نوع مقاله: **پژوهشی**

تاریخ دریافت: ۱۴۰۰/۰۹/۰۸
تاریخ پذیرش: ۱۴۰۰/۱۲/۰۶
صفحه: ۵۱ الی ۷۴

International Legal Research
تحقیقات حقوقی بین المللی

Volume 15, Issue 58, Winter 2022

Received: 2021/12/29
Accepted: 2022/01/26
Pages: 51-74

System: alr.ctb.iau.ir doi: 10.30495/alr.2022.1946192.2231

Article Type: **Research**

دوره ۱۵ / شماره ۵۸ / زمستان ۱۴۰۱

Cyber Security Regime in International Aviation Law

Hamid Reza Seyedi[1], Seyed Bagher Mirabbasi✉[2], Sohrab Salahi[3]

Abstract

Background and Purpose:

Aviation cyber security is becoming a very serious subject. The air industry is a complex, advanced, multidimensional with an international scope industry is distinguished became its complexity among industries. One of the most important and vital issues of aviation is to ensure the accuracy of navigation systems and air traffic control, which has a direct impact on flight safety. The article is prepared to explain and evaluate the rules of cyber security regime in the field of international aviation law and the responsibility of governments and international organizations in sight of the existing rules of international responsibility plan and through this to examine the conditions and effects of each.

Methodology:

This article was written by descriptive-analytical method in terms of collecting library data and reviewing documents.

Results:

The International Cyber Security Regime is a mechanism for cooperation between governments and cause trust and security, and the protection of aviation infrastructure is a top priority for governments. The aviation industry is facing novel threats, and there are various cyber security concerns at airports and in-flight aircraft, and the need to "smarten up" airports is being seriously felt due to increased connectivity of systems and processes and protection of navigation systems. The development of security rules and regulations is one of the strategic goals of the International Civil Aviation Organization and its member countries, in order to ensure sustainable aviation security measures.

Keywords: Cyber Security Aviation Security International responsibility International Aviation Law

*Citation (APA): Seyedi, H., Mirabbasi, S., & Salahi, S. (2023). Cyber Security Regime in International Aviation Law. International Legal Research, 15(58), 51 -74
https://alr.ctb.iau.ir/article_698512.html

1. PHD student in International Law, Islamic Azad University, Qeshm Branch Email: ab.fars@yahoo.com
2. Professor, Faculty of Law and Political Science, University of Tehran (Corresponding Author) Email: mirabbasi@ut.ac.ir
3. Assistant Professor in Imam Hosain University, Tehran, Iran Email: Salahi.sohrab@gmail.com

Volume 15, Issue 58, Winter 2022

Received: 2021/12/29
Accepted: 2022/01/26
Pages: 51-74

تحقیقات حقوقی بین المللی
International Legal Research

نوع مقاله: **پژوهشی**

تاریخ دریافت: ۱۴۰۰/۰۹/۰۸
تاریخ پذیرش: ۱۴۰۰/۱۲/۰۶
صفحه: ۵۱ الی ۷۴

Article Type: **Research**

doi: 10.30495/alr.2022.1946192.2231 **سامانه:** alr.ctb.iau.ir

دوره ۱۵ / شماره ۵۸ / زمستان ۱۴۰۱

رژیم امنیت سایبری در حقوق بین‌الملل هوانوردی

حمیدرضا سیدی[۱]، سیدباقر میرعباسی ✉[۲]، سهراب صلاحی[۳]

چکیده

زمینه و هدف: امنیت سایبری هوانوردی در حال تبدیل شدن به موضوعی بسیار جدی است. صنعت حمل‌ونقل هوایی، صنعتی پیچیده، با تکنولوژی پیشرفته، چند بعدی و دارای گستره‌ای بین‌المللی می‌باشد و پیچیدگی خاص به لحاظ ماهوی، آن را از سایر صنایع متمایز نموده‌است. یکی از مسائل مهم و حیاتی هوانوردی، اطمینان از دقت سامانه‌های ناوبری و کنترل ترافیک هوایی است، که تاثیر مستقیم بر ایمنی پرواز دارد. قوانین هوانوردی اتحادیه اروپا و همچنین حقوق بین‌الملل مرتبط، با تأکید ویژه بر امنیت سایبری به عنوان موضوعی حیاتی، مدعی‌اند، که وضع موجود، ضوابط مناسبی ندارد و باید تغییر کند. این مقاله در صدد است تا به تبیین و ارزیابی قواعد رژیم امنیت سایبری در حوزه حقوق هوانوردی بین‌المللی و مسئولیت دولت‌ها و سازمان‌های بین‌المللی در پرتو قواعد موجود طرح مسئولیت بین‌المللی بپردازد و از این رهگذر شرایط و آثار هر یک را بررسی نماید.

روش‌شناسی: این مقاله از حیث گردآوری داده‌ها به روش کتابخانه‌ای و به شیوه توصیفی - تحلیلی نگارش گردید.

