इजराइल की साइबर सुरक्षा संरचनाः विशेष अध्ययन

डॉ. जतिन कुमार
शोधकर्ता
मनोहर पर्रीकर इंस्टिट्यूट ऑफ डिफेन्स स्टडीज एंड एनालिसिस, नई दिल्ली

गुंचा प्रकाश
स्वतंत्र शोधकर्ता
लोक नीति और भू-अर्थशास्त्र,
यूनाइटेड किंगडम के वारविक विश्वविद्यालय से अर्थशास्त्र में स्नातकोत्तर

आधुनिक समय में युद्ध केवल सीमा पर होने वाले टकरावों एवं परम्परागत टकरावों तक ही सीमित नहीं हैं। वर्तमान समय में राज्य तथा गैर–राज्य अभिकर्ताओं ने साइबर स्पेस का जमकर दोहन करना शुरू कर दिया हैं, जो कि विशेष रूप से गुप्त और असीमित रूप से उपलब्ध होने की वजह से दुश्मन राज्य को व्यापक स्तर पर नुकसान पहुंचाने में सक्षम हैं। आज देश अपने तकनीकी ज्ञान को उन्नत करने के लिए प्रतिस्पर्धा कर रहे हैं और अपने हितों को पूरा करने के लिए दुश्मनों देशों को आधी–अधूरी तथा गलत जानकारी प्रदान करने के लिए साइबर स्पेस का भरपूर उपयोग कर रहे हैं। पिछले कुछ वर्षों में कई देशों में चुनावों के परिणामों को निर्धारित करने के लिए दूसरे देशों के कथित हस्तक्षेप को व्यापक रूप से देखा गया हैं। इस बात में बिलकुल भी संदेह नहीं हैं की वर्तमान समय में साइबर युद्ध ने, जो कि "न्यूनतम हस्तक्षेप, अधिकतम क्षति" के सिद्धांत का पालन करता हैं, अंतरराष्ट्रीय समुदाय की असुरक्षाओं को और बढ़ा दिया हैं। साथ ही इसने एक ऐसा वातावरण भी बनाया हैं, जिसमें एक देश दूसरे देश को अधिकतम नुकसान पहुंचाने के लिए अपनी साइबर तकनीक को लगातार उन्नत करने में लगे हुए हैं।

एक ऐसे दौर में जहाँ साइबर सुरक्षा देशों की राष्ट्रीय सुरक्षा में एक बड़ी चुनौती के रूप में उभरी हैं, एक देश ऐसा भी हैं जिसने अपने आप को साइबर सुरक्षा व तकनीक के क्षेत्र में एक प्रमुख अभिनेता के रूप में स्थापित किया हैं और वो देश हैं, इजरायल। यह इस तथ्य में स्पष्ट दिखाई देता हैं कि कोविड 19 संकट के बावजूद, इजरायल के साइबर उद्योग ने 2020 में सकारात्मक वृद्धि की हैं, इसने पिछले वर्ष की तुलना में 100 से अधिक सौदों से जुटाई गई राशि में 70 प्रतिशत की वृद्धि (एक रिकॉर्ड अमेरिकी डॉलर 2.9 बिलियन) की हैं।[i] साथ ही एक मजबूत साइबर संरचना को विकसित किया हैं। इस क्षेत्र में इजराइल की प्रगति वास्तव में आजादी के बाद से पैदा हुई असुरक्षा का परिणाम हैं जिसने समय–समय पर इजराइल के अस्तित्व पर खतरा पैदा किया हैं। वास्तव में इजराइल चारों ओर से अरब राष्ट्रों द्वारा घिरा हुआ है, साथ ही 1948 के बाद से ही इसे अपने पड़ोसी देशों के द्वारा सैन्य विवादों को झेलना पड़ा है। इजराइल ने शांति संधि पर हस्ताक्षर जरूर किये हैं पर उनके साथ रिश्तों को भी "शीत शांति" के रूप में देखा जा सकता हैं। अरब देशों की तुलना में इजराइल के सीमित मानव संसाधन (लगभग 9 मिलियन), यहूदी देश की असुरक्षा में और इजाफा करते हैं। इसके अलावा, सीरिया, लेबनान, इराक और यमन में ईरान की उपस्थिति इजराइल की राष्ट्रीय सुरक्षा में एक गंभीर चुनौती साबित हुई हैं। जिसे पिछले कुछ वर्षों में दोनों के बीच सीरिया, इराक तथा लेबनान में हो रहे प्रत्यक्ष तथा अप्रत्यक्ष टकरावों में भी देखा गया है।

