8 जुलाई, 2015

अप्रतिरोध्य साइबर आक्रमणों के निशाने पर अमरीका

*डॉ ओमैर अनास**

"रक्षा विभाग साइबर रणनीति 2015" की घोषणा के कुछ महीने के भीतर ही अमरीका को 15 जून, 2015 को एक बड़े साइबर आक्रमण का सामना करना पड़ा। लगभग चालीस लाख अमरीकी संघीय कार्मिकों की व्यक्तिगत जानकारी/सूचना चुरा ली गई है, जिसमें समाजिक सुरक्षा संख्या और अन्य महत्वपूर्ण ब्यौरे शामिल हैं। अमरीकी मीडिया ने इस आक्रमण के लिए तत्काल चीन को दोषी ठहराया है और अधिकारियों ने चीन की संलिप्तता का संकेत देने वाले वक्तव्य जारी किए हैं। चीनी विदेश मंत्रालय ने इन आरोपों को "अवैज्ञानिक और गैरजिम्मेदाराना"[1] बताते हुए इन्हें खारिज कर दिया है। तथाकथित चुराए गए आंकड़े कार्मिकों के रिकार्ड तथा सुरक्षा भुगतान के संबंध में थे। अमरीकी साइबर सुरक्षा विशेषज्ञ मानते हैं कि यह सूचना भविष्य में अधिक व्यापक, बेहतर समायोजित आक्रमणों के लिए उपयोग में लाई जा सकती है। उनका मानना है कि यह आक्रमण और इसी प्रकृति के पूर्व आक्रमण सामान्य साइबर अपराधियों के नहीं, बल्कि किसी राष्ट्र के लिए काम कर रहे हैकरों की ही करतूत होगी।[2] इस आक्रमण के पीछे किसी राष्ट्र की संलिप्तता के आरोपों में कुछ दम है, क्योंकि ओपीएम (कार्मिक प्रबंध कार्यालय) के डाटा बेस में एकत्र सुरक्षा भुगतान आंकड़ों में इसके कर्मचारियों और उनके परिवारों की सामाजिक सुरक्षा संख्या मौजूद है जिसके माध्यम से वे आगामी हथियार कार्यक्रमों को हैक कर सकते हैं।[3] गोल्डमैन सैश ग्लोबल इन्वेस्टमेंट रिसर्च के अनुसार, इस आक्रमण से पहले जुलाई 2014 से जून 2015 के बीच आईआरएस, स्टारबक्स, तेस्ला मोटर्स, उबेर, टर्बो टैक्स, एन्थम, मलेशिया एयरलाईन्स, यूएस सेन्ट्रल कमांड, कैलीफोर्निया युनिवर्सिटी, यूएसपीएस, स्नैपचैट, जेपी मॉर्गन, एपल, एटी एण्ड टी मोबिलिटी, एलएलसी, यूरोपियन सेन्ट्रल बैंक और बैंक ऑफ अमेरिका साइबर आक्रमणों के हाई-प्रोफाइल शिकार बन चुके हैं।

