International Journal of Education and Science Research Review
E-ISSN 2348-6457
Volume-10, Issue-5 Sep - Oct – 2023
P-ISSN 2349-1817
www.ijesrr.org
Email- editor@ijesrr.org

साइबर आतंकवाद

कृष्णकांत वरुण कुमार
(LL.B, LL.M., Research Scholar, the Department of Law, University of Allahabad)

डॉ मुक्ता वर्मा
(Assistant Professor, the Department of Law, University of Allahabad)

सारांश

यह लेख साइबर आतंकवाद की उभरती घटना पर ध्यान केंद्रित करते हुए डिजिटल युग के संदर्भ में आतंकवाद के विकास की पड़ताल करता है। 21वीं सदी के आगमन के साथ, द्वेषपूर्ण इरादे के साथ तकनीकी प्रगति के संगम ने आतंक की एक नई नस्ल को जन्म दिया है, जो पारंपरिक भौतिक सीमाओं को पार कर साइबरस्पेस के दायरे में प्रवेश कर रही है। आतंकवाद और प्रौद्योगिकी के बीच जटिल अंतरसंबंध की जांच की गई है, जो डिजिटल नेटवर्क के साथ गहराई से जुड़ी हुई दुनिया की कमजोरियों को उजागर करता है। साइबर आतंकवाद को परिभाषित करने और समझने की चुनौतियों से लेकर इसके संभावित वैश्विक निहितार्थों तक, यह लेख इस समकालीन खतरे से जुड़ी जटिलताओं का व्यापक अवलोकन प्रदान करना चाहता है। यह चर्चा इन उभरती चुनौतियों के खिलाफ हमारे आपस में जुड़े डिजिटल और भौतिक भविष्य की सुरक्षा के लिए वैश्विक सहयोग, सतर्कता और सक्रिय उपायों की तत्काल आवश्यकता पर जोर देती है।

मुख्य शब्द

साइबर आतंकवाद, डिजिटल कमजोरियाँ, प्रौद्योगिकी प्रगति, वैश्विक अंतर्संबंध, साइबर सुरक्षा उपाय

परिचय

अभूतपूर्व तकनीकी प्रगति के युग में, जहां कनेक्टिविटी और डिजिटलीकरण हमारे जीवन के हर पहलू पर राज करता है, एक नया खतरा छाया से उभरता है, जो हमारे डिजिटल दुनिया के ताने-बाने के साथ जुड़ जाता है। जो ख़तरा कभी भौतिक क्षेत्र में छिपा था, अब वह रूप धारण कर रहा है और अपनी खतरनाक पहुंच को आभासी स्थान तक फैला रहा है, जिससे सुरक्षा और रक्षा का परिदृश्य बदल रहा है। यह खतरा, जिसे साइबर आतंकवाद के रूप में जाना जाता है, 21वीं सदी में प्रवेश करते समय दुनिया के सामने आने वाली दो अलग लेकिन भयानक चुनौतियों के संलयन का प्रतीक है: आतंकवाद का सर्वव्यापी खतरा और साइबर डोमेन की जटिलताएँ।

ऐतिहासिक रूप से, आतंकवाद में बमबारी, अपहरण और अपहरण की छवियां शामिल थीं। हालाँकि, जैसे-जैसे दुनिया प्रौद्योगिकी पर अधिक निर्भर होती गई, अराजकता और व्यवधान का एक नया रास्ता स्पष्ट हो गया। अब, केवल कुछ कीस्ट्रोक्स के साथ, द्वेषपूर्ण अभिनेता अर्थव्यवस्थाओं को पंगु बना सकते हैं, आवश्यक सेवाओं को बाधित कर सकते हैं, या धारणाओं में हेरफेर कर सकते हैं। आतंकवाद के इस रूप को विशेष रूप से डरावना बनाने वाली बात इसकी सीमाओं को सहजता से पार करने की क्षमता, इसकी गुमनामी और पारंपरिक भौतिक उपस्थिति के बिना बड़े पैमाने पर तबाही मचाने की इसकी क्षमता है।

जैसे-जैसे हमारी दुनिया अधिक एकीकृत होती जा रही है, देश संचार, बैंकिंग, परिवहन और बहुत कुछ के लिए जटिल नेटवर्क पर बहुत अधिक निर्भर हो गए हैं, इसने अनजाने में इन साइबर आतंकवादियों के लिए कमजोरियों का फायदा उठाने का द्वार खोल दिया है। महत्वपूर्ण बुनियादी ढांचे को प्रभावित करने से लेकर वैश्विक संचार प्रणालियों में संभावित हेरफेर तक, जो उपकरण प्रगति और सुविधा के लिए बनाए गए थे, वे अब गलत व्यक्तियों के हाथों में सामूहिक विनाश के संभावित हथियारों में बदल गए हैं।

