Indian companies through FDI route in the background of COVID-19 could fall under this category.

HYBRID MILITANT

Security forces in Kashmir are facing a new challenge on the militancy front — the **presence of "hybrid" militants.**

Hybrid Militants are Militants that are not listed as ultras but **persons radicalised enough to carry out a terror strike and then slip back into the routine life.**

On similar lines, the security forces also identified **Over ground workers (OGWs).** OGWs are people who help militants, or terrorists, with logistical support, cash, shelter, and other infrastructure.

CYBERSECURITY THREATS

Cybersecurity threats from China represent an omnipresent danger to National Security. These dangers have been further compounded by increased use of technology and use of coronavirus information handles as phishing tools. One such fraudulent email ID was found to be "ncov2019@gov.in". Following can be cited as major cyberthreats:

- **Privacy and personal data theft:** The Zhenhua case (Chinese firm tracking influential Indians) validates the concern regarding violation of privacy and personal data theft attempted through cyberattacks. This is generally done by introducing malwares in the system. For example-
    - **Remote Access Trojan (RAT):** This malware enters a user's device through an email attachment or as part of larger software package such as a video game, in effect piggybacking on seemingly legitimate files. Once the user clicks on it, a bot (named RAT) is released which allows the hacker to completely take over control of the user device remotely.
- **Mobile apps:** India has the world's highest number of Internet users downloading millions of apps every year. However, 80% of these apps are insecure from security standpoint. This makes the users vulnerable to possible data theft.
    - Some reports suggest that Chinese mobile app firms tend to extract the information that can **compromise a person, and which can be used to blackmail him/her.**
- **Intellectual Property:** According to an American intelligence agency report, Chinese firms have stolen billions of terabytes of data from 141 companies across 20 major industries.
    - According to Maharashtra government, hackers based in **China attempted over 40,000 cyber-attacks on India's Information Technology infrastructure** and banking sector in a span of 5 days.
- **Cyberattacks and Cyber-espionage:** Cyberattacks from Pakistan-based hacker groups targeting India have increased. The stepped-up cyber activity comes in the backdrop of Islamabad's new cyber security policy and expanded digital cooperation with China.
- **China backed threats:** There have been various instances where China-backed states have generated threats in India. For example-
    - Recently, a malware was found on one of the systems of Nuclear Power Corporation of India's **Kudankulam plant.** The malware was designed for data extraction and was linked to the **Lazarus Group,** which is **known to have ties to North Korea.**
    - **Pakistan's malicious and motivated fake news propaganda** through **technological products and applications** coming out of the country.

In the light of these threats, the Government had set up an **expert committee under the National Cyber Security Coordinator.** It will evaluate the "implications" of the digital surveillance and "assess any violations of law and **submit its recommendations within thirty days."**

Apart from the Government, business and individuals should also to make an effort make their cyber environment more secure. Adoption of practices like following increasing security in work systems by **increasing encryption,** adoption of **multiple factor authentication** wherever possible and spreading awareness to ensure **universal adoption of standard cyber hygiene practices.**

In Conversation!

Economic Warfare via Counterfeit Currency

Vinay: Hey Vini. Yesterday, when I was paying for my grocery, the cashier told me that the currency note I was giving him was a fake.

Vini: That is concerning. But how did he know it was fake?

Vinay: He noticed that the currency was missing some essential features of original currency, then he showed the same to me on RBI's website.

Vini: From where did you get this currency note

Vinay: I don't remember. I have done a lot of small transactions of late. But I don't understand, how does fake currency come into circulation?

Vini: Such notes are called Fake Indian Currency Notes (FICN). Majority of them get printed in foreign countries and then are put into circulation in India.

Vinay: Okay. But what is the point of doing this?

Vini: From what I have read, it is said to be a form of Economic Warfare.

Vinay: If it is Economic Warfare, how does circulation of fake currency help the foreign country?

Vini: Circulation of fake currency creates many issues like terror financing, disturbing the money supply causing inflation, black economy and many more.