साइबर आक्रमण आजकल "नई सामान्य" बात होती जा रही है। पिछले दो महीनों में अनेक देशों में रिकार्ड संख्या में साइबर आक्रमण हुए हैं। अज्ञात स्थानों से किए जाने वाले इन आक्रमणों के माध्यम से बड़ी संख्या में आंकड़े चुराए गए हैं अथवा कुछ ऑपरेशनों/कार्यों को बाधित किया गया है। ये आक्रमण इस बात के खतरनाक संकेत हैं कि साइबर जगत दिन-प्रति-दिन कितना असुरक्षित होता जा रहा है। कोई भी देश इन आक्रमणों से (सु)रक्षित नहीं है। इस वर्ष मार्च में चीनी इंटरनेट कम्पनी कीहू 360 के स्काईआई प्रयोगशालाओं ने ओसन लोटस पर अप्रैल 2012 के बाद से चीन की समुद्री एजेंन्सियों, वैज्ञानिक अनुसंधान संस्थानों और नौवहन कम्पनियों पर "अत्यधिक संगठित" ऑनलाइन अटैक करने का आरोप लगाया।[4] साइबर सुरक्षा पर अमरीका और चीन के बीच इस परंपरागत लुका-छिपी के खेल के अलावा इज़राइल पर भी वायरस कार्यक्रम के माध्यम से ईरानी परमाणु वार्ताओं की जासूसी का आरोप लगाया गया था। रूसी साइबर सुरक्षा कम्पनी कास्पर्स्की लैब ने सुझाया कि इज़रायल ने ईरान और विश्व शक्तियों के बीच वार्ताओं की मेजबानी करने वाले सुविधा-सम्पन्न होटलों के नेटवर्क को हैक करने के लिए "डूकू 2" नामक एक नए इंटरनेट वर्म का प्रयोग किया है।[5] 17 जून को कनाडा की सामान्य वेबसाइट Canada.ca और अन्य वेबसाइटों जैसेकि कनाडा के राजनीतिज्ञों द्वारा एक नए आतंकवाद विरोधी कानून पारित करने का विरोध करने हेतु कनाडियाई सुरक्षा आसूचना सेवा (सीएसआईआर) पर *अज्ञात* (एनोनिमस) नामक एक समूह ने आक्रमण किया था।[6] केवल आस्ट्रेलिया में ही अप्रैल माह में 3500 साइबर आक्रमणों की रिपोर्टें दर्ज की गई हैं। आस्ट्रेलियाई प्राधिकारियों के अनुसार "आस्ट्रेलिया में साइबर खतरों को आम तौर पर स्रोत दोषारोपण के मामले में राष्ट्र-प्रायोजित अथवा आपराधिक रूप से अभिप्रेरित (खतरे) के रूप में वर्गीकृत किया गया है। आस्ट्रेलियाई एजेंसी इन खतरों को दूर करने तथा इन पर नज़र रखने के लिए 'नीतिपरक हैकरों' की भर्ती करने पर विचार कर रही है।"[7] साइबर आक्रमणों की तीव्रता और विस्तार के साथ ही राष्ट्रों तथा व्यावसायिक समूहों दोनों द्वारा साइबर डोमेन की सुरक्षा दुरूस्त करने का कार्य बढ़ता जा रहा है। अमरीका जैसे देश की सीनेट सशस्त्र सेवा समिति आयुध/हथियार कार्यक्रमों की साइबर समीक्षा के लिए पेन्टागन के राजकोषीय बजट 2016 में 2 अरब डॉलर जोड़ने पर विचार कर रही है। व्यावसायिक समूहों के लिए साइबर सुरक्षा कार्यक्रम, सॉफ्टवेयर और साइबर बीमा अधिक महत्वपूर्ण होते जा रहे हैं। साइबर जगत के विस्तार के साथ ही साइबर आक्रमण भी अधिक पेशेवर और विशेषज्ञ संचालित बनते जा रहे हैं।

संभावित अमेरिकी प्रतिक्रियाएं

अतीत में अमरीका की प्रतिक्रियाएँ आक्रमक के साथ-साथ रक्षात्मक रही हैं। ईरान की परमाणु अवसंरचना पर स्टक्सनेट वायरस के आक्रमण और उत्तर कोरिया की परमाणु अवसंरचना पर आक्रमण सर्वाधिक लक्षित साइबर आक्रमण थे। चीन और अमरीका साइबर आक्रमणों के लिए लगातार एक दूसरे पर दोषारोपण करते

रहते हैं। अमरीकी ओबीएम नेटवर्कों पर हुए हाल के साइबर आक्रमण के संबंध में अपने लेख में रोसेंबच का उल्लेख करते हुए मार्क पोमर लू कहते हैं कि अमरीका को किसी संभावित आक्रमण के वांछित प्रभाव को नकारने की क्षमता विकसित करने की आवश्यकता है; दूसरे, अमरीका को साइबर आक्रमण पर की जानेवाली कार्रवाई के लिए लागत बढ़ानी होगी; तीसरे, उन्हें सुनिश्चित करना होगा कि उनमें (इन आक्रमणों से) उबरने की क्षमता बनी रहे।[8]