यह लेख साइबर आतंकवाद के विकास और जटिलताओं, इसकी उत्पत्ति, इसे परिभाषित करने में आने वाली चुनौतियों और नवाचार और सुरक्षा के चौराहे पर खड़ी दुनिया के लिए इसके निहितार्थों की पड़ताल करता है। इस अन्वेषण के माध्यम से, हम इस डिजिटल खतरे की गहराई को उजागर करेंगे और वैश्विक स्थिरता और व्यवस्था पर इसके संभावित प्रभाव को समझेंगे।

अपराधी और डाकू अपनी अवैध गतिविधियों को अंजाम देने के लिए प्रौद्योगिकी का उपयोग करने में विशेषज्ञ बन गए हैं। कई वर्षों से समाज को त्रस्त करने वाली आतंकवाद की महामारी से निपटने के लिए चल रहे संघर्ष के बावजूद, साइबरस्पेस

के दायरे में इस खतरे के विलय ने इसके संभावित खतरों को बढ़ा दिया है और इसके खतरे के स्तर को बढ़ा दिया है। विशेष रूप से, हमारी आधुनिक दुनिया के आवश्यक घटक जैसे महत्वपूर्ण बुनियादी ढाँचा, बड़े पैमाने पर राष्ट्र, वैश्विक संचार प्रणालियाँ, व्यापक बैंकिंग नेटवर्क और यहां तक कि विमानन और खुफिया प्रणालियाँ इन दुर्भावनापूर्ण ताकतों के प्रति संवेदनशील हो गए हैं, जिससे वे असुरक्षित और उजागर हो गए हैं।

साइबर आतंकवाद

साइबर आतंकवाद, आतंक की नवीनतम अभिव्यक्ति, गुप्त और अशुभ बादलों में डूबा हुआ है,[1] और कहा जाता है कि आतंकवाद की एक नई नस्ल बढ़ रही है।[2] इस अवधारणा में साइबर और आतंकवाद का मिश्रण शामिल है, जो व्यक्तिगत रूप से 20वीं सदी के अंत में उभरे दो सबसे भयावह खतरों का प्रतिनिधित्व करता है। ये दोनों तत्व अपरिचित के डर में निहित भय की भावना पैदा करते हैं। अप्रत्याशित और आक्रामक कृत्यों की आशंका कंप्यूटर प्रौद्योगिकी में प्रगति को लेकर व्यापक संदेह और स्पष्ट आतंक के साथ सहज रूप से मेल खाती है।[3] आतंकवाद एक व्यापक मुद्दा बन गया है जिसने मानवता को गहराई से प्रभावित किया है, खासकर प्रौद्योगिकी में प्रगति के साथ। इस संयोजन से समाज के लिए एक अत्यंत खतरनाक खतरा उत्पन्न हो गया है। विशेष रूप से, साइबर आतंकवाद की अवधारणा इस मुद्दे के साथ जटिल रूप से जुड़ी हुई है, और इसे सार्वभौमिक रूप से स्वीकार्य तरीके से सटीक रूप से परिभाषित करने का प्रयास इसकी जटिल और मायावी प्रकृति के कारण एक महत्वपूर्ण चुनौती है।

"साइबर" शब्द साइबरनेटिक्स के क्षेत्र से लिया गया है, जिसमें संचार और नियंत्रण प्रणालियों का अध्ययन शामिल है। दूसरी ओर, "आतंकवाद" का तात्पर्य राजनीतिक या वैचारिक लक्ष्यों को प्राप्त करने के लिए हिंसा और धमकी का उपयोग करना है। इन दो शब्दों के बीच संबंध साइबर आतंकवाद की अवधारणा में निहित है, जिसमें हिंसा के कृत्यों को अंजाम देने या नुकसान पहुंचाने के लिए डिजिटल उपकरणों और रणनीति का उपयोग शामिल है। हालाँकि, साइबर आतंकवाद की परिभाषा को लेकर एक निश्चित स्तर की अस्पष्टता मौजूद है, जिससे अलग-अलग व्याख्याएं और दृष्टिकोण सामने आते हैं कि किन कार्यों को इस तरह वर्गीकृत किया जा सकता है। इस विसंगति का उदाहरण डोरोथी डेनिंग के अवलोकन से मिलता है कि एक एकल कार्य, जैसे कि ईमेल, को कुछ व्यक्तियों द्वारा हैकटिविज्म माना जा सकता है जबकि अन्य द्वारा इसे साइबर

[1] वी.के. गेरा, "साइबर आतंकवाद: आतंक का सबसे नया चेहरा", वरिंदर ग्रोवर, अंतर्राष्ट्रीय आतंकवाद का विश्वकोश, खंड 2, 66।
[2] वॉन हर्बरस्टीन, "साइबरटेरर अटैक रॉक्स अमेरिका" इंडिपेंडेंट 5-3-98, 1, <http://www.infosec.com/denial/denial_last 030498 ए.html> अंतिम बार 7-20-2000 तक पहुंचा।
[3] पॉलिट, "साइबर आतंकवाद: तथ्य या फैंसी?" एफबीआई प्रयोगशाला, <http://www.cs.georgetown/edu/ denning/infosec/pollitt.html> अंतिम बार 15-4-2005 को एक्सेस किया गया था।

