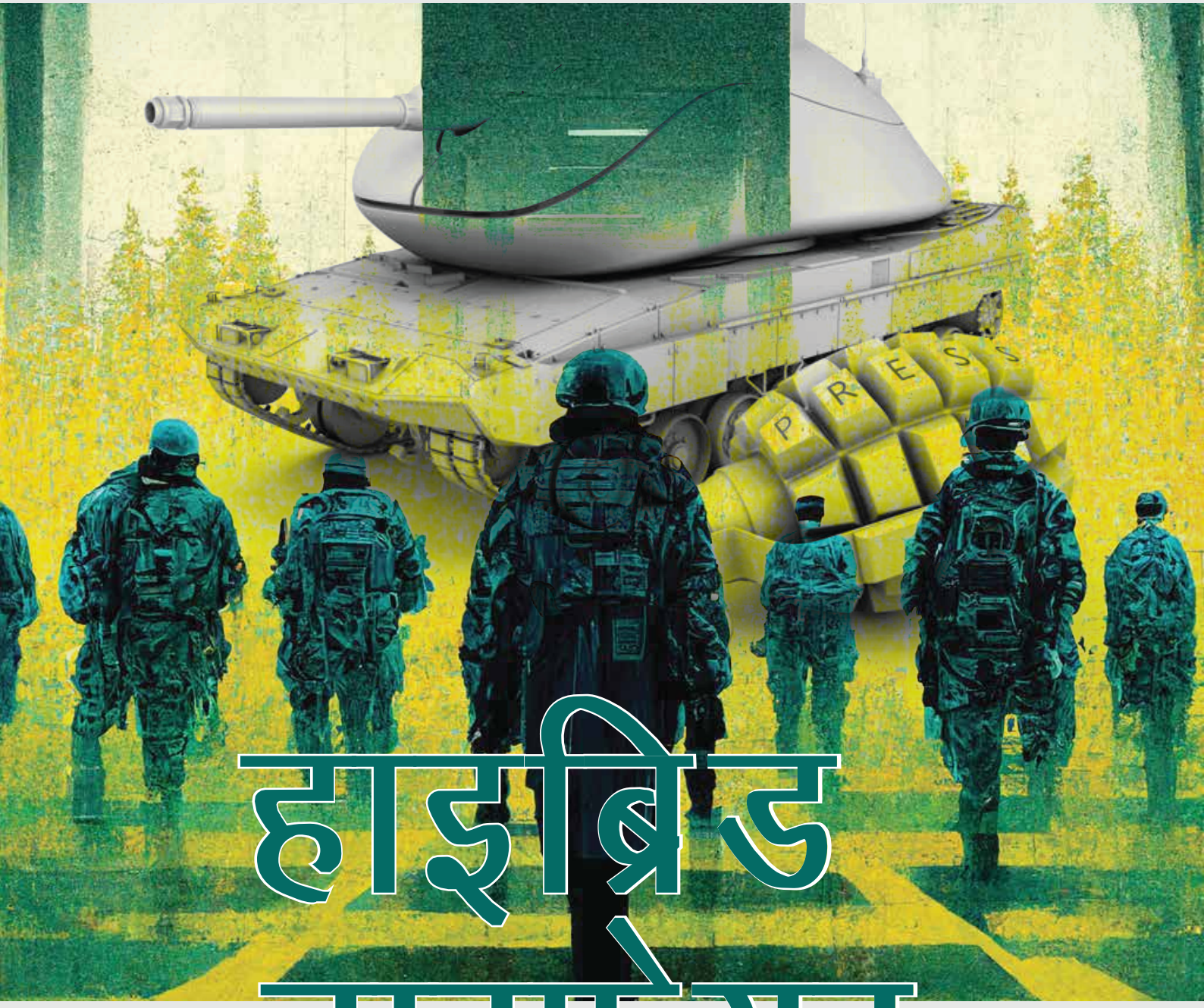
WEEKLY FOCUS
#73 | AUG 2022



हाइब्रिड वारफेयर

नए युग के युद्ध में नए युग की प्रतिक्रिया आवश्यक होगी

परिचय

छल और अप्रत्याशित आक्रमण उतने ही पुराने हैं जितना कि युद्ध।

- आर्ट ऑफ़ वॉर, सन त्ज़ू (5वीं शताब्दी ईसा पूर्व)

ऐसा देखा गया है कि अंतर्राष्ट्रीय सुरक्षा और संघर्षों की प्रकृति सदैव समान रही है। देश सदियों से बिना किसी लाभ व हानि वाली सैन्य एवं आर्थिक प्रतिस्पर्धाओं में संलग्न रहे हैं। सैन्य संघर्ष अभी भी अपरिहार्य प्रतीत होते हैं। साथ ही, सुरक्षा संबंधी दुविधा भी लगातार अस्तित्वमान है। हालांकि, युद्ध संबंधी कार्यप्रणाली में बदलाव आया है, अर्थात् अब वह पहले जैसी नहीं रही है।

वर्ष **2014** में, क्रीमिया में बिना सैन्य रैंक वाले रहस्यमयी "लिटिल ग्रीन मेन" प्रकट हुए थे। इन्होंने क्रीमिया पर बिना किसी रक्तपात के अधिकार कर लिया था। पश्चिमी देशों ने इन्हें रूसी सैनिक बताया था, परन्तु रूस ने यह अस्वीकार कर दिया था। इसके तुरंत बाद, पूर्वी यूक्रेन में, विभिन्न तरह के सशस्त्र समूहों और रूसी सैन्य बलों के एक समूह ने डोनबास क्षेत्र के ज्यादातर इलाकों पर कब्ज़ा कर लिया। इनका दावा था कि ऐसा करके उन्होंने यूक्रेन से अपनी स्वतंत्रता हासिल कर ली है। बाद में रूस ने वर्ष **2014** में ही क्रीमिया को अपने अधीन कर लिया था। तब से, इन घटनाओं और रूस की कई संदिग्ध कार्रवाइयों को "हाइब्रिड युद्ध" कहा जाता है। इसमें साइबर हमले, विदेशों में हत्याएं, पश्चिमी देशों के चुनावों में हस्तक्षेप और दूसरे देश पर आक्रमण करना शामिल हैं।

हाइब्रिड वारफेयर वास्तव में क्या है? राज्य और गैर–राज्य अभिकर्ता हाइब्रिड वारफेयर का सहारा क्यों ले रहे हैं? हाइब्रिड वारफेयर और हाइब्रिड खतरे भारत के लिए कैसे संभावित जोखिम उत्पन्न कर सकते हैं? इन समस्याओं से निपटने के लिए क्या किया जा सकता है? इस संस्करण में हम इन प्रश्नों के उत्तर देने का प्रयास करेंगे।

हाइब्रिड वारफेयर क्या है?

