ISSN 2278-8808
An International Peer Reviewed
SCHOLARLY RESEARCH JOURNAL
FOR INTERDISCIPLINARY STUDIES

संयुक्त राज्य अमेरिका, चीन, पाकिस्तान, रूस और भारत में सूचना युद्ध

Hemant Kumar Pandey, Ph. D.
Department of Defense Students
Meerut College, Meerut

नई सूचना प्रौद्योगिकियों द्वारा लाए गए परिवर्तनों के कारण दुनिया तेजी से बदलाव के दौर से गुजर रही है। यह मौलिक रूप से लोगों और समाजों के बीच बातचीत के तरीकों को बदल रहा है। इन परिवर्तनों का हमारी राष्ट्रीय सुरक्षा पर गहरा प्रभाव पड़ सकता है, जिन खतरों का हम सामना करते हैं, जिस तरह से हम लड़ते हैं, और हम अपने राष्ट्रीय हितों को कैसे आगे बढ़ाते हैं। सूचना के बुनियादी ढांचे पर हमला किया जा रहा है और इसका सेना और समाज दोनों के लिए व्यापक प्रभाव हो सकता है। जीवन के सभी क्षेत्रों में सूचना प्रौद्योगिकी पर हमारी निर्भरता बढ़ रही है। अंतर्निहित कमजोरियों का अध्ययन और खतरों से सुरक्षा समग्र रूप से समाज और विशेष रूप से सेना के लिए रुचिकर है।

संयुक्त राज्य अमेरिका में सूचना युद्ध

संयुक्त राज्य अमेरिका में, IW के आक्रामक पहलुओं को सरकारी एजेंसियों - रक्षा विभाग (DOD), राज्य विभाग (DOS), केंद्रीय खुफिया एजेंसी (CIA) और व्हाइट हाउस द्वारा नियंत्रित किया जाता है। आक्रामक आईओ से जुड़े किसी भी ऑपरेशन को इनमें से कुछ या सभी से मंजूरी की आवश्यकता होगी। हालांकि रक्षात्मक आईओ को ऐसी कोई मंजूरी की आवश्यकता नहीं है। सूचना आश्वासन, बल सुरक्षा या संचालन सुरक्षा जैसे पहलू स्वयं संगठनों की जिम्मेदारियां हैं। प्रत्येक संगठन अंततः IW के खिलाफ अपनी रक्षा के लिए जिम्मेदार है। इसलिए, सामान्य यू.एस. सरकार आईओ डिजाइन सीधा नहीं है। कार्य व्यवस्था कई वर्षों में विकसित हुई है और अंतर-एजेंसी सहयोग को शामिल करते हुए एक सुसंगत आईओ संरचना विकसित करने के प्रयास जारी हैं।

यूएस IW क्षमताएं

IO को यू.एस. सामरिक कमान द्वारा एक प्रमुख सैन्य योग्यता के रूप में माना जाता है। किसी विरोधी की सूचना-संरचना को निष्क्रिय या नियंत्रित करने के लिए EM ऊर्जा या साइबर हमले का उपयोग, विरोधी की धारणाओं में हेरफेर करने के लिए मनोवैज्ञानिक संचालन जोर के प्रमुख क्षेत्रों का निर्माण करते हैं। सूचना को अब एक दायरे, एक हथियार और एक लक्ष्य के रूप में माना जाता है। युद्ध. कंप्यूटर नेटवर्क हमलों और रक्षा के लिए अमेरिकी क्षमताएं बेजोड़ हैं। आईओ के संचालन के लिए, पांच मुख्य क्षमताओं को सूचीबद्ध किया गया है: Psy Ops, सैन्य धोखे, संचालन सुरक्षा, CNO और EW। इन अंतर-निर्भर क्षमताओं के समन्वय के लिए एक एकीकृत कार्यान्वयन योजना नियोजित की गई है।

एक अमेरिकी सैन्य संगठन, जिसे नेटवर्क वारफेयर (JFCC NW) के लिए संयुक्त कार्यात्मक घटक कमांड कहा जाता है, CNA के विकसित मिशन के लिए जिम्मेदार है। इसकी क्षमताओं को अत्यधिक वर्गीकृत किया गया है, और अमेरिकी अधिकारियों ने हमेशा सीएनए में किसी भी प्रयास से इनकार किया है। इसमें NSA, CIA, FBI, सेना के प्रतिनिधि और सहयोगी दलों के सदस्य शामिल हो सकते हैं। नवीनतम अमेरिकी साइबर नीति हाल ही में जारी की गई है। इस नीति के अनुसार, संयुक्त राज्य अमेरिका अब 'साइबर पर्ल हार्बर' के बारे में चिंतित नहीं है। अमेरिका को लगातार खतरे की आशंका व्यक्तियों, फर्मों और औद्योगिक प्रणालियों के खिलाफ निम्न स्तर के हमले। अपने तकनीकी और सैन्य लाभ को नष्ट करने के लिए यू.एस. बौद्धिक संपदा की चोरी की पहचान के रूप में की जाती

है। इस संबंध में चीन का विशेष उल्लेख किया गया है। अतीत में अमेरिका ने कभी भी सार्वजनिक रूप से आक्रामक IW हथियारों के कब्जे को स्वीकार नहीं किया। नया दस्तावेज़ विशेष रूप से स्वीकार करता है कि यू.एस. अन्य देशों के सूचना बुनियादी ढांचे पर हमले शुरू करने में सक्षम है, और कुछ परिस्थितियों में ऐसा करने के लिए तैयार है। यह घोषणा करता है कि संचालन के क्षेत्र में यू.एस. के हितों की रक्षा के लिए अमेरिकी सेना के लिए CNA का संचालन करना कभी-कभी उपयुक्त हो सकता है।