आतंकवाद के रूप में लेबल किया जा सकता है। ये अलग-अलग दृष्टिकोण साइबर आतंकवाद को प्रभावी ढंग से संबोधित करने और मुकाबला करने से जुड़ी जटिलता और चुनौतियों में योगदान करते हैं।[4]

शब्द "साइबर आतंकवाद" पहली बार 1997 में बैरी कॉलिन द्वारा प्रस्तुत और परिभाषित किया गया था। कॉलिन ने इसे साइबरनेटिक्स और आतंकवाद के विलय के रूप में वर्णित किया, जो इन दो क्षेत्रों के प्रतिच्छेदन को दर्शाता है। [5] यह वाक्यांश अब व्यापक रूप से उपयोग किया जाने लगा है और इसकी व्याख्या "कमजोर लक्ष्यों के खिलाफ तोड़फोड़ के कृत्यों में संलग्न कंप्यूटर" के रूप में भी की जा सकती है, जिससे कंप्यूटर प्रौद्योगिकी पर हमारे अत्यधिक निर्भर समाज के लिए विनाशकारी परिणाम हो सकते हैं।[6] साइबर आतंकवाद के दायरे में, आतंकवादी एक अत्यधिक सुलभ और सुरक्षित रास्ता खोजते हैं जिसके लिए न्यूनतम निवेश की आवश्यकता होती है। उनकी अंतर्निहित प्रेरणाओं के बावजूद, चाहे वह राजनीतिक या आर्थिक कारकों से प्रेरित हो, आतंकवादी स्वाभाविक रूप से भय पैदा करने के लिए प्रेरित होते हैं, और "आतंकवाद" शब्द का मात्र उल्लेख व्यापक विनाश, पीड़ा और निर्दोष व्यक्तियों की निरंतर दुर्दशा की भयावह कल्पना को उजागर करता है।

साइबर आतंकवाद की सबसे व्यापक और व्यापक रूप से स्वीकृत परिभाषाओं में से एक संघीय जांच ब्यूरो (एफबीआई) द्वारा प्रदान की गई है, जो इस क्षेत्र में एक प्रसिद्ध प्राधिकरण है। एफबीआई के अनुसार, साइबर आतंकवाद को इस प्रकार परिभाषित किया जा सकता है।

सूचना, कंप्यूटर सिस्टम, कंप्यूटर प्रोग्राम और डेटा को लक्षित करने वाली पूर्व-निर्धारित और राजनीति से प्रेरित आक्रामकताएं अंततः गुप्त कार्यकर्ताओं और उप-राष्ट्रीय संगठनों द्वारा नागरिकों के खिलाफ हिंसक कार्रवाइयों का कारण बनती हैं।[7]

साइबर आतंकवाद का तात्पर्य राजनीतिक उद्देश्यों वाले गुप्त व्यक्तियों या समूहों द्वारा जानबूझकर कंप्यूटर का उपयोग करना है। उनका उद्देश्य दर्शकों या सरकार पर दबाव डालकर उन्हें अपने आदेश या नीतियों को बदलने के लिए मजबूर करना है। परिभाषा को यह देखते हुए बढ़ाया जा सकता है कि सूचना युद्ध के लिए रक्षा विभाग (डीओडी) के संचालन[8] में कंप्यूटर सुविधाओं और ट्रांसमिशन लाइनों पर शारीरिक हमले भी शामिल हैं। फिर भी, यह ध्यान रखना महत्वपूर्ण है कि

[4] डोरोथी डेनिंग, "एक्टिविज्म, हैक्टिविज्म और साइबर आतंकवाद: विदेश नीति को प्रभावित करने के लिए एक उपकरण के रूप में इंटर्नट", <http://www.nautilis.org/info-policy/work shop/papers/denning.html> 6-7-2000 को एक्सेस किया गया।
[5] बैरी सी कोलिन, "साइबर आतंकवाद का भविष्य"। आपराधिक न्याय के मुद्दों पर 11 वीं वार्षिक अंतर्राष्ट्रीय संगोष्ठी की कार्यवाही।
[6] डेव पेटिनारी, "साइबर आतंकवाद, सूचना युद्ध और हमले अभी और भविष्य में अमेरिका के गढ़ में शुरू किए जा रहे हैं", पुलिस फ्यूचरिस्ट इंटरनेशनल ने <http://policefuturists.org/fall97/terror.html। अंतिम बार 6-2-2000 को एक्सेस किया गया।
[7] "साइबर आतंकवाद: आतंकवाद का नया प्रकार", सीसीआरसी (8-4-2004)।
[8] क्ले विल्सन - सूचना युद्ध और साइबर युद्ध: क्षमताएं और संबंधित नीतिगत मुद्दे : (सीआरएस) रिपोर्ट आरएल (14-3-2003)

