دوفصلنامه ایرانی مطالعات سازمان ملل متحد

دوره ۵، شماره ۲، تابستان و پاییز ۲۰۲۳
صص: ۲۲۰ -۲۰۶

مسئله مرگ و زندگی؛ حملات سایبری به زیرساخت‌های بهداشتی با تاکید بر مباحث مطروحه در جلسه نوامبر ۲۰۲۴ شورای امنیت

کیان بیگلربیگی*، ستار عزیزی**

DOI: 10.22034/iruns.2025.512631.1169

تاریخ دریافت: ۱۴۰۳/۱۲/۲۷ تاریخ پذیرش: ۱۴۰۴/۰۴/۲۱

چکیده

حق بهره‌مندی از پیشرفت‌های علمی از جمله فناوری‌های نوین، همواره یکی از حقوق اساسی بشر قلمداد شده است. امروزه فناوری به ابزاری بسیار مفید برای شناسایی نقص‌ها در یک صنعت خاص و هم‌چنین برای رفع سریع و کارآمد مشکلات تبدیل شده است. این فناوری که به سرعت در حال پیشرفت است، به ویژه در حوزه بهداشت و درمان اهمیت زیادی دارد. در این سیاق، امروزه بدون شک فناوری توانسته است احقاق حق سلامت را تقویت کند. با این حال، از سویی باعث نقض و تضعیف این حق شده است؛ چرا که حملات سایبری به مراکز بهداشتی و درمانی در حال افزایش است، زیرساخت‌های مراقبت‌های بهداشتی جهان در معرض خطر جدی قرار دارد، تاثیرات قابل توجهی بر ارائه خدمات بهداشتی صورت گرفته، ایمنی بیماران به خطر افتاده و سیستم‌های بهداشتی در سراسر جهان متزلزل شده است. از این رو حملات سایبری به زیرساخت-های مراقبت‌های بهداشتی، تهدیدی جهانی است که نمی‌توان آن را نادیده گرفت. در جلسه مورخ

* دانشجوی دکتری حقوق بین الملل، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران.

** استاد، گروه حقوق، دانشکده علوم انسانی، دانشگاه بوعلی سینا، همدان، ایران.s.azizi@basu.ac.ir

۸ نوامبر ۲۰۲۴ شورای امنیت نیز که به درخواست فرانسه، ژاپن، مالت، جمهوری کره، اسلوونی، بریتانیا (رئیس دوره‌ای شورای امنیت در ماه نوامبر) و ایالات متحده آمریکا برگزار شد، ایالات متحده آمریکا به صورت خاص، روسیه را به انجام این حملات متهم کرد. لذا در این مقاله سعی شده است با استفاده از روش توصیفی ـ تحلیلی و شیوه گردآوری اطلاعات به صورت کتابخانه‌ای، به بررسی این موضوع در پرتو این جلسه پرداخته شود.

واژگان کلیدی: حملات سایبری، باج‌افزار، حق بر سلامت، سازمان جهانی سلامت، شورای امنیت.

مقدمه

حق بهره‌مندی از پیشرفت‌های علمی از جمله فناوری‌های نوین، همواره یکی از حقوق اساسی بشر قلمداد شده است. با این حال، همان‌طور که تلالنگ موفوکنگ[1]، گزارشگر ویژه شورای حقوق بشر در مورد حق همه افراد برای برخورداری از بالاترین استاندارد قابل دستیابی سلامت جسمی و روانی[2]، با ارائه گزارش خود در مورد نوآوری دیجیتال، فناوری‌ها و حق سلامت[3] در ۲۲ ژوئن ۲۰۲۳ بیان می‌دارد:«نوآوری دیجیتال حق سلامت را برای برخی تقویت کرده است، اما می‌تواند باعث نقض و تضعیف این حق شود».[4] برای مثال، سوگیری‌های موجود در هوش مصنوعی، نه‌تنها منجر به ناکارآمدی در صنعت مانند تولید می‌شود، همچنین می‌تواند عواقب خطرناکی در

[1] Tlaleng Mofokeng.
[2] Special Rapporteur on the Right of Everyone to the Enjoyment of the Highest Attainable Standard of Physical and Mental Health.
[3] Digital Innovation, Technologies and the Right to Health.
[4] OHCHR. "Special Rapporteur on the Right to Health Says Digital Innovation Has Strengthened the Right to Health for Some, but Warns it Could Enable Violations and Undermine this Right". (2023). Retrieved from https://www.ohchr.org/en/news/2023/06/special-rapporteur-right-health-says-digital-innovation-has-strengthened-right-health.