रूस में सूचना युद्ध

आधुनिक युद्ध में सूचना के महत्व को रूसी सेना के संचालन में रेखांकित किया गया है। राष्ट्रीय सुरक्षा से संबंधित रूस के वर्तमान दस्तावेज़ सूचना सुरक्षा के मुद्दों पर एक उच्च चिंता को उजागर करते हैं। पहले अप्रत्यक्ष रणनीतिक संचालन, IW के तरीकों और सूचना अवरोधों का उपयोग करके सूचना तैयार करने और जनमत को आकार देने की आवश्यकता पर ध्यान केंद्रित किया गया था। रूस का मानना है कि सूचना श्रेष्ठता रखने वाले राष्ट्र पहले से कहीं अधिक जोखिम की कमी और जीवन के नुकसान के डर के कारण सैन्य बल को नियोजित करने के लिए इच्छुक हो सकते हैं। उनके हाल के ऑपरेशन कानूनी प्रतिबंधों के अभाव में IW का उपयोग करने की उनकी उत्सुकता को प्रकट करते हैं।

नब्बे के दशक में, रक्षा और राष्ट्रीय सुरक्षा प्रमुख के पूर्व प्रथम उप मंत्री आंद्रेई कोकोशिन ने IW के पांच उपखंड दिए - EW, खुफिया, संचार, दुश्मन के प्रभाव और परिचालन कमांड और नियंत्रण प्रणालियों के खिलाफ कमांड और नियंत्रण प्रणालियों की सुरक्षा के लिए सुविधाएं। वी.आई. त्सिम्बल, एक रूसी मंत्री ने बाद में IW के लिए एक एकीकृत दृष्टिकोण का प्रस्ताव दिया।

रूसी मानव मन को प्रभावित करने के तरीकों के अध्ययन में अग्रणी हैं। Informatsionnaya voina (सूचना युद्ध) पुस्तक ने मानव व्यवहार का अनुमान लगाने वाले एल्गोरिदम को समायोजित करके मन में हेरफेर करने के तरीकों की जांच की। इसने एक मानव सूचना वायरस का सुझाव दिया जिसे वस्तुनिष्ठ तर्क को रोकने या मन की सोच प्रक्रिया को प्रभावित करने के लिए "सूचक प्रभाव" के रूप में पेश किया जा सकता है। रूसी सूचना हथियार न केवल हार्डवेयर और सॉफ्टवेयर सिस्टम, बल्कि दिमाग को भी निशाना बनाते हैं। रूसियों का मानना है कि सूचनात्मक और मनोवैज्ञानिक योग्यता सेना और नागरिकों द्वारा समान रूप से बारीकी से जांच की जाती है।

साथ ही, अनुनय के तरीकों को IW का हथियार माना जाता है। IW पर रूसी साहित्य में चिंतनशील नियंत्रण विधियों का उल्लेख किया गया है। रिफ्लेक्सिव कंट्रोल का उद्देश्य किसी व्यक्ति को स्वेच्छा से निर्णय लेने के लिए प्रभावित करने के लिए विशेष रूप से तैयार की गई जानकारी को खिलाना है जो नियंत्रक द्वारा वांछित है। साहित्य में पाई जाने वाली ऐसी गतिविधि के कुछ उदाहरणों में सैन्य इकाई 10003 शामिल है, जो समूहों के मस्तिष्क धोने के लिए तकनीकों का अध्ययन करती है, रणनीतिक रॉकेट बलों में एंटी-ईएसपी प्रशिक्षण और हिंसक घटनाओं की भविष्यवाणी करने के लिए ज्योतिष का उपयोग करती है।

रूसी विशेषज्ञों ने नोट किया है कि कोसोवो में नाटो अभियान ने आभासी सूचना-तकनीकी युद्ध की शुरुआत का संकेत दिया। C4I2 सिस्टम ने गठबंधन बलों को सबसे बड़ा फायदा दिया। संयुक्त राज्य अमेरिका के साथ प्रतिस्पर्धा करने में असमर्थ, रूस ने युद्ध छेड़ने के लिए असममित विकल्पों की तलाश शुरू कर दी।

रूसियों के अनुसार, टोही और कमान और नियंत्रण प्रणाली पर जोर दिया जाना चाहिए। उनके विशेषज्ञों के अनुसार, नए IW हथियारों के लिए रूस के मुख्य फोकस क्षेत्रों को निर्देशित और EM ऊर्जा हथियारों, साइबर-हथियारों और चुपके मानव रहित लड़ाकू प्लेटफार्मों पर केंद्रित होना चाहिए।

हाल के सैन्य सिद्धांत दस्तावेज IW और असममित युद्ध पर बढ़ती निर्भरता के लिए बल पर बल पर पिछले जोर से स्पष्ट बदलाव दिखाते हैं। यह संभवत: हाल के दिनों में रूस द्वारा सामना की जा रही वित्तीय कठिनाई के कारण है।

यूक्रेन में IW

रूस IW विशेष रूप से 2014 की शुरुआत से यूक्रेन में 'रिफ्लेक्सिव कंट्रोल' की अवधारणा को नियोजित कर रहा है। रिफ्लेक्सिव कंट्रोल एक प्रतिद्वंद्वी को स्वेच्छा से उन विकल्पों को बनाने के लिए बनाता है जो धारणा प्रबंधन द्वारा

स्वयं के उद्देश्यों के लिए सबसे अधिक फायदेमंद होते हैं। रूसियों ने यूक्रेन में कार्रवाई के दौरान पश्चिमी शक्तियों को निष्क्रिय रहने के लिए मनाने के लिए इस तकनीक का प्रभावी ढंग से उपयोग किया है।

रूसियों द्वारा अपनाई जाने वाली कार्यप्रणाली में यूक्रेन में अपने सैनिकों की उपस्थिति को छिपाना शामिल है, बिना किसी स्पष्ट प्रतीक के अंदर सैनिकों को भेजकर वे संघर्ष में अपने लक्ष्यों और उद्देश्यों को छिपाते रहे हैं, जिससे दुनिया को संकेत मिलता है कि उनकी अनदेखी की जा सकती है। इन प्रयासों की सोशल मीडिया सहित सभी उपलब्ध प्लेटफार्मों के माध्यम से धारणा प्रबंधन के एक बहुत ही ठोस वैश्विक अभियान के साथ सराहना की गई है।