कंप्यूटर हमले और साइबर आतंकवाद दो अलग-अलग संस्थाएं हैं, इस तथ्य के बावजूद कि कुछ कंप्यूटर हमले अपनी विनाशकारी और विघटनकारी प्रकृति के माध्यम से पीड़ित पर आतंक फैलाने की क्षमता रखते हैं। आतंकित करने की इस क्षमता को अक्सर इसके प्रभाव की गंभीरता से मापा जाता है, जिसके परिणामस्वरूप संभावित रूप से घातक परिणाम, शारीरिक क्षति, लंबे समय तक बिजली की विफलता, विमानन दुर्घटनाएं, आग, संदूषण या यहां तक कि महत्वपूर्ण आर्थिक मंदी हो सकती है। ऐसे चरम मामलों में, इन कृत्यों को उचित रूप से साइबर आतंकवाद के उदाहरणों के रूप में वर्गीकृत किया जा सकता है।[9]

साइबर आतंकवादियों की छिपी और अज्ञात रहने की क्षमता उनके लिए सबसे बड़ी बाधा और सबसे महत्वपूर्ण लाभ दोनों प्रस्तुत करती है। आतंकवाद के पारंपरिक रूपों के विपरीत, जिसमें सीमा पार करना, तस्करी करना और बम लगाना, बंधकों का अपहरण करना या जीवन का बलिदान देना जैसे शारीरिक कृत्यों की आवश्यकता होती है, आधुनिक आतंकवादी केवल कीबोर्ड का उपयोग करके अधिक प्रभाव प्राप्त कर सकता है। साइबर[10] आतंकवाद मुख्य रूप से किसी देश के राष्ट्रीय बुनियादी ढांचे को लक्षित करता है और साइबर आतंकवादियों में परमाणु रिएक्टरों जैसे विभिन्न महत्वपूर्ण बुनियादी ढांचे पर नियंत्रण हासिल करने की तीव्र इच्छा होती है, जिनमें हेरफेर किए जाने पर विनाशकारी परिणामों की अपार संभावना होती है। वे गैस और तेल जैसे रणनीतिक कच्चे माल के प्रमुख भंडारण प्रणालियों के साथ-साथ जल आपूर्ति, बिजली वितरण, यातायात केंद्रों और यहां तक कि गोपनीय संचार नेटवर्क के लिए जिम्मेदार महत्वपूर्ण प्रणालियों में भी हेरफेर करना चाहते हैं।

तकनीक

इंटरनेट आतंकवादियों को विशेष अवसर देता है।[11] तकनीकी दृष्टिकोण से, साइबर आतंकवादियों के पास वर्तमान में इंटरनेट के उपयोग के माध्यम से पूरे देश में प्रभावी ढंग से भय पैदा करने और आतंकित करने के लिए आवश्यक स्तर की शक्ति नहीं है। वर्तमान में, आतंकवादी समूहों के पास महत्वपूर्ण प्रभाव पैदा करने वाले पर्याप्त अभियानों को अंजाम देने की क्षमता नहीं है। यह मुख्य रूप से इस तथ्य के कारण है कि साइबर हमले, हालांकि वे व्यवधान और क्षति का कारण बन सकते हैं, आतंक और रक्तपात की भावना पैदा करने में विफल रहते हैं जो किसी भी आतंकवादी एजेंडे का अंतिम उद्देश्य है। वास्तव में, मई 2000 में पेरिस में आयोजित एक आतंकवाद-केंद्रित सम्मेलन के दौरान, उपस्थित लोगों ने यह विश्वास व्यक्त किया कि आतंकवादी संगठन अपने द्वेषपूर्ण इरादों को आगे बढ़ाने के साधन के रूप में प्रौद्योगिकी का उपयोग करने की अत्यधिक

[9] डोरोथी डेनिंग, "क्या साइबर युद्ध अगला है?" नवंबर 2001, सामाजिक विज्ञान अनुसंधान परिषद, <http://www.ssrc.org/setp11/essays/denning.htm>
[10] सुप्रा, एन।
[11] माइकल विन, "साइबरस्पेस: चरमपंथियों द्वारा संचार, कमान और नियंत्रण के लिए एक नया माध्यम", <http://www.ict.org.il/>