بخش مراقبت‌های بهداشتی داشته باشد.[۵] علاوه براین، تاثیر پیشرفت فناوری در بُعد وسیع‌تر آن، یعنی ارتباطات و تعاملات دولت‌ها با یکدیگر قابل کتمان نیست. این پیشرفت‌ها از یک سو، باعث تسهیل در امور بشر، زندگی راحت‌تر و افزایش دموکراسی شده است اما از سوی دیگر دارای آثار و تبعات مخربی نظیر مواجهه روزافزون دولت‌ها با حملات سایبری می‌باشد.[۶]

حملات سایبری به زیرساخت‌های مراقبت‌های بهداشتی، تهدیدی جهانی است که نمی‌توان آن را نادیده گرفت. افزایش نگران‌کننده حملات باج‌افزاری[۷]، زیرساخت‌های مراقبت‌های بهداشتی جهان را در معرض خطر جدی قرار داده، ایمنی بیماران را به خطر انداخته و سیستم‌های بهداشتی را متزلزل کرده است. تدروس آدهانوم گبریسوس[۸]، مدیرکل سازمان جهانی سلامت[۹]، در جریان جلسه شورای امنیت که برای بررسی راهبردهای مقابله با این تهدید فزاینده برگزار شد، این هشدار را اعلام کرد، بر لزوم مقابله فوری با این بحران تاکید نمود و خواستار اقدام جهانی هماهنگ برای محافظت از سیستم‌های بهداشتی در برابر تاثیرات مخرب و بالقوه تهدیدآمیز این حملات سایبری شد.[۱۰] او هشدار داد که هکرها از «تهدید علیه ایمنی بیماران، محرمانگی و اختلال

---

[۵] برای مطالعه بیشتر بنگرید به صلحچی، سارا، بیگلربیگی، کیان و عزیزی، ستار، **سوگیری هوش مصنوعی علیه زنان در حوزه سلامت**، مجله علمی پژوهشی حقوق پزشکی، دوره ۱۸، شماره ۵۹، ۱۴۰۳، صص ۲۱۷-۲۳۵.

[۶] برای مطالعه بیشتر بنگرید به بیگلربیگی، کیان. «حملات سایبری و نقض اصل عدم مداخله». پایان‌نامه کارشناسی ارشد حقوق بین-الملل. به راهنمایی ابراهیم بیگ‌زاده. تهران: دانشگاه شهید بهشتی، دانشکده حقوق.

[7] Ransomware Attacks.

حملات باج‌افزاری نوعی حمله سایبری است که در آن یک عامل مخرب فایل‌ها را در یک کامپیوتر یا کل شبکه هک و رمزگذاری کرده و برای رمزگشایی از آن داده‌ها، تقاضای پرداخت وجه می‌کند. این حملات با گذشت زمان در مقیاس و پیچیدگی رشد کرده‌اند، به‌طوری که اکنون هزینه آن‌ها به ده‌ها میلیارد دلار در هر سال می‌رسد.

Fortinet. "Types Of Cyber Attacks". (n.d). Retrieved from https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks; Shafaqna English. "WHO: An alarming surge in cyberattacks putting world's healthcare infrastructure at critical risk". (2024). Retrieved from https://en.shafaqna.com/388655/who-an-alarming-surge-in-cyberattacks-is-putting-worlds-healthcare-infrastructure-at-critical-risk/

[8] Tedros Adhanom Ghebreyesus.

[9] World Health Organization (WHO).

[10] WHO. "WHO Director-General's remarks at Meeting of the United Nations Security Council on the situation of the health system in Gaza – 6 November 2024". (2024). Retrieved from https://www.who.int/director-general/speeches/detail/who-director-general-s-remarks-at-

در خدمات» برای افزایش درخواست‌های باج‌گیرانه خود سوءاستفاده می‌کنند و تحقیقات نشان داده که حملات به بخش‌های بهداشتی از نظر مقیاس و تکرار افزایش یافته‌اند و این به‌دلیل «موفقیت هکرها در حمله به بیمارستان‌ها یا مراکز بهداشتی» است.[۱۱] بر اساس یک نظرسنجی جهانی در سال ۲۰۲۱، بیش از یک‌سوم از موسسات بهداشتی پاسخ‌دهنده، حداقل یک حمله باج-افزاری را در سال گذشته گزارش داده‌اند و یک‌سوم از آن‌ها اعلام کرده‌اند که باج پرداخت کرده‌اند.[۱۲] با این حال، ۳۱ درصد از پاسخ‌دهندگان دسترسی به داده‌های رمزگذاری‌شده خود را بازیابی نکردند.[۱۳]

بحث

در این راستا، جلسه‌ای در روز جمعه ۸ نوامبر ۲۰۲۴ در شورای امنیت سازمان ملل متحد به درخواست فرانسه، ژاپن، مالت، جمهوری کره، اسلوونی، بریتانیا (رئیس دوره‌ای شورای امنیت در ماه نوامبر) و ایالات متحده آمریکا برگزار شد[۱۴] که ایالات متحده آمریکا به‌طور خاص روسیه را مقصر قلمداد کرد.[۱۵]

---

meeting-of-the-united-nations-security-council-on-the-situation-of-the-health-system-in-gaza---6-november-2024

[11] Aydogan, M. "Ransomware attacks on hospitals are 'issues of life and death,' warns WHO chief". ***Anadolu Ajansi***. (2024). Retrieved from https://www.aa.com.tr/en/world/ransomware-attacks-on-hospitals-are-issues-of-life-and-death-warns-who-chief/3388792

[12] Sobers, R. "Ransomware Statistics, Data, Trends, and Facts [updated 2024]". ***Varonis***. (2024). Retrieved from https://www.varonis.com/blog/ransomware-statistics; Aydogan, supra note 11; WHO, "WHO Director-General's remarks at Meeting of the UN Security Council on threats posed by ransomware attacks against hospitals and other health-care facilites and services". (2024). Retrieved from https://www.who.int/director-general/speeches/detail/who-director-general-s-remarks-at-meeting-of-the-un-security-council-on-threats-posed-by-ransomware-attacks

[13] Aydogan, supra note 11.