रूस ने अपना 2010 सैन्य सिद्धांत प्रकाशित किया जिसमें IW की भूमिका में वृद्धि और IW के लिए बलों और संसाधनों को विकसित करने का संकल्प स्वीकार किया गया। सिद्धांत नोट करता है कि आधुनिक सैन्य संघर्षों को शत्रुता के प्रकोप से पहले भी IW के उपायों के कार्यान्वयन की विशेषता है। इस प्रकार विश्व समुदाय से अनुकूल प्रतिक्रिया को आकार देते हुए सैन्य बल के नियोजन के बिना राजनीतिक उद्देश्यों को प्राप्त किया जा सकता है।

वर्तमान रूसी साइबर क्षमताएं

राष्ट्रीय खुफिया निदेशक जेम्स क्लैपर ने 2015 में अमेरिकी खुफिया समुदाय के विश्वव्यापी खतरे के आकलन की प्रस्तुति के दौरान अमेरिकी सीनेट सशस्त्र सेवा समिति को बताया कि रूसी साइबर खतरा पहले की तुलना में अधिक गंभीर था। रिपोर्ट से पता चलता है कि रूस IW को एक नए स्तर पर ले जा रहा है, जहां साइबर खतरे आवृत्ति, पैमाने, परिष्कार और प्रभाव की गंभीरता में बढ़ रहे हैं। रूस को साइबर स्पेस में सबसे परिष्कृत खिलाड़ियों में से एक माना जाता है। रिपोर्ट में कहा गया है कि रूसी अपनी समर्पित साइबर कमांड स्थापित कर रहा है, जिसके पास आक्रामक आईओ आयोजित करने का कार्य होगा। औद्योगिक नियंत्रण प्रणालियों पर हमला करने और इस तरह महत्वपूर्ण नेटवर्क पर हमला करने के लिए "अनिर्दिष्ट रूसी साइबर अभिनेताओं" की क्षमताओं का उल्लेख किया गया है।

ट्रेंड माइक्रो द्वारा अंडरग्राउंड रूसी साइबर की समीक्षा ने इसे दुनिया का सबसे परिष्कृत घोषित किया। हर कोई हैकिंग हमलों के लिए चीन पर आरोप लगाता है, लेकिन जब परिष्कार और व्यावसायिकता की बात आती है तो रूसी साइबर अंडरग्राउंड से मेल खाने के लिए कुछ भी नहीं है। एक रिपोर्ट में सिक्योरिटी फर्म ट्रेंड माइक्रो में फॉरवर्ड लुकिंग थ्रेट असेसमेंट टीम का यह आकलन है। रिपोर्ट से पता चलता है कि हैकिंग रूस में एक व्यवसाय के रूप में आयोजित की जाती है, जिसमें स्वचालित बिक्री प्रक्रिया और श्रम विभाजन होता है। व्यावसायिक रूप से संगठित अवैध हैकिंग टीमें रूस में एक प्रमुख साइबर क्षमता का गठन करती हैं।

पीपुल्स रिपब्लिक ऑफ चाइना में सूचना युद्ध

चीनी आधिकारिक श्वेत पत्रों से पता चलता है कि पीआरसी भविष्य के संघर्षों में IW तकनीकों के अपने संस्करण को नियोजित करने की संभावना है। कई PLA लेखक जैसे जनरल हुआई गुओमो ने अपने प्रकाशनों में IW तकनीकों पर ध्यान दिया है। इन लेखों के अनुसार, युद्ध शुरू होने से कई घंटे पहले, कमांडर शुरू में आक्रामक IW हथियारों जैसे कि सटीक निर्देशित हथियार, EW, EMP हथियार और कंप्यूटर वायरस को दुश्मन सूचना प्रणाली पर हमला करने के लिए नियोजित करेंगे। यह दुश्मन के निर्णय लेने के तंत्र को नीचा या नष्ट कर देगा जिससे उसे हमलावर के लिए फायदेमंद शर्तों पर शत्रुता समाप्त करने के लिए मजबूर होना पड़ेगा। साथ ही हमलों को रोकने के लिए रीयल-टाइम डिटेक्टर स्थापित करके स्वयं की सूचना और सूचना प्रणाली को दुश्मन से सुरक्षित रखा जाएगा। इस तरह के IW उपाय भविष्य के युद्धों का केंद्र बनेंगे। सूचना में वर्चस्व के लिए संघर्ष धीरे-धीरे लड़ाई की जड़ बन जाएगा, और रणनीतिक स्तर पर निवारक के रूप में कार्य करेगा।

चीनी रक्षा बल बड़े पैमाने पर आधुनिकीकरण अभियान के दौर से गुजर रहे हैं। PLA 21वीं सदी के एक उच्च तकनीकी बल के रूप में उभर रहा है। बहुत से लोग मानते हैं कि आरएमए पहले ही IW द्वारा निर्देशित हो चुका है।

चीनी अवधारणाओं और IW की क्षमताएं

पीपुल्स लिबरेशन आर्मी युद्ध के बदलते स्वरूप को अपनाती रही है। राष्ट्रीय रक्षा पर चीन के नवंबर 2004 के श्वेत पत्र ने 'सूचनाकृत' सशस्त्र बलों के निर्माण की चीनी अवधारणाओं को निर्धारित किया। "सूचना की परिस्थितियों में स्थानीय युद्ध" की अवधारणा ने "उच्च तकनीकी स्थितियों के तहत सीमित युद्ध" को बदल दिया। चीनियों ने यह नोटिस किया कि तकनीकी रूप से बेहतर ताकत इराक जैसे मजबूत देश को आसानी से मात दे सकती है। श्वेत पत्र में उल्लेख किया गया था कि PLA का मुख्य उद्देश्य सूचना युद्ध में एक सूचनात्मक बल और जीत का निर्माण करना था। यह रेखांकित किया गया कि चीनी विशेषताओं के साथ एक RMA प्राप्त करने के लिए सुधार आवश्यक थे।