संभावना नहीं रखते थे।[12] इसके अतिरिक्त, ऐसी रिपोर्टें हैं जो दर्शाती हैं कि अल-कायदा के जब्त किए गए अधिकांश दस्तावेज़ या तो एन्क्रिप्शन से रहित हैं या उनमें अपर्याप्त एन्क्रिप्शन उपाय हैं। इसके अलावा, यह कहा गया है कि ओसामा बिन लादेन ने संगठन की गोपनीयता बढ़ाने और तकनीकी प्रगति का प्रभावी ढंग से उपयोग करने के लिए उपाय लागू किए हैं।[13] हाल के दिनों में, आतंकवादियों की गतिविधियों में एक चिंताजनक प्रवृत्ति देखी गई है, क्योंकि वे अपने द्वेषपूर्ण इरादों को सुव्यवस्थित करने और अपने शारीरिक हमलों के प्रभाव को बढ़ाने के उद्देश्य से अपनी भयावह योजनाओं में उत्तरोत्तर प्रौद्योगिकी को शामिल कर रहे हैं। नवीन उपकरणों और तकनीकों को धीरे-धीरे लेकिन लगातार अपनाना चिंताजनक रूप से स्पष्ट होता जा रहा है। यह पता चला है कि अल-कायदा जैसे कुख्यात संगठनों ने अपने सदस्यों के कंप्यूटरों को जब्त कर लिया है और उनकी जांच की है, जिससे एक चौंकाने वाली बात सामने आई है: ये आतंकवादी सक्रिय रूप से हैकर उपकरणों की एक विस्तृत श्रृंखला से खुद को परिचित कर रहे हैं, जिन तक आसानी से पहुंचा जा सकता है। इंटरनेट का विस्तार. यह रहस्योद्घाटन आतंकवाद के उभरते परिदृश्य की मार्मिक याद दिलाता है, जिसमें अपराधी न केवल पारंपरिक तरीकों का सहारा ले रहे हैं, बल्कि अपने विनाशकारी उद्देश्यों को आगे बढ़ाने के लिए प्रौद्योगिकी की शक्ति का भी उपयोग कर रहे हैं।[14] यह सुनिश्चित करने के लिए कि उनकी योजनाएँ अज्ञात रहें, ये आतंकवादी नकली साइबर हमलों के प्रारंभिक परीक्षण करते हैं जिन्हें उन्होंने स्वयं तैयार किया है। यह सुविचारित कदम उनके प्रारंभिक प्रयासों से उत्पन्न होने वाले किसी भी संदेह से बचने के लिए एहतियाती उपाय के रूप में कार्य करता है।

अल-कायदा और विभिन्न आतंकवादी संगठन अपने सदस्यों के बीच निर्बाध संचार की सुविधा, हमलों की रणनीति बनाने, वित्तीय सहायता उत्पन्न करने और अपने वैचारिक प्रचार को प्रसारित करने के लिए एन्क्रिप्शन सॉफ्टवेयर जैसी अत्याधुनिक तकनीक का उपयोग करके इंटरनेट की विशाल क्षमता का प्रभावी ढंग से दोहन करते हैं। [15] उपलब्ध साक्ष्यों के अनुसार, यह सुझाव दिया गया है कि 11 सितंबर 2001 के कुख्यात हमलों का नेतृत्व करने वाले व्यक्ति मोहम्मद अत्ता ने अपने हवाई आरक्षण टिकट बनाने के लिए ऑनलाइन प्लेटफ़ॉर्म की सुविधा का उपयोग किया था। इसके अतिरिक्त, यह भी पता चला है कि अल-कायदा आतंकवादी संगठन के विभिन्न सदस्य विदेशों में स्थित अन्य कोशिकाओं के साथ संचार चैनल स्थापित करने के लिए इंटरनेट-आधारित टेलीफोन सेवाओं पर भी निर्भर थे। इसके अलावा, यह बताया गया है कि वर्ल्ड ट्रेड सेंटर पर सावधानीपूर्वक सुनियोजित हमलों के पीछे के मास्टरमाइंड खालिद शेख मोहम्मद ने दुखद घटनाओं में शामिल कम से कम

[12] डेविड टकर, "सशस्त्र प्रतिरोध साइबर आतंक का भविष्य? बड़े पैमाने पर विनाश?" सितंबर 2000, विश्वविद्यालय पैंथियॉन-असस, पेरिस में आयोजित सम्मेलन पर रिपोर्ट, 15 से 17 मई, 2000, <http://www.nps.navy.mil/ctiw/files/substate संघर्ष गतिशीलता पीडीएफ>।

[13] डेविड कपलान, "खेल अपराध: द इनसाइड स्टोरी ऑफ यूएस टेररिस्ट हंटर्स अलकायदा के पीछे कैसे जा रहे हैं". 2-6-2003, यूएस न्यूज एंड वर्ड रिपोर्ट, 19-29।

[14] रिचर्ड क्लार्क, "भेद्यता: अल-कायदा की क्षमताएं क्या हैं?", अप्रैल 2003, पीबीएस फ्रॉंटिलाइन: साइबरवार, <http://www.pbs.org>।

[15] साइबर आतंकवाद, <http://www.terrokrismanswers.com/terrorism> अंतिम बार 9-3-2005 को एक्सेस किया गया था।