[14] Mishra, V. "Cyberattacks on healthcare: A global threat that can't be ignored". ***UN News***. (2024). Retrieved from https://news.un.org/en/story/2024/11/1156751

[15] Thehindu. "WHO, 50 countries warn United Nations of increasing ransomware attacks against hospitals". (2024). Retrieved from https://www.thehindu.com/sci-tech/health/who-50-countries-warn-united-nations-of-increasing-ransomware-attacks-against-hospitals/article68848665.ece/amp/

تدروس آدهانوم گبریسوس در توضیحات خود به نمایندگان کشورهای حاضر، به تاثیر شدید حملات سایبری بر بیمارستان‌ها و خدمات مراقبت‌های بهداشتی اشاره کرد و خواستار اقدام فوری و جمعی جهانی برای مقابله با این بحران فزاینده شد. او گفت:«حملات باج‌افزارها و سایر حملات سایبری به بیمارستان‌ها و سایر مراکز بهداشتی تنها مسائل امنیتی و محرمانه نیستند؛ آن‌ها می‌توانند به مقوله مرگ و زندگی مربوط باشند ... در بهترین حالت، این حملات باعث اختلال و زیان مالی می‌شوند و در بدترین حالت، اعتماد به سیستم‌های بهداشتی را که مردم به آن وابسته هستند، تضعیف می‌کنند و حتی باعث آسیب و مرگ بیماران می‌شوند». وی ادامه داد که تحول دیجیتالی مراقبت‌های بهداشتی، همراه با ارزش بالای داده‌های سلامت، این بخش را به هدف اصلی مجرمان سایبری تبدیل کرده است. او به مواردی مانند حمله باج‌افزاری سال ۲۰۲۰ به بیمارستان دانشگاه برنو در چک[۱۶] که بیمارستان را مجبور به خاموش کردن شبکه‌اش کرد و نقض امنیتی سرویس بهداشتی ایرلند[۱۷] در ماه مه ۲۰۲۱ اشاره نمود که خدمات پرتودرمانی را در پنج مرکز اصلی متوقف کرد. حملات سایبری همچنین فراتر از بیمارستان‌ها، زنجیره تامین زیست‌پزشکی[۱۸] را مختل کرده‌اند. در طول همه‌گیری، آسیب‌پذیری‌هایی در شرکت‌های تولیدکننده واکسن‌های کووید-۱۹، فروشندگان نرم‌افزارهای آزمایش‌های بالینی و آزمایشگاه‌ها آشکار شد. او واقعیت نگران‌کننده‌ای را برجسته کرد که حتی درصورت پرداخت باج، دسترسی به داده‌های رمزگذاری شده تضمین نمی‌شود و این مسئله مسیر مقاومت سیستم‌های بهداشتی در سطح جهانی را پیچیده‌تر می‌کند. سازمان جهانی سلامت با همکاری شرکای بین‌المللی متعهد به تقویت تدابیر امنیت سایبری در سراسر بخش بهداشت و درمان است تا از بیماران، داده‌های بهداشتی و یکپارچگی سیستم‌های بهداشتی در سراسر جهان محافظت کند. او با دعوت به همکاری بین‌المللی، از شورای امنیت خواست تا از اختیارات خود برای تقویت امنیت سایبری جهانی و تضمین پاسخ‌گویی استفاده کند. او گفت:«همان‌طور که ویروس‌ها به مرزها احترام نمی‌گذارند، حملات سایبری نیز این‌گونه‌اند.

[16] Brno University Hospital in Czechia.
[17] Health Service Executive (HSE).
[18] Biomedical Supply Chain.

بنابراین همکاری بین‌المللی ضروری است». وی هشدار داد که جرایم سایبری از جمله باج‌افزار، تهدید جدی برای امنیت بین‌المللی است و از اعضای شورای امنیت خواست:«همان‌طور که از اختیارات خود برای تصویب قطعنامه‌ها و تصمیمات در مورد مسائل امنیت فیزیکی استفاده کرده‌اید، اکنون نیز از شما می‌خواهیم که از همان اختیارات برای تقویت امنیت سایبری جهانی، مسئولیت‌پذیری و پاسخ‌گویی استفاده کنید».[۱۹]