1991 के पहले खाड़ी युद्ध के बाद, जिसमें IW ने अपनी छाप छोड़ी, चीनी सैन्य और राजनीतिक नेतृत्व व्यापक राष्ट्रीय ताकत हासिल करने के इच्छुक थे। PLA ने अपनी परिस्थितियों के अनुरूप IW की पश्चिमी अवधारणाओं को अनुकूलित किया। PLA के एक जनरल ने IW के महत्व और चुनौतियों पर लिखते हुए कहा कि निकट भविष्य में युद्ध के स्वरूप और भविष्य को IW द्वारा नियंत्रित किया जाएगा। IW को चीन की सैन्य तैयारियों में एक उत्प्रेरक के रूप में मान्यता प्राप्त है और भविष्य के युद्धों में जीतने के लिए यह अत्यधिक महत्वपूर्ण होगा।

अंतरिक्ष और साइबरस्पेस अब रणनीतिक प्रतिस्पर्धा में नए युद्ध के मैदान हैं। अपने सामरिक और आर्थिक हितों की रक्षा के लिए चीन इन दोनों क्षेत्रों में पर्याप्त रक्षा क्षमताओं के लिए प्रयास करेगा। कागज का दावा है कि चीन का केवल रक्षात्मक रुख है और वह "बाहरी अंतरिक्ष में हथियारों के निर्माण और हथियारों की दौड़" का विरोध करता है। यह घोषणा करता है कि चीन हैकर हमलों का एक बड़ा शिकार है और साइबर डोमेन में अपने बुनियादी ढांचे के लिए गंभीर खतरों का सामना कर रहा है।

PLA की IW क्षमताएं

PLA के केंद्रीय सैन्य आयोग के सामान्य सेवा मुख्यालय का तीसरा विभाग अपनी सीमाओं के साथ रणनीतिक संकेतों की खुफिया जानकारी का संग्रह आयोजित करता है। चतुर्थ सशस्त्र बल विभाग का आयोजन IW के संचालन के लिए किया गया है। चीनी सैन्य प्रकाशनों से पता चलता है कि 'आठ क्षैतिज और आठ ऊर्ध्वाधर ग्रिड' पहल के तहत देश के अधिकांश हिस्से को कवर करने के लिए उपग्रह लिंक के साथ पूरक फाइबर ऑप्टिक केबल का एक जटिल संचार नेटवर्क बनाया गया है। ISR क्षमताओं के लिए पश्चिमी देशों से बहुत परिष्कृत इलेक्ट्रॉनिक उपकरण प्राप्त किए गए हैं। PLA ने 'तीन हमले और तीन रक्षा रणनीति' बनाई है जिसमें चुपके विमान हेलीकॉप्टर और क्रूज मिसाइल सटीक हमलों, EW और दुश्मन टोही द्वारा हमलों का बचाव करते हैं। DZ 9002 (बैटलफील्ड ELINT सिस्टम), DZ 9001 (EW), DZ 9300 (मैन पैक रडार सिस्टम), और बॉडीगार्ड लेजर प्रोटेक्शन सिस्टम PLA के आधुनिकीकरण कार्यक्रम में विकसित किए गए कुछ उपकरण हैं। AWACS को पहले ही PLAF में शामिल किया जा चुका है और UAV और ELINT विमानों की एक बहुत बड़ी सूची को शामिल किया गया है।

कांग्रेस को 2014 की अमेरिकी रक्षा विभाग की वार्षिक रिपोर्ट के अनुसार, चीन की सेना IW के लिए आक्रामक साइबर क्षमताओं का विकास जारी रखे हुए है। रिपोर्ट में कहा गया है कि भविष्य के संघर्षों में, साइबर संचालन PLA की रणनीति का एक प्रमुख घटक होने की संभावना है। साइबरस्पेस संचालन का उपयोग सेना द्वारा एक विरोधी के संचालन को अक्षम करने और सूचना प्रभुत्व हासिल करने के लिए किया जाएगा। साइबर ऑपरेशन खुफिया जानकारी के लिए डेटा संग्रह की अनुमति देते हैं और भविष्य के आक्रामक साइबर हमलों के लिए कमजोरियों को प्रकट करते हैं। जब पारंपरिक बलों के साथ संयोजन में नियोजित किया जाता है, तो साइबर हमले बल गुणक के रूप में कार्य करते हैं। चीन संयुक्त राज्य अमेरिका सहित विश्व स्तर पर कंप्यूटर सिस्टम को लक्षित करना जारी रखता है। कई उन्नत देशों के राजनयिक, आर्थिक और रक्षा क्षेत्रों से संबंधित कंप्यूटर नेटवर्क को चीन के रक्षा और उच्च तकनीक उद्योगों को लाभ पहुंचाने के उद्देश्य से खुफिया जानकारी हासिल करने के उद्देश्य से लक्षित किया जाता है।

सूचना संचालन

चीन ने लगातार अपने नागरिकों के साथ-साथ बाहरी दुनिया के लिए सूचना को नियंत्रित करने की आवश्यकता प्रदर्शित की है। चीन अपने स्वयं के महत्वपूर्ण सूचना बुनियादी ढांचे की रक्षा के लिए रक्षात्मक IW उपायों के कार्यान्वयन में आक्रामक है। साथ-साथ, आक्रामक IW क्षमताओं को विकसित किया जा रहा है। परिष्कृत EW सिस्टम, काउंटर-स्पेस हथियार और साइबरस्पेस संचालन में बहुत भारी निवेश सूचना लाभ के लिए क्षमता का निर्माण कर रहे हैं। चीन में इंटरनेट सेंसरशिप चरम पर है। चीन अपने नागरिकों के इंटरनेट के इस्तेमाल पर सख्त नियंत्रण रखता है। चीन में Google जैसे खोज इंजनों की अनुमति नहीं है और उसके अपने स्वयं के संस्करण हैं जैसे सोगौ, Baidu, और 360 खोज। इंटरनेट नियंत्रण की स्थापना को दुनिया में सबसे गंभीर माना जाता है। सरकार की नीतियों की आलोचना करने वाली वेबसाइटों को अक्सर ब्लॉक कर दिया जाता है और व्यक्तियों की इंटरनेट एक्सेस पर लगातार नजर रखी जाती है।