साथ ही सूचना और परिचालन प्रौद्योगिकी पर इज़राइल की अर्थव्यवस्था की भारी निर्भरता ने देश के साइबर खतरों को व्यापक रुप से बढ़ा दिया है। इसने साइबर जोखिमों को भी बढ़ाया है। इन सभी कारकों ने इजरायल को तकनीकी श्रेष्ठता प्राप्त करने, साइबर निगरानी और साइबर युद्ध में वर्चस्व हासिल करने के लिए मजबूर किया है, ताकि वह अपने विरोधियों का प्रभावी ढंग से सामना कर सके और अपने आर्थिक प्रतिष्ठानों की रक्षा कर सके। 2000 के दशक के मध्य में साइबर डोमेन में तेजी से हुए विस्तार ने तथा 2010 के दशक में घटित हाई–प्रोफाइल साइबर उल्लंघनों ने इजरायल के लिए यह आवश्यक बना दिया कि वह अपने साइबर सुरक्षा संगठनों में पर्याप्त निवेश करे। इस बात को ध्यान में रखते हुए 2012 में राष्ट्रीय साइबर ब्यूरो की स्थापना की गयी साथ ही 2016 में राष्ट्रीय साइबर डायरेक्टरेट की स्थापना भी की गयी। राष्ट्रीय सुरक्षा आवश्यकताओं को पूरा करने के अलावा, इजराइल ने साइबर ज्ञान को व्यावसायिक अवसर के रूप में उपयोग करने के महत्व को भी भली–भांति समझा हैं। जिसे तेल–अवीव विश्वविद्यालय के 7 वें वार्षिक साइबरस्पेस सम्मेलन में प्रधान मंत्री बेंजामिन नेतन्याहू के भाषण में बहुत खूबसूरती से देखा जा सकता हैं। सम्मेलन में उन्होंने कहा "साइबर एक महान व्यवसाय है। यह ज्यामितीय रूप से बढ रहा हैं क्योंकि इसका कोई स्थायी समाधान नही हैं, यह कभी न खत्म होने वाला व्यवसाय है।"[ii]

साइबर सुरक्षा में सरकारी एजेंसियों की भूमिका

इजराइल में साइबर और प्रौद्योगिकी क्षेत्र को विकसित करने और बनाए रखने में सरकार एक महत्वपूर्ण भूमिका अदा करती है। विद्वानों में इस बात पर आम सहमति हैं कि इजराइल में आर्मी (आई.डी.एफ.) रक्षात्मक और आक्रामक साइबर क्षमताओं के उद्भव तथा विकास के लिए एक महत्वपूर्ण स्थान साबित हुई हैं। इसरायली आर्मी के पास यूनिट 8200 और यूनिट 9900 जैसी विशेष इकाइयां मौजूद हैं, जो साइबर सुरक्षा चुनौतियों से निपटने तथा उनके समाधानों को ढूंढने में युवा आई. डी. एफ. सैनिकों को व्यावहारिक अनुभव प्रदान करती हैं।[iii] इजराइल में कई साइबर विशेषज्ञों ने इन इकाइयों में काम करके अपने तकनीकी कौशल को प्रभावी ढंग से निखारा है, इन इकाइयों की स्टार्ट–अप जैसे कामकाज ने तथा टीम–उन्मुख वातावरण ने इन्हे पर्याप्त जगह व तकनीकी समझ का विकास करने के आवश्यक अवसर प्रदान किये हैं।

साइबर खतरों से निपटने के लिए सेना में निवेश करने के अलावा, इजराइल ने नागरिक क्षेत्र में साइबर चुनौतियों का मुकाबला करने के लिए एक मजबूत तंत्र विकसित किया हैं। इस सन्दर्भ में इजराइल राष्ट्रीय साइबर निदेशालय (INCD) नीतियों का निर्माण करता हैं और साइबर स्पेस की रक्षा के लिए तकनीकी