بیانیه‌ای مشترک که توسط بیش از ۵۰ کشور - از جمله کره جنوبی، اوکراین، ژاپن، آرژانتین، فرانسه، آلمان و بریتانیا - امضا شده بود، هشداری مشابه داد. این بیانیه که توسط آنه نیوبرگر[۲۰]، هماهنگ‌کننده سیاست امنیت ملی ایالات متحده آمریکا در زمینه سایبر و فناوری‌های نوظهور ارائه شد، بیان داشت:«این حملات تهدیدی مستقیم برای ایمنی عمومی بوده و جان انسان‌ها را با تاخیر در ارائه خدمات بهداشتی حیاتی به خطر می‌اندازند، خسارت اقتصادی قابل توجهی وارد می‌کنند و می‌توانند تهدیدی برای صلح و امنیت بین‌المللی باشند». این بیانیه همچنین کشورهایی را محکوم کرد که «آگاهانه»[۲۱] به کسانی که مسئول حملات باج‌افزاری هستند اجازه فعالیت از خاک خود را می‌دهند. در این جلسه، نیوبرگر مستقیماً مسکو را مورد انتقاد قرار داد و گفت:«برخی کشورها – به ویژه روسیه – همچنان به بازیگران باج‌افزاری اجازه می‌دهند که بدون مجازات از خاک آن‌ها فعالیت کنند». فرانسه و کره جنوبی نیز کره شمالی را متهم کردند. روسیه با ادعای این‌که شورای امنیت محل مناسبی برای بررسی جرایم سایبری نیست، از خود دفاع کرد. واسیلی نبنزیا[۲۲]، نماینده روسیه، گفت:«ما باور داریم که جلسه امروز به سختی می‌تواند استفاده معقول از وقت و منابع شورا

---

[19] The United Nations Meetings Coverage and Press Releases, 9779TH MEETING (AM), SC/15891, "Ransomware Attacks on Healthcare Sector 'Pose a Direct and Systemic Risk to Global Public Health and Security', Executive Tells Security Council". (2024). Retrieved from https://press.un.org/en/2024/sc15891.doc.htm; Wam, "Cyberattacks on healthcare: A global threat to patient safety". (2024). Retrieved from https://www.wam.ae/en/article/147ldvr-cyberattacks-healthcare-global-threat-patient; Mishra, supra note 14.

[20] Anne Neuberger.

[21] Knowingly.

[22] Vassily Nebenzia.

تلقی شود». او افزود:«اگر همکاران غربی ما خواهان بحث درباره امنیت مراکز درمانی هستند، باید در شورای امنیت بر سر گام‌های مشخصی برای توقف حملات وحشتناک اسرائیل به بیمارستان-های نوار غزه توافق کنند».[۲۳]

ادواردو کونرادو[۲۴]، رئیس شرکت «آسِنشن»[۲۵] - سومین سیستم بهداشتی بزرگ ایالات متحده آمریکا - موسسه کاتولیک مذهبی است که سالانه به بیش از ۶ میلیون نفر مراقبت‌های بهداشتی غیرانتفاعی در ایالات متحده آمریکا ارائه می‌کند، بینش‌های دست اولی از واقعیت‌های تلخ حملات باج‌افزاری ارائه داد. او جزئیات حمله سایبری ماه مه ۲۰۲۴ به «آسِنشن» را تشریح کرد که به شدت عملیات را در ۱۲۰ بیمارستان آن مختل کرد. این حمله هزاران سیستم کامپیوتری را رمزگذاری کرد و دسترسی به پرونده‌های الکترونیک سلامت را مختل ساخت و خدمات تشخیصی کلیدی از جمله تصویربرداری پرتو مغناطیسی[۲۶] و سی‌تی اسکن[۲۷] را تحت تاثیر قرار داد. آقای کونرادو چالش‌های عملی به‌وجود آمده را شرح داد:«پرستاران قادر نبودند از ایستگاه‌های کامپیوتری خود پرونده بیماران را مشاهده کنند و مجبور بودند در پشتیبان‌های کاغذی جستجو کنند ... تیم‌های تصویربرداری نمی‌توانستند به سرعت آخرین اسکن‌ها را به جراحانی که در اتاق عمل منتظر بودند ارسال کنند و مجبور بودیم از افرادی برای ارسال نسخه‌های چاپی اسکن‌ها به دستان تیم‌های جراحی استفاده کنیم». این اختلالات نه‌تنها مراقبت را به تعویق انداخت، بلکه خطرات بیماران را افزایش داد و بار فوق‌العاده‌ای بر کارکنان پزشکی که در شرایط پرتنش کار می‌کردند، وارد کرد. بازیابی عملیات ۳۷ روز طول کشید، در این مدت حجم پرونده‌های کاغذی به اندازه معادل یک مایل رشد کرد. او افزود «آسِنشن» که در حال همکاری نزدیک با مقامات ایالات متحده آمریکا است و در حال طی کردن فرآیند طولانی دیجیتال‌سازی داده‌های تمام

---

[23] Thehindu, supra note 15.
[24] Eduardo Conrado.
[25] Ascension Healthcare.
برای مطالعه بیشتر رجوع نمایید به: https://healthcare.ascension.org/
[26] Magnetic Resonance Imaging (MRI) .
[27] Computed Tomography Scan (CT Scan).

سوابق بیمار است که طی آن دوره به صورت کاغذی ایجاد شده است، از نظر مالی حدود ۱۳۰ میلیون دلار برای پاسخ به این حمله هزینه کرد و تقریباً ۰.۹ میلیارد دلار درآمد عملیاتی خود را تا پایان سال مالی ۲۰۲۴ از دست داد.[۲۸]

از سوی دیگر، نمایندگان حاضر در شورای امنیت نیز نگرانی فزاینده‌ای درباره تاثیر این حملات سایبری بر امکانات و خدمات بهداشتی به ویژه در کشورهای در حال توسعه که ظرفیت کافی برای واکنش ندارند، ابراز کردند.