दो एयरलाइन अपहर्ताओं के साथ बातचीत करने के साधन के रूप में इंटरनेट चैट सॉफ़्टवेयर का उपयोग किया था। ये उदाहरण इस बात के उल्लेखनीय उदाहरण हैं कि कैसे आधुनिक तकनीक और इंटरनेट ने आतंकवाद के इन जघन्य कृत्यों की योजना और कार्यान्वयन को सुविधाजनक बनाने में महत्वपूर्ण भूमिका निभाई।[16] वैश्विक स्तर पर आतंकवादी संगठन अपने घृणित कृत्यों को अंजाम देने के लिए पहले से ही अत्याधुनिक तकनीकी रणनीतियों की ओर रुख कर चुके हैं। उदाहरण के लिए, रामजी यूसुफ, जिसे वर्ल्ड ट्रेड सेंटर बमबारी में शामिल होने के लिए आजीवन कारावास की सजा मिली थी, कथित तौर पर एक इलेक्ट्रिकल इंजीनियर के कौशल से लैस था और उसने अमेरिकी एयरलाइंस को लक्षित करने वाले विस्फोटक घटकों के रूप में अप्रचलित इलेक्ट्रॉनिक उपकरणों का उपयोग करने की योजना तैयार की थी। उसने न केवल सावधानीपूर्वक इस हमले की रणनीति बनाई, बल्कि उसने अपने डेटा की सुरक्षा के लिए जटिल एन्क्रिप्शन तरीकों को भी लागू किया और कानून प्रवर्तन एजेंसियों द्वारा उसके भयावह इरादों को समझने के किसी भी प्रयास को बाधित किया।[17] आभासी दुनिया आतंकवादियों के लिए स्वर्ग बन गई है, जो उन्हें एक विशाल और स्वागत योग्य खेल का मैदान प्रदान करती है जहां वे आसानी से नज़रों से दूर रहते हुए अपनी दुर्भावनापूर्ण गतिविधियों में संलग्न हो सकते हैं। अतीत में, आतंकवादियों ने बमबारी जैसी हिंसात्मक गतिविधियों के जरिए मुख्य रूप से महत्वपूर्ण बुनियादी ढांचे, सरकारी कंप्यूटर सिस्टम और टेलीफोन नेटवर्क जैसे भौतिक स्थानों को निशाना बनाया था। हालाँकि, भौतिक और आभासी क्षेत्रों के बढ़ते अभिसरण के साथ, आतंकवादी गतिविधियों की प्रकृति में काफी विकास हुआ है। आजकल, आतंकवादी कई प्रकार की गुप्त कार्रवाइयों को अंजाम देने की क्षमता रखते हैं जिनके विनाशकारी परिणाम हो सकते हैं, वह भी छिपे हुए और अज्ञात रहते हुए। उदाहरण के लिए, वे अनाज में आयरन के स्तर में हेरफेर कर सकते हैं, जिससे पूरे देश में अनगिनत शिशुओं और बच्चों की मृत्यु हो सकती है। इसके अतिरिक्त, वे अस्पतालों में दवाओं के नुस्खे के साथ छेड़छाड़ भी कर सकते हैं, जिससे मरीजों की जान जोखिम में पड़ सकती है, [18] एक ऐसी शक्ति मौजूद है जो इतनी शक्तिशाली है कि इसमें असंख्य व्यक्तियों को अत्यधिक नुकसान पहुंचाने, गैस पाइपलाइनों के भीतर दबाव में हेरफेर करने, बांध के भीतर फ्लडगेट के खुलने और बंद होने को नियंत्रित करने के साथ-साथ आश्चर्यजनक 3,00,000 वोल्ट बिजली का सामना करने की क्षमता है। जिसके परिणामस्वरूप मूल्यवान परिसंपत्तियों और संपत्तियों का संभावित विनाश हो सकता है।

ज़मीन पर उत्पन्न होने वाले संभावित जोखिमों के अलावा, साइबर आतंकवादियों के पास शारीरिक रूप से उड़ान भरने के खतरनाक कार्य में शामिल हुए बिना हवाई यातायात प्रणाली में हेरफेर करने की क्षमता होती है। सिस्टम में कमजोरियों का

[16] रॉबर्ट विंडरेम, "9/11 बंदी: अटैक स्केल्ड बैक", <http://www.msnbc.com/news/969759.asp> अंतिम बार 21-09-2003 को एक्सेस किया गया था।
[17] रॉबर्ट विंडरेम, "9/11 बंदी: हमला वापस किया गया", <http://www.msnbc.com/news/969759.asp> आखिरी बार 21-9-2003 को स्वीकार किया गया था।
[18] बैरी सी कोलिन, "साइबर आतंकवाद का भविष्य", सुरक्षा और खुफिया संस्थान, <Afgen.com/terrosisml.html> अंतिम बार 16-4-2005 को एक्सेस किया गया था।

फायदा उठाकर, वे संभावित रूप से नियंत्रण हासिल कर सकते हैं और इसे इस तरह से हेरफेर कर सकते हैं कि हवाई जहाज एक-दूसरे से टकराएं, जिससे जीवन की भयावह क्षति हो। हालाँकि, यह ध्यान रखना महत्वपूर्ण है कि यह परिप्रेक्ष्य विमान नियंत्रण में मानव ऑपरेटरों द्वारा निभाई गई महत्वपूर्ण भूमिका को नजरअंदाज करता है। मानवीय तत्व की उपेक्षा करके, साइबर आतंकवादियों को व्यापक अराजकता और तबाही मचाने के लिए एक सुरक्षित और लागत प्रभावी साधन प्रदान किया जाता है।