सुरक्षा का भार मुख्य रूप से सरकार पर होता है कि वह व्यावसायिक समूहों को, विशेषकर, विदेशों से प्रारंभ होने वाले आक्रमणों से सुरक्षा प्रदान करे। व्यावसायिक समूहों द्वारा उठाई गई विशाल वित्तीय हानि ने उन्हें यह मांग करने पर मज़बूर कर दिया है कि सरकार हानि में हिस्सेदारी करे। ऐसी मांगें भी उठी हैं कि विदेशी शक्तियों द्वारा होने वाले आक्रमण झेल रहे अमरीकी व्यापार को दण्डित करना नैतिकता के विरूद्ध है और इसलिए वैधानिक परिवर्तन की मांग की जा रही है। इसमें यह मांग भी शामिल है कि यदि आक्रमण किसी बाहरी राष्ट्र अथवा उसके सहयोगियों की ओर से प्रारंभ किया गया पाया जाए तो सरकार द्वारा थोपे गए डाटा अतिक्रमण संबंधी सभी दण्ड निरस्त किए जाएं। साथ ही, अमरीकी सरकार को राष्ट्र प्रायोजित अथवा निरपेक्ष हैकर समूहों को सूचीबद्ध करके उपर्युक्त सुरक्षा (व्यवस्था) को निशाना बनाने वाले हैकरों का पता लगाने में सहायता करनी चाहिए।[9]

भौतिक/सशरीर पहचानयोग्य शत्रु के विपरीत, साइबर खतरा आसानी से पहचाने जाने वाले ऐसे किसी शत्रु की ओर से नहीं आता, जिसमें किसी निश्चित राष्ट्र का पता लगाया जा सके। अमरीकी रक्षा के केन्द्र में होने के बावजूद, साइबर अवरोध अब तक (पूर्णतया) विकसित हुआ प्रतीत नहीं होता। किसी अवरोध सिद्धांत के विकास की समस्या (खतरे की) वह लाल रेखा है जो अब तक साइबर आक्रमणों के लिए तय नहीं की गई है। कांग्रेस को दिए गए अपने बयान में पूर्वी एशिया, प्रशांत वक्तव्य उपसमिति, और अंतरराष्ट्रीय साइबर सुरक्षा नीति सीनेट की विदेश संबंध समिति पर जेम्स ए लेविस कहते हैं:

> शीत युद्ध के दौरान, परमाणु खतरे ने सोवियत संघ को पश्चिमी यूरोप और जापान पर आक्रमण करने अथवा अमरीका के विरूद्ध सामरिक आक्रमण प्रारंभ करने से रोक दिया। हालांकि यह अक्सर तर्क-वितर्क का विषय रहा कि परमाणु "छतरी" ने (खतरे की) वह लाल रेखा तय कर दी जिसे सोवियत संघ ने समझा और विश्वसनीय पाया क्योंकि वे मूल अमरीकी हितों से संबद्ध थे। अमरीका की नीतियां सीमायुक्त अथवा घोषित नीतियां हैं लेकिन वे अनेकों प्रतिवादों से घिरी हैं। यह "रणनीतिक अस्पष्टता" जैसा प्रतीत होता है लेकिन वास्तव में, यह हमारे विरोधियों को भ्रामक

लगता है। यदि विराधी नहीं जानते कि किस सीमा को उन्हें नहीं लांघना चाहिए अथवा वे नहीं मानते कि इन सीमाओं को पार करने के लिए हम उन्हें दण्डित करेंगे, तो उन्हें रोकना कठिन होगा।[10]

जेम्स के अनुसार, सीमा को परिभाषित करने में अस्पष्टता के संदर्भ में, साइबरस्पेस में सुरक्षा और स्थिरता लाने के लिए एक भिन्न दृष्टिकोण अपेक्षित है। और चूंकि एकपक्षीय रूकावट प्रभावहीन होता है इसलिए अंतर्राष्ट्रीय करार की आवश्यकता है। ये लक्ष्य साइबरस्पेस के लिए डीओडी के तीन तय लक्ष्यों के अतिरिक्त हैं: "मौजूदा डीओडी नेटवर्क का बचाव, महत्वपूर्ण आक्रमणों के विरूद्ध समग्र अमेरिकी नेटवर्क का बचाव, और सैन्य अभियानों के लिये सम्पूर्ण साइबर सहयोग उपलब्ध कराना।"[11]