آنه نیوبرگر بر مقیاس تهدیدات باج‌افزاری در بخش بهداشت تاکید کرد و به بیش از ۱۵۰۰ حادثه در کشورش در سال ۲۰۲۳ اشاره کرد که بالغ بر ۱.۱ میلیارد دلار در پرداخت‌ها بوده است که نسبت به سال ۲۰۱۸ ده برابر و نسبت به سال ۲۰۱۴ صد برابر افزایش داشته است. او اشاره نمود برای مختل کردن چنین حملاتی، کشور او در سال ۲۰۲۱ ابتکار بین‌المللی مقابله با باج‌افزار را با عضویت ۶۸ کشور راه‌اندازی کرد که بر مختل کردن حملات باج‌افزار، تقویت امنیت زیرساخت-های حیاتی و افزایش ظرفیت و توانایی پاسخ‌گویی شرکای خود متمرکز است. او با اشاره به تعهد ایالات متحده آمریکا به همراه ۴۰ دولت دیگر برای عدم پرداخت یا اجازه به پرداخت باج‌افزارها توسط نهادهایشان، به این نکته اشاره کرد که برخی دولت‌ها – به ویژه فدراسیون روسیه – همچنان به بازیگران باج‌افزار اجازه می‌دهند که بدون مجازات از قلمرو آن‌ها، حتی پس از درخواست از آن‌ها برای مهار این مسئله، فعالیت کنند. همچنین توسعه‌دهنده گروه جنایتکار سایبری «لاک-بیت»[۲۹] که مسئول بخش بزرگی از حملات باج‌افزار به سیستم‌های بهداشتی در جهان است، دیمیتری خروشِف[۳۰]، شهروند روسی است که توسط وزارت دادگستری ایالات متحده آمریکا متهم به ارتکاب جرائم هک شده است. او اضافه کرد که مجرمان سایبری مرتبط با خطرناک‌ترین

[28] The United Nations Office at Geneva, "Cyberattacks on healthcare: A global threat that can't be ignored". (2024). Retrieved from https://www.ungeneva.org/en/news-media/news/2024/11/100103/cyberattacks-healthcare-global-threat-cant-be-ignored; The United Nations Meetings Coverage and Press Releases, supra note 19.
[29] LockBit.
[30] Dmitry Khoroshev.

گونه‌های باج‌افزار از جمله حمله‌ای که علیه سیستم بهداشتی «آسِنشن» انجام شد نیز با آن کشور ارتباط دارند. او هشدار داد که تا زمانی که باج پرداخت می‌شود و مجرمان می‌توانند از دستگیری فرار کنند، «به ویژه با فرار به کشورهای دیگر»، حملات ادامه خواهد یافت و عاملان افزایش پیدا خواهد کرد. او گفت که جامعه بین‌المللی می‌تواند با عمل جمعی، با تبعیت از مجموعه‌ای از اصول مشترک، اجتناب از پرداخت به باندهای مجرمانه و کمک به یکدیگر برای دستگیری مجرمان سایبری که فکر می‌کنند می‌توانند از سیستم ما پیشی بگیرند، این بلای اجتماعی را ریشه‌کن کند. او همچنین از کشورها خواست که بر خلاف برخی دولت‌ها، به ویژه روسیه، که همچنان اجازه می‌دهند عاملان باج‌افزار از قلمرو آن‌ها بدون مجازات فعالیت کنند، از این رویه پیروی نکنند و به جای آن، مسئولانه در فضای سایبر عمل کرده و به صلح و امنیت بین‌المللی احترام بگذارند.[۳۱] به‌طور مشابه، نمایندگان جمهوری کره و سوئیس به جمهوری دموکراتیک خلق کره اشاره کردند که حدود ۵۰ درصد از درآمد ارزی خود را از طریق «فعالیت‌های سایبری مخرب» به دست می‌آورد.[۳۲]

سایر سخنرانان به بیان تجربیات کشورشان در مقابله با این تهدیدات و ارائه راه حل‌هایی برای کاهش و مقابله با آن‌ها پرداختند. نماینده بریتانیا یادآور شد که سیستم ملی بهداشت این کشور در سال ۲۰۱۷ تحت تاثیر نوعی باج‌افزار قرار گرفت که ۱۱۸ میلیون دلار برای بازیابی هزینه داشت و کشورش ۳۶ مورد تحریم علیه عاملان این فعالیت ها اعمال کرده است.[۳۳] نماینده اسلوونی اشاره کرد که شورا می‌تواند مجرمان سایبری را نیز تحت رژیم تحریمی خود قرار دهد.[۳۴] جی

[31] United States Mission to the United Nations, "Remarks at a UN Security Council Briefing on Ransomware Attacks against Hospitals and Other Healthcare Facilities and Services". (2024). Retrieved from https://usun.usmission.gov/remarks-at-a-un-security-council-briefing-on-ransomware-attacks-against-hospitals-and-other-healthcare-facilities-and-services/

[32] The United Nations Meetings Coverage and Press Releases, supra note 19.