क्षमताओं का निर्माण करता हैं। INCD का यह दायित्व है की वह "साइबर साइंस–एंड–टेक्नोलॉजी" के विकास व सुदृढ़ीकरण में नीव की ईंट की भुमिका निभाये, साथ ही उच्चस्तरीय मानव संसाधन, उन्नत शैक्षिक अनुसंधान, गहन तकनीकी अनुसंधान एवं विकास तथा साइबर उधोग के विकास में भी महत्वपूर्ण भुमिका अदा करे।[v]

इजराइल और साइबर युद्ध

1948 से, इजरायल ने अपने पड़ोसी अरब देशों से विभिन्न प्रकार के सैन्य व अन्य हमलों (पारंपरिक और गैर–पारंपरिक) का सामना किया है। हालांकि, पिछले दशक में, इसने अपने साइबर स्पेस में घुसपैठ के कई प्रयासों को सफलतापूर्वक निष्प्रभावी भी किया हैं, किन्तु इसरायली विशेषज्ञों का यह मानना हैं कि प्रौद्योगिकी के क्षेत्र में हो रहे व्यापक बदलाव को ध्यान में रखते हुए यह कहा जा सकता हैं की इस तकनीकी अंतर को काफी हद तक हम कम कर पाएंगे।

पिछले एक दशक में इजराइल के ऊपर हुए साइबर हमलों ने देश की अर्थव्यवस्था तथा सुरक्षा बलों समक्ष एक बड़ी चुनौती को रेखांकित किया हैं। इस सन्दर्भ में कुछ महत्वपूर्ण उदाहरण इस प्रकार हैं। 2013 में, हैकर्स के एक अनाम समूह ने एक इजरायली एनजीओ की वेबसाइट को निशाना बनाया जो कैंसर से पीड़ित बच्चों की सहायता करती है।[v] वर्ष 2013 से, इजराइल एक वार्षिक साइबर–हमले से निपट रहा है, जिसे ओप्सराएल के रूप में जाना जाता हैं जिसने वार्षिक आधार पर सरकार और कॉर्पोरेट वेबसाइटों को लक्षित किया है। अगस्त 2018 में, ईरानी हैकर्स "लीफमिनर" ने इजरायल और अन्य अरब देशों, सऊदी अरब, यूएई, कतर, कुवैत, बहरीन और मिस्र को निशाना बनाया।[vi] अप्रैल 2020 में, ईरान ने कथित रूप से इजरायल की जल संरचना सुविधाओं को लक्षित किया जिसके बाद कथित तौर पर 9 मई 2020 को इजरायल के द्वारा जवाबी हमला किया गया था जो कि समुद्री व्यापार के लिए ईरान के सबसे व्यस्त हब बांदर अब्बास में शाहिद राजा पोर्ट पर किया गया था।[vii] 18 दिसंबर 2020 को एक प्रमुख साइबर हमले ने विभिन्न इजरायली लॉजिस्टिक कंपनियों का काम रोक दिया था।

इस तरह के साइबर हमलों से निपटने के लिए, इजराइल ने साइबर क्षेत्र में आक्रामक और रक्षात्मक क्षमताओं का विकास किया है तथा व्यापक रूप से साइबर सुरक्षा और अनुसंधान को पाठ्यक्रमों के रूप में तथा शैक्षणिक स्तर पर प्रोत्साहित किया है। इजराइल ने, आक्रामक स्तर पर, साइबरस्पेस का उपयोग हथियार के रूप में अपने विरोधियों को पार पाने के लिए किया हैं।[viii] उदाहरण के लिए, 2010 में, यूएस –इजरायल ने मिलकर स्टक्सनेट (Stuxnet) वायरस के साथ ईरान के परमाणु कार्यक्रम को निशाना बनाया।[ix] ऐसा माना जाता हैं कि दोनों देशों ने साथ मिलकर कथित तौर पर फ्लेम वायरस का उपयोग कर ईरान के परमाणु कार्यक्रम को भी निशाना बनाया था।[x] सीरिया में, परमाणु रिएक्टरों को निशाना बनाते समय आई.डी.एफ. ने कई तरीके के साइबर टूल्स का उपयोग अपने ऑपरेशन का सहयोग करने के लिए भी किया था। इन टूल्स के माध्यम से हमले के दौरान आई.डी.एफ. ने सीरियाई राडार को हैक कर लिया और उन्हें रिप्रोग्राम भी कर दिया था, जिसकी वजह से सीरिया को हमले के समय लगा कि सब कुछ ठीक चल रहा था।[xi] 2019 में, एक इजराइली कंपनी (एनएसओ समूह) ने सर्विलांस सॉफ्टवेयर के साथ व्हाट्सएप उपयोगकर्ताओं (फिलिस्तीनी और ईरानी) के एक समूह को लक्षित किया जो आईफोन और एंड्रॉइड दोनों से जानकारी प्राप्त करने में सक्षम था।[xii]