आक्रमण के उद्गम का पता लगाना

अमरीकी प्राधिकारी और मीडिया सर्वाधिक व्यवहारिक तरीके से (ही नहीं) बल्कि कुछ उन्मादपूर्ण प्रतिक्रिया के तहत अधिकांश साइबर आक्रमणों के लिए चीन और रूस को दोषी ठहराते रहे हैं। अमरीका, चीन और रूस के बीच प्रमुख दोषारोपणों का कारण यह है कि अमरीका और चीन साइबर जगत में बड़े हिस्सेदार हैं। अकामई द्वारा प्रलेखित एक रिपोर्ट के अनुसार, अधिकांश आक्रमणों के मार्ग/ट्रैफिक 194 अलग-अलग देशों/क्षेत्रों से प्रारंभ हुए और चीन पहले स्थान पर (41% ट्रैफिक) बना रहा, जिसके बाद अमरीका (11%), इंडोनेशिया (7%), ताइवान (3%), ब्राजील (3%), रूस (2.9%) और भारत (2.6%) का स्थान है। उद्योग जगत और अंतर्राष्ट्रीय वाणिज्य नए आक्रमणों के सबसे ज्यादा शिकार हुए, जहां क्रमश: 28 और 27% साइबर आक्रमण हुए जिसके बाद सार्वजनिक क्षेत्र (20%) का स्थान आता है। यह अर्थपूर्ण है क्योंकि अमरीका और चीन का अधिकांश इंटरनेट (उपयोग) जगत में बोलबाला है। 240 अलग-अलग देशों/क्षेत्रों के 7 करोड 95 लाख से भी अधिक IPV4 यूनिक एड्रेसों में से 1 करोड़ 64 लाख अमरीका के हैं और 1 करोड़ 23 लाख चीन के हैं, 41 लाख ब्राजील के, 40 लाख जापान के, 37 लाख जर्मनी के और 18 लाख भारत के हैं।[12] ई-कॉमर्स बाज़ारों पर चीन और अमरीका के आधिपत्य, जिनकी (हिस्सेदारी) कुल मिला कर वर्ष 2014 में वैश्विक इंटरनेट खुदरा बिक्री के 55 प्रतिशत से अधिक है तथा जिसमें 1.316 खरब डॉलर का लेन-देन हुआ है, के साथ ही अमरीका और चीन में साइबर सुरक्षा सर्वाधिक संवेदनशील मुद्दा बन गया है।[13] इतने अधिक इंटरनेट आधारित आर्थिक और प्रशासनिक लेन-देनों को देखते हुए वहां साइबर अपराध भी उतने ही अधिक होते हैं। अमरीका और चीन का सूचना प्रौद्योगिकी के हार्डवेयर उद्योग में भी आधिपत्य है जबकि भारत विश्व में दूसरा सबसे बड़ा सॉफ्टवेयर निर्यातक है। इन तथ्यात्मक वास्तविकताओं को देखते हुए अमरीकी और चीनी व्यापारियों में हितों का टकराव बहुत ज्यादा है जो बौद्धिक सम्पदा अधिकारों का दावा करने के कारण

अधिक गंभीर हो गया है। हालांकि रूस सूचना प्रौद्योगिकी के व्यापक उपयोग में चीन से काफी पीछे है, फिर भी अमरीकियों के साथ इसके असामान्य संबंध वैचारिक तथा राजनीतिक दोनों स्तरों पर ऐतिहासिक हैं। नई डीओडी साइबर सुरक्षा 2015 ने अमरीकी साइबर सुरक्षा के लिए चीन और रूस दोनों को प्रमुख साइबर खतरे के रूप में स्पष्ट रूप से चिन्हित किया है। डीओडी रिपोर्ट में उल्लेख है:

> डीओडी साइबर रणनीति 2015 में कहा गया है कि प्रभावशाली विरोधियों ने साइबर में अत्यधिक निवेश किया है क्योंकि यह उन्हें अमरीकी मातृभूमि को लक्ष्य बनाकर अमरीकी हितों को नष्ट करने के लिये एक व्यवहार्य, अनुग्राह्यतापूर्वक अस्वीकार्य क्षमता प्रदान करता है। रूस और चीन ने उन्नत साइबर सामर्थ्य और रणनीतियां विकसित कर ली हैं। रूसी कार्यकर्ता अपने साइबर व्यापार-कौशल में गोपनीय हैं और कभी-कभार उनके इरादों का पता लगाना कठिन होता है। चीनी कम्पनियों को लाभ पहुंचाने और अमरीकी प्रतियोगिता का जड़ काटने के लिए चीन वैश्विक व्यापार से बौद्धिक सम्पदा (आईपी) चुराता है। हालांकि ईरान और उत्तरी कोरिया कम विकसित साइबर क्षमता-प्राप्त देश हैं, फिर भी इन्होंने साइबरस्पेस में अमरीका और अमेरिकी हितों के प्रति शत्रुतापूर्ण प्रत्यक्ष स्तर के इरादों को दर्शाया है।[14]