हाइब्रिड वारफेयर एक उभरती हुई अवधारणा है। इसे अब तक उचित रूप से परिभाषित नहीं किया जा सका है। इसके तहत सामान्यतः युद्ध लड़ने के **बहु–पक्षीय दृष्टिकोण के भाग** के रूप में गैर–परंपरागत विधियों का उपयोग किया जाता है। इन विधियों का उद्देश्य **खुली शत्रुतापूर्ण गतिविधियों में शामिल होकर या उसके बिना ही प्रतिद्वंद्वी की कार्रवाइयों को बाधित कर उसे अक्षम** बनाना होता है।

इसके तहत अपनाई जाने वाली विधियों में कई प्रकार की कार्रवाइयों का उपयोग किया जाता है। इनमें **दुष्प्रचार, आर्थिक हेरफेर, छद्म युद्ध और विद्रोह का उपयोग, कूटनीतिक दबाव तथा सैन्य कार्रवाइयां शामिल हैं।** उदाहरण के लिए– यूक्रेन संघर्ष में रूस द्वारा प्राकृतिक गैस और ऋण जैसे साधनों का उपयोग किया जाना।

निम्नलिखित को हाइब्रिड वारफेयर के प्रमुख स्वरूपों के रूप में चिन्हित किया जा सकता है:

राजनीतिक वारफेयर: इसके अंतर्गत किसी देश की राजनीतिक गतिविधियों में हस्तक्षेप करके उस देश को हानि पहुंचाई जाती है। इसमें दुष्प्रचार या भ्रामक सूचनाओं के प्रसार द्वारा विरोध प्रदर्शनों को बढ़ावा देने तथा लोकतांत्रिक संस्थानों की कार्यप्रणाली को बाधित करने के प्रयास किए जाते हैं। उदाहरण के लिए– ऐसा संदेह व्यक्त किया गया है कि वर्ष **2016** के अमेरिकी चुनाव और ब्रेक्जिट से संबंधित मतदान में रूस ने हस्तक्षेप किया था।

तकनीकी वारफेयर: इसके तहत नागरिकों, उद्यमों, संस्थानों आदि जैसी इकाइयों को नुकसान पहुंचाने के लिए तकनीकी क्षमताओं का उपयोग किया जाता है। उदाहरण के लिए– साइबर हमलों के माध्यम से परमाणु ऊर्जा संयंत्र के सॉफ्टवेयर सिस्टम को लक्षित करना आदि।

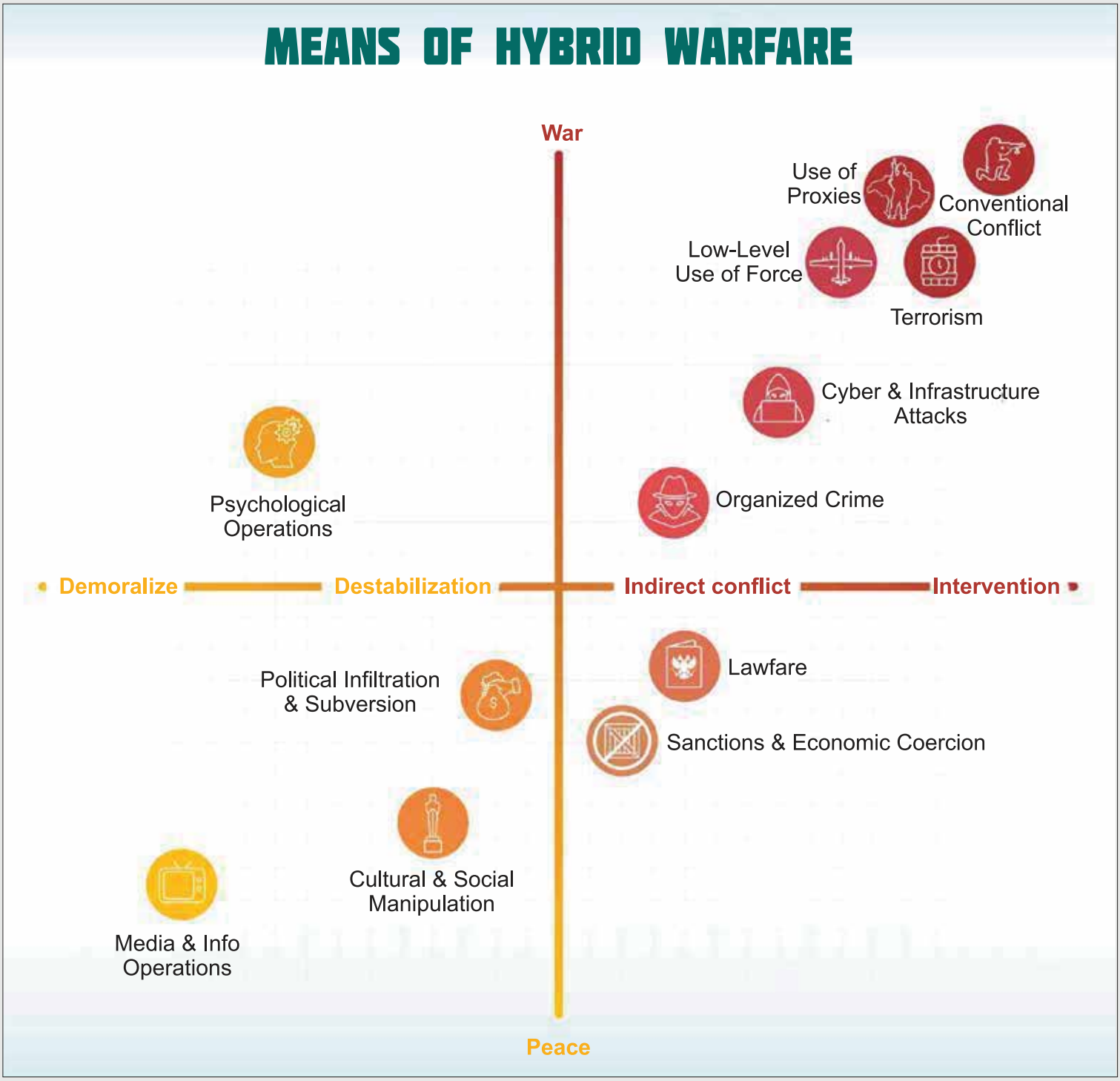
सैन्य वारफेयर: इसके तहत पारंपरिक तकनीकों के साथ–साथ इम्प्रोवाइज्ड एक्सप्लोसिव, लक्षित कमांडो अभियान, गुरिल्ला युद्ध पद्धति आदि जैसी सैन्य कार्रवाइयों का प्रयोग किया जाता है। उदाहरण के लिए– वर्ष 2006 के इजरायल–हिज्बुल्लाह युद्ध में इजरायल ने क्लस्टर बमों का प्रयोग किया था।

आर्थिक वारफेयर: इसके तहत राज्य और गैर–राज्य अभिकर्ताओं द्वारा आपूर्ति श्रृंखलाओं को बाधित किया जाता है। साथ ही, इसमें नकली/ जाली मुद्राओं को बढ़ावा देकर लक्षित देश की अर्थव्यवस्था को कमजोर किया जाता है।

सामाजिक वारफेयर: इसमें दुष्प्रचार, भड़काऊ संदेशों आदि के द्वारा पहले से प्रचलित सामाजिक मुद्दों और कमजोरियों का फायदा उठाकर सामाजिक सौहार्द बिगाड़ने की कोशिश की जाती है। उदाहरण के लिए– ईरान और ISIL (इस्लामिक स्टेट ऑफ इराक एंड द लेवेंट) दोनों ने अपने रणनीतिक उद्देश्यों को साकार करने हेतु सीरियाई समाज में प्रचलित सांप्रदायिक, नृजातीय और आर्थिक विभाजन का दुरुपयोग किया था।