साइबर आतंकवाद से सामना

भय पैदा करने की इच्छा और प्रौद्योगिकी की तीव्र प्रगति के संगम के कारण, साइबर आतंकवाद एक जटिल और बहुआयामी समस्या बन गई है जिसे किसी एक समाधान के माध्यम से प्रभावी ढंग से संबोधित नहीं किया जा सकता है। इसलिए, इस खतरे से निपटने में सफल परिणाम प्राप्त करने के लिए एक व्यापक और बहुआयामी दृष्टिकोण अपनाना जरूरी है। अंतरराष्ट्रीय स्तर पर लागू किए गए विभिन्न जवाबी उपायों की जांच करते समय, उन्हें निम्नलिखित शीर्षकों के तहत वर्गीकृत और चर्चा की जा सकती है।

विधिक कार्रवाई

साइबर आतंकवाद में मुख्य रूप से संगठित अपराध सिंडिकेट, आपराधिक सिंडिकेट, साथ ही घरेलू और वैश्विक आपराधिक संस्थाओं की भागीदारी शामिल है। [19] लगभग हर देश के साइबर कानून में, कानूनी प्रणाली साइबर आतंकवादियों की आपराधिक जिम्मेदारी को स्वीकार करती है। 11 सितंबर, 2001 को हुई दुखद घटनाओं के बाद, यह सुनिश्चित करने के लिए कानून स्थापित किए गए कि आतंकवादी गतिविधियों को वित्तपोषित करने वालों को जवाबदेह ठहराया जाए। नतीजतन, दोषी पाए जाने पर, इन व्यक्तियों के धन को जब्त करने और उनकी संपत्ति को जब्त करने के उपाय लागू किए जाते हैं।

अफसोस की बात है कि किसी भी देश ने साइबर आतंकवाद के मुद्दे को प्रभावी ढंग से संबोधित करने के लिए एक समर्पित कानून नहीं बनाया है। हालाँकि, साइबर आतंकवादी गतिविधियों, जैसे हैकिंग और डिस्ट्रीब्यूटेड डिनायल ऑफ सर्विस (डीओएस) हमलों में शामिल व्यक्तियों की आपराधिक देनदारी के संबंध में देशों के बीच आम सहमति है। यह दृष्टिकोण,

[19] गोलुबेव, "कंप्यूटर आतंकवाद के लिए काउंटरएक्शन के संगठनात्मक कानूनी पहलू," उद्यमिता, राज्य, राज्य और कानून, कीव, 2004 वैज्ञानिक व्यावहारिक मैगजिंग, 121-124।

जिसका उद्देश्य साइबर आतंकवादियों को उनके द्वेषपूर्ण इरादों और कार्यों के लिए जिम्मेदार ठहराना है, को अंतर्राष्ट्रीय समुदाय में व्यापक रूप से मान्यता प्राप्त है और इसकी सराहना की जाती है।

भारत का दृष्टिकोण

अन्य देशों की तरह, भारत ने भी सूचना प्रौद्योगिकी और इंटरनेट के दुरुपयोग के साथ-साथ इंटरनेट बर्बरता की घटनाओं को संबोधित करने के लिए उपाय किए। इन मुद्दों से निपटने के लिए, भारत ने 2000 में आईटी अधिनियम पेश किया, जो विशेष रूप से साइबर अपराधों को लक्षित करने वाला देश का एकमात्र कानून था। हालाँकि, इस अधिनियम को लागू करने के अलावा, भारत ने कुछ पारंपरिक कानूनों में आवश्यक संशोधन भी किए ताकि यह सुनिश्चित किया जा सके कि वे डिजिटल युग में प्रासंगिक बने रहें। जबकि अधिनियम के प्रारंभिक संस्करण में मुख्य रूप से साइबर अपराधों और डेटा बर्बरता को संबोधित किया गया था, 2008 तक "साइबर आतंकवाद" की अवधारणा और इसके संबंधित पहलुओं को कानून में शामिल करने के लिए संशोधन नहीं किए गए थे।

सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 (2009 का 10) न केवल साइबर आतंकवाद की परिभाषा को शामिल करता है बल्कि इसमें कई धाराएं भी शामिल हैं जो इस प्रावधान से निकटता से संबंधित हैं। संशोधित अधिनियम के भीतर विभिन्न धाराओं को मिलाकर, इसका उद्देश्य साइबर आतंकवाद से उत्पन्न महत्वपूर्ण खतरे से निपटने और निपटने के लिए एक व्यापक और कुशल कानूनी ढांचा स्थापित करना है।

<u>अंतर्राष्ट्रीय प्रतिक्रिया</u>

अंतर्राष्ट्रीय स्तर पर इस बात पर व्यापक सहमति है कि कानूनी कमियाँ किसी हैकर के लिए सजा से बचने का साधन नहीं बननी चाहिए। [20] वैश्विक स्तर पर चल रहे साइबर आतंकवाद के मुद्दे को विभिन्न देशों में सुसंगत कानूनों की स्थापना और अंतर्राष्ट्रीय समुदाय के सहयोगात्मक प्रयास के बिना प्रभावी ढंग से संबोधित नहीं किया जा सकता है। जिस तरह क्षेत्रीय और वैश्विक स्तर पर संयुक्त प्रयासों और सहयोग के माध्यम से आतंकवाद से निपटा जा रहा है, उसी तरह साइबर आतंकवाद की रोकथाम और शमन तभी किया जा सकता है जब देश एकजुट हों और इस सामान्य लक्ष्य की दिशा में सक्रिय रूप से मिलकर काम करें।

[20] जॉनसन, "उचित प्रक्रिया और साइबर अधिकार क्षेत्र", साइबर लॉ इंस्टीट्यूट, <http://www.ascur.org/jeme/vol2/issues1/due.html>।

सरकार की प्रतिक्रिया

2 सितंबर 2001 की विनाशकारी घटनाओं के मद्देनजर, संयुक्त राज्य सरकार ने तेजी से और कुशलता से एक ऐसे समाज की स्थापना के लिए कार्रवाई की जो किसी भी प्रकार के आतंकवाद का सामना करने के लिए बेहतर ढंग से सुसज्जित हो। हालाँकि, इस दुखद घटना से पहले भी, सरकार ने पहले से ही आवश्यक बुनियादी ढांचे, विशेष रूप से पर्यवेक्षी नियंत्रण और डेटा अधिग्रहण (एससीएडीए) प्रणालियों की सुरक्षा के उद्देश्य से रणनीतियाँ पेश की थीं, जो पूरे देश में महत्वपूर्ण औद्योगिक प्रक्रियाओं की निगरानी के लिए जिम्मेदार हैं। यह सक्रिय दृष्टिकोण राष्ट्रीय सुरक्षा सुनिश्चित करने के लक्ष्य के साथ लागू किया गया था। संयुक्त राज्य अमेरिका की अत्यधिक परस्पर जुड़ी और अभिसरण प्रकृति को देखते हुए, यह साइबर आतंकवाद के प्रति काफी संवेदनशील है, जो इसे ऐसे हमलों के लिए एक आकर्षक लक्ष्य बनाता है। नतीजतन, अमेरिकी सरकार ने अन्य देशों की तुलना में सबसे मजबूत और व्यापक प्रतिक्रिया उपाय लागू किए हैं। [21]

निष्कर्ष

जैसा कि हमने साइबर आतंकवाद की बहुमुखी दुनिया की यात्रा की है, यह स्पष्ट हो जाता है कि प्रौद्योगिकी और द्वेषपूर्ण इरादे का अभिसरण हमारे समय की सबसे महत्वपूर्ण चुनौतियों में से एक प्रस्तुत करता है। डिजिटल डोमेन, जिसने अद्वितीय प्रगति और वैश्विक अंतर्संबंध लाया है, विरोधाभासी रूप से वैचारिक युद्ध, राजनीतिक जोड़-तोड़ और बड़े पैमाने पर व्यवधान के लिए एक संभावित युद्धक्षेत्र के रूप में भी खड़ा है।

साइबर आतंकवाद की अस्पष्ट प्रकृति, इसकी लगातार विकसित हो रही कार्यप्रणाली के साथ मिलकर एक सक्रिय, गतिशील और विश्व स्तर पर समन्वित प्रतिक्रिया की आवश्यकता बनाती है। हमारे डिजिटल भविष्य की सुरक्षा करना केवल व्यक्तिगत राष्ट्रों की जिम्मेदारी नहीं है, बल्कि अंतर्राष्ट्रीय समुदाय का सामूहिक कर्तव्य है। परिभाषाओं का मानकीकरण करना, खुफिया जानकारी साझा करना और साइबर सुरक्षा को मजबूत करना वैश्विक आतंकवाद विरोधी पहल में सबसे आगे होना चाहिए।

इसके अलावा, जैसे-जैसे प्रौद्योगिकी आगे बढ़ती है, वैसे-वैसे उन लोगों के तरीकों में भी बदलाव आएगा जो इसका दुरुपयोग करना चाहते हैं। सरकारों, निजी क्षेत्रों और नागरिकों के लिए ऐसे खतरों के सामने सतर्क, शिक्षित और लचीला रहना

[21] एस वेंकटेश, साइबर आतंकवाद में "साइबर आतंकवाद का नियंत्रण"। (ऑथर्सप्रेस, नई दिल्ली 2003) 277.

अनिवार्य है। साइबर सुरक्षा में निवेश करना, डिजिटल साक्षरता को बढ़ावा देना और अंतर्राष्ट्रीय सहयोग को बढ़ावा देना इस प्रयास में महत्वपूर्ण है।

इस डिजिटल युग में, आतंक के खिलाफ लड़ाई अब भौगोलिक सीमाओं या भौतिक संस्थाओं तक ही सीमित नहीं है। यह सुरक्षा और युद्ध की हमारी पारंपरिक समझ को चुनौती देते हुए साइबरस्पेस के विशाल विस्तार तक फैला हुआ है। जैसा कि हम एक नए युग की शुरुआत पर खड़े हैं, हमें साइबर आतंकवाद के खिलाफ अपने प्रयासों में एकजुट होना चाहिए, यह समझते हुए कि हमारी डिजिटल दुनिया का संरक्षण हमारी भौतिक दुनिया की स्थिरता और समृद्धि के लिए अंतर्निहित है।