अमरीका द्वारा चीन को सबसे बड़ा साइबर सुरक्षा खतरा क्यों माना जाता है? अमरीकी दृष्टिकोण से, चीनी कम्युनिस्ट पार्टी और सम्पूर्ण राष्ट्र पर इसका केन्द्रीयकृत नियंत्रण चीनी साइबर व्यवहार के शीर्ष पर है। आमी चांग संकेत देते हैं कि आर्थिक वृद्धि और स्थिरता बनाए रखना, चीनी कम्युनिस्ट नेटवर्क का उपयोग करना, सैन्य परिदृश्य की तैयारी करना और सैन्य श्रेष्ठता सुनिश्चित करना, सैन्य अवसंरचनाओं, प्रेरणाओं और उद्देश्यों के प्रभावी प्रतिद्वन्द्वियों का अध्ययन करना और अंत में अंतराष्ट्रीय स्तर पर साइबर सुरक्षा पर सरकारी नियंत्रण के वैकल्पिक आख्यान चीनी साइबर सुरक्षा रणनीति के प्रमुख उद्देश्य हैं। अमी का तर्क है कि माओ जेडॉग की 'सक्रिय सुरक्षा' आज भी वर्ष 2013 के इसके श्वेत पत्र में वर्णित चीन की साइबर सुरक्षा रणनीति के मार्गदर्शक सिद्धांत हैं, जो चीन के सशस्त्र (सैन्य) बलों के विविध रोजगार के बारे में है।[15]

चीनी जुनून ने जून 2009 में अमरीका को अमरीकी साइबर कमांड (CYBERCOM) की स्थापना की घोषणा करने और वर्ष 2011 साइबरस्पेस को साइबर युद्ध का एक नया क्षेत्र घोषित करने पर मजबूर कर दिया था।[16] अमरीकी रक्षा विभाग द्वारा घोषित 2015 साइबर रणनीति ने एक पांच-सूत्री रणनीति का खाका तैयार किया है: (1) साइबरस्पेस कार्यों का संचालन करने के लिए क्षमताओं का सृजन करना तथा बलों को तैयार रखना; (2) डीओडी सूचना नटवर्क को सुरक्षित रखना; (3) महत्वपूर्ण हितों को विघटनकारी अथवा

विनाशकारी साइबर आक्रमणों से सुरक्षित रखना; (4) संघर्ष वृद्धि पर नियंत्रण करने के लिये व्यवहार्य साइबर विकल्प तैयार करके उन्हें कायम रखना; और (5) साझे खतरों को रोकने और अंतर्राष्ट्रीय सुरक्षा एवं स्थिरता बढ़ाने के लिए मजबूत अंतर्राष्ट्रीय गठजोड़ व भागीदारी बनाना तथा उन्हें कायम रखना। इन कार्यनीतियों के अनुसार, अमरीका साइबर प्रतिरोधक का निर्माण करना चाहता है। तदनुसार, अमरीका न केवल अपनी क्षमताओं को विकसित कर रहा है बल्कि चीन को परोक्ष रूप से दिमाग में रखकर यूरोप से लेकर एशिया प्रशांत व पश्चिम एशिया तक एक बड़ा गठबंधन भी तैयार कर रहा है।