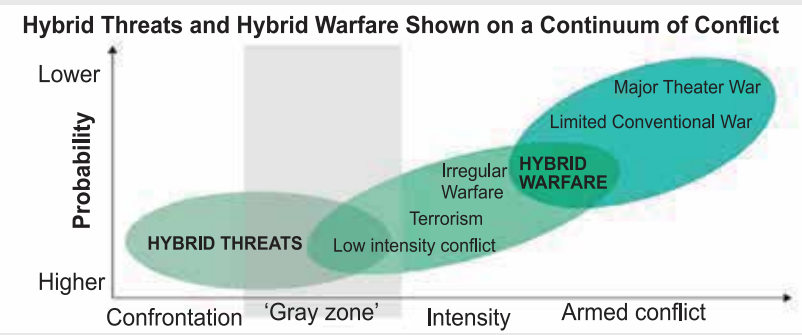
हालांकि, उपर्युक्त हाइब्रिड वारफेयर के स्वरूपों को एकल रूप से अंजाम नहीं दिया जाता है। इन्हें आम तौर पर एक दूसरे के साथ संयुक्त रूप से संचालित किया जाता है। उदाहरण के लिए– रूस ने यूक्रेन में अपने राजनीतिक उद्देश्यों को हासिल करने हेतु हाइब्रिड वारफेयर जैसे तरीकों का प्रयोग किया था। इनमें साइबर हमले, दुष्प्रचार, भ्रामक सूचनाओं को फैलाना, आर्थिक नियंत्रण एवं राजनयिक दबाव के साथ–साथ गुप्त अभियान तथा प्रॉक्सी वॉरियर्स (छद्म लड़ाकों) को सशक्त बनाने जैसे सैन्य तरीके भी शामिल थे।

हाइब्रिड वारफेयर के साधन



क्या हाइब्रिड वारफेयर और हाइब्रिड खतरे समान हैं?

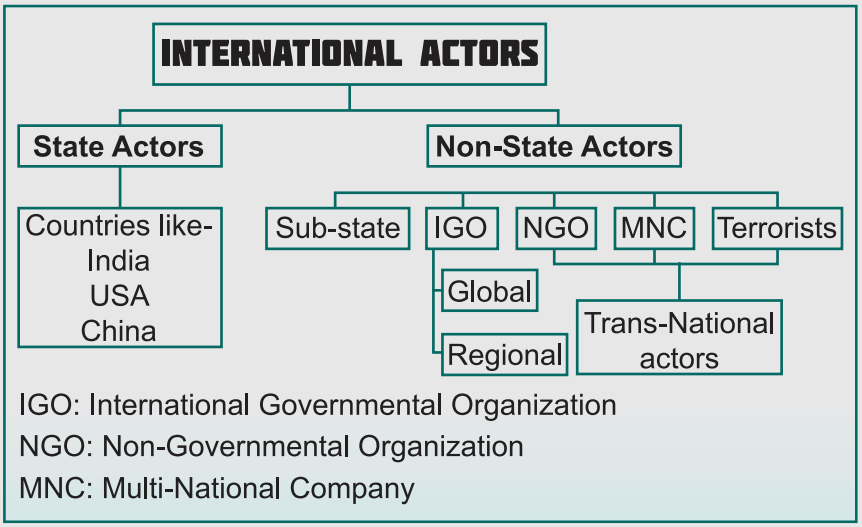
- हाइब्रिड वारफेयर वस्तुतः सशस्त्र संघर्ष के दौरान हिंसक विरोधियों के खिलाफ **युद्ध के स्वरूप में हो रहे परिवर्तन को संदर्भित** करता है।
- दूसरी ओर, हाइब्रिड खतरा **अहिंसक** रणनीतियों द्वारा उत्पन्न होता है। उदाहरण के लिए– आर्थिक प्रतिबंध, पायरेसी से संबंधित खतरे आदि। इसके तहत जवाबी कार्रवाई करने की बजाए **'ग्रे जोन'** का लाभ उठाने की कोशिश की जाती है।



▶ **ग्रे जोनः** यह संघर्ष की उस स्थिति को संदर्भित करता है जिसमें न तो शांतिपूर्ण स्थिति होती है और न ही स्थिति युद्ध की सीमा तक पहुंचती है।

राज्य और गैर–राज्य अभिकर्ता हाइब्रिड वारफेयर का उपयोग क्यों कर रहे हैं?

वैश्विक सैन्य प्रसार (जैसे– सैन्य प्रौद्योगिकी में वृद्धि), गैर–राज्य सैन्य अभिकर्ताओं (जैसे– ISIL, जैश–ए–मोहम्मद आदि) की बढ़ती उपस्थिति और विशिष्ट भू–राजनीतिक उद्देश्यों ने **पारंपरिक युद्ध को एक 'हानिकारक परिणाम प्रदान करने वाले परिदृश्य'** में बदल दिया है। इस संदर्भ में, पारंपरिक युद्ध की तुलना में हाइब्रिड वारफेयर निम्नलिखित लाभ प्रदान कर सकते हैं:



- **गतिविधियों की असमान प्रकृति– खतरों के आकलन में अक्सर इसकी अनदेखी की जाती है:** हाइब्रिड वारफेयर के तहत सैन्य, राजनीतिक, आर्थिक, नागरिक और सूचना आधारित साधनों के व्यापक समूह का उपयोग किया जाता है। ज्ञातव्य है कि **खतरों के आकलन की पारंपरिक पद्धति में सामान्यतः इनकी अनदेखी** की जाती है।

- **अत्यधिक सुभेद्य क्षेत्रों को लक्षित करना: इसके तहत अत्यधिक सुभेद्य क्षेत्रों को लक्षित** किया जाता है, जहां न्यूनतम प्रयास से अधिकतम नुकसान किया जा सकता है।

- **सिंक्रनाइज़ और बहु–अभिकर्ता:** इसमें राज्य अभिकर्ता, गैर–राज्य अभिकर्ता या दोनों, एक ही समय पर सुव्यवस्थित तरीके से अलग–अलग भूमिकाएं निभाते हैं। इनका उद्देश्य अधिकतम नुकसान पहुंचाना होता है।

  ▶ उदाहरण के लिए– एक शहर में साइबर हमला और लोन वुल्फ हमला एक साथ किया जा सकता है, लेकिन यदि इन्हें समकालिक बना दिया जाए तो, इससे जीवन और संपत्ति को बहुत अधिक नुकसान हो सकता है।

- **हमले की व्यापकता और लक्ष्य पर सुव्यवस्थित नियंत्रण:** ऐसे हमलों को अपने **विरूद्ध जवाबी कार्रवाई (विशेष रूप से अंतर्राष्ट्रीय प्रतिक्रिया) और अपनी पहचान के प्रकट होने की संभावना** से बचते हुए परिस्थितियों के अनुसार तैयार किया जा सकता है। इस प्रकार लक्षित देश की निर्णय लेने की प्रक्रिया प्रभावित होती है। इससे ऐसे **हमलों के विरुद्ध कार्रवाई करना और भी कठिन हो जाता है।**

हाइब्रिड लक्ष्य: हाइब्रिड वारफेयर में शहरी क्षेत्रों को ही क्यों लक्षित किया जाता है?