पाकिस्तान में IW का विकास

आईटी और संचार क्षमता विकसित करने के लिए, पाकिस्तान ने चार आईटी विश्वविद्यालयों की स्थापना की है। साथ ही, पाकिस्तान निश्चित रूप से अपनी परिचालन क्षमताओं को आगे बढ़ाने के लिए चीन और अमेरिका के साथ घनिष्ठ संबंधों का लाभ उठाएगा। पाकिस्तान के पास अच्छी तरह से विकसित EW और हैकर युद्ध क्षमताएं हैं। भारतीय वेबसाइटों को निशाना बनाने वाले कुछ प्रसिद्ध हैकरों में पाकिस्तान हैकर्स क्लब (पीएचसी), जीफोर्स-पाकिस्तान और हरकत-उल मोस शामिल हैं। पिछले दिनों ज़ी टेलीविज़न, सोनी और इलेक्ट्रॉनिक्स विभाग और भारतीय विज्ञान कांग्रेस से संबंधित वेबसाइटों के ख़राब होने की सूचना मिली है। यह संदेह है कि इन हैकिंग गतिविधियों को पाकिस्तान द्वारा वित्त पोषित किया जा सकता है। पाकिस्तान के पास अपने क्षेत्र संरचनाओं में IW संगठन हैं

पाकिस्तान के पास कम से कम 1998 से साइबर युद्ध क्षमता होने की सूचना है जब वह भारत में वेबसाइटों को ख़राब करने में लगा हुआ था। भारतीय मीडिया रिपोर्टों ने 2003 में इस गतिविधि में वृद्धि दिखाई, जब यह बताया गया कि भारत सरकार के सर्वरों पर हमला किया गया था। हो सकता है कि पाकिस्तान के पास साइबर युद्ध के लिए अलग से साइबर वारफेयर समन्वय केंद्र न हो। ऐसा प्रतीत होता है कि साइबर हमले सरकारी विभागों से जुड़े अलग-अलग साइबर अनुभागों द्वारा किए गए हैं।

इंटरनेट स्रोत 1998 से पाकिस्तान और भारत के हैकर समूहों के बीच लगातार साइबर संघर्ष का खुलासा करते हैं जब भारत ने एक शांतिपूर्ण परमाणु विस्फोट किया था। जवाबी कार्रवाई में, पाक हैकर समूह मिलवॉर्म द्वारा भारत विरोधी नारे लगाकर BARC वेबपेज को विकृत कर दिया गया और अनुसंधान केंद्र नेटवर्क पर ईमेल संदेशों को चुरा लिया गया। इसके तुरंत बाद, भारतीय सेना के वेबपेज पर हमला किया गया। यह सामाजिक माध्यम से हासिल किया गया था। साइट को होस्ट करने के लिए जिम्मेदार व्यक्ति को हैकर्स ने साइट का पता बदलने के लिए कहा था। यह संभव था क्योंकि उस समय होस्टिंग सर्वर भारत में नहीं थे। 1998 - 2001 की अवधि में, भारतीय सीईआरटी के अनुसार, पाकिस्तानी विरूपण हमलों की संख्या 1998 में चार से बढ़कर 2001 में 150 से अधिक हो गई। 2000 में भारतीय हमलों की संख्या सात और एक साल बाद 18 थी। भारत और पाकिस्तान के बीच पहला साइबर युद्ध PHC, gForce और भारतीय समूह NEO के बीच शत्रुता की समाप्ति के कारण समाप्त हुआ। इस संघर्ष में भारत में 150 से अधिक और पाकिस्तान में लगभग 10 स्थलों को विरूपित किया गया था।

नवंबर 2008 में बॉम्बे में हुए आतंकी हमले के बाद एक नया साइबर संघर्ष शुरू हुआ। भारतीय हैकर समूह एचएमजी ने तेल और प्राकृतिक गैस मंत्रालय पाकिस्तान वेबपेज पर हमला किया। पाकिस्तानियों ने जवाबी कार्रवाई में ओएनजीसी सहित कुछ भारतीय स्थलों को विरूपित किया। पाकिस्तानी समूह केएसए ने दावा किया कि उन्होंने बैंक ऑफ बड़ौदा की वेबसाइट में प्रवेश किया था। जब एचएमजी और भारतीय साइबर योद्धाओं ने पाकिस्तान में इंटरनेट सेवाओं पर हमला करने की धमकी दी तो एक संघर्ष विराम का आह्वान किया गया। यह संघर्ष जारी है।

गैर-राज्य की भूमिकाएं

साइबर अपराधियों की एक नई नस्ल सामने आई है जो केवल लाभ के लिए काम करने में विश्वास रखती है। ऐसे हैकर्स के लिए राष्ट्रीयता या धर्म की कोई संबद्धता नहीं है। कुछ ऐसे भी हैं जो डेटा चुराते हैं और उसे सबसे अधिक बोली लगाने वाले को बेचते हैं। कई अन्य लोग भोले-भाले इंटरनेट उपयोगकर्ताओं से धन उगाहने के लिए ब्लैकमेल का उपयोग करते हैं। 'रैनसम-वेयर' का उपयोग करते हुए हालिया हमले, जो कंप्यूटर पर डेटा को एन्क्रिप्ट करता है, जिसे केवल प्रीमियम का भुगतान करने पर ही डिक्रिप्ट किया जा सकता है, एक नया चलन है। कई तथाकथित 'हैक्टिविस्ट' वेबसाइटों को हैक करते हैं और नारे लगाते हैं जो उनके कारण की ओर ध्यान आकर्षित करते हैं।