आगे क्या हो सकता है

परिणामस्वरूप, चीन और अमरीका के बीच एक दृष्टिगोचर साइबर संघर्ष प्रतिस्पर्धा चल रही है। एक देश की हर नई साइबर प्रौद्योगिकी दूसरे की प्रतिक्रिया में विकसित की जा रही है। इस प्रतियोगिता के बीच, अनेक असफल प्रयासों के बाद संयुक्त राष्ट्र द्वारा नियुक्त सरकारी विशेषज्ञ समूह ने अंतर्राष्ट्रीय कानून की प्रयोज्यता स्वीकार करने और विशेषकर, साइबर जगत में भी संयुक्त राष्ट्र चार्टर को स्वीकार करने के लिए चीन को समझा लिया है। ओपीएम पर हाल के आक्रमण ने अमरीकी नीति निर्माताओं को सर्तक कर दिया है क्योंकि यह विगत कई वर्षों में डाटा चोरी की सबसे बड़ी घटनाओं में से एक है। अधिकार कटौती के कारण चीन के इनकार को हमेशा मान लिया गया है; हालांकि लगातार ऐसे व्यापक तथा ठोस आक्रमण राष्ट्र के प्राधिकारियों के समर्थन के बिना नहीं हो सकते। अमरीकी मामलों में चीन प्रमुख आरोपी है क्योंकि अमरीका के पास इन आक्रमणों के मूल स्थान का पता लगाने के पर्याप्त संसाधन हैं। उन देशों का क्या होगा जिनकी सूचना प्रौद्यौगिकी अवसंरचना अत्यधिक कमज़ोर है? यह परिदृश्य अत्यंत भयावह है क्योंकि यह बताता है कि सूचना प्रौद्योगिकी में पिछड़े अधिकांश राष्ट्र बड़े देशों की अत्याधुनिक निगरानी और जासूसी मशीनरी के सामने लगभग पूरी तरह निरावरण हैं। अधिकांशत: अमरीकी राष्ट्रीय सुरक्षा एजेंसी द्वारा जर्मन चांसलर के फोन और फ्रांसीसी तथा ब्रिटिश राजनीतिज्ञों के फोनों में छिपा हुआ माइक्रोफ़ोन लगाने (बग्गिंग) के कृत्य ने अमरीका–यूरोप परस्पर विश्वास को अत्यधिक डगमगा दिया है। एडवर्ड स्नोडन के खुलासों और अनेक राष्ट्रों के गोपनीय तथा राजनीतिक दस्तावेजों तक विकिलिक्स की पहुंच स्पष्ट उदाहरण हैं कि बड़े देश और उनके प्रायोजित अथवा स्वतंत्र व्यक्ति (गोपनीय) सूचना प्राप्ति के लिए संघर्षरत हैं। छोटे राष्ट्रों, समुदायों और व्यक्तियों की गोपनीयता और संपत्ति निरंतर असुरक्षित अवस्था में रहती है। अधिकार कटौती और लगातार इनकार की समस्या के बीच, इस विशाल डाटा चोरी ने अमरीकी शक्ति की सीमाओं को उजागर कर दिया है। ऐसा प्रतीत होता है कि इस आक्रमण के बाद भी बहुत ज्यादा परिवर्तन नहीं आएगा। अमरीका-चीन साइबर संघर्ष एक प्रमुख साइबर सुरक्षा चिन्ता बनी रहेगी और दोनों देश हमेशा की तरह अपने-अपने रूख पर कायम रहेंगे। व्यक्तियों, समुदायों, व्यापार और राष्ट्रों का प्रतिनिधित्व करने वाले सभी भागीदारों को शामिल करके अत्यंत मजबूत बहुपक्षीय और बहु-क्षेत्रीय हस्तक्षेप के अभाव में गुप्त साइबर

संघर्ष तथा तत्पश्चात सूचना प्रौद्योगिकी को हथियारयुक्त बनाना एक खतरनाक परिदृश्य के रूप में उभरेगा।

डॉ. ओमैर अनास विश्व मामलों की भारतीय परिषद में अनुसंधान अध्येता हैं।

समाप्ति नोट :

[1] "बीजिंग कहता है कि वाशिंगटन द्वारा लगाए गए संघीय साइबर हमले के आरोप 'अवैज्ञानिक' हैं," *ग्लोबल टाइम्स*, 6 जून 2015. ऑनलाइन पुन: प्राप्त http://www.globaltimes.cn/content/925632.shtml (23 जून, 2015 को एक्सेस किया गया)।

[2] "निशाने पर चीन क्योंकि लाखों अमरीकी संघीय कार्यकर्ता साइबर हमले की चपेट में", *रॉयटर*, 5 जून, 2015. पुन: प्राप्ति http://www.reuters.com/article/2015/06/05/cybersecurity-usa-idUSL1N0YQ2GW20150605 (26 जून, 2015 को एक्सेस किया गया)।