[33] GOV.UK, "The UK will work with international partners to dismantle the cyber criminal ecosystem: UK statement at the UN Security Council". (2024). Retrieved from https://www.gov.uk/government/speeches/the-uk-will-work-with-international-partners-to-dismantle-the-cyber-criminal-ecosystem-uk-statement-at-the-un-security-council

[34] Mirage News, "Ransomware Threats Endanger Global Health Security". (2024). Retrieved from https://www.miragenews.com/ransomware-threats-endanger-global-health-1353751/

دارمادیکاری[۳۵]، نماینده فرانسه با اشاره به رشد حملات باج‌افزاری در کشورش و این که ۱۰ درصد از این‌گونه حملات تاسیسات بهداشتی را هدف حملات خود قرار می‌دهند، از کشورها خواست تا بر سر هنجارهای رفتار مسئولانه برای جلوگیری و مدیریت حوادث سایبری توافق کنند و خواستار پایبندی به هنجارهای بین‌المللی شد و از دولت‌ها خواست تا از استفاده از قلمرو خود برای فعالیت‌های سایبری مخرب جلوگیری کنند. او گفت:«جلساتی مانند جلسه امروز به [شورای امنیت] اجازه می‌دهد تا در جریان تغییرات در حوزه تهدیدات سایبری قرار گیرد». او افزود:«فرانسه آماده است که به همکاری در جهت بهبود درک شورای امنیت از چالش‌های سایبری ادامه دهد». او همچنین از ابتکار ایالات متحده آمریکا که تبادل بهترین شیوه‌ها را برای تقویت واکنش جمعی در برابر چنین ریسک‌هایی که جوامع و دموکراسی‌ها را تهدید می‌کند، حمایت کرد. نماینده ژاپن با اشاره به این‌که حملات باج‌افزار در کشورش مانع از ارائه خدمات به بیماران اورژانسی و انجام جراحی‌های برنامه‌ریزی‌شده شده است؛ بر لزوم تبادل اطلاعات و همکاری بین کشورها از جمله سازمان‌های مجری قانون و افزایش آگاهی نسبت به اهداف بالقوه حملات باج‌افزار تاکید کرد. او افزود که برنامه اقدام کارگروه باز[۳۶] باید به عنوان بستری دائمی برای تضمین انتقال یکپارچه از کارگروه پس از سال ۲۰۲۵ عمل کند. همچنین نماینده مالت تاکید کرد که این حملات حقوق اساسی مرتبط با حریم خصوصی افراد را نقض می‌کنند و رفاه و امنیت کلی شهروندان را تهدید می‌نمایند. او از کشورهای عضو خواست اطمینان حاصل کنند که کارکنان فناوری اطلاعات و ارتباطات[۳۷] به ویژه در حوزه بهداشت، دارای مهارت‌های بروز امنیت سایبری باشند.[۳۸]

سایر هیئت‌ها به ضرورت برگزاری این جلسه تردید داشتند. واسیلی نبنزیا، نماینده فدراسیون روسیه، بیان کرد که مشخص نیست چه تهدید ملموسی برای صلح و امنیت بین‌المللی ایجاد شده است. سازکارهای فراگیر دیگری برای بحث درباره چنین موضوعاتی وجود دارد، کشورش نیز

---

35 Jay Dharmadhikari.
36 The Programme of Action of the Open-Ended Working Group.
37 Information and communications technology (ICT).
38 The United Nations Meetings Coverage and Press Releases, supra note 19.

مکرراً هدف حملات سایبری علیه مراقبت‌های بهداشتی قرار گرفته و بر تعهد طولانی مدت خود به امنیت فناوری اطلاعات و ارتباطات تاکید می‌نماید. او دلیل گنجاندن حملات باج‌افزاری در دستور کار نشست فعلی شورای امنیت را زیر سوال برد و گفت که بحث‌های دیگری در مورد موضوع امنیت سایبری مانند کمیته ویژه سازمان ملل متحد برای تدوین کنوانسیون جامع بین‌المللی مقابله با استفاده از فناوری‌های اطلاعات و ارتباطات برای مقاصد مجرمانه[۳۹] که کشورش آن را آغاز کرده است، وجود دارد و خواستار تسریع در اجرای این کنوانسیون شد و از اعضای شورای امنیت خواست تا پروتکل‌های اضافی از جمله در زمینه حفاظت از زیرساخت‌های حیاتی مانند مراکز بهداشتی در برابر سوءاستفاده از فناوری اطلاعات و ارتباطات را در نظر بگیرند. همچنین به کارگروه باز سازمان ملل متحد درباره امنیت و استفاده از فناوری اطلاعات و ارتباطات اشاره نمود. او تاکید کرد که کشورش طرفدار یک ابزار قانونی بین‌المللی است که تمامی جنبه‌های تامین امنیت در استفاده از فناوری اطلاعات و ارتباطات را پوشش دهد و از طریق سازکاری تحت نظارت سازمان ملل متحد مذاکره شود. او با انتقاد از هیئت نمایندگی ایالات متحده آمریکا به خاطر استفاده از شورا برای ارائه یک «روایت غیرواقعی» که شامل کلیشه رایج و قدیمی «هکرهای روسی» است، خواستار همکاری کمتر سیاسی شد و به تلاش‌های کشورش از جمله راه‌اندازی فهرست تماس‌های بین دولتی در حوزه فناوری اطلاعات و ارتباطات در ماه مه اشاره کرد و گفت که بحث‌ها درباره هکرهای روسی که ظاهراً در برخی حملات دست داشته‌اند، «به نظر می‌رسد به یک شوخی تبدیل شده است، چرا که هر فرد عاقلی می‌تواند به سادگی این ادعا را رد کند».[۴۰] گنگ شوانگ[۴۱]، نماینده چین، نیز موافق بود و بر لزوم راهبردهای جامع و همکاری جهانی برای