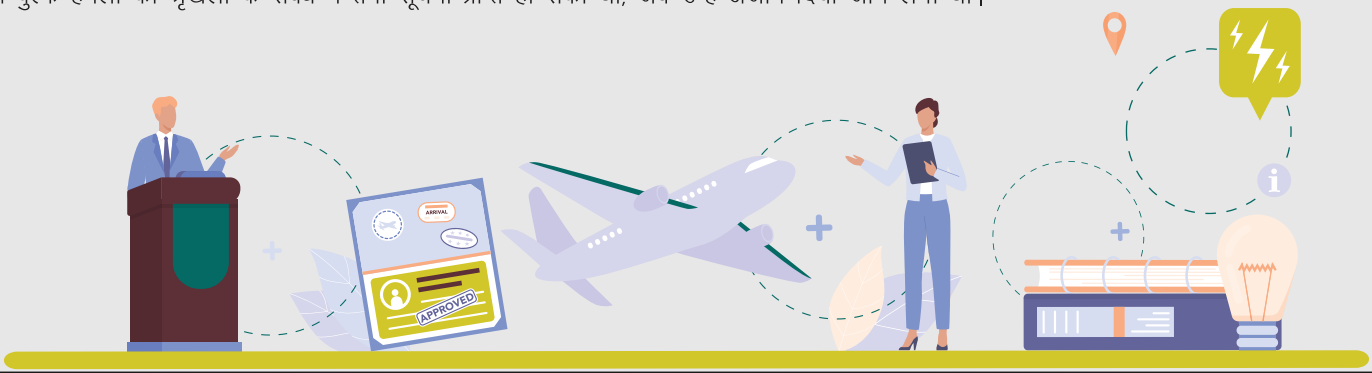
शहर **बड़ी आबादी और आर्थिक गतिविधियों का केंद्र होते हैं।** यह स्थिति आतंकवादियों और गैर–राज्य अभिकर्ताओं को बड़े पैमाने पर क्षति पहुंचाने का **पर्याप्त अवसर प्रदान करती है।** वे **"आघात और भय" की रणनीति** द्वारा शहरी आबादी को आतंकित करते हैं।

विशाल जनसंख्या वाले भीड़–भाड़ से युक्त शहरी क्षेत्रों में ऐसे हमलों से निपटने के लिए **पारंपरिक सशस्त्र बल** पर्याप्त रूप से **प्रशिक्षित नहीं हैं। साथ ही, उनके पास ऐसी स्थिति से निपटने के लिए आवश्यक संसाधनों का भी अभाव है।**

पारंपरिक युद्ध में विरोधी के साथ आमने–सामने की लड़ाई होती है। हाइब्रिड वारफेयर के दौरान **अप्रत्यक्ष या छद्म संसाधनों का उपयोग करते हुए सीमित मात्रा में युद्ध जैसी स्थितियों का निर्माण** किया जाता है।

▶ हाइब्रिड वारफेयर में अभिकर्ता आमतौर पर हमले में स्वयं की भागीदारी से मना करता है। इस प्रकार **ऐसे हमलों के प्रति किसी की जवाबदेही सुनिश्चित** कर पाना कठिन हो जाता है। ऐसी स्थिति में इन अभिकर्ताओं के विरुद्ध अंतर्राष्ट्रीय स्तर पर कोई जवाबी कार्रवाई करना भी मुश्किल हो जाता है। उदाहरण के लिए– रूस ने स्पष्ट रूप से यूक्रेन में अपनी भागीदारी से इनकार कर दिया था।

- **खुफिया प्रणालियों द्वारा भी पहचान करना कठिन:** ऐसा भी हो सकता है कि हाइब्रिड वारफेयर का **तब तक पता न लग पाए, जब तक कि वह पूर्ण रूप से प्रभावी न हो जाए।** तात्पर्य यह है कि ऐसे हमले जब तक हानिकारक प्रभाव उत्पन्न करते हुए स्वयं को प्रकट नहीं करते हैं, तब तक उनका पता लगाना कठिन होता है। ऐसी स्थिति में लक्षित देश या संस्था की जवाबी कार्रवाई नकारात्मक रूप से प्रभावित हो जाती है। उदाहरण के लिए– वर्ष 2008 में मुंबई हमलों और यूरोप में लोन वुल्फ हमलों की श्रृंखला के संबंध में तभी सूचना प्राप्त हो सकी थी, जब उन्हें अंजाम दिया जाने लगा था।



युद्ध अब "लंबे समय तक बने रहने वाले संघर्षों" में तब्दील हो गए हैं।

पारंपरिक युद्ध में किसी एक पक्ष की जीत के बावजूद भी दोनों पक्षों को जीवन और संपत्ति का व्यापक नुकसान उठाना पड़ता है। इसी के परिणामस्वरूप, राज्य और गैर–राज्य अभिकर्ताओं ने हाइब्रिड वारफेयर तकनीकों को अपनाना शुरू कर दिया है।

ये तकनीकें **युद्ध की प्रकृति को परिवर्तित कर रही हैं।** ये तकनीकें **युद्ध की व्यापकता और गहनता को सीमित करते हुए इसे दीर्घकालिक संघर्ष में तब्दील कर रही हैं। उदाहरण के लिए–**

- ग्वाटेमाला में तीस से अधिक वर्षों तक विद्रोह चलता रहा।
- वर्तमान में चल रहा कोलंबिया का युद्ध 1960 के दशक में शुरू हुआ था।
- सभी अफ्रीकी विद्रोह एक दशक से भी अधिक समय से जारी हैं।
- इजरायल और दक्षिणी लेबनान में हिजबुल्लाह के बीच अठारह वर्षों तक संघर्ष चलता रहा।

ऐसे परिदृश्य **युद्ध और शांति के बीच के अंतर को अस्पष्ट** कर देते हैं। साथ ही, ये साइबर हमलों, आतंकवाद, राजनीतिक हस्तक्षेप आदि जैसे हाइब्रिड वारफेयर गतिविधियों को सामान्य बनाने में मदद करते हैं।

हाइब्रिड वारफेयर और हाइब्रिड खतरे भारत के लिए संभावित चुनौतियां कैसे हैं?

हाइब्रिड वारफेयर के संदर्भ में देखें तो भारत ऐसी घटनाओं का भुक्तभोगी रहा है। इसमें पाकिस्तान द्वारा राज्य प्रायोजित आतंकवाद और साइबर **सुरक्षा संबंधी खतरों** के माध्यम से की जाने वाली हाइब्रिड वारफेयर गतिविधियां शामिल हैं। राज्य और गैर–राज्य अभिकर्ताओं दोनों का हाइब्रिड वारफेयर की ओर बढ़ता झुकाव निम्नलिखित मुद्दों को उत्पन्न कर सकता है:

- **आतंकवादी हमलों के नए रूप:** हाइब्रिड वारफेयर का विचार **'लोन–वुल्फ' हमलों, 'स्लीपर सेल' के निर्माण और हाइब्रिड लड़ाकों के उद्भव** जैसे आतंकवादी हमलों के नए रूपों को प्रोत्साहित करता है। ऐसे हमलों का पता लगाना अत्यधिक कठिन होता है और अधिकतर मामलों में तो ऐसे हमलों का वित्तीय एवं वैचारिक स्रोत अज्ञात ही बना रहता है।
  - हाइब्रिड वारफेयर संबंधी घटनाओं को अंजाम देने के लिए लक्षित देश की आबादी में चरमपंथी विचारधारा को बढ़ावा देने की दिशा में कार्य किया जाता है। इससे लक्षित देश **सांप्रदायिकता, नक्सलवाद और अलगाववाद** जैसे मुद्दों से लंबे समय तक ग्रस्त रहता है।
- **साइबर हमले:** इसके तहत हाइब्रिड वारफेयर संबंधी हमला करने वाले, आबादी पर विनाशकारी साइबर हमलों की धमकी देते हैं। इस प्रकार, वे अपनी मांगों को मनवाने के लिए सरकार को विवश कर सकते हैं। इसमें अस्पतालों या विद्युत तथा जल–आपूर्ति को नियंत्रित करने वाले नेटवर्कों पर हमले करना आदि शामिल है।
  - उदाहरण के लिए– अनुच्छेद 370 के निरस्त होने के बाद से भारतीय संस्थानों पर साइबर हमलों में वृद्धि हुई है। इसमें कई **साइबर हमलावरों** ने खुलकर पाकिस्तान के साथ अपने संबंधों को स्वीकार भी किया है।
- **चुनाव प्रक्रियाओं में हस्तक्षेप:** इसके तहत मीडिया और सोशल नेटवर्क के माध्यम से प्रचार करना शामिल है। साथ ही, संबंधित राजनीतिक दल के लिए धन जुटाने जैसी गतिविधियों को भी अंजाम दिया जाता है। इसके द्वारा हाइब्रिड वारफेयर संबंधी हमला करवाने वाले अपने राजनीतिक हितों के पक्ष में चुनाव के परिणाम को प्रभावित कर सकते हैं।
- **दुष्प्रचार और फेक न्यूज:** हाइब्रिड वारफेयर के तहत **लक्षित समाज में मतभेद को बढ़ावा देने** के लिए झूठे तथ्यों पर आधारित एक अलग वास्तविकता का निर्माण किया जाता है। इन कार्यों के पीछे का उद्देश्य जनता को गुमराह करना और सरकार में जनता के विश्वास को कम करना होता है।
- **वित्तीय प्रभाव:** हाइब्रिड वारफेयर के माध्यम से लक्षित देश में ऐसे निवेश व प्रतिकूल ऊर्जा–आपूर्ति सौदे या ऋण प्रदान किए जा सकते हैं, जो लक्षित देश को लंबे समय तक राजनीतिक दबाव के प्रति सुभेद्य बना देते हैं। उदाहरण के लिए– हाल ही में कोविड–19 के दौरान चीन की कंपनियों द्वारा प्रत्यक्ष विदेशी निवेश के माध्यम से भारतीय कंपनियों का लक्षित रूप से अधिग्रहण करने की प्रवृत्ति को इस श्रेणी में शामिल किया जा सकता है।

हाइब्रिड लड़ाके

कश्मीर में तैनात सुरक्षा बलों को आतंकवाद–रोधी मोर्चे पर एक नई चुनौती का सामना करना पड़ रहा है। उदाहरण के लिए– **'हाइब्रिड' आतंकवादियों की मौजूदगी सुरक्षा बलों के लिए एक नई चुनौती के रूप में उभरकर सामने आई है।**

हाइब्रिड लड़ाके ऐसे लड़ाके होते हैं, जो अतिवादियों के रूप में सूचीबद्ध नहीं होते हैं। हालांकि, चरमपंथी विचारधारा से ग्रस्त ऐसे व्यक्ति **आतंकी हमलों को अंजाम देने में सक्षम होते हैं। साथ ही, ऐसे व्यक्ति घटना को अंजाम देने के बाद सामान्य नागरिक की तरह जीवनयापन करते रहते हैं।**

इसी तर्ज पर सुरक्षाबलों ने **ओवर ग्राउंड वर्कर्स** (OGWs) की पहचान की है। OGWs ऐसे व्यक्ति होते हैं, जो लड़ाकों या आतंकवादियों को मानवीय सहायता, रसद, नकदी, आवास और अन्य सुविधाएं प्रदान करते हैं।

साइबर सुरक्षा से संबंधित खतरे

चीन द्वारा संचालित साइबर सुरक्षा खतरे, भारत की सुरक्षा के समक्ष सर्वव्यापी जोखिम पैदा करते हैं। प्रौद्योगिकी के बढ़ते प्रयोग और कोरोना वायरस संबंधी सूचना हैंडल प्लेटफॉर्म के फ़िशिंग टूल के रूप में उपयोग ने इन खतरों को और बढ़ा दिया है। इस संबंध में 'ncov2019@gov.in' के नाम से एक फर्जी ईमेल आई.डी. पाई गई थी। अतः ऐसे में निम्नलिखित पहलुओं को प्रमुख साइबर खतरों के रूप में चिन्हित किया जा सकता है:

- **निजता का उल्लंघन और व्यक्तिगत डेटा की चोरी:** झेन्हुआ प्रभावशाली भारतीयों पर नज़र रखने वाली चीन की एक कंपनी है। झेन्हुआ मामले में साइबर हमलों के द्वारा निजता के उल्लंघन और व्यक्तिगत डेटा की चोरी से जुड़े मुद्दे सामने आए थे। इसे आमतौर पर कंप्यूटर/मोबाइल सिस्टम में मैलवेयर को प्रवेश कराकर अंजाम दिया गया था। उदाहरण के लिए–

  - **रिमोट एक्सेस ट्रोजन (RAT):** ऐसे मैलवेयर को ईमेल अटैचमेंट के द्वारा या वीडियो गेम जैसे बड़े सॉफ्टवेयर पैकेज के एक भाग के रूप में उपयोगकर्ता के डिवाइस में प्रवेश कराया जाता है। जब उपयोगकर्ता इस (ईमेल अटैचमेंट या सॉफ्टवेयर) पर क्लिक करता है, तब एक बॉट (जिसका नाम RAT है) सिस्टम में प्रवेश कर जाता है। इसकी मदद से हैकर दूर से ही उपयोगकर्ता के डिवाइस को पूरी तरह से नियंत्रित कर सकता है। इसकी मदद से उपयोगकर्ता की फ़ाइलों को अवैध तरीके से एक्सेस करने की कोशिश की जाती है। हालांकि, यह पूर्णतः वैध प्रक्रिया की तरह दिखती है। ऐसी गतिविधियों को पिग्गीबैकिंग (Piggybacking) के रूप में जाना भी जाता है।

- **मोबाइल ऐप्स:** भारत दुनिया का सर्वाधिक इंटरनेट उपभोग करने वाला देश है। यहां प्रतिवर्ष लाखों ऐप डाउनलोड की जाती हैं। इनमें से 80% ऐप्ससुरक्षा की दृष्टि से असुरक्षित होती हैं। इससे उपयोगकर्ताओं के डेटा की चोरी की संभावना बढ़ जाती है।

  - कुछ रिपोर्ट्स से पता चला है कि चीन की मोबाइल ऐप कंपनियों द्वारा उपयोगकर्ता के मोबाइल से उसकी व्यक्तिगत जानकारी की चोरी की जाती है। ऐसी जानकारियों का उपयोग उस **व्यक्ति को ब्लैकमेल करने के लिए भी किया जा सकता है।**

- **बौद्धिक संपदा:** एक अमेरिकी खुफिया एजेंसी की रिपोर्ट के अनुसार, चीन की कंपनियों द्वारा **20** प्रमुख उद्योगों की **141** कंपनियों से अरबों टेराबाइट डेटा की चोरी की गई है।

  - महाराष्ट्र सरकार के अनुसार, **चीन स्थित हैकरों ने 5 दिनों में ही भारत की सूचना प्रौद्योगिकी अवसंरचना और बैंकिंग क्षेत्रक पर 40,000 से अधिक बार साइबर हमले** किए थे।

- **साइबर हमले और साइबर जासूसी:** भारत को निशाना बनाने के उद्देश्य से पाकिस्तान स्थित हैकर समूहों द्वारा किए जाने वाले साइबर हमलों की संख्या में बढ़ोतरी हुई है। ऐसे हमलों में वृद्धि हेतु पाकिस्तान की नई साइबर सुरक्षा नीति और चीन के साथ पाकिस्तान का बढ़ता डिजिटल सहयोग मुख्य रूप से उत्तरदायी है।

- **चीन प्रायोजित खतरे:** ऐसे कई उदाहरण हैं, जहां चीन समर्थित देशों द्वारा भारत में खतरों को उत्पन्न करने के प्रयास किए गए हैं। उदाहरण के लिए–

  - हाल ही में, न्यूक्लियर पॉवर कॉर्पोरेशन ऑफ इंडिया के कुडनकुलम संयंत्र के सिस्टम में मैलवेयर पाया गया था। इस मैलवेयर को डेटा की चोरी करने के लिए डिज़ाइन किया गया था। यह मैलवेयर लाजर समूह से संबद्ध था। ऐसा माना जाता है कि यह समूह उत्तर कोरिया से संबंधित है।

  - **पाकिस्तान द्वारा दुर्भावनापूर्ण और फेक न्यूज़ के प्रसार हेतु** भारत में बाहर से आने वाले **तकनीकी उत्पादों और ऐप्स का सहारा** लिया जाता है।

इन खतरों के आलोक में सरकार ने **राष्ट्रीय साइबर सुरक्षा समन्वयक (National Cyber Security Coordinator)** की अध्यक्षता में एक विशेषज्ञ समिति का गठन किया है। यह समिति डिजिटल निगरानी से जुड़े "निहितार्थों" का मूल्यांकन करेगी और कानून के किसी भी प्रकार के उल्लंघन का आकलन करेगी। साथ ही, **तीस दिनों के भीतर अपनी सिफारिशें** प्रस्तुत करेगी।

सरकार के अलावा, व्यवसायियों तथा व्यक्तियों को भी अपने साइबर परिवेश को और अधिक सुरक्षित बनाने का प्रयास करना चाहिए। कार्य प्रणालियों में बेहतर साइबर सुरक्षा को सुनिश्चित करने हेतु निम्नलिखित कार्य किए जाने चाहिए:

- एन्क्रिप्शन संबंधी तकनीकों का अधिक से अधिक उपयोग करना चाहिए;
- जहां भी संभव हो, बहु–कारक आधारित प्रमाणीकरण को अपनाना चाहिए और
- साइबर सुरक्षा संबंधी मानक प्रणालियों के सार्वभौमिक अंगीकरण को सुनिश्चित करने के लिए जागरूकता का प्रसार करना चाहिए।

एक छोटी सी वार्ता!

नकली मुद्रा के माध्यम से आर्थिक वारफेयर

विनय: अरे विनी कल, जब मैं किराने के सामान का भुगतान कर रहा था, तब दुकानदार ने मुझे कहा कि मेरा नोट नकली है।

विनी: यह तो चिंता की बात है। लेकिन, दुकानदार को कैसे पता चला कि वह नोट नकली था?

विनय: उसने देखा कि मेरे नोट में असली नोट की कुछ आवश्यक विशेषताएं मौजूद नहीं थी। साथ ही, उसने मुझे RBI की वेबसाइट पर भी असली नोट की वही विशेषताएं दिखाई, जो मेरे नोट में नहीं थीं।

विनी: तुमने ये नोट कहां से लिया था?

विनय: मुझे याद नहीं है। मैंने पिछले दिनों कई सारे छोटे–छोटे लेनदेन किए थे। लेकिन, मुझे समझ में नहीं आता कि नकली नोट प्रचलन में कैसे आ जाते हैं?

विनी: ऐसे नोटों को नकली भारतीय नोट कहा जाता है। इनमें से अधिकांश को विदेशों में मुद्रित किया जाता है और फिर भारत में इनको चलाया जाता है।

विनय: ठीक है। लेकिन, ऐसा करने के पीछे क्या उद्देश्य है?

विनी: जैसा कि मैंने एक जगह पढ़ा था, यह आर्थिक वारफेयर का एक रूप है।

विनय: अगर यह आर्थिक वारफेयर है, तो नकली मुद्रा के प्रचलन से बाहरी देशों को कैसे फायदा मिलता है?

विनी: नकली मुद्रा के प्रचलन से आतंकवाद के वित्तपोषण, मुद्रा की आपूर्ति में बाधा, मुद्रास्फीति में बढ़ोतरी, काला धन आदि जैसी कई समस्याओं को बढ़ावा मिलता है।

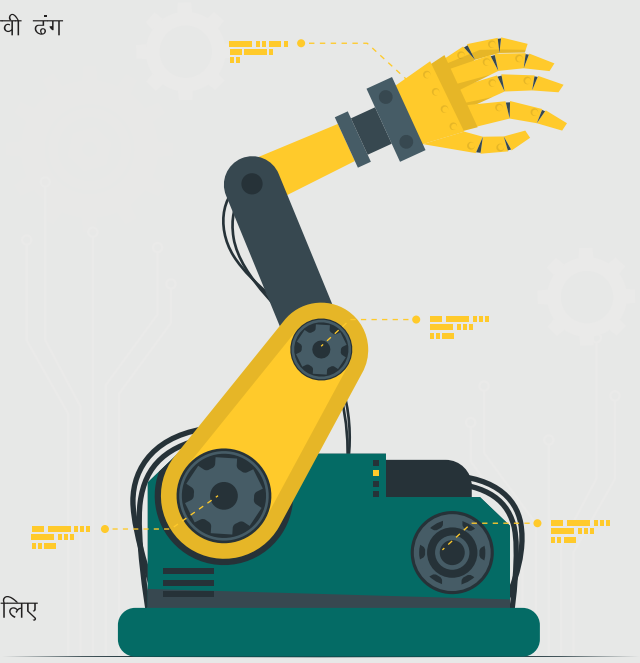
विनय: यह तो एक गंभीर समस्या है। इसका समाधान करने के लिए हमें क्या करना चाहिए?

विनी: चिंता मत करो। इसके लिए तुम्हें बस असली नोट की विशेषताओं की सही जानकारी होनी चाहिए। साथ ही, नकली नोट के बारे में तुरंत रिपोर्ट करना चाहिए।

विनय: ज़रूर। मैं तुरंत इसकी रिपोर्ट करूंगा। बहुत–बहुत धन्यवाद विनी।

हाइब्रिड वारफेयर से निपटने हेतु क्या किया जा सकता है?

हाइब्रिड वारफेयर वस्तुतः कई मोर्चों पर लड़ी जाने वाली एक युद्ध–पद्धति है। इसलिए इसे प्रभावी ढंग से निष्फल करने के लिए समग्र रूप से उपाय किए जाने की आवश्यकता है:



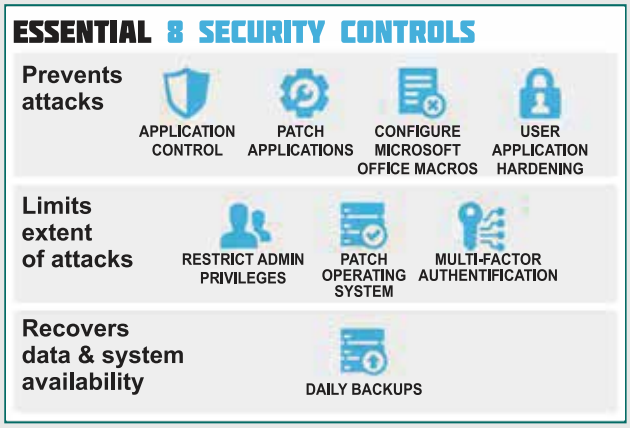
- **व्यवस्थित और समकालिक रूप से रियल टाइम आधारित कार्रवाई करना:** इसके तहत प्रभावी कार्रवाई सुनिश्चित करने के लिए सशस्त्र बलों को आवश्यक प्रशिक्षण प्रदान किया जाना चाहिए। हाइब्रिड वारफेयर जैसी स्थिति में सशस्त्र बलों को आबादी की रक्षा के साथ–साथ शत्रु को अक्षम करने जैसी दोहरी भूमिका निभानी पड़ती है। इसलिए, इस संबंध में निम्नलिखित तकनीकों को अपनाया जा सकता है:
  - किसी संभावित हाइब्रिड हमले की स्थिति में त्वरित कार्रवाई को सुनिश्चित करने हेतु एक **संस्थागत तंत्र का निर्माण** किया जाना चाहिए।
  - **कार्रवाई के विभिन्न क्षेत्रों के मध्य प्रभावी समन्वय सुनिश्चित** करने के लिए ड्रिल और अभ्यास जैसी गतिविधियां आयोजित की जानी चाहिए।
  - **युद्ध संबंधी विशेष तकनीकों और** कौशल के संबंध में प्रशिक्षण प्रदान किया जाना चाहिए। साथ ही, **शहरी क्षेत्रों में संघर्ष जैसी स्थितियों का सामना करने में सक्षम बनाने हेतु** भी प्रशिक्षित किया जाना चाहिए।
  - स्मार्ट रोबोट, मानव रहित विमान (UAVs) आदि जैसे **तकनीकी उपकरणों** के उपयोग के लिए भी प्रशिक्षण प्रदान किया जाना चाहिए।
  - **शहरी बस्तियों में कार्रवाई संबंधी अभियानों की सटीकता को सुनिश्चित करने के लिए रियल टाइम सिचुएशनल अवेयरनेस (RTSA)** जैसे आसूचना साधनों के उपयोग को बढ़ावा दिया जाना चाहिए।
- **संस्थागत उपाय:** ये सुभेद्यताओं के आकलन और संभावित हाइब्रिड जोखिमों के अनुमान हेतु अत्यंत महत्वपूर्ण हैं।

- सभी क्षेत्रकों से संबंधित महत्वपूर्ण कार्यप्रणालियों और सुभेद्यताओं का **स्व–आकलन** करते हुए उनकी नियमित निगरानी की जानी चाहिए। उदाहरण के लिए– देश में **महत्वपूर्ण फिनटेक प्रणालियों को नियमित रूप से अपडेट करते रहना चाहिए।**

- अपारंपरिक राजनीतिक, आर्थिक, नागरिक व अंतर्राष्ट्रीय (PECI) साधनों और क्षमताओं को शामिल करते हुए **खतरे का आकलन करने संबंधी पारंपरिक गतिविधियों में सुधार करना चाहिए।** इस संबंध में इस पक्ष पर भी मुख्य रूप से विचार करना चाहिए कि कैसे हमले के इन साधनों को किसी लक्ष्य की विशिष्ट सुभेद्यताओं को लक्षित करते हुए समकालिक रूप से उपयोग किया जाता है।

- हाइब्रिड खतरों को समझने, पता लगाने और उनके विरुद्ध कार्रवाई सुनिश्चित करने के क्रम में सभी स्तरों पर सरकार द्वारा व्यापक रूप से प्रयास किए जाने चाहिए।

- **डिजिटल पारितंत्र की सुरक्षा को मजबूत करना:** वर्तमान समय में डिजिटल पारितंत्र या साइबर–स्पेस का महत्व बहुत तेजी से बढ़ा है। इसलिए, इन्हें अधिक सुरक्षित और मजबूत बनाने के लिए समर्पित प्रयास किए जाने की आवश्यकता है। इस संबंध में, ऑस्ट्रेलिया की साइबर सुरक्षा संबंधी नीति की 'एसेंशियल **8**' विशेषताओं पर विचार किया जा सकता है।



- **लोकतांत्रिक संस्थाओं को मज़बूत बनाना:** लोकतांत्रिक संस्थाओं को मज़बूत करके सरकार **नागरिकों का विश्वास और सहयोग प्राप्त कर सकती है।** इससे हाइब्रिड वारफेयर के विभिन्न रूपों, जैसे– **दुष्प्रचार और चरमपंथ को बढ़ावा देने वाले प्रयासों को निष्फल करने** में सरकार को सहायता प्राप्त हो सकती है।

- ऐसे खतरों का मुकाबला करने में थिंक टैंक जैसे कि **नागरिक समाज संबंधी संस्थानों को शामिल** करके सरकार अपनी क्षमता में वृद्धि कर सकती है।

- **मीडिया संबंधी साक्षरता बढ़ाने हेतु पत्रकारिता में निवेश करना:** वैश्विक स्तर पर किए गए शोध दर्शाते हैं कि मीडिया द्वारा "हाइब्रिड खतरे" शब्द का 70 प्रतिशत मामलों में गलत तरीके से उपयोग किया गया है। इसलिए, पत्रकारिता में निवेश करने से नागरिकों को अप्रत्यक्ष रूप से इस खतरे को समझने में सहायता मिलेगी।

- **अंतर्राष्ट्रीय सहयोग विकसित करना:** अंतर्राष्ट्रीय स्तर पर सहयोग और भागीदारी को साकार करने के लिए बहुराष्ट्रीय फ्रेमवर्क का विकास किया जाना चाहिए। इसके तहत मौजूदा संस्थानों और प्रक्रियाओं का भी उपयोग किया जा सकता है।

- हाइब्रिड वारफेयर से संबंधित हाइब्रिड खतरों और गतिविधियों को पहचानने एवं उन्हें चिन्हित करने के लिए **स्पष्ट परिभाषा तथा प्रोटोकॉल विकसित** किए जाने चाहिए।

- हाइब्रिड वारफेयर से निपटने से संबंधित **हस्तक्षेप से जुड़े चरणों और तरीकों को संस्थागत रूप प्रदान करना** चाहिए। इससे हाइब्रिड वारफेयर से पीड़ित लोगों को अंतर्राष्ट्रीय समुदाय से समर्थन प्राप्त करने में मदद मिलेगी।

- आतंकवाद, मनी लॉन्ड्रिंग आदि जैसे मुद्दों पर जारी सुरक्षा संबंधी वार्ताओं में **हाइब्रिड वारफेयर से संबंधित मुद्दों को शामिल और एकीकृत** किया जाना चाहिए।

निष्कर्ष

दबाव, आक्रामकता, संघर्ष और युद्ध को कैसे समझा जाता है, इस संबंध में हाइब्रिड वारफेयर ने एक नया आयाम जोड़ा है। इस संबंध में, नए भू–सामरिक समीकरण, प्रौद्योगिकियों के नए–नए उपयोग तथा नए संगठनों के गठन से हाइब्रिड वारफेयर वर्तमान तथा भविष्य में और अधिक विकसित होता रहेगा। हाइब्रिड वारफेयर की प्रकृति ऐसी है कि यह समाज के सभी वर्गों को किसी न किसी तरीके से अवश्य प्रभावित करता है।

इस संदर्भ में, सैन्य (संयुक्त और बहुराष्ट्रीय बलों), सरकारी विभागों व एजेंसियों तथा समाज (नागरिक समाज संगठनों सहित) की क्षमताओं को एकीकृत करने हेतु प्रयास किए जाने चाहिए। शायद, यह भविष्य में हाइब्रिड वारफेयर से संबंधित विकसित होते बहुआयामी खतरों का मुकाबला करने का एकमात्र तरीका हो सकता है।

टॉपिक – एक नजर में

हाइब्रिड वारफेयर

इसके तहत सामान्यतः **कई मोर्चों पर युद्ध उपागमों के भाग** के रूप में अपरंपरागत विधियों का उपयोग किया जाता है। इन विधियों का उद्देश्य **खुली शत्रुतापूर्ण गतिविधियों में संलग्न हुए बिना प्रतिद्वंद्वी की कार्रवाईयों को बाधित कर उसे अक्षम बनाना** होता है।

निम्नलिखित को हाइब्रिड वारफेयर की प्रमुख गतिविधियों के रूप में रेखांकित किया जा सकता है:

राजनीतिक वारफेयर: इसके अंतर्गत किसी देश की राजनीतिक गतिविधियों में हस्तक्षेप करके उस देश को हानि पहुंचाई जाती है।	**तकनीकी वारफेयर:** इसके तहत नागरिकों, उद्यमों, संस्थानों आदि जैसी इकाइयों को नुकसान पहुंचाने के लिए तकनीकी क्षमताओं का उपयोग किया जाता है।	**सैन्य वारफेयर:** इसके तहत पारंपरिक तकनीकों के साथ–साथ इम्प्रोवाइज्ड एक्सप्लोसिव, लक्षित कमांडो अभियान, गुरिल्ला युद्ध पद्धति आदि जैसी सैन्य कार्रवाईयों का प्रयोग किया जाता है।	**आर्थिक वारफेयर:** इसके तहत राज्य और गैर–राज्य अभिकर्ताओं द्वारा आपूर्ति श्रृंखलाओं को बाधित करके तथा नकली/जाली मुद्राओं आदि को बढ़ावा देते हुए लक्षित देश की अर्थव्यवस्था को कमजोर किया जाता है।	**सामाजिक वारफेयर:** इसमें दुष्प्रचार, भड़काऊ संदेशों आदि के द्वारा पहले से प्रचलित सामाजिक मुद्दों और कमजोरियों का फायदा उठाकर सामाजिक सौहार्द बिगाड़ने की कोशिश की जाती है।

हाइब्रिड वारफेयर की बढ़ती स्वीकार्यता के कारण

- हाइब्रिड वारफेयर के तहत सैन्य, राजनीतिक, आर्थिक, नागरिक और सूचना आधारित साधनों के व्यापक समूह का उपयोग किया जाता है। ज्ञातव्य है कि **खतरों के आकलन की पारंपरिक पद्धति में सामान्यतः इनकी अनदेखी** की जाती है।
- इसके तहत **अत्यधिक सुभेद्य क्षेत्रों को लक्षित** किया जाता है, जहां न्यूनतम प्रयास से अधिकतम नुकसान होने की संभावना होती है।
- इसमें सुव्यवस्थित तरीके से अधिकतम नुकसान पहुंचाने के एजेंडे के साथ **राज्य अभिकर्ता, गैर–राज्य अभिकर्ता या दोनों** अलग–अलग भूमिकाएं निभाते हैं, परंतु समकालिक रीति से।
- **हमले की व्यापकता और लक्ष्य पर सुव्यवस्थित नियंत्रण:** ऐसे हमलों को **अपने विरूद्ध जवाबी कार्रवाई (विशेष रूप से अंतर्राष्ट्रीय प्रतिक्रिया) और अपनी पहचान के प्रकट होने की संभावना** से बचते हुए परिस्थितियों के अनुसार तैयार किया जा सकता है।
- हाइब्रिड वारफेयर का तब तक पता न लग पाए, जब तक की वह पूर्ण रूप से प्रभावी न हो जाए।

हाइब्रिड वारफेयर– भारत के लिए एक संभावित मुद्दा

- **आतंकवादी हमलों के नए रूप:** हाइब्रिड वारफेयर का विचार **'लोन–वुल्फ' हमलों, 'स्लीपर सेल' के निर्माण और हाइब्रिड लड़ाकों के उद्भव** जैसे आतंकवादी हमलों के नए रूपों को प्रोत्साहित करता है।
- **साइबर हमले:**
  - **निजता का उल्लंघन और व्यक्तिगत डेटा की चोरी,**
  - मोबाइल ऐप्स का असुरक्षित ढांचा,
  - पाकिस्तान और चीन द्वारा साइबर जासूसी का मुद्दा,
  - बौद्धिक संपदा से संबंधित सुभेद्यताएं आदि।
- **निर्वाचन संबंधी प्रक्रियाओं में हस्तक्षेप:** इसमें मीडिया और सोशल नेटवर्क द्वारा प्रचार करना तथा किसी राजनीतिक दल के लिए वित्तीय संसाधन जुटाना शामिल हैं।
- **दुष्प्रचार और फेक न्यूज:** हाइब्रिड वारफेयर के तहत **लक्षित समाज में मतभेद को बढ़ावा** देने के लिए मिथ्या तथ्यों पर आधारित एक अलग वास्तविकता का निर्माण किया जाता है।
- निवेश सौदों द्वारा उत्पन्न किए जाने वाले वित्तीय प्रभाव।

हाइब्रिड वारफेयर से निपटने हेतु अपनाए जाने वाले तरीके

- **व्यवस्थित और समकालिक रूप से रियल टाइम आधारित कार्रवाई करना:**
  - त्वरित कार्रवाई को सुनिश्चित करने हेतु **एक संस्थागत तंत्र का निर्माण** किया जाना चाहिए।
  - **कार्रवाई के विभिन्न क्षेत्रों के मध्य प्रभावी समन्वय सुनिश्चित** किया जाना चाहिए।
  - **रियल टाइम सिचुएशनल अवेयरनेस** (RTSA) जैसे आसूचना साधनों के उपयोग को बढ़ावा दिया जाना चाहिए।
- **संस्थागत उपाय:**
  - सभी क्षेत्रकों से संबंधित महत्वपूर्ण कार्यप्रणालियों और सुभेद्यताओं का **स्व–आकलन** करते हुए उनकी नियमित निगरानी की जानी चाहिए।
  - खतरे का आकलन करने संबंधी पारंपरिक गतिविधियों में सुधार करना चाहिए।
- हालिया समय में डिजिटल पारितंत्र या साइबर–स्पेस का महत्व बहुत तेजी से बढ़ा है। इसलिए, इन्हें अधिक सुरक्षित और मजबूत बनाने के लिए समर्पित प्रयास किए जाने की आवश्यकता है।
- **लोकतांत्रिक संस्थाओं को मज़बूत बनाना:**
  - ऐसे खतरों का मुकाबला करने के लिए **नागरिक समाज संबंधी संस्थानों को शामिल करने पर** बल दिया जाना चाहिए।
  - **मीडिया साक्षरता बढ़ाने हेतु पत्रकारिता में निवेश** बढ़ाया जाना चाहिए।
- **अंतर्राष्ट्रीय सहयोग विकसित करना:**
  - इसके लिए स्पष्ट परिभाषा और प्रोटोकॉल विकसित किए जाने चाहिए।
  - हाइब्रिड वारफेयर से निपटने से संबंधित हस्तक्षेप से जुड़े चरणों और तरीकों को संस्थागत रूप प्रदान करना चाहिए।
  - सुरक्षा संबंधी वार्ताओं में हाइब्रिड वारफेयर से संबंधित मुद्दों को शामिल और एकीकृत किया जाना चाहिए।