रक्षात्मक स्तर पर, इजराइल लगातार साइबर डोमेन में अपने तकनीकी ज्ञान को आगे बढ़ा रहा हैं और अपने हथियारों और संचार प्रणाली को समय पर अद्यतन कर रहा हैं जो साइबर हमले के लिए अतिसंवेदनशील हो सकते हैं। सैन्य संचार प्रणाली की सुरक्षा की जिम्मेदारी आई.डी.एफ. की C4I शाखा के कंधों पर हैं जबकि INCD नागरिक साइबर क्षेत्र की सुरक्षा के लिए जिम्मेदार हैं। इसके अलावा, मोसाद व अन्य खुफिया एजेंसियों की साइबर क्षमताएं दुश्मनों के खिलाफ इजरायल के साइबर युद्ध में महत्वपूर्ण सहयोग करती हैं।

आंतरिक संस्थागत तंत्र स्थापित करने के अलावा, इजरायल ने विभिन्न देशों के साथ मिलकर साइबर स्पेस की रक्षा करने में भी भागीदारी की है। उदाहरण के लिए, जुलाई 2014 में, इजरायल और जापान ने साइबर सुरक्षा के क्षेत्रों में संयुक्त अनुसंधान के लिए इजरायल और जापानी कंपनियों को फंड्स प्रदान करने वाले एक समझौते पर हस्ताक्षर किए।[xiii] 2017 में, साइबर सुरक्षा पर सहयोग को आगे बढ़ाने के लिए एक यूएस–इजरायल साइबर वर्किंग ग्रुप की स्थापना की गई थी।[xiv] इसी तरह, जनवरी 2018 में, भारत और इजरायल ने प्रधानमंत्री बेंजामिन नेतन्याहू की भारत यात्रा के दौरान साइबर सुरक्षा सहयोग पर एक समझौता ज्ञापन पर हस्ताक्षर किए।[xv] कोविड 19 संकट के दौरान तेजी से बढ़ते हुए डिजिटलीकरण के बीच साइबर खतरे से निपटने के लिए, इजराइल के राष्ट्रीय साइबर निदेशालय (INCD) के महानिदेशक, यिगाल उन्ना (Yigal Unna), और इजराइल में भारतीय राजदूत, संजीव सिंगला ने दोनों देशों के बीच साइबर सम्बन्धों का विस्तार करने के लिए एक और समझौता ज्ञापन (जुलाई 16, 2020) पर हस्ताक्षर किए।[xvi] साइबर सुरक्षा की समस्या से निपटने के लिए इस तरह के द्विपक्षीय प्रयास भविष्य में अतिमहत्वपूर्ण साबित हो सकते हैं।

निष्कर्ष

साइबर आतंकवाद, मैलवेयर और रैंसमवेयर हमले, सामरिक और गैर–सामरिक बुनियादी ढांचे और डेटा चोरी, के रूप में मंडरा रहे साइबर सुरक्षा खतरों ने दुनिया के प्रत्येक देश के प्रमुखों राष्ट्रीय सुरक्षा चिंताओं को बढ़ाया है। साथ ही इन विषयो पर ध्यान देने की आवश्यकता अब पहले से कई अधिक महसूस की जा रही है। इन सब को ध्यान मे रखते हुए साइबर सुरक्षा में क्षेत्र में इजराइल अग्रणी होने के साथ, दुनिया की सहायता करने में इसकी भूमिका को नजर अंदाज नही किया जा सकता है। लगातार विभिन्न तरह के आंतरिक और बाहरी खतरों जूझते हुए इजरायल ने अपनी साइबर सुरक्षा संरचना को, आई. डी. एफ. की इकाइयों और INCD जैसे प्रभावी संस्थानों की स्थापना करके मजबूत किया है। इसके अलावा, इजरायल में विभिन्न इजरायली बिजनेस स्टार्ट–अप भी सक्रिय रूप से साइबर डोमेन में नए समाधान को विकसित कर रहे हैं। साइबर सिक्योरिटी क्षेत्र में अपनी नेतृत्व की काबिलियत के साथ इजराइल वैश्विक समुदाय को भी लाभान्वित कर सकता है।