نتایج و یافته‌ها: رژیم امنیت سایبری بین‌المللی، مکانیزمی برای همکاری بین دولت‌ها و موجب اعتماد و امنیت است و حفاظت زیرساخت‌های هوانوردی برای دولت‌ها، اولویت اصلی می‌باشد. صنعت هوانوردی با تهدیدات نوظهور مواجه است و نگرانی‌های امنیتی سایبری مختلفی در فرودگاه‌ها و هواپیماهای در حال پرواز وجود دارد و ضرورت «هوشمندسازی» فرودگاه‌ها به دلیل افزایش اتصال سیستم‌ها و فرآیندها و محافظت سیستم‌های ناوبری به‌طور جدی احساس می‌شود. تدوین قوانین و دستورالعمل‌های امنیتی جزء اهداف راهبردی سازمان بین‌المللی هواپیمایی کشوری و کشورهای عضو، به منظور اطمینان از اقدامات پایدار امنیت هوانوردی است.

واژگان کلیدی: امنیت سایبری، امنیت هوانوردی، مسئولیت بین‌المللی، حقوق بین‌الملل هوانوردی

*استناددهی (APA): سیدی، حمیدرضا، میرعباسی، سید باقر، صلاحی، سهراب. (۱۴۰۱). رژیم امنیت سایبری در حقوق بین‌الملل هوانوردی. تحقیقات حقوقی بین‌المللی، ۱۵(۵۸)، ۷۴ -۵۱

https://alr.ctb.iau.ir/article_698512.html

۱. دانشجوی دکتری حقوق بین‌الملل دانشگاه آزاد اسلامی قشم
۲. استاد دانشکده حقوق و علوم سیاسی دانشگاه تهران (نویسنده مسؤول)
۳. استادیار گروه حقوق دانشگاه جامع امام حسین(ع) تهران

مقدمه

یکی از مسائل بسیار مهم در هوانوردی، ناوبری و کنترل ترافیک هوایی است که تاثیر مستقیم بر ایمنی و امنیت پرواز دارد. هر سال بیش از ۴/۵ میلیارد مسافر[1] در سراسر دنیا توسط شبکه حمل‌ونقل هوایی جابجا می‌شوند. حفظ و تقویت ایمنی و امنیت برای این حجم بالای مسافر مستلزم توسعه راهکارهای جدید در حوزه هدایت و ناوبری هوایی است. سامانه‌های ناوبری مبتنی بر ماهواره یکی از بهترین و دقیق‌ترین روش‌های ارائه شده برای موقعیت‌یابی هواپیماها هستند. این مقاله توجه خاصی به حملات جعل[2] و اخلال[3] در پخش سیگنال سامانه ماهواره‌ای ناوبری جهانی (GNSS)[4] و سیستم‌های ارتباطی، ناوبری و راداری[5] (CNS) زمینی که توسط هواپیماها دریافت می‌شود، دارد. زیرا سیستم‌های ناوبری ماهواره‌ای هوانوردی فعلا در اختیار دو کشور ابرقدرت جهان (امریکا و روسیه) قرار دارند و آینده بهره‌برداری و استفاده امن و مطمئن برای کشورهای متخاصم با این کشورها و بویژه جمهوری اسلامی ایران که بیش از چهار دهه با امریکا خصومت دارد و تحت «فشار حداکثری» تحریم است، با افزایش تنش‌های بی‌سابقه و درگیری‌های منطقه‌ای مانند؛ هک سیستم هواپیمای بدون سرنشین«RQ-170 ایالات متحده امریکا» دسامبر ۲۰۱۱ و فرود آن در ایران و یا سرنگونی هواپیمای بدون سرنشین« RQ-4،گلوبال هاوک» متعلق به نیروی هوایی آمریکا در دریای عمان، آینده پرتلاتمی صنعت هوانوردی ایران خواهد داشت.

یک تحلیلگر ارشد هوانوردی و نویسنده[6] در خصوص "پیش‌بینی امنیت سایبری هوانوردی ۲۰۱۵- ۲۰۲۵"، در مارس۲۰۱۵ اظهار داشت: "تهدید حمله سایبری صنعت هوانوردی واقعی است" و بیشتر این حملات با اهداف جنایت‌کارانه یا تروریستی خواهد بود. او همچنین در تحلیل خود چهار حوزه فرعی را ارائه کرد که عبارتند از: سیستم‌های هواپیما/ هواپیمایی، سیستم‌های فرودگاه‌ها، سیستم‌های رزرو کامپیوتری/ سیستم توزیع جهانی (CRS/GDS)[7]، و سیستم‌های مدیریت ترافیک هوایی (Others, 2016 & Holt).