दुनिया उस खतरे से अवगत हो रही है जो साइबर-आतंकवाद ने इंटरनेट के लिए उत्पन्न किया है। हालाँकि, आतंकवादियों द्वारा इंटरनेट के उपयोग से उत्पन्न चुनौती के बारे में बहुत कम जानकारी है। हाल के वर्षों में मीडिया रिपोर्टें स्पष्ट रूप से दिखाती हैं कि आतंकवादी संगठन इंटरनेट का उपयोग समर्थकों की भर्ती, धन जुटाने और दुनिया भर में भय का अभियान शुरू करने के लिए करते रहे हैं। इंटरनेट आतंकवादियों को परमाणु ऊर्जा संयंत्रों, सार्वजनिक भवनों, हवाई अड्डों और बंदरगाहों और यहां तक कि आतंकवाद विरोधी उपायों जैसे लक्ष्यों और स्थानों के बारे में रेडीमेड डेटा भी प्रदान करता है! इस बात के प्रमाण मिले हैं कि अल-कायदा के संचालक बिजली, पानी, परिवहन और संचार ग्रिड चलाने वाले डिजिटल स्विच को नियंत्रित करने के तरीकों की लगातार तलाश कर रहे थे ताकि विनाशकारी हमलों को उनसे दूर किया जा सके। ऑनलाइन चैट रूम का उपयोग आतंकवादी कारणों से सहानुभूति रखने वालों की भर्ती के लिए किया जाता है जैसा कि 2015 में आईएसआईएस के मामले में देखा गया है। आतंकवादी संगठनों द्वारा होस्ट की जाने वाली वेबसाइटों का उपयोग सफल हमलों और खतरों को जारी करने के लिए किया जाता है। इंटरनेट आतंकवादियों को अपने भयावह संदेशों को आसानी से दुनिया तक पहुंचाने का एक आसान तरीका प्रदान करता है।

अन्य राष्ट्रों में IW के अध्ययन से सीखे गए सबक

1. IW युग में, संचार नेटवर्क और सिस्टम, दोनों नागरिक और सैन्य, में पर्याप्त अतिरेक, उत्तरजीविता और इलेक्ट्रॉनिक सुरक्षा होनी चाहिए।
2. भारत में एक जीवंत आईटी क्षेत्र है। यह IW के लिए आवश्यक जनशक्ति और प्रौद्योगिकियों के विकास के लिए एक ठोस आधार प्रदान कर सकता है, जिसका सैन्य और नागरिक क्षेत्रों द्वारा संयुक्त रूप से शोषण किया जाना चाहिए।
3. संयुक्त नेटवर्क और व्यक्तिगत रक्षा सेवा नेटवर्क परमाणु सहित सभी वातावरणों में कार्य करने में सक्षम होना चाहिए, कुछ को ईएमपी सख्त करने की आवश्यकता हो सकती है।
4. हमें आईएसआर, इमेजरी और नेविगेशन के लिए अपनी रणनीतिक क्षमताओं को उन्नत करने के लिए विभिन्न प्रकार के नागरिक और सैन्य उपग्रहों को शामिल करने की आवश्यकता है।
5. हमें इस बात की जांच करने की आवश्यकता है कि क्या हम अपने मिलिशिया पर लागू किए गए शुद्ध बल आधारित चीनी मॉडल को अपनाकर IW के लिए अपनी प्रादेशिक सेना इकाइयों को कार्य सौंप सकते हैं।
6. विश्व शक्तियां IW के खिलाफ अपने महत्वपूर्ण बुनियादी ढांचे की सुरक्षा और आक्रामक क्षमताओं को विकसित करने में तेजी से कदम उठा रही हैं। हमारे प्रयासों को उनसे मेल खाने की जरूरत है।

भारत में IW के संचालन के लिए संगठनात्मक संरचना

इस सूचना युग में, श्री बी.जी. एक अनुभवी पत्रकार और कारगिल समीक्षा समिति (KRC) के सदस्य वर्गीज का बहुत महत्व है; उन्होंने कहा, "उच्च रक्षा प्रबंधन का पुनर्गठन और हाल ही में स्थापित राष्ट्रीय सुरक्षा परिषद (NSC) के जनादेश में एक व्यापक सुरक्षा अवधारणा को शामिल करने से रक्षा/राष्ट्रीय सुरक्षा सूचना के संबंधित पुनर्संगठन और पुनर्संरचना के लिए बाध्य होना चाहिए। भारत सरकार (GOI) ने राष्ट्रीय सुरक्षा के सभी पहलुओं से निपटने के लिए एनएससी की स्थापना की है। IW के महत्व को भारत सरकार द्वारा मान्यता दी गई है। IW के खतरों और क्षमताओं का विश्लेषण करने के लिए मंत्रियों के एक समूह (GOM) को काम सौंपा गया था। 'राष्ट्रीय

सुरक्षा प्रणाली में सुधार' शीर्षक वाली रिपोर्ट ने IW के लिए भारत की तैयारियों की विस्तृत समीक्षा करते हुए कई दूरगामी सिफारिशें कीं। IW की अवधारणा की बहुआयामी प्रकृति ने राष्ट्रीय सूचना बोर्ड (NIB) की स्थापना को निर्देशित किया।

जीओएम की उपर्युक्त रिपोर्ट की खोज में, भारत सरकार ने राष्ट्रीय सूचना बोर्ड (NIB), राष्ट्रीय सूचना युद्ध एजेंसी (NIWA), राष्ट्रीय तकनीकी सुविधाएं संगठन (NRFO), सूचना सुरक्षा कार्य बल (ISTF), कंप्यूटर इमरजेंसी जैसे संगठनों की स्थापना की थी। रिएक्शन टीम - इंडिया (CERT-IN), आदि। साथ ही, विभिन्न प्रकार के IW से निपटने के लिए नोडल एजेंसियों की पहचान की गई थी।