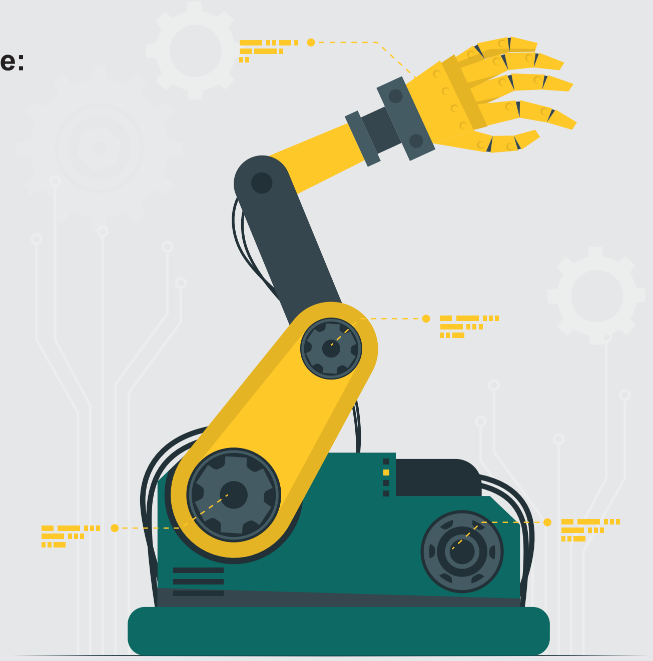
Vinay: This is a major issue. What should we do to help?

Vini: Don't worry. Just be aware of the features of original currency and immediately report the fake currency that you have encountered.

Vinay: Definitely. I will immediately report it. Thanks.

WHAT CAN BE DONE TO COMBAT HYBRID WARFARE?

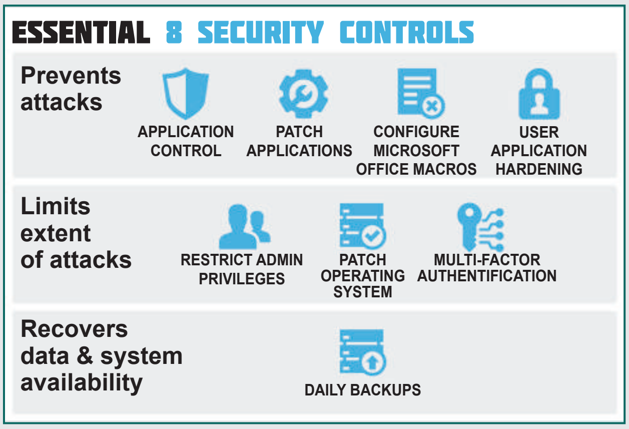
Hybrid Warfare is a multi-pronged warfare methodology, thus, to effectively negate it, the response should also be **holistic in nature:**



- **Systematic and synchronized real time response:** Training of armed forces is critical to ensure appropriate response. In the hybrid warfare, the armed forces have a dual role of protecting the civilian population and disabling the enemy. Following techniques can be adopted:
  - **Creating an institutional mechanism** to ensure nimble response to a potential hybrid attack whenever and wherever it arises.
  - Drills and exercises to ensure **effective coordination between different response domains.**
  - Training in **special battle techniques** and tactics, as well as conditioning to overcome **urban combat stress.**
  - Training in use of **technological tools** such as smart robots, Unmanned Aerial Vehicles (UAVs) etc.
  - **Intelligence tools like Real Time Situational Awareness (RTSA)** will be integral to the precise operations required in urban settings.
- **Institutional measures:** These are critical to keep vulnerabilities in check and estimate possible hybrid threats.

- **Conduct a self-assessment** of critical functions and vulnerabilities across all sectors and subject these vulnerabilities to regular maintenance. For example, regularly **upgrading the critical Fintech systems** in the country.
- **Enhance traditional threat assessment activity** to include non-conventional political, economic, civil, international (PECI) tools and capabilities. Most importantly, this analysis must consider how these means of attack may be formed into a synchronized attack package tailored to the specific vulnerabilities of its target.
- Enable processes to make **comprehensive cross-government efforts** to understand, detect and **respond to hybrid threats.**

- **Strengthening the safety of digital ecosystem:** The growing importance of the digital ecosystem or cyberspace warrants dedicated efforts to make it more secure and robust. To enable the same, Australia's 'essential 8' features for cybersecurity could be emulated.
- **Strengthening our democracy from within:** Strengthening the democratic institutions enables government to **gain trust and cooperation of its citizens.** This helps the government **negate various forms of hybrid warfare** such as disinformation and radicalization.
    - **Inclusion of Civil Society Institutions** such as think tanks multiply the government's capabilities to counter such threats.
    - **Investing in Journalism to raise media literacy:** Global research shows that 70 percent of uses of the term "hybrid threats" by the media are inaccurate. As a result, investing in journalism will indirectly help citizens in understanding the threat.
- **Developing international cooperation:** Multinational frameworks – preferably using existing institutions and processes – should be developed to facilitate cooperation and collaboration across borders.
    - **Developing clear definitions and protocols** to identify and flag hybrid threats and actions intended as hybrid warfare.
    - **Institutionalizing intervention stages and methods** to ensure that victims of hybrid warfare can find support in international community.
    - **Mainstreaming and integrating the issue of hybrid warfare** in the prevalent security dialogues such as on terrorism, money laundering etc.