در بیان ضرورت طرح رژیم امنیت سایبری می‌توان اذعان نمود؛ وجود سامانه‌های ماهواره‌ای ناوبری جهانی برای جهت‌یابی مقصد امروزه به یکی از تجربیات روزمره هر یک از ما تبدیل شده است. صنعت حمل‌ونقل هوایی خیلی زودتر با راهکارهای مبتنی بر سامانه ماهواره‌ای ناوبری جهانی پیوند یافته است. سرویس‌های مبتنی بر سامانه ماهواره‌ای ناوبری جهانی با فعالیت دو سیستم

1. https://www.iata.org/contentassets/iata-annual-review-2020.pdf
2. Spoofing
3. jamming
4. Global Navigation Satellite Systems
5. Communication, Navigation, Surveillance
6. Visiongain
7. Computer reservations systems/ Global Distribution System

ماهواره‌ای؛ سیستم موقعیت‌یاب جهانی (GPS)[۱] و سیستم ماهواره‌ای ناوبری جهانی (Glonass)[۲] که به ترتیب توسط ایالات متحده و فدراسیون روسیه ارائه می‌شوند، امکان‌پذیر شد. سیگنال‌های GPS و گلوناس در استانداردها و روش‌های توصیه‌شده (SARPs)[۳] در پیوست ۱۰ کنوانسیون شیکاگو تحت عنوان «مخابرات هوانوردی»[۴] تعریف شده‌اند. شورای ایکائو هر دو پیشنهاد را پذیرفت. هر دو کشور در حال ارتقای ماهواره‌های خود هستند و به ایکائو متعهد شده‌اند که تمام اقدامات لازم را برای حفظ قابلیت اطمینان خدمات انجام دهند. اروپا و چین نیز در حال توسعه سیستم‌هایی[۵] هستند به ترتیب گالیله[۶] و سیستم ماهواره‌ای ناوبری BeiDou[۷] که با GPS و گلوناس ارتقای یافته قابل همکاری خواهند بود. (Doc9849, 2017: 5) از این رو در اواخر دهه ۱۹۸۰ میلادی، کارگروه سیستم‌های ناوبری هوایی آینده ایکائو، معروف به (FANS)[۸] فعالیت خود را برای آگاهی بخشی از اهمیت نقش سامانه ماهواره‌ای ناوبری جهانی در آینده هوانوردی آغاز کرد.

در ماه مارس ۱۹۹۱، نشریه ایکائو مقاله‌ای را با عنوان «ورود به عصر ناوبری ماهواره‌ای» منتشر کرد. از سال ۱۹۹۳، سیستم موقعیت‌یابی جهانی مورد استقبال گسترده کشورها و شرکت‌های هواپیمایی قرار گرفت. (Doc9849, 2017: 2) با گسترش سامانه‌های ماهواره‌ای و استفاده هواپیماها، افزایش پیچیدگی و مقیاس جعل سیگنال‌های سیستم موقعیت‌یابی جهانی، گزارش شد و اخیراً در حوزه دریایی نیز مشاهده شده است و نشان می‌دهد که چگونه تکنیک‌های دشمن به سرعت در حال پیشرفت است.

علاوه بر جعل ماهواره‌ها، سال‌هاست که امنیت سایبری «سامانه نظارتی خودکار وابسته» معروف به (ADS-B)[۹] مورد بحث قرار گرفته است. این سامانه به عنوان یک فناوری نظارتی که از GPS و پخش موقعیت برای کمک به آگاهی از موقعیت و جداسازی استفاده می‌کند، به سرعت به سنگ بنای سیستم مدیریت ترافیک هوایی تبدیل می‌شود. اما، چالش‌ها همچنان باقی است. قطعی‌های ناشی از وقفه سیگنال‌ها یا جعل می‌تواند به سرعت باعث ایجاد اثرات مخرب عملیاتی شود. به عنوان مثال، در سال ۲۰۱۹، یک مدت کوتاه ایجاد خطای سیستمی در برخی از واحدهای ADS-B باعث لغو حدود ۴۰۰ پرواز شد (Atlantic Council, 2019: 5).[۱۰]

---

۱. سیستم ناوبری ماهواره‌ای یا موقعیت‌یاب جهانی ایالات متحده معروف به (GPS) System Global Positioning.

۲. سیستم ناوبری ماهواره‌ای روسیه معروف به گلوناس (Glonass Global Navigation Satellite System).

3. Standards and Recommended Practices
4. Annex 10, Aeronautical Telecommunications
5. https://www.gps.gov/systems/gnss/

۶. سیستم ناوبری ماهواره‌ای اروپا معروف به گالیله. Galileo

۷. سیستم ناوبری ماهواره‌ای چین معروف به BeiDou

8. Future Air Navigation System (FANS(
9. Automatic Dependent Surveillance- Broubcast
10. Website :www.atlanticcouncil.org

اهمیت موضوع پژوهش از این باب است که؛ تدوین مقررات و تعیین مسئولیت برای دولت‌ها ضروری است، تا به یک تعهد بین‌المللی به طور مؤثر عمل کنند.

در واقع عرف نیز ممکن است به یک وظیفه صریح برای دولت‌ها تبدیل شود، مانند؛ «احتیاط لازم»[1] یا «مراقبت لازم یا شایسته»[2] که به عنوان «استاندارد منطقی قابل انطباق با واقعیت‌ها و شرایط خاص در چارچوب قانون کلی» توصیف می‌شود و در هوانوردی زیربنای اصل ایمنی قرار می‌گیرد.

اگرچه تعریف دقیق اصل احتیاط لازم دشوار است، