International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
ISSN :2581-9925, Impact Factor (Cosmos: 7.555&I2OR: 5.105), Volume 08, No. 01(III) (Special Issue), January- March, 2026, pp. 69-82

हाइब्रिड युद्धकर्म, दुष्प्रचार और भारत की रणनीतिक स्थिति

डॉ दिनेश कुमार गुप्ता*

असिस्टेंट प्रोफेसर, रक्षा एवं स्त्रॉतेजिक अध्ययन विभाग, दयानन्द वैदिक कॉलेज, उरई (जालौन), उत्तर प्रदेश

*Corresponding Author: drdkguptadefencedvc@gmail.com

सार

21वीं सदी में हाइब्रिड युद्ध संघर्ष के एक बहुआयामी और अस्पष्ट परिदृश्य का प्रतिनिधित्व करता है, जिसमें विरोधी राष्ट्रीय शक्ति और स्थिरता को कमजोर करने के लिए साइबर हमलों और दुष्प्रचार से लेकर छद्म मिलिशिया और आर्थिक दबाव तक, गतिज और गैर–गतिज रणनीतियों के पूरे स्पेक्ट्रम का उपयोग करते हैं। भारत के लिए, यह सामरिक विकास केवल सैद्धांतिक नहीं है; यह उपमहाद्वीप की सीमाओं और डिजिटल क्षेत्रों में प्रतिदिन साकार होता है, जहाँ शत्रुतापूर्ण पड़ोसी – विशेष रूप से पाकिस्तान और चीन पारंपरिक, अनियमित और संज्ञानात्मक उपकरणों के मिश्रण का लाभ उठाते हैं। यह शोध पत्र हाइब्रिड युद्ध के जटिल विकास, प्रमुख रणनीतियों और परिचालन वास्तविकताओं की पड़ताल करता है, जिसमें ऑपरेशन सिंदूर (2025), भारत के महत्वपूर्ण बुनियादी ढाँचे पर साइबर हमले और दुष्प्रचार के प्रसार जैसी हालिया घटनाओं पर ध्यान केंद्रित किया गया है। यह विश्लेषण भारत के संस्थागत और नीतिगत सुधारों–जैसे कि चीफ ऑफ डिफेंस स्टाफ (सीडीएस), डिफेंस साइबर एजेंसी और डिफेंस एआई प्रोजेक्ट एजेंसी की स्थापना तक विस्तृत है और तैयारी, कमियों और आगे के रास्ते का आकलन करता है। समकालीन घटनाओं, नीतिगत बहसों और वैश्विक सर्वोत्तम प्रथाओं का हवाला देते हुए, यह शोधपत्र ऐसे युग में भारत की रणनीतिक स्थिति को मजबूत करने के लिए स्पष्ट सुझाव प्रदान करता है जहाँ अग्रिम पंक्ति हर जगह मौजूद है, और लड़ाइयाँ जमीनी स्तर पर जितनी लड़ी जाती हैं, उतनी ही जनधारणा और डिजिटल निष्क्रियता में भी।

शब्दकोश: *हाइब्रिड युद्ध, भारत, साइबर युद्ध, दुष्प्रचार, छद्म युद्ध, ग्रे जोन, तीन युद्ध, चीन, पाकिस्तान, ऑपरेशन सिंदूर, कुडनकुलम साइबर हमला, रक्षा आधुनिकीकरण, सीडीएस, डीएआईपीए, डीएआईसी, रक्षा साइबर एजेंसी, क्वाड, जीएसओएमआईए, एआई, ड्रोन, हिंद–प्रशांत, संसदीय निगरानी।*

प्रस्तावना

21वीं सदी में अंतर्राष्ट्रीय सुरक्षा परिदृश्य निर्धारित लड़ाइयों से नहीं, बल्कि हाइब्रिड खतरों की निरंतर बौछार से आकार लेता है। ऐसे परिष्कृत अभियान जो प्रत्यक्ष युद्ध के बिना राष्ट्रों को अस्थिर करने के लिए दृश्य और अदृश्य, वैध और अवैध, सभी को एक साथ मिलाते हैं। भारत, जो एक अस्थिर पड़ोस में स्थित है और वैश्विक मंच पर तेजी से आगे बढ़ रहा है, इस विकसित होती गतिशीलता में एक प्राथमिक लक्ष्य और एक निर्णायक खिलाड़ी है। तकनीकी नवाचार और संस्थागत प्रयोगों से प्रेरित हाइब्रिड युद्ध का उदय, भारत के पारंपरिक रक्षा सिद्धांतों को चुनौती देता है और समग्र, अनुकूली रणनीतियों को अपनाने के लिए बाध्य करता है[1]

हाइब्रिड युद्ध, पारंपरिक या विशुद्ध रूप से अनियमित संघर्ष से अलग, पारंपरिक सैन्य बल, अनियमित रणनीति, साइबर अभियान, आर्थिक प्रतिबंध, दुष्प्रचार, छद्म मिलिशिया और कानूनी हेरफेर का एक अस्पष्ट,

A Special Issue for the papers accepted for publication in the International Multidisciplinary Conference on India's Foreign Policy and International Relations:A Future Roadmap (IFPIR-2026) (Hybrid Mode)(22-24 January 2026) Organized by Geo-Politics & Defence Study Research Cell, Faculty of Arts, Education and Social Sciences, Jai Narain Vyas University, Jodhpur, Rajasthan.

समन्वित अनुप्रयोग शामिल करता है। इसका उद्देश्य निर्णय लेने की प्रक्रिया को पंगु बनाना, समाजों का ध्रुवीकरण करना. महत्वपूर्ण बुनियादी ढाँचे को कमजोर करना और प्रतिद्वंद्वी की प्रतिक्रिया को धीमा और अप्रभावी बनाना है।[2,3] उल्लेखनीय रूप से, हाइब्रिड युद्ध, शत्रुतापूर्ण तत्वों, चाहे वे सरकारी हों या गैर–सरकारी, को घोषित युद्ध की दहलीज पार किए बिना हमला करने में सक्षम बनाता है– यह वास्तविकता उस 'ग्रे जोन' के लिए उपयुक्त है जो अब वैश्विक रणनीतिक विमर्श पर हावी है।[4,5]

भारत के लिए, ये खतरे अमूर्त नहीं हैं। पिछले पाँच वर्षों में जम्मू–कश्मीर में पाकिस्तानी छद्म हमलों में वृद्धि, वास्तविक नियंत्रण रेखा पर चीन के त्रि–युद्ध सिद्धांत का क्रियान्वयन, और भारत के परमाणु, ऊर्जा और वित्तीय बुनियादी ढाँचे को निशाना बनाकर साइबर हमले देखे गए हैं। पहलगाम नरसंहार के जवाब में मई 2025 का ऑपरेशन सिंदूर, हाइब्रिड खतरों के विरुद्ध भारत के नए, मुखर रुख का प्रतीक है जिसमें सटीक सैन्य जवाबी कार्रवाई, साइबर रक्षा, सूचना अभियान प्रतिवाद और आर्थिक संसाधन शामिल हैं। फिर भी, प्रत्येक परिचालन सफलता के साथ, लगातार कमजोरियाँ और टकराव बने रहते हैं, जो अवसर और खतरे दोनों को आमंत्रित करते हैं।

इस शोधपत्र का उद्देश्य हाइब्रिड युद्ध की अवधारणा और विकास को उजागर करना, भारतीय संदर्भ में इसके उपकरणों और विधियों का विश्लेषण करना, और भारत के रक्षा आधुनिकीकरण और रणनीतिक रुख[6] पर इसके प्रभावों का आलोचनात्मक मूल्यांकन करना है। हाल के केस स्टडीज और नीतिगत सुधारों के आधार पर, यह भविष्य के लिए कार्यान्वयन योग्य सुझावों का एक संग्रह भी प्रस्तुत करता है।

अवधारणा एवं विकास

हाइब्रिड युद्ध, विभिन्न तरीकों–पारंपरिक बल, अनियमित रणनीति, साइबर ऑपरेशन और मनोवैज्ञानिक हेरफेर का एक कलात्मक एकीकरण है, जिसका उद्देश्य बिना किसी प्रत्यक्ष संघर्ष को भड़काए रणनीतिक उद्देश्यों को प्राप्त करना है। 2006 के लेबनान युद्ध में हिज्बुल्लाह द्वारा सैन्य, राजनीतिक और मीडिया उपकरणों के उपयोग, क्रीमिया और यूक्रेन के प्रति रूस के 'छोटे हरे आदमी' दृष्टिकोण और मध्य पूर्व में ईरान द्वारा छद्म बलों को समर्थन के बाद इस अवधारणा पर विद्वानों और रणनीतिक लोगों का ध्यान बढ़ा। अमेरिकी मरीन कॉर्प्स अधिकारी फ्रैंक जी. हॉफमैन ने औपचारिक रूप से हाइब्रिड युद्ध को 'एक ही युद्ध क्षेत्र में पारंपरिक, अनियमित, आतंकवादी और आपराधिक व्यवहार' के संयोजन के रूप में परिभाषित किया।

यह दृष्टिकोण दक्षिण एशिया के लिए नया नहीं है। विभाजन के बाद से, भारत को अपनी सीमाओं पर संकर खतरों का सामना करना पड़ा है। 1947–48 में पाकिस्तानी अनियमितताएं, 1980 के दशक के उत्तरार्ध से कश्मीर में छद्म युद्ध, और पंजाब और पूर्वोत्तर में उग्रवाद और आतंकवादी कृत्यों का प्रायोजन।[7] हालांकि, तकनीकी त्वरण विशेष रूप से डिजिटल संचार, एआई, मानवरहित प्रणालियां और सोशल मीडिया ने एक नए युग की शुरुआत की है. जिससे शत्रुतापूर्ण कार्रवाई की लागत और सीमा दोनों कम हो गई है। जैसा कि 2025 में रक्षा मंत्री ने कहा, 'सीमांत रेखा की पारंपरिक अवधारणा तेजी से बदल रही है... आतंकवाद, उग्रवाद, साइबर युद्ध... राष्ट्रीय सीमाओं को पार कर रहे हैं और आंतरिक सुरक्षा की स्थापित धारणाओं को चुनौती दे रहे हैं'।

दुनिया भर में, संकर युद्ध ने आक्रमण और रक्षा, युद्ध और शांति, घरेलू मोर्चे और युद्धक्षेत्र की परिभाषाओं को धुंधला कर दिया है। कार्रवाई का कारण स्थानीय (जैसे पहलगाम नरसंहार या मणिपुर अशांति) या अंतरराष्ट्रीय (साइबर हमले और आवश्यक सेवाओं को बाधित करने वाले दुष्ट एआई बॉट) हो सकता है, लेकिन इसका परिणाम लगभग सार्वभौमिक अनिश्चितता और सभी सरकारों और समाजों के लिए निरंतर सतर्कता है।

घटक एवं रणनीति

हाइब्रिड युद्ध तालमेल, अस्पष्टता और अस्वीकार्यता पर पनपता है। इसके आवश्यक उपकरणों में शामिल हैं:

- **पारंपरिक सैन्य बलः** अनियमित सैन्य बलों के साथ तैनात या अन्य साधनों के सक्रिय होने पर निवारण के लिए उपयोग किया जाता है (उदाहरण के लिए, पुलवामा के बाद भारत द्वारा नियंत्रण रेखा पार हमलेः वास्तविक नियंत्रण रेखा पर पीएलए की स्थिति)।
- **अनियमित रणनीति और छद्म युद्धः** प्रॉक्सी पर दीर्घकालिक निर्भरता–कश्मीर में पाकिस्तान द्वारा लश्कर–ए–तैयबा और जैश–ए–मोहम्मद के इस्तेमाल से लेकर उग्रवाद और स्लीपर सेल को प्रायोजित करने तक केंद्रीय बनी हुई है।[8]
- **साइबर युद्ध और सूचना अभियानः** इसमें हैकिंग, मैलवेयर, रैंसमवेयर, सेवा निषेध (डीओएस) और सरकारी, सैन्य, कॉर्पोरेट या व्यक्तिगत प्रणालियों से संवेदनशील डेटा का समन्वित निष्कर्षण या हेरफेर शामिल है। ये अभियान अक्सर परमाणु संयंत्रों (कुडनकुलम), पावर ग्रिड (मुंबई) और वित्तीय प्रणालियों जैसे महत्वपूर्ण बुनियादी ढाँचे को निशाना बनाते हैं। [9,10]
- **दुष्प्रचार और दुष्प्रचार अभियानः** विरोधी जनता की भावनाओं को ध्रुवीकृत करने, भ्रम फैलाने, विश्वास को कम करने या अंतर्राष्ट्रीय धारणाओं को प्रभावित करने के लिए समन्वित संदेश (अक्सर बॉट्स, डीपफेक, फर्जी खबरों से प्रेरित) का इस्तेमाल करते हैं। उल्लेखनीय रूप से, 2025 के पहलगाम हमले के बाद, पड़ोसियों और घरेलू दोनों ही पक्षों ने वैकल्पिक आख्यान गढ़ने के लिए डिजिटल मीडिया का दुरुपयोग किया।
- **ग्रे जोन ऑपरेशन और कानूनी युद्धः** युद्ध की सीमा से नीचे की जगह का दोहन करके अतिरिक्त लाभ प्राप्त करना (दक्षिण चीन सागर या एलएसी में चीनी 'सलामी स्लाइसिंग'; नशीले पदार्थों और हथियारों के जरिए पाकिस्तानी घुसपैठ; विदेशों में भारतीय हितों को नुकसान पहुँचाने के लिए विदेशी कानूनी तरीकों का दुरुपयोग)।
- **आर्थिक दबाव, प्रतिबंध और तोड़फोड़ः** निर्भरताएँ पैदा करने या विकास को बाधित करने के लिए व्यापार, निवेश, ऊर्जा आपूर्ति और आपूर्ति श्रृंखलाओं का लाभ उठाना। दवा आपूर्ति और महत्वपूर्ण इलेक्ट्रॉनिक्स के माध्यम से चीन का आर्थिक लाभ, या भारत के डिजिटल भुगतान बुनियादी ढांचे पर सुनियोजित हमले, इस उपकरण के उदाहरण हैं।[11]
- **उभरती प्रौद्योगिकियाँ (एआई, ड्रोन, स्वायत्त प्रणालियाँ, क्वांटम कंप्यूटिंग):** मानवरहित हवाई प्रणालियाँ (ड्रोन), घूमने वाले हथियार, एआई–संचालित गलत सूचनाएँ और पूर्वानुमानित विश्लेषण, हाइब्रिड ऑपरेशनों के लिए तेजी से केंद्रीय भूमिका निभा रहे हैं। एआई आक्रमण (सोशल इंजीनियरिंग, पेलोड लक्ष्यीकरण) और रक्षा (खतरे का पता लगाना, डीपफेक का मुकाबला)[12,13] को समान रूप से सशक्त बना सकता है।

भारत के विरोधियों ने इन तत्वों को मिलाने और क्रमबद्ध करने की कला में महारत हासिल कर ली है। कभी–कभी स्पष्ट समकालिकता में, और अक्सर सोची–समझी अस्पष्टता में–ताकि अधिकतम प्रभाव प्राप्त हो सके।

हाइब्रिड के प्रत्येक आयाम जैसा कि ऊपर बताया गया है, युद्ध भारत की नागरिक, सैन्य और डिजिटल प्रणालियों में दरारों का सीधा सामना करता है या उनका फायदा उठाता है, जिससे अस्पष्टता की लागत बढ़ जाती है और पूरे देश की प्रतिक्रिया की आवश्यकता होती है।

साइबर युद्ध और सूचना संचालन

भारत एक डिजिटल ज्वालामुखी के शिखर पर स्थित है, जहाँ 90 करोड़ इंटरनेट उपयोगकर्ता (2025). एक फलता–फूलता स्टार्टअप इकोसिस्टम और तेजी से डिजिटल हो रहा सरकारी और रक्षा क्षेत्र[14] है। हालाँकि,

यह डिजिटल उछाल अपने साथ विस्तारित हमले के क्षेत्र भी लाता है। हाल के वर्षों में, साइबर युद्ध जासूसी या झुंझलाहट से रणनीतिक व्यवधान में बदल गया है।

उल्लेखनीय घटनाएँ

- **कुडनकुलम परमाणु संयंत्र हमला (2019) :** मैलवेयर ने एंटरप्राइज नेटवर्क में घुसपैठ की, कथित तौर पर भविष्य के हमलों के लिए एक टेम्पलेट प्रदान किया। साइबर परमाणु इंटरफेस को और मजबूत करने की एक चेतावनी।[15]
- **मुंबई ग्रिड हमला (2020) :** चीनी सरकारी तत्वों द्वारा किए गए इस हमले ने भारत के सबसे बड़े शहरी ग्रिडों में से एक को ऑफलाइन कर दिया, जिससे लाखों लोग प्रभावित हुए और 'रिमोट कंट्रोल द्वारा राष्ट्रीय बुनियादी ढांचे को बंधक बनाने' के इरादे का संकेत मिला।[16]
- **मई 2025 (ऑपरेशन सिंदूर) :** सरकार और प्रमुख बुनियादी ढांचे पर 15 लाख से ज्यादा साइबर हमले हुए, जिनमें से ज्यादातर पाकिस्तान से संचालित थे। रक्षा साइबर एजेंसी और ब्स्ज्.प्द सहित भारतीय साइबर रक्षा अवसंरचना ने अधिकांश प्रयासों को विफल कर दिया, जिससे हमलों की बढ़ती जटिलता और संख्या उजागर हुई।
- **दुष्प्रचार अभियान :** संकट के दौरान हेरफेर किए गए आख्यानों का तेजी से प्रसार– जैसे पहलगाम नरसंहार के बाद समन्वित अभियान, डीपफेक वीडियो और एन्क्रिप्टेड प्लेटफॉर्म का दुरुपयोग ने न केवल घरेलू दर्शकों को भ्रमित किया है, बल्कि अंतर्राष्ट्रीय धारणाओं को भी प्रभावित किया है। ऑपरेशन सिंदूर के दौरान, पाकिस्तानी सोशल मीडिया ने ग फेसबुक और टेलीग्राम पर मनगढंत तस्वीरें रुप्दकपंदथ्सेमथ्संह जैसे हैशटैग की बाढ़ ला दी, जिसका उद्देश्य भारत के आख्यान को कमजोर करना और भ्रम पैदा करना था।[17]
- **AI का दोहरा लाभ :** जनरेटिव ।एएस्स्ड और डीपफेक टूल के उदय के साथ, दुष्प्रचार और पहचान दोनों में तेजी आ रही है। ।ै का उपयोग न केवल फर्जी खबरें फैलाने, अशांति पैदा करने और सेवा से इनकार करने के लिए किया जाता है, बल्कि यह भारतीय पहचान एल्गोरिदम, खतरे की निगरानी और तथ्य जांच अभियानों[18] को भी शक्ति प्रदान करता है।

दुष्प्रचार और प्रचार अभियान

हाइब्रिड युद्ध, जानबूझकर, खुले समाजों की सूचना विकार के प्रति संवेदनशीलता का फायदा उठाता है। भारत के संदर्भ में, इसकी विशाल, भाषाई रूप से विविध डिजिटल आबादी, परिवर्तनशील मीडिया साक्षरता और राजनीतिक ध्रुवीकरण के कारण यह भेद्यता और भी बढ़ जाती है। विश्व आर्थिक मंच की 2025 की वैश्विक जोखिम रिपोर्ट में दुष्प्रचार और भ्रामक सूचनाओं को सबसे बड़ा उभरता वैश्विक खतरा बताया गया है।

तंत्र और प्रभाव

- **कथानक में हेरफेरः** डिजिटल कलाकार सामाजिक दोष रेखाओं (जैसे, धार्मिक, जातिगत, आर्थिक) का मानचित्रण करते हैं, सनसनीखेज और ध्रुवीकरणकारी सामग्री फैलाते हैं, और इन संदेशों को बढ़ाने के लिए बॉट्स का उपयोग करते हैं। नागरिकता संशोधन अधिनियम विरोध प्रदर्शन 2019 और 2024 के मणिपुर अशांति, दोनों में दुष्प्रचार के कारण वास्तविक दुनिया में लामबंदी और हिंसा भड़क उठी।
- **विदेशी अभियानः** भारत की जी–20 अध्यक्षता के दौरान, चीन और पाकिस्तान ने भारत को दबाव डालने वाला या अस्थिर दिखाने के लिए बॉट नेटवर्क, सरकारी मीडिया और नकली एनजीओ का इस्तेमाल किया, जिससे राजनयिक और आर्थिक जुड़ाव प्रभावित हुए।[19]

- **घरेलू राजनीतिक दुष्प्रचारः** डीपफेक, फर्जी उद्धरण और 'वायरल लीक' ने संसद, मीडिया और सुरक्षा बलों में संस्थागत विश्वास को कम करने की कोशिश की है जिससे लोकतंत्र में विश्वास के क्षरण की चिंता बढ़ रही है।
- **प्रतिवादः** भारत ने डिजिटल साक्षरता कार्यक्रम शुरू किए हैं, चुनावों के दौरान समर्पित तथ्य जांच इकाइयाँ (शक्ति तथ्य जांच सामूहिक) स्थापित की हैं, और सामग्री हटाने के लिए कानूनी शक्तियों को बढ़ाया है। हालाँकि, ऐसे प्रति–अभियानों के पैमाने और गति में तेजी लानी होगी।
- हाइब्रिड युद्ध में डिजिटल दुष्प्रचार की शक्ति न केवल जनता को भ्रमित करने में निहित है, बल्कि घरेलू एकता को कमजोर करने, सशस्त्र बलों का मनोबल गिराने और अंतर्राष्ट्रीय भागीदारों को हतोत्साहित करने में भी निहित है।

ग्रे जोन और कानूनी युद्ध रणनीतियाँ

- ग्रे जोन युद्ध, युद्ध और शांति के बीच के अस्पष्ट अंतराल में संचालित होता है, जहाँ कानूनी, प्रक्रियात्मक और मानक अस्पष्टताओं का उपयोग करके रक्षकों को पंगु बनाया जाता है। भारत के दोनों प्रमुख विरोधियों ने ऐसी रणनीतियों से अपने हितों को आगे बढ़ाया है।

चीन

- **तीन युद्ध रणनीतियाँः** पीएलए ने जनमत युद्ध (मीडिया हेरफेर), मनोवैज्ञानिक युद्ध (मनोबल ह्रास, गलत सूचना), और कानूनी युद्ध (कानूनी युद्ध – यथास्थिति को पुनर्परिभाषित करने के लिए दावों, संधियों और अंतर्राष्ट्रीय निकायों का उपयोग को संस्थागत रूप दिया। प्रमुख उदाहरणों में चीन द्वारा संधियों का चुनिंदा हवाला देना (जैसे, डोकलाम में 1890 का कन्वेंशन), अग्रिम संगठनों का समर्थन करना और दक्षिण चीन सागर तथा वास्तविक नियंत्रण रेखा पर अंतर्राष्ट्रीय कानून की अपनी व्याख्याओं पर जोर देना शामिल है।
- **समुद्री ग्रे जोन ऑपरेशनः** विवादित जलक्षेत्र में 'समुद्री मिलिशिया' जहाजों का इस्तेमाल, मछली पकड़ने वाली नावों को टक्कर मारना, और धीरे–धीरे अतिक्रमण करना– ये सब सीधे संघर्ष या अंतर्राष्ट्रीय निंदा से बचते हुए।[20]

पाकिस्तानः

- **संभावित अस्वीकार्यताः** आतंकवादी प्रॉक्सी नार्कोटेररिज्म और साइबर ऑपरेटिव्स के व्यापक उपयोग के माध्यम से, पाकिस्तान 'बिना प्रत्यक्ष जिम्मेदारी लिए भारत को अस्थिर' करना चाहता है, जिससे अंतर्राष्ट्रीय निंदा की सीमा बढ़ जाती है और विघटनकारी प्रभाव अधिकतम हो जाता है।
- **विदेश में कानूनी कार्रवाईः** अंतर्राष्ट्रीय गैर–सरकारी संगठनों का उपयोग करना, बहुपक्षीय मंचों पर घटनाओं को गलत तरीके से प्रस्तुत करना, और विदेशों में भारतीयों को कानूनी रूप से परेशान करना, विशेष रूप से कश्मीर जैसे मुद्दों पर।

इसके जवाब में, भारत ने कानूनी कार्रवाई के विरुद्ध रणनीतियाँ तैयार करना शुरू कर दिया है और अंतर्राष्ट्रीय मध्यस्थता और मीडिया के कानूनी हथियारीकरण के प्रति अधिक सतर्क हो गया है। अंतर्राष्ट्रीय समर्थन जुटाना–जैसे कि बालाकोट के बाद और ऑपरेशन सिंदूर हमलों के दौरान, जहाँ भारत ने संयुक्त राष्ट्र सुरक्षा परिषद को जानकारी दी और अनुच्छेद 51 के तहत आत्मरक्षा के रूप में कार्रवाई की रूपरेखा तैयार की– एक बढ़ती हुई कानूनी परिष्कृतता का प्रतिनिधित्व करता है।

आर्थिक दबाव और प्रतिबंध हाइब्रिड उपकरणों के रूप में

आज के संघर्ष युद्ध के मैदान में जितने प्रभावी हैं, उतने ही बोर्ड रूम और व्यापार गलियारों में भी।

- **चीन की रणनीतिः** चीन व्यापार प्रतिबंधों, नियामक उत्पीड़न और आपूर्ति श्रृंखला में हेरफेर के माध्यम से परिणामों को प्रभावित करने के लिए दुनिया के कारखाने के रूप में अपनी स्थिति का इस्तेमाल करता है। एपीआई और सेमीकंडक्टरों का निर्यात, संवेदनशील क्षेत्रों (जैसे बंदरगाह और दूरसंचार) में निवेश नियंत्रण, और बुनियादी ढाँचा परियोजनाएँ (बीआरआई), सभी का उपयोग अनुपालन को पुरस्कृत करने या प्रतिरोध को दंडित करने के लिए किया जाता है।
- **पाकिस्तान की हाइब्रिड अर्थव्यवस्थाः** पाकिस्तान मादक पदार्थों की तस्करी और नकली मुद्रा के माध्यम से सीमा पार आतंकवाद और उग्रवाद को वित्तपोषित करता है, जिससे वित्तीय और सुरक्षा दोनों चुनौतियाँ उत्पन्न होती हैं। कभी–कभी सीमा पार व्यापार मार्गों को बंद करने और जल–बंटवारे पर बातचीत के माध्यम से भी आर्थिक दबाव डाला जाता है।
- **भारतीय प्रतिवादः** भारत ने उकसावे के जवाब में पारस्परिक व्यापार प्रतिबंधों (पाकिस्तान के साथ), आपूर्ति श्रृंखला विविधीकरण (एपीआई और इलेक्ट्रॉनिक्स के लिए), और जल–बंटवारे या वीजा नीतियों के पुनर्निर्धारण के साथ तेजी से प्रतिक्रिया व्यक्त की है (ऑपरेशन सिंदूर के तहत सिंधु जल संधि को स्थगित कर दिया गया, व्यापार बंद कर दिया गया और सीमा पार आवाजाही को निलंबित कर दिया गया)।

छदा युद्ध और गैर–सरकारी तत्व

पाकिस्तान 1980 के दशक से ही अपनी मिश्रित रणनीति के एक मुख्य घटक के रूप में छद्म युद्ध को अपनाता रहा है, जिसमें लश्कर–ए–तैयबा (स्मज) और जैश–ए–मोहम्मद (श्रमड) जैसे आतंकवादी समूहों के साथ–साथ द रेजिस्टेंस फ्रंट (ज्त्थ्) जैसी उभरती हुई संस्थाओं का इस्तेमाल करके भारतीय सैन्य और नागरिक ठिकानों पर हमले किए जाते हैं, जबकि वे संभावित रूप से इनकार करने की क्षमता बनाए रखते हैं। अप्रैल 2025 में पहलगाम में हुए हमले, जिसमें 26 नागरिक मारे गए थे, के लिए पाकिस्तान स्थित या उससे प्रभावित किसी समूह को जिम्मेदार ठहराया गया था;इसके कारण भारत ने ऑपरेशन सिंदूर चलाया।[21]

छद्म युद्ध के उभरते रुझानों में शामिल हैंः

- **वितरित नेतृत्वः** नए समूह क्लाउड–आधारित संचार पर निर्भर करते हैं, जिससे हस्ताक्षर कम होते हैं और सीधे तौर पर जिम्मेदारी तय करना मुश्किल हो जाता ळें
- **ड्रोन युद्ध और नार्को–विद्रोह :** सीमा पार हथियार, गोला–बारूद और ड्रग्स पहुँचाने के लिए ड्रोन का बढ़ता उपयोग।
- **स्थानीय सहयोगीः** प्रॉक्सी गतिविधियाँ अब बाहरी और घरेलू तत्वों के बीच की खाई को धुंधला कर रही हैं, जिससे बेहतर खुफिया जानकारी और केंद्रीय सुरक्षा एजेंसियों और राज्य पुलिस के बीच बेहतर तालमेल की आवश्यकता है।

प्रॉक्सी गतिशीलता संघर्ष प्रबंधन को खतरनाक बना देती है, क्योंकि जिम्मेदारी के शुरुआती दावों (जिन्हें वापस लिया जा सकता है या उनमें हेरफेर किया जा सकता है) और अस्पष्ट साक्ष्यों को हमेशा राज्य की संलिप्तता को छिपाने और घरेलू और वैश्विक दोनों आख्यानों को प्रभावित करने के लिए गढ़ा जा सकता है।

पाकिस्तान की हाइब्रिड युद्ध रणनीतियाँ

भारत के विरुद्ध पाकिस्तानी हाइब्रिड युद्ध चार प्रमुख धुरी पर फैला हुआ हैः

- **प्रॉक्सी आतंकवादः** कश्मीर और अन्य भारतीय राज्यों में सक्रिय समूहों को समर्थन।
- **सूचना और मनोवैज्ञानिक अभियानः** भारतीय और अंतर्राष्ट्रीय दोनों दर्शकों को लक्षित करने वाले अभियान, भारत को दमनकारी और गैर–जिम्मेदार के रूप में चित्रित करते हैं।

- **साइबर अभियानः** डिजिटल रूप से सक्षम जासूसी, रैंसमवेयर और महत्वपूर्ण बुनियादी ढाँचे को निशाना बनाना।
- **अंतर्राष्ट्रीयकरण और कानूनी युद्धः** अंतर्राष्ट्रीय निकायों में आक्रामक रूप से पैरवी करना, कानूनी शिकायतें दर्ज करना और वैश्विक मीडिया में शत्रुतापूर्ण कवरेज को प्रोत्साहित करना।

भारत का सैद्धांतिक विकास अब राज्य समर्थित बड़े आतंकवादी हमलों को युद्ध के कृत्यों के रूप में मानता है, जिसके लिए कठोर सैन्य और असैन्य जवाबी कार्रवाई की आवश्यकता होती है, जैसा कि ऑपरेशन सिंदूर और हालिया संसदीय नीतिगत बहसों में परिलक्षित होता है।

चीन का ग्रे जोन और तीन युद्ध

- चीन के 'तीन युद्ध' उसके दृष्टिकोण का आधार हैंः
- **मीडिया/जनमत युद्धः** अपने पक्ष में वैश्विक और क्षेत्रीय जनमत तैयार करना; सूचना नियंत्रण, फर्जी समाचारों और वैश्विक थिंक टैंकों या शैक्षणिक आदान–प्रदानों पर कब्जा करके असहमतिपूर्ण आख्यानों को दबाना या विकृत करना।
- **मनोवैज्ञानिक युद्धः** प्रचारित धमकियों, कूटनीतिक दबावों और सोशल मीडिया अभियानों का उपयोग करके विरोधी आबादी और निर्णयकर्ताओं का मनोबल गिराने के उद्देश्य से।
- **कानूनी युद्ध (लॉफेयर):** विस्तारवादी कदमों (जैसे, दक्षिण चीन सागर, डोकलाम) को सही ठहराने के लिए आक्रामक कानूनी व्याख्याओं का सहारा लेना, और अंतरराष्ट्रीय मंचों पर विरोधियों की वैधता पर चुनिंदा हमले करना।

डोकलाम गतिरोध (2017), वास्तविक नियंत्रण रेखा (एलएसी) पर लगातार घुसपैठ, और कोविड–19 के मद्देनजर दुष्प्रचार का प्रसार, ये सभी इन रणनीतियों को दर्शाते हैं। चीन हिंद–प्रशांत क्षेत्र में अपने हितों को आगे बढ़ाने के लिए आर्थिक ब्लैकमेल (बहिष्कार, प्रतिबंध) और तकनीकी प्रभुत्व (5जी, दूरसंचार अवसंरचना) का भी लाभ उठाता है। बेल्ट एंड रोड पहल और सैन्य रसद ('दोहरे उपयोग' वाले बंदरगाहों) का अंतर्संबंध इन रेखाओं को और धुंधला कर देता है।

हिंद–प्रशांत हाइब्रिड खतरा परिदृश्य

बहुध्रुवीय, लघु–पक्षीय हिंद–प्रशांत क्षेत्र में हाइब्रिड युद्ध फल–फूल रहा है। इस क्षेत्र के खुले समुद्र, परस्पर जुड़े डिजिटल क्षेत्र और व्यवस्था के लिए प्रतिस्पर्धी दृष्टिकोण (चीनी 'साझा नियति समुदाय' बनाम अमेरिका–जापान–भारत–ऑस्ट्रेलिया की नियम–आधारित व्यवस्था) इसके लिए उपजाऊ जमीन प्रदान करते हैं।

- **सामरिक प्रतिस्पर्धाः** चीन अब वियतनाम, फिलीपींस, जापान (जैसे, सेनकाकू द्वीप समूह) और भारत के विरुद्ध नियमित रूप से हाइब्रिड रणनीतियाँ अपना रहा है। समुद्री मिलिशिया, साइबर नाकेबंदी और व्यापार में हेराफेरी दक्षिण चीन सागर और उसके बाहर प्रभुत्व के लिए चल रही प्रतिस्पर्धा का हिस्सा है।[22]
- **लघु–पक्षीय समाधानः** क्वाड, ।न्झ्नै और रणनीतिक समझौतों (ळैव्डप्।एस्म्डव्।एठम्ब्।) जैसी साझेदारियाँ खुफिया जानकारी साझा करने, संयुक्त साइबर अभ्यास और क्षेत्रीय लचीलेपन को बढ़ावा देने के लिए डिजाइन की गई हैं।[23] आपदाओं, समुद्री सुरक्षा और मानवीय सहायता में 'प्रथम प्रतिक्रियाकर्ता' के रूप में भारत की बढ़ती भूमिका विश्वसनीय महत्व और जटिलता जोड़ती है।

भारत का रक्षा आधुनिकीकरण और तैयारी

हाइब्रिड युद्ध के प्रति भारत की प्रतिक्रिया बहुआयामी होनी चाहिए। जिसमें सैन्य क्षमताओं का आधुनिकीकरण, संस्थागत सुधार और एकीकृत सैद्धांतिक बदलाव शामिल हों।

आधुनिकीकरण के महत्वपूर्ण पड़ाव

- **रक्षा व्यय में वृद्धिः** रक्षा बजट ₹2.53 लाख करोड़ (2013–14) से बढ़कर ₹6.81 लाख करोड़ (2025–26) हो गया है, जिसमें घरेलू क्षमता निर्माण और स्वदेशीकरण (रक्षा उत्पादन ₹1.5 लाख करोड़, 2024–25) पर विशेष ध्यान दिया गया है।
- **स्वदेशी तकनीकः** पाँचवीं पीढ़ी के स्टील्थ एएमसीए लड़ाकू विमानों, आकाशतीर सी2 नेटवर्क, प्रलय मिसाइल रेजिमेंट और स्वार्म ड्रोन प्रणालियों का विकास और समावेश आधुनिकीकरण की गति को दर्शाता है।
- **साइबर सुरक्षा और डिजिटल संचालनः** रक्षा साइबर एजेंसी (2021 में चालू) तीनों सेनाओं की साइबर सुरक्षा का नेतृत्व करती है और ब्न्त्ज्.प्द जैसी नागरिक एजेंसियों के साथ मिलकर काम करती है। रक्षा अंतरिक्ष एजेंसी और ।ष्ध्क्वांटम तकनीक अपनाने (जैसे, प्रोजेक्ट सीकर, भारत छब) इस लड़ाई को उभरते हुए क्षेत्रों तक ले जाते हैं।[24]

संरचनात्मक सुधार

- **चीफ ऑफ डिफेंस स्टाफ (CDS):** 2019–20 में स्थापित, ब्वै अंतर–सेवा नियोजन को एकीकृत करता है, सैन्य मामलों के विभाग का प्रबंधन करता है, और निर्बाध, बहु–डोमेन संचालन[24] के उद्देश्य से एकीकृत थिएटर कमांड के निर्माण की अध्यक्षता करता है।
- **रक्षा AI परियोजना एजेंसी (DAIPA) और रक्षा AI परिषद (DAIC):** सशस्त्र बलों में ।प् अनुसंधान, अधिग्रहण और सैद्धांतिक एकीकरण को समन्वित करने के लिए बनाया गया।
- **संसदीय निरीक्षणः** रक्षा संबंधी स्थायी समिति ने गैर–गतिज और हाइब्रिड खतरों के विरुद्ध तैयारी को प्राथमिकता दी है, साइबर, ड्रोन–रोधी और सूचना क्षेत्रों में तैयारियों की समीक्षा की है। [26,27]
- **संयुक्तता और थिएटर कमांडः** एकीकृत थिएटर कमांड की ओर बदलाव से थल सेना, नौसेना और वायु सेना की संपत्तियों का भूगोल और कार्य के आधार पर समन्वय होगा, जो विभिन्न मोर्चों पर बहुआयामी खतरों को रोकने के लिए आवश्यक है।[28]

संस्थागत सुधारः सीडीएस, डीएआईपीए, डीएआईसी

हाइब्रिड खतरों की विकसित होती प्रकृति ने संस्थागत पुनर्गठन की एक लहर को जन्म दिया हैः

- **सीडीएस (चीफ ऑफ डिफेंस स्टाफ):** संयुक्तता, बल पुनर्गठन और परिचालन निरीक्षण का कार्यभार।
- **डीएआईपीए और डीएआईसीः** ये एजेंसियां एआई को अपनाने में सहायक हैं, एआई–आधारित निर्णय प्रणालियों का समर्थन करती हैं, और आक्रामक और रक्षात्मक हाइब्रिड ऑपरेशनों दोनों के लिए तकनीकी मार्गदर्शन प्रदान करती हैं।
- **वैश्विक साझेदारियांः** क्वाड, जीएसओएमआईए जैसे समझौतों में भारत का प्रवेश और क्षेत्रीय सुरक्षा वार्ताओं में भागीदारी खुफिया आदान–प्रदान, साइबर अभ्यास और रणनीतिक प्रौद्योगिकी विकास के लिए एक वैश्विक जाल बनाती है।

भारत की साइबर सुरक्षा और रक्षा साइबर एजेंसी

भारत ने रक्षा साइबर एजेंसी (क्ब।) की स्थापना करके दृढतापूर्वक प्रतिक्रिया व्यक्त की है, जो 2021 से कार्यरत है। DCA रक्षात्मक (सैन्य नेटवर्क, महत्वपूर्ण बुनियादी ढाँचे की सुरक्षा) और आक्रामक (साइबर हमलों का मुकाबला, डिजिटल फॉरेंसिक) दोनों प्रकार के कार्यों पर केंद्रित है। यह एजेंसी खुफिया जानकारी, प्रशिक्षण और खतरे के शमन के लिए नागरिक समकक्षों, छब्प्ब्ब और अंतर्राष्ट्रीय भागीदारों के साथ समन्वय करती है। ऑपरेशन सिंदूर के दौरान, क्ब। और छप्ब–सशक्त टीमों ने भारत की कमान और नियंत्रण, बिजली और वित्तीय

प्रणालियों को लक्षित करने वाले साइबर हमलों की बाढ़ को सफलतापूर्वक कम किया। छप्ड की ।प् निभृत (च्प्ड डेटा को छिपाने के लिए), निगरानी उपकरण और फेसलेस डिजिटल सेवाएँ स्वचालित और ।प्संचालित साइबर सुरक्षा उपायों की ओर बढ़ते रुझान को दर्शाती हैं।

अंतर्राष्ट्रीय साझेदारियाँः क्वाड और ळैव्डप्।

हिंद–प्रशांत और उसके बाहर हाइब्रिड खतरों का मुकाबला करने के लिए, भारत ने लघु–पक्षीय और द्विपक्षीय व्यवस्थाओं के साथ गहन जुड़ाव की ओर रुख किया हैः

- **क्वाडः** भारत, अमेरिका, जापान और ऑस्ट्रेलिया खुफिया, प्रौद्योगिकी और समुद्री सुरक्षा पर सहयोग करते हैं, और साइबर युद्ध और बुनियादी ढाँचे की मजबूती जैसे गैर–पारंपरिक खतरों पर अधिक ध्यान केंद्रित करते हैं।
- **ळैव्डप्। और अन्य समझौतेः** अमेरिका के साथ ळैव्डप्।एस्म्डव्।एब्ब्डब्। और ठम्ब्। जैसे समझौते सुरक्षित संचार, रीयल–टाइम भू–स्थानिक खुफिया जानकारी और संयुक्त परिचालन क्षमताओं को बढ़ावा देते हैं।[29]
- **रणनीतिक तकनीकी साझाकरणः** यूके, जापान और इजराइल के साथ संयुक्त अनुसंधान एवं विकास भारत की निगरानी, ड्रोन और साइबर–रक्षा तकनीक को आगे बढ़ाता है, और घरेलू कार्यक्रमों को पूरक बनाता है।

केस स्टडी – ऑपरेशन सिंदूर (मई 2025)

ऑपरेशन सिंदूर भारत के हाइब्रिड–विरोधी सिद्धांत में एक महत्वपूर्ण मोड़ है। पहलगाम आतंकी नरसंहार (22 अप्रैल, 2025) से प्रेरित इस अभियान में 7 मई, 2025 को पाकिस्तान और पीओके में नौ आतंकी ढाँचे वाले ठिकानों पर सटीक हवाई और मिसाइल हमले किए गए।

- **सटीक हमलेः** राफेल जेट, हैमर और स्कैल्प हथियारों और इजराइली ड्रोन का इस्तेमाल करते हुए, भारत ने लश्कर–ए–तैयबा और जैश–ए–मोहम्मद के शिविरों को निशाना बनाया और कथित तौर पर 100 से ज्यादा 'उच्च मूल्य' वाले आतंकवादियों का सफाया कर दिया।
- **ड्रोन–रोधी अभियानः** ड्रोन झुंडों और मिसाइलों के जरिए पाकिस्तानी जवाबी कार्रवाई को आकाशतीर जैसी उन्नत ड्रोन–रोधी प्रणालियों द्वारा काफी हद तक बेअसर कर दिया गया।
- **डिजिटल और नागरिक सुरक्षाः** राष्ट्रव्यापी नागरिक सुरक्षा अभ्यास और डिजिटल निगरानी ने भारत की समग्र समाज–जुटाव को प्रदर्शित किया, जबकि भारतीय अधिकारियों ने गलत सूचनाओं का खंडन करने और कथानक पर नियंत्रण बनाए रखने के लिए काम किया।
- **कूटनीतिक विस्तारः** ऑपरेशन सिंदूर को भारत की आत्मरक्षा स्थिति और सिंधु जल संधि के निलंबन, व्यापार प्रतिबंधों और वीजा प्रतिबंधों सहित सख्त आर्थिक और कूटनीतिक उपायों को समझाने के लिए एक अंतर्राष्ट्रीय संक्षिप्त विवरण के साथ जोड़ा गया था।

प्रभाव और सबकः

- **रेडलाइन और निवारणः** प्रधानमंत्री मोदी ने ऑपरेशन सिंदूर को एक ष्नया सामान्यष् घोषित किया – किसी भी आतंकवादी हमले का, पाकिस्तानी परमाणु रुख की परवाह किए बिना, त्वरित, पूर्ण–स्पेक्ट्रम जवाबी कार्रवाई से जवाब दिया जाएगा।[30]
- **हाइब्रिड समन्वयः** इस ऑपरेशन में सैन्य, आर्थिक, डिजिटल और कूटनीतिक उपकरणों को शामिल किया गया – जो भविष्य के हाइब्रिड संकटों के लिए आवश्यक 'जटिल निवारण' का मॉडल था।

- **आख्यान और सूचनाः** तीव्र सैन्य सफलता के बावजूद, इस ऑपरेशन ने भारत के सूचना युद्ध ढांचे में कमियों को उजागर किया, जिससे बेहतर समन्वित आख्यान नियंत्रण और एक केंद्रीय ५ कमांड[31] की आवश्यकता पर प्रकाश डाला गया।

केस स्टडी – कुडनकुलम और मुंबई ग्रिड पर साइबर हमले

भारत के महत्वपूर्ण बुनियादी ढाँचे को बार–बार चीन और पाकिस्तान दोनों से जुड़े साइबर हमलों का निशाना बनाया गया है।

- **कुडनकुलम परमाणु संयंत्र, 2019:** मैलवेयर (डीट्रैक, उत्तर कोरिया से जुड़ा) ने बिजली संयंत्र के व्यावसायिक नेटवर्क में घुसपैठ की। हालाँकि किसी भी परिचालन प्रणाली से समझौता नहीं हुआ, लेकिन इसने विक्रेता और प्रशासनिक सुरक्षा में कमियों को उजागर किया, और सुरक्षा की झूठी भावना के रूप में 'एयर गैप्स' पर चिंता जताई।[32]
- **मुंबई ग्रिड, 2020:** चीन से जुड़े हैकरों ने कथित तौर पर शहर के ग्रिड सिस्टम को संक्रमित कर दिया, जिससे यह कुछ समय के लिए अंधेरे में डूब गया और 'डिजिटल संप्रभुता' के लिए खतरे का संकेत दिया। जाँच 'रेड इको' की ओर इशारा करती है, जो एक चीनी समूह है जो भारतीय बुनियादी ढाँचे पर केंद्रित है।
- **मई 2025:** ऑपरेशन सिंदूर में कम से कम सात पाकिस्तानी और कई 'लोन वुल्फ' हैकरों द्वारा भारतीय नेटवर्क पर साइबर हमलों की एक समन्वित बौछार देखी गई; अधिकांश हमलों को विफल कर दिया गया, लेकिन पैमाने ने राष्ट्रीय बुनियादी ढाँचे के निरंतर उन्नयन और रेड–टीमिंग की आवश्यकता को रेखांकित किया।[32]
- **विश्लेषणात्मक दृष्टिकोण:** दोनों हमले जिम्मेदारी तय करने की चुनौती. घटना पर त्वरित प्रतिक्रिया की आवश्यकता और एक सतत सीखने वाले, सार्वजनिक निजी साइबर सुरक्षा पारिस्थितिकी तंत्र की अनिवार्यता को दर्शाते हैं।

संसदीय निगरानी और नीतिगत बहस

संघर्ष के स्वरूप में आ रही क्रांति को स्वीकार करते हुए, भारतीय संसद और रक्षा संबंधी संसदीय स्थायी समिति ने हाइब्रिड और गैर–गतिज युद्ध की तैयारी की समीक्षा और निगरानी को प्राथमिकता दी है। प्रमुख फोकस क्षेत्रों में शामिल हैं:

- **साइबर और डिजिटल खतरे:** साइबर हमलों, ड्रोन–रोधी तकनीकों और एआई एवं उन्नत सूचना प्रणालियों के एकीकरण की तैयारियों की वार्षिक समीक्षा।
- **स्वदेशी आधुनिकीकरण:** मेक–इन–इंडिया पहलों, रक्षा खरीद प्रक्रियाओं और नए संयुक्त कमांडों के संचालन का नियमित ऑडिट।
- **नीतिगत सैद्धांतिक बहस:** प्रति–आक्रामक साइबर अभियानों की सीमाओं और वैधता, सूचना युद्ध पारदर्शिता और उभरती प्रौद्योगिकियों के उपयोग पर निगरानी के बारे में चल रही नीतिगत बहसें।

संसदीय जाँच अधिक तकनीकी और तात्कालिक हो गई है, जो समग्र, बहु–क्षेत्रीय रक्षा योजना की ओर बदलाव का संकेत देती है।

उभरती प्रौद्योगिकियाँ: एआई, ड्रोन, स्वायत्त प्रणालियाँ

भारत का रक्षा आधुनिकीकरण अब तकनीकी बढ़त पर केंद्रित है:

- **एआई और पूर्वानुमान विश्लेषणः** भारतीय सेना का प्रोजेक्ट सीकर, व्यक्तिगत पहचान (पीआईआई) को छिपाने के लिए एआई , और लड़ाकू ड्रोन निगरानी और गतिज मिशनों में एआई को मुख्यधारा में लाने का संकेत देते है।
- **लोइटरिंग म्यूनिशन और स्वार्म ड्रोनः** प्रलय प्रिसिजन ड्रोन, यूएलपीजीएम–वी3 ड्रोन और लोइटरिंग म्यूनिशन को अपनाने से युद्धक्षेत्र की प्रतिक्रियाशीलता और सीमा गश्त में बदलाव आ रहा है।
- **क्वांटम और अगली पीढ़ी के नेटवर्क** : क्वांटम प्रौद्योगिकी और अनुप्रयोगों पर राष्ट्रीय मिशन (एनएम–क्यूटीए) सुरक्षित सी2 संचार के लिए क्वांटम क्रिप्टोग्राफी को बढ़ावा देता है।[33]
- **चुनौतियाँ** : एआई और क्वांटम प्रणालियाँ हथियारों की होड़ को तेज करती हैं, और गैर–राज्यीय तत्व या आपराधिक समूह हाइब्रिड या साइबर अपराध अभियानों के लिए इनका उपयोग कर सकते हैं। नैतिक, कानूनी और सैद्धांतिक ढाँचों की तत्काल आवश्यकता है।[34]

भारत के लिए सुझाव और रणनीतिक रुख

हाइब्रिड खतरों के विरुद्ध भारत के रणनीतिक रुख को मजबूत करने के लिए, निम्नलिखित रोडमैप प्रस्तावित हैः

- **संपूर्ण राष्ट्र सिद्धांत को संस्थागत बनाएँः** सैन्य, खुफिया, नागरिक और निजी क्षेत्र की प्रतिक्रियाओं को एकीकृत करें। गतिशील, अंतर क्षेत्रीय अभ्यास और योजना सुनिश्चित करें।
- **साइबर और सूचना युद्ध क्षमताओं को मजबूत करेंः** सूचना युद्ध के लिए एक केंद्रीकृत कमान स्थापित करें।
- **राष्ट्रीय ब्त्ज् को निरंतर उन्नत करेंः** सार्वजनिक निजी साइबर नवाचार को प्रोत्साहित करें; प्रारंभिक चेतावनी प्रणालियों में ।प् को शामिल करें।
- **कानूनी और ग्रे जोन तैयारी को उन्नत करेंः** स्वदेशी कानूनी सिद्धांत विकसित करें और वैश्विक कानूनी मंचों पर अभियोजन और बचाव दोनों के लिए विशेष टीमों को प्रशिक्षित करें।
- **दुष्प्रचार के विरुद्ध लचीलापन बनाएँः** डिजिटल साक्षरता अभियानों का विस्तार करें, स्वतंत्र तथ्य–जांच का समर्थन करें और सरकारी सूचना संचालन में पारदर्शिता बढ़ाएँ।
- **स्वदेशी प्रौद्योगिकी विकास को आगे बढ़ानाः** एआई, ड्रोन, क्वांटम और स्वायत्त प्रणालियों में अनुसंधान एवं विकास को प्राथमिकता देनाय प्रत्यक्ष सैन्य–उद्योग–अकादमिक इंटरफेस के साथ रक्षा नवाचार क्लस्टर स्थापित करना।
- **अंतर्राष्ट्रीय रणनीतिक साझेदारी को गहरा करनाः** क्वाड, एयूकेयूएस और जीएसओएमआईए ढांचे के भीतर खुफिया और प्रौद्योगिकी साझाकरण को संस्थागत बनानाः क्षेत्रीय बहुपक्षीय साइबर अभ्यास का नेतृत्व करना।
- **संसदीय निगरानी को बढ़ानाः** साइबर, एआई और गैर–गतिज तत्परता की नियमित समिति समीक्षाय मंत्रालयों (रक्षा, आईटी, गृह मामले, विदेश मामले) के बीच नीति समन्वय को सुगम बनाना।
- **रेड टीम और निरंतर अनुकूलनः** उभरते हाइब्रिड खतरों से निपटने के लिए युद्ध अभ्यास, महत्वपूर्ण बुनियादी ढांचे की 'रेड टीमिंग' और आवधिक सैद्धांतिक समीक्षाओं को संस्थागत बनाना।

निष्कर्ष

हाइब्रिड युद्ध कल का युद्ध नहीं है यह आज का संघर्ष है। भारत के लिए, मई 2025 के ऑपरेशन सिंदूर और बार–बार हुए साइबर और सूचना हमलों के अनुभव स्पष्ट करते हैं कि युद्ध का मैदान हर जगह है।