---

[۳۹] برای مطالعه بیشتر بنگرید به بیگلربیگی، کیان. «نگاهی اجمالی بر کنوانسیون جامع بین‌المللی مقابله با استفاده از فناوری‌های اطلاعات و ارتباطات برای مقاصد مجرمانه»، تالار گفتگوی تخصصی حقوقی و سیاسی بین‌المللی انجمن ایرانی مطالعات سازمان ملل متحد، (۱۴۰۳). قابل دسترس در: https://unstudies.ir/iauns-forum/

[40] Permanent Mission of the Russian Federation to the United Nations, "Statement by Permanent Representative Vassily Nebenzia at a UNSC briefing on Ransomware Attacks against Hospitals and Other Healthcare Facilities and Services". (2024). Retrieved from https://russiaun.ru/en/news/081124

[41] Geng Shuang.

مقابله با تهدیدات باج‌افزاری و تهدیدات سایبری گسترده‌تر تاکید کرد و به چالش‌های «پیچیده و متنوع» امنیت سایبری که چین با آن روبه‌روست، اشاره کرد. او بیان کرد که حملات سایبری، جرایم سایبری و تروریسم سایبری از جمله باج‌افزارها به طور فزاینده‌ای در حال تبدیل شدن به معضلات جهانی هستند و مسئله باج‌افزار بسیار تخصصی و فنی است و اظهار داشت که هر چند باج‌افزار یک تهدید بزرگ جهانی است، او از اقدام شتاب‌زده اعضای شورا برای تشکیل جلسه امروز حمایت نمی‌کند و امیدوار است بتواند در بحث‌های عمیق‌تر و عملی‌تر از طریق بسترهای مناسب‌تر شرکت کند. جامعه بین‌المللی باید مسئله را از جنبه‌های مختلف از جمله تمرکز بر منبع باج‌افزار، مسیرهای انتشار آن و کانال‌های پولی‌سازی آن، مورد تحلیل و بررسی قرار دهد.[۴۲]

چندین هیئت از جمله الجزایر و اکوادور، به فقدان منابع و تخصص در کشورهای در حال توسعه برای مقابله با تهدیدات سایبری اشاره کردند. نماینده سیرالئون خواستار حمایت از اجرای ابتکارات امنیت سایبری اتحادیه آفریقا و تقویت رویکرد منطقه‌ای برای اطمینان از حفاظت زیرساخت‌های بهداشتی قاره آفریقا در برابر تهدیدات دیجیتالی شد. نماینده موزامبیک خواستار یک استراتژی جامع و متناسب برای مقابله با حملات سایبری در کشورهای در حال توسعه با تمرکز بر آمادگی، پاسخ، بروزرسانی سیستم‌های قدیمی و ایجاد سیاست‌های نظارتی و مشارکت-های قوی شد. نماینده گویان خواستار پاسخ‌گویی مرتکبان حملات باج‌افزار از جمله از طریق همکاری و مشارکت برای تحقیق و پیگرد قانونی جرائم سایبری شد. رئیس هیئت نمایندگی اتحادیه اروپا از همه کشورها خواست تا بر اساس چارچوب سازمان ملل متحد برای رفتار مسئولانه دولت‌ها، اجازه ندهند قلمرو آن‌ها برای چنین فعالیت‌های مخربی استفاده شود و به درخواست‌های مناسب برای کاهش این فعالیت‌ها پاسخ دهند. او تاکید کرد که «ایجاد سازکار دائمی سازمان ملل متحد – برنامه اقدام سایبری سازمان ملل متحد – به ما این امکان را می‌دهد که توانایی جمعی خود را برای مقابله با تهدیداتی مانند باج‌افزار که جوامع و اقتصادهای ما را تهدید می‌کند، ارتقا دهیم» و

[42] Mishra, supra note 14.