ESSENTIAL 8 SECURITY CONTROLS

Prevents attacks

APPLICATION CONTROL

PATCH APPLICATIONS

CONFIGURE MICROSOFT OFFICE MACROS

USER APPLICATION HARDENING

Limits extent of attacks

RESTRICT ADMIN PRIVILEGES

PATCH OPERATING SYSTEM

MULTI-FACTOR AUTHENTIFICATION

Recovers data & system availability

DAILY BACKUPS

CONCLUSION

Hybrid warfare adds a new dimension to how coercion, aggression, conflict, and war are to be understood. In this respect, new geostrategic contexts, new applications of technologies, and new organizational forms suggest the likelihood that this form of warfare will persist and continue to evolve into the future. The nature of this warfare is such that it directly impacts all sections of the society in some or the other manner.

In this context, the integration of capabilities of military (joint and multi-national forces), government departments and agencies, and society (including Civil Society Organizations) may be the only way forward to counter the multitude of ever-evolving threats in the future.

TOPIC AT A GLANCE

Hybrid Warfare

It generally refers to the use of unconventional methods as part of a **multi-domain warfighting approach.** These methods aim to **disrupt and disable an opponent's** actions **with or without engaging in open hostilities.** Following can be cited as key domains of Hybrid Warfare-

Political Warfare: Interference in the political activities of the countries to the detriment of the country.	**Technological warfare:** Using technological capabilities to inflict harm on entities.	**Military warfare:** Hybrid warfare includes military actions such as use of improvised explosives, guerrilla warfare etc.	**Economic warfare:** It is used by the state and non-state actors to weaken the economy by disrupting the supply chains, introduction of counterfeit currency etc.	**Social warfare:** This involves exploiting already prevalent social issues and vulnerabilities via propaganda, provocative messaging etc.

Reasons for growing adoption of Hybrid Warfare

- Hybrid warfare uses a wider set of military, political, economic, civilian and informational instruments which are **usually overlooked in traditional threat assessments.**
- It tends to **target areas which are highly vulnerable** and where maximum damage can be caused.
- It can involve **state actors, non-state actors or both** indulging in different **roles but in a synchronized manner.**
- **Scale and target of the attack can be precisely controlled** by staying below certain detection and response thresholds, including international legal thresholds.
- A hybrid warfare campaign **may not be discovered until it is already well underway.**

Hybrid Warfare- A potential issue for India

- **New forms of terrorist attacks** such as **'lone-wolf' attacks,** creation of **'sleeper cells'** and **emergence of hybrid militants.**
- **Cyber-attacks:**
  - ▶**Privacy and personal data theft**
  - ▶**Insecure framework of Mobile Apps**
  - ▶**Cyber-espionage** issues from Pakistan and China
  - ▶Vulnerabilities to **Intellectual Property**
- **Interference in electoral processes** with techniques like campaigning through the media and social networks and securing financial resources for a political group.
- **Using disinformation and fake news** to create a parallel reality and use falsehoods to fuel social fragmentation.
- Financial influence through investments, unfavorable energy-supply deals, or loans that make a country vulnerable in the long run to political pressure.

Ways to combat Hybrid Warfare

- **Systematic and synchronized real time response:**
  - ▶Institutional mechanism to ensure **nimble response.**
  - ▶**Effective coordination** between different response domains.
  - ▶**Use of intelligence tools** like Real Time Situational Awareness (RTSA).
- **Institutional measures:**
  - ▶**Conduct a self-assessment** of critical functions and vulnerabilities.
  - ▶Enhance traditional **threat assessment activity.**
- **Strengthening the safety of digital ecosystem** to make it more secure and robust.
- **Strengthening our democracy from within:**
  - ▶**Inclusion of Civil Society Institutions** to counter such threats.
  - ▶Investing in Journalism to **raise media literacy.**
- **Developing international cooperation:**
  - ▶Developing clear **definitions and protocols.**
  - ▶Institutionalizing **intervention stages and methods.**
  - ▶**Mainstreaming and integrating the issue** of hybrid warfare in the prevalent security dialogues.