[3] "अमरीकी रक्षा उद्योग नवीनतम व्यापक साइबर हमले की जद में है", *द बिजनेस इनसाइडर*, 18 जून, 2015. पुन: प्राप्त http://www.businessinsider.com/r-us-cyber-hack-unsettles-frustrates-us-defense-industry-2015- 6 #ixzz3dsetKSDf (23 जून, 2015 को एक्सेस किया गया)

[4] "साइबर आक्रमण" को चीन का जवाब," *ग्लोबल टाइम्स*, 3 जून, 2015. पुन: प्राप्ति http://www.globaltimes.cn/content /925076.shtml (23 जून, 2015 को एक्सेस किया गया)।

5 "ईरान के साथ परमाणु वार्ता पर साइबर हमलों की रिपोर्टों से इज़रायल का इनकार", *ग्लोबल टाइम्स*, 12 जून, 2015. पुन: प्राप्ति http://www.globaltimes.cn/content/926697.shtml (23 जून, 2015 को एक्सेस किया गया)।

6 "साइबर हमले में कनाडा सरकार की वेबसाइटों की अवमानना", *द गार्जियन*, 18 जून, 2015. पुन:प्राप्ति http://www.theguardian.com/technology/2015/jun/18/canada-government-websites-taken-down-in-cyber- attack (23 जून, 2015 को एक्सेस किया गया)।

7 "साइबर आक्रमण: अप्रैल में 3500 से अधिक उल्लंघन और धमकियां बढ़ना तय, एएफपी कहता हैं", ऑस्ट्रेलियाई प्रसारण निगम, *15 जून, 2015,* पुन:प्राप्ति http://www.abc.net.au/news/2015-06-15/threat-of-cyber- attacks-set-to-increase-says-afp/6547696 (23 जून, 2015 को एक्सेस किया गया)।

8 मार्क पोमरलु, "अमरीका साइबर आक्रमणों का उत्तर कैसे दे सकता है?", पुन: प्राप्ति http://defensesystems.com/Articles/2015/06/10/US-response-scenario-cyber-attack.aspx?Page=4 (10 जून, 2015 को एक्सेस किया गया)।

[9] *ब्रायन ई. फिन्च,* "राष्ट्रीय-राज्यों के साइबर हमलों का सामना कर रही कंपनियों को बेहतर कानूनी संरक्षण की आवश्यकता", वॉल स्ट्रीट पत्रिका, 22 जून, 2015. पुन: प्राप्ति http://blogs.wsj.com/cio/2015/06/22/companies-facing-cyberattacks-from-nation-states-need-better-legal-protection/ (24 जून, 2015 को एक्सेस किया गया)।

[10] जेम्स ए. लुईस, "पूर्वी एशिया, प्रशांत और अंतर्राष्ट्रीय साइबर सुरक्षा गवाही संबंधी उपसमिति एवं नीति सीनेट विदेश संबंध समिति", द यूएस सीनेट, 14 मार्च, 2015. पुन: प्राप्ति http://www.foreign.senate.gov/imo/media/doc /051415_REVISED_Lewis_Testimony.pdf (24 जून, 2015 को एक्सेस किया गया)।

[11] पूर्वोक्त

[12]अकामाई, "अकामाई इंटरनेट की स्थिति: प्रोलेक्सिक त्रैमासिक वैश्विक डीडीओएस हमले की रिपोर्ट", क्यू1 2014 रिपोर्ट, खण्ड 7, संख्या 1. पुन: प्राप्ति http://www.akamai.com/dl/akamai/akamai-soti-q114.pdf (24 जून, 2015 को एक्सेस किया गया)।

[13] ई विपणन, "इस वर्ष दुनिया भर में खुदरा बिक्री 22 खरब डॉलर को पार कर जाएगी", 23 दिसम्बर, 2014. पुन: प्राप्ति http://www.emarketer.com/Article/Retail-Sales-Worldwide-Will-Top-22-Trillion-This-Year/101175 (15 जून, 2015 को एक्सेस किया गया)।

[14] रक्षा विभाग, "डीओडी साइबर रणनीति 2015", रक्षा विभाग।

[15] चांग, एमी, "युद्धरत राज्य: चीन की साइबर सुरक्षा रणनीति", दिसंबर 2014, एक नई अमेरिकी सुरक्षा केन्द्र

[16] पूर्वोक्त