राष्ट्रीय स्तर पर मौजूदा IW संगठन

NIB and NIWA

NIBको मई 2002 में राष्ट्रीय सुरक्षा सलाहकार (NSA) की अध्यक्षता में मंजूरी दी गई थी। सदस्यों में कैबिनेट सचिव, तीनों सेवाओं के प्रमुख, रक्षा, मानव संसाधन विकास, वित्त, अंतरिक्ष जैसे महत्वपूर्ण मंत्रालयों के सचिव और सभी खुफिया एजेंसियों के प्रमुख शामिल हैं। . NIB के व्यापक चार्टर में सूचना सुरक्षा, IW पर समग्र राष्ट्रीय स्तर की नीति तैयार करना, तैयार नीतियों और कार्यों के कार्यान्वयन के लिए आवश्यक संस्थानों और संरचनाओं की स्थापना और इन निकायों की निगरानी करना और समय-समय पर सीसीएस को रिपोर्ट करना शामिल है। NIB की भूमिका सभी की समीक्षा करना है। सूचना सुरक्षा के पहलुओं और उभरते खतरों का मुकाबला करने के लिए उपाय करना। NIBने विशेष रूप से IW से निपटने के लिए NIWA की स्थापना की। NIWA को रक्षा खुफिया एजेंसी (DIA) के परिचालन नियंत्रण में रखा गया था।

राष्ट्रीय IW संरचना

भारत सरकार की महत्वपूर्ण पहल

भारत सरकार द्वारा कई महत्वपूर्ण पहल शुरू की गई हैं; इनमें एम्बेडेड सिस्टम के खतरे का मुकाबला करने के लिए आईटी उत्पादों का स्वदेशीकरण, सूचना सुरक्षा और साइबर फोरेंसिक में पाठ्यक्रम संचालित करना शामिल था। इन्हें निम्नानुसार संक्षेपित किया जा सकता है:-

संगठनात्मक सेट-अप पहल

- सूचना सुरक्षा प्रौद्योगिकी विकास परिषद।
- राष्ट्रीय सूचना सुरक्षा आश्वासन ढांचा - सीईआरटी-इन और एनओसी (नेटवर्क संचालन केंद्र)।
- सूचना प्रणाली उत्पाद प्रमाणन एजेंसी।
- राष्ट्रीय अवसंरचना संरक्षण केंद्र।
- राष्ट्रीय साइबर फोरेंसिक संस्थान, तिरुवनंतपुरम।

विकासात्मक पहल

- सूचना सुरक्षा उत्पादों और सेवाओं में स्वदेशी क्षमताएं।
- सूचना सुरक्षा प्रमाणन और लेखा परीक्षा में पाठ्यक्रम।
- साइबर फोरेंसिक में विशेषज्ञता।
- इंटरनेट और आईएसपी निगरानी तंत्र को मजबूत बनाना।
- साइबर हमलों के खिलाफ काउंटर उपाय।
- तकनीकी खुफिया को मजबूत करना।
- क्रिटिकल इंफ्रास्ट्रक्चर प्रोटेक्शन (CIP) योजना।

भारतीय सशस्त्र बलों में IW के लिए संगठन

मुख्यालय एकीकृत रक्षा कर्मचारी (मुख्यालय आईडीएस)

भारतीय सशस्त्र बलों, मुख्यालय आईडीएस की तीन सेवाओं के कामकाज के समन्वय के लिए, 2001 में नई दिल्ली में एक त्रि-सेवा संयुक्त संगठन स्थापित किया गया है। आईडीएस में सेवा अधिकारी, नागरिक अधिकारी और

वैज्ञानिक शामिल हैं। मुख्यालय आईडीएस के प्रमुख विभाग सीआईएससी सचिवालय, नीति, योजनाएं और बल विकास, संचालन, रक्षा खुफिया एजेंसी, सिद्धांत, संगठन और प्रशिक्षण, अंतर्राष्ट्रीय मामले और शुद्ध मूल्यांकन हैं।

रक्षा खुफिया एजेंसी (DIA)

DIA केंद्रीय एजेंसी है जो भारतीय सशस्त्र बलों के लिए सभी खुफिया जानकारी एकत्र करने की गतिविधियों का समन्वय करती है। रक्षा मंत्रालय के तहत काम करते हुए, DIA सभी रक्षा संबंधी खुफिया के लिए जिम्मेदार नोडल एजेंसी है। इसका बजट और संचालन वर्गीकृत रहता है। DIA के तहत सिग्नल इंटेलिजेंस निदेशालय (दुश्मन संचार से SIGINT के अधिग्रहण के लिए जिम्मेदार) और रक्षा छवि प्रसंस्करण और विश्लेषण केंद्र (DIPAC) (उपग्रह आधारित छवि अधिग्रहण क्षमताओं के लिए जिम्मेदार) कार्य करता है। DIA रक्षा सूचना युद्ध एजेंसी (DIWA) को भी नियंत्रित करता है जो IW के सभी तत्वों को संभालती है। इसके संचालन को वर्गीकृत किया गया है और इसने राष्ट्र के लिए कई सफलताएँ हासिल की हैं जो एक गुप्त 116 बनी रहेगी। भारत के पड़ोस में सेना की आवाजाही पर नज़र रखना, आतंकवादी समूहों की निगरानी करना, इसके प्राथमिक कार्य हैं।