بر لزوم یک رویکرد جهانی متحد و هماهنگ برای مقابله موثر با تهدید فزاینده باج‌افزار تأکید کرد.[۴۳]

نتیجه گیری

در مقام نتیجه‌گیری می‌توان گفت که خلأ اسناد معاهداتی و حقوق بین‌المللی عرفی در عرصه‌ی حملات سایبری در فضای سایبر بسیار مشهود است. با این حال، فقدان قواعد خاص به این‌معنا نیست که دولت‌ها می‌توانند بدون محدودیت اقدام به حملات سایبری نمایند و هر چند حقوق عرفی و معاهداتی موجود به صراحت در خصوص حملات سایبری قاعده‌ای ندارد، اما به کمک ابزارهای تفسیر می‌توان قواعد موجود را به حملات سایبری نیز تعمیم داد؛ سازمان‌های بین‌المللی مانند سازمان ملل متحد، اتحادیه اروپا و دولت‌های متعدد از جمله ایالات متحده آمریکا، ایران، بریتانیا، روسیه، ایتالیا، استرالیا، چین، هلند، قطر، کوبا، مجارستان و مالی این نظریه را پذیرفته‌اند؛[۴۴] لذا در پاسخ به این حملات، تا کنون سازمان جهانی سلامت و سایر نهادهای سازمان ملل متحد به طور فعال درحال کمک به دولت‌ها از طریق ارائه کمک‌های فنی، تعیین هنجارها و دستورالعمل‌ها برای تقویت تاب‌آوری زیرساخت‌های بهداشتی در برابر حملات هستند.[۴۵] چنان که آدهانوم گبریسوس بیان داشت:«گزارش کارگروه باز سازمان ملل متحد توصیه‌های متعددی درباره اقدامات قابل انجام توسط کشورهای عضو برای تقویت امنیت سایبری ارائه می‌دهد» و سازمان جهانی سلامت و شرکای آن درحال پیگیری بسیاری از آن توصیه‌ها هستند. وی افزود که در دسامبر ۲۰۲۳، کارشناسان دعوت‌شده توسط سازمان جهانی سلامت چندین چالش کلیدی را شناسایی کردند: ناکامی در انتقال روشن تهدید باج‌افزار و ارزش سرمایه-گذاری در امنیت سایبری به تصمیم‌گیران؛ نبود یک چارچوب روشن برای حکمرانی امنیت سایبری؛ زیرساخت‌های پیچیده‌ای که ایمن‌تر کردن آن‌ها چالش‌برانگیز است؛ شکاف قابل توجه

---

[43] The United Nations Meetings Coverage and Press Releases, supra note 19.

[۴۴] بیگلربیگی، پاورقی شماره ۶، ص ۲.

[45] Aydogan, supra note 11.

بین تقاضا و عرضه جهانی مهارت‌ها و کارشناسان امنیت سایبری و موارد دیگر.[۴۶] در ماه ژانویه، سازمان جهانی سلامت با همکاری اینترپل[۴۷] و دفتر مبارزه با مواد مخدر و جرم سازمان ملل متحد[۴۸] دو گزارش کلیدی با عناوین ابتکار جهانی در زمینه سلامت دیجیتال[۴۹] و ابتکار جهانی هوش مصنوعی[۵۰] برای تقویت امنیت سایبری[۵۱] و مقابله با اطلاعات نادرست[۵۲] منتشر کرده است که برای سلامت، بستری برای گفتگوی بین‌المللی فراهم می‌کند. سازمان جهانی سلامت همچنین در حال آماده‌سازی راهنمای جدیدی درباره امنیت سایبری و حریم خصوصی دیجیتال است که انتظار می‌رود سال آینده منتشر شود.[۵۳] او همچنین بر اهمیت یک رویکرد جامع و با تاکید بر این‌که «امنیت سایبری یک مسئولیت همه‌جانبه برای دولت‌ها است»، گفت که مسئولان و تامین‌کنندگان بخش بهداشت همچنان در قبال تامین امنیت زیرساخت‌های بهداشت دیجیتال مسئول هستند و از کشورها خواست تا نه‌تنها در فناوری‌های پیشرفته برای شناسایی و کاهش حملات سایبری سرمایه‌گذاری کنند بلکه کارکنان را نیز برای واکنش به چنین حوادثی آموزش دهند و تجهیز کنند.[۵۴] او یادآور شد که فناوری نقش کلیدی در امنیت سایبری دارد و تأکید کرد که «باید طرز فکر ما به‌طور ریشه‌ای تغییر کند و بپذیریم که نمی‌توانیم تنها به سیستم‌های فناوری اطلاعات تکیه کنیم».[۵۵] وی توضیح داد که سرمایه‌گذاری در نیروی انسانی و تقویت همکاری‌های بین‌المللی حیاتی است، چرا که «انسان‌ها هم ضعیف‌ترین و هم قوی‌ترین حلقه‌های امنیت سایبری هستند ...

---

46 The United Nations Meetings Coverage and Press Releases, supra note 19.
47 The International Criminal Police Organization (INTERPOL).
48 United Nations Office on Drugs and Crime (UNODC).
49 Global Initiative on Digital Health.
برای مطالعه بیشتر در این‌خصوص رجوع نمایید به: https://www.who.int/initiatives/gidh
50 Global Initiative on AI for Health.
برای مطالعه بیشتر در این‌خصوص رجوع نمایید به: https://www.who.int/initiatives/global-initiative-on-ai-for-health
51 Cybersecurity.
52 Disinformation.
53 WHO, supra note 12.
54 Aydogan, supra note 11.
55 Ibid.

انسان‌ها کسانی هستند که هم حملات باج‌افزاری را انجام می‌دهند و هم می‌توانند آن‌ها را متوقف کنند».[۵۶]

[56] Mishra, supra note 14.