हिमालय की ऊँचाइयों से लेकर देश के पावर ग्रिड के सबसे गहरे केंद्रों तक, गुमनाम ऑनलाइन चौट रूम से लेकर न्यूयॉर्क और जिनेवा के सर्वोच्च राजनयिक मंचों तक।

हाल के वर्षों में भारत की प्रतिक्रिया में उल्लेखनीय प्रगति हुई है। सैन्य सटीकता और तकनीकी आत्मनिर्भरता बढ़ी है और संस्थागत सुधार राष्ट्र को अधिक चुस्त और लचीला बना रहे हैं। सीडीएस कार्यालय का गठन, सशस्त्र बलों का आधुनिकीकरण, रक्षा उत्पादन का स्वदेशीकरण और मजबूत संसदीय निगरानी, ये सभी एक स्वस्थ रणनीतिक गतिशीलता को दर्शाते हैं। हालाँकि, स्थायी कमियों विशेष रूप से एकीकृत सूचना युद्ध, साइबर पारिस्थितिकी तंत्र को मजबूत बनाने, आख्यान निर्माण और सैद्धांतिक स्पष्टता को तत्काल और नवीनता के साथ दूर किया जाना चाहिए।

विरोधी जाँच–पड़ताल, व्यवधान पैदा करना और भ्रम फैलाने की कोशिश करते रहेंगे। इस संकर युग में रणनीतिक स्वायत्तता और राष्ट्रीय सुरक्षा सुनिश्चित करने के लिए, भारत को प्रतिक्रियात्मक रणनीतियों से आगे बढ़ना होगा। भविष्य एक ऐसी स्थिति की माँग करता है जो पूर्वानुमानित, बहुआयामी, तकनीक–प्रेमी और गहन सहयोगात्मक हो। केवल वही राष्ट्र जो अपनी डिजिटल, सूचनात्मक, कानूनी और सामाजिक सीमाओं को सुरक्षित रखता है साथ ही नैतिक और कानूनी उच्च स्तर बनाए रखता है 21 वीं सदी के अस्पष्ट युद्धों में विजयी होगा।

संदर्भ ग्रन्थ सूची

1. Hybrid Warfare: Features, Examples, Implications & Challenges. https://testbook.com/ias-preparation/hybrid-warfare
2. Disinformation Campaigns Targeting India https://disa.org/disinformation-campaigns-targeting-india/
3. Grey Zone Warfare and its Significance UPSC IAS Exam. https://www.iasexam.com/grey-zone-warfare-and-its-significance/
4. Three warfares - Wikipedia. https://en.wikipedia.org/wiki/Three_warfares
5. CHINA - Three Warfares Strategy, https://imrmedia.in/china-three-warfares-strategy/
6. India-Pakistan Tensions in the Wake of the Pahalgam Attack (2025): New https://www.ijfmr.com/papers/2025/4/52754.pdf
7. Hybrid Warfare as Lawfare: Towards 0 Comprehensive Legal Approach. https://link.springer.com/chapter/10.1007/978-3-319-60798-6_4
8. Hybrid Threats: The Coming Storm, or Smart Power by Other Means?. https://theyonseijournal.com/wp-content/uploads/2025/07/Hybrid-Threats-The-Coming-Storm-or-Smart-Power-by-Other-Means.pdf
9. Lessons from the cyberattack on India's largest nuclear power plant. https://thebulletin.org/2019/11/lessons-from-the-cyberattack-on-indias-largest-nuclear-power-plant/
10. Digital Defence: India's Cybersecurity Landscape. https://dras.in/digital-defence-indias-cybersecurity-landscape/
11. Preparing for the Future: The Need for India to Develop Hybrid Warfare https://www.orfonline.org/research/preparing-for-the-future-the-need-for-india-to-develop-hybrid-warfare-capabilities
12. AI as Tool of Hybrid Warfare: Challenges and Responses. https://www.jinfowar.com/journal/volume-21-issue-2/ai-tool-hybrid-warfare-challenges-responses
13. From Cybersecurity to Cyberwarfare: India's preparedness to be truly

https://government.economictimes.indiatimes.com/news/from-cybersecurity-to-cyberwarfare-indias-preparedness-to-be-truly-viksit/122198826

14. 02 Apr 2025: Tackling the disinformation threat in India. https://chahalacademy.com/the-hindu-editorial-analysis/02-apr-2025/1776
15. Had informed govt about Kudankulam nuclear power plant cyber attack https://www.indiatoday.in/india/story/had-informed-govt-about-kudankulam-nuclear-power-plant-cyber-attack-former-ntro-cyber-security-analyst-1616304-2019-11-06
16. Information and Cyber in Non-Kinetic https://www.usiofindia.org/pdf/DP_Pandey_Final.pdf Warfare: Counter Strategies
17. 100 days of Operation Sindoor: What all has happened since India hit https://www.firstpost.com/india/operation-sindoor-100-days-india-counter-terror-strategy-13925160.html
18. AI and Defence https://visionias.in/current-affairs/monthly-magazine/2024-11-14/security/ai-and-defence
19. India-Pakistan Tensions: Narrative Warfare, Hybrid Threats, and https://www.cyberworldinsight.com/news/india-pakistan-tensions-narrative-warfare-hybrid-threats-and-pakistans-strategic-response/
20. Indo-Pacific Futures The grey zone, hybrid war, and minilateralism. https://www.policyforum.net/resource/indo-pacific-futures-the-grey-zone-hybrid-war-and-minilateralism/index.html
21. 2025 India-Pakistan conflict https://en.wikipedia.org/wiki/2025_India%E2%80%93Pakistan_conflict
22. Prime Minister of India Slams Pakistan on Use of Proxy War against India. https://visionias.in/current-affairs/download/9127
23. Quadrilateral Security Dialogue (QUAD) दृष्टि आईएएस. https://www.drishtiias.com/daily-updates/daily-news-editorials/quad-3
24. 2025: The Year of Defence Reforms chronicleindia.in. https://www.chronicleindia.in/online-magazine/csce-march-2025/2025-the-year-of-defence-reforms
25. Chief of Defence Staff (CDS) - Vajiram & Ravi. https://vajiramandravi.com/current-affairs/chief-of-defence-staff-cds/
26. Standing Committee on Defence (India) https://en.wikipedia.org/wiki/Standing_Committee_on_Defence_%28India%29
27. Roles & Responsibilities https://drdo.gov.in/drdo/headquarter-directorates/area-of-work/directorate-parliamentary-affairs-dpa
28. Evolving Warfare & India's Defence Transformation Strategy 2025. https://www.thetargetclasses.com/defence/evolving-warfare-indias-defence-transformation-strategy/
29. India-US Relationship - PWOnlyIAS. https://pwonlyias.com/current-affairs/india-us-relationship/
30. Artificial intelligence in hybrid and information warfare. https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003284093-4/artificial-intelligence-hybrid-information-warfare-wesley-moy-kacper-gradon

31. Hybrid Warfare International Relations Oxford Bibliographies. https://www.oxfordbibliographies.com/abstract/document/obo-9780199743292/obo-9780199743292-0260.xml

32. Armed forces' preparedness to deal with non-kinetic warfare. https://pwonlyias.com/current-affairs/armed-forces-to-deal-with-non-kinetic-warfare/

33. Hybrid CoE Trend Report 10: Threat potential in the economy: from https://www.hybridcoe.fi/publications/hybrid-coe-trend-report-10-threat-potential-in-the-economy-from-vulnerabilities-to-chinas-increased-coercion/

34. Defence Cyber Agency (DCA) - GKToday. https://www.gktoday.in/defence-cyber-agency-dca/

❑❑❑