तीन सेवाओं की संगठनात्मक संरचना

IW संगठन: भारतीय सेना

भारतीय सेना ने सभी स्तरों पर यानी सेना, कमान, कोर, ब्रिगेड और बटालियन मुख्यालय में संगठनात्मक ढांचे को औपचारिक रूप देने में काफी प्रगति की है। MoD (सेना) के एकीकृत मुख्यालय में सैन्य संचालन महानिदेशालय (DGMO) IW के लिए समग्र रूप से जिम्मेदार है। इसी तरह, प्रत्येक क्षेत्र में, संचालन शाखा IW के सभी पहलुओं की योजना और समन्वय करती है। भारतीय सेना के पास IW/EW कार्यों को निष्पादित करने के लिए एक समर्पित IW/EW ब्रिगेड/समूह और बटालियन हैं। वर्तमान में ये इकाइयाँ कम हैं, IW को क्रियान्वित करने के लिए तीनों सेवाओं में और अधिक बढ़ाने और उपयुक्त रूप से सुसज्जित करने की आवश्यकता है। सुरक्षा कारणों से आगे के विवरण को शोध पत्र में शामिल नहीं किया गया है। IW सभी परिचालन योजना का एक अभिन्न अंग है।

IW संगठन: भारतीय वायु सेना

IAF में भी, IW को शीर्ष स्तर पर संचालन शाखा से निपटा जाता है। इसके अलावा, EW और IW एक साथ एक शीर्ष द्वारा निपटाए जाते हैं। जबकि EW के संचालन के लिए पर्याप्त संसाधन उपलब्ध हैं, अब तक साइबर सुरक्षा के रूप में केवल रक्षात्मक IW ही फोकस का क्षेत्र है।

IW संगठन: भारतीय नौसेना

सहायक नौसेनाध्यक्ष IW और संचालन (ACNS IW & Ops) IW से संबंधित सभी मामलों को देखता है। नौसेना सिग्नल निदेशालय (DNS) EW के लिए जिम्मेदार है; नौसेना खुफिया निदेशालय (DNI) और IW संयुक्त रूप से मनोवैज्ञानिक संचालन से संबंधित मामलों को संबोधित करते हैं। एक समान संरचना कमांड मुख्यालय में मौजूद है, जहां एक स्टाफ अधिकारी फ्लैग ऑफिसर-इन-कमांड को IW इनपुट प्रदान करता है।

निष्कर्ष

राष्ट्रीय स्तर पर और भारतीय सशस्त्र बलों में वर्तमान संगठनात्मक संरचना IW की चुनौतियों का सामना करने के लिए आ रही है। समय की मांग IW रणनीतियों का जमीनी स्तर पर कार्यान्वयन और विभिन्न सरकारी एजेंसियों और सेवाओं के बीच अधिक समन्वय है। IW के लिए दृष्टिकोण सूचना संचालन पर आधारित होना चाहिए जो मुख्य रूप से संगठनात्मक सीमाओं को काटकर सभी स्तरों पर एक साथ कार्यान्वयन की तलाश करता है।

साइबर सुरक्षा और सुविचारित आक्रामक IW के क्षेत्र में हमारे प्रसिद्ध आईटी क्षेत्र की क्षमताओं का उपयोग करने की आवश्यकता है। जबकि हमारे नेटवर्क को साइबर हमलों से बचाने के लिए ध्यान दिया जा रहा है, ऐसा लगता है कि हैकर युद्ध जैसी आक्रामक क्षमताओं की उपेक्षा की जा रही है। अब जबकि उच्च स्तर पर IW संगठनात्मक संरचना जगह में है, निष्पादन और कार्यान्वयन स्तर पर अत्याधुनिक क्षमताओं के निर्माण पर ध्यान केंद्रित करना चाहिए।

सूचना संचालन की अवधारणाओं को भारत में लागू नहीं किया गया है। प्रभावी IW के लिए सरकारी एजेंसियों, सेना के साथ-साथ विशाल नागरिक बुनियादी ढांचे का समन्वय किया जाना चाहिए। भारत के पास दुनिया

का सबसे बड़ा तकनीकी रूप से जानकार जनशक्ति पूल है। फिर भी राष्ट्र ने इस क्षेत्र में अपनी ताकत बनाने के लिए सामूहिक क्षमताओं का लाभ नहीं उठाया है। अगर सरकार आईओ रक्षात्मक और आक्रामक क्षमताओं के लिए मजबूत उपकरणों और विधियों के विकास को वित्तपोषित करती है, तो भारत सबसे मजबूत शक्ति के रूप में उभर सकता है।

आतंकवाद के खिलाफ भी खुफिया जानकारी साझा करने के मामलों में केंद्र और राज्यों के बीच समन्वय की कमी ने आतंकवादियों को हमारे शहरों में अपनी मर्जी से हमला करने में सक्षम बनाया है। यदि IW के पूरे विषय को राष्ट्रीय स्तर पर समन्वित तरीके से निपटाया जाए, तो भारत हमारी राष्ट्रीय सुरक्षा की चुनौतियों से पार पा सकता है।

संदर्भ

लेह आर्मस्ट्रांग, सूचना संचालन, युद्ध और सॉफ्ट पावर की कठोर वास्तविकता, पोटोमैक बुक्स, वाशिंगटन डीसी, 2004, URL: https://books.google.co.in/books?isbn=1597973556

राष्ट्रीय सुरक्षा परिषद संगठन URL: http:www.whitehouse.gov/wh/eop/nsc

जॉन लस्कर, यू.एस. मिलिट्री का एलीट हैकर क्रू, 18 अप्रैल, 2005, वायर्ड न्यूज, URL: http://www.wired.com/news/privacy/0,67223-0.html?tw=wn_story_page_prev2.

रूसी 2010 सैन्य सिद्धांत, कार्नेगी URL: http://carnegieendowment.org/files/2010russia_military_doctrine.pdf

कांग्रेस को वार्षिक रिपोर्ट, 'पीआरसी 2015 में सैन्य और सुरक्षा विकास', URL: http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf

मुख्यालय आईडीएस, URL: http://ids.nic.in/organisation.htm

एस. पी. रस्तोगुएव, सूचनात्मक आवाज [सूचना युद्ध], (मास्को: रेडियो और संचार, 1998) I