भारत के साइबर डोमेन में भारत–इजरायल के सहयोग को घनिष्ठ करने से वास्तव में भारत की एक स्थायी साइबर पारिस्थितिकी तंत्र स्थापित करने में मदद मिलेगी। इस दिशा में, सहयोग निम्नलिखित क्षेत्रों में हो सकता है: सरकारी और निजी संस्थानों में साइबर पेशेवरों द्वारा लगातार संगोष्ठियों में छात्र और कर्मचारी एक्सचेंजों को शामिल करना, शैक्षिक और व्यावसायिक पाठ्यक्रमों की शुरूआत करना तथा नियमित शैक्षणिक आदान–प्रदान को बढ़ाया जा सकता है। इसके अलावा, दोनों देशों के बीच स्टार्ट–अप्स के बीच सहयोग हो सकता है और साथ ही रियल टाइम इनफार्मेशन साझा करने के चैनल स्थापित किए जा सकते हैं। इन सभी क्षेत्रों में सहयोग को बढ़ा कर तथा साइबर डोमेन में सूचना और ज्ञान साझा करके दोनों देश आपसी फायदों को सुनिश्चित कर सकते हैं।

References

1. Israel National Cyber Directorate, "The Israeli cyber industry continues to grow: record fundraising in 2020", https://www.gov.il/en/departments/news/2020ind

2. Gil Press, "6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry

", https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/?sh=6ee4b0ab420a

3. Ibid.

4. Israel National Cyber Directorate, https://www.gov.il/en/departments/about/newabout

5. The Guardian, "Anonymous hacker attack on Israeli websites 'causes little real damage" https://www.theguardian.com/technology/2013/apr/08/anonymous-hacker-attack-israeli-websites

6. Sandeep Singh Grewal, "Report: Iran hacks Israel in cyber-attack" https://www.jpost.com/israel-news/politics-and-diplomacy/report-iran-targeted-israel-in-cyber-attack-563937

7. Gil Baram and Kevjn Lim, "Israel and Iran Just Showed Us the Future of Cyberwar with Their Unusual Attacks", https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/

8. Cohen, Matthew & Freilich, Charles & Siboni, Gabi. (2016). Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives. 17. 307-321. 10.1093/isp/ekv023.

9. Stuart Winer, " 'Dutch mole' planted Stuxnet virus in Iran nuclear site on behalf of CIA, Mossad", https://www.timesofisrael.com/dutch-mole-planted-infamous-stuxnet-virus-in-iran-nuclear-site-report/#:~:text=The%20Stuxnet%20virus%20was%20uncovered,by%20speeding%20up%20its%20centrifuges

10. Reuters, "Israel developed Flame computer virus: newspaper", https://www.reuters.com/article/net-us-usa-cyber-flame-idUSBRE85I1QQ20120619U.S.

11. Cohen, Matthew & Freilich, Charles & Siboni, Gabi. (2016). Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives. 17. 307-321. 10.1093/isp/ekv023.

12. The Financial Times, "WhatsApp voice calls used to inject Israeli spyware on phones", https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab

13. Franz-Stefan Gady, "Japan and Israel to Work Together in Cyberspace" , https://thediplomat.com/2015/01/japan-and-israel-to-work-together-in-cyberspace/

14. Josh Kram, "US-Israel Cybersecurity Collaborative: A Roadmap for Global Private, Public Partnership", https://www.uschamber.com/series/above-the-fold/us-israel-cybersecurity-collaborative-roadmap-global-private-public

15. Ministry of External Affairs, "List of MoUs/Agreements signed during the visit of Prime Minister of Israel to India (January 15, 2018)", https://mea.gov.in/bilateral documents.htm?dtl/29356/List_of_MoUsAgreements_signed_during_the_visit_of_Prime_Minister_of_Israel_to_India_January_15_2018

16. Press Trust of India, "India and Israel sign agreement to expand cooperation in cyber security" (Published in Hindu), https://www.thehindu.com/news/national/india-and-israel-sign-agreement-to-expand-cooperation-in-cyber-security/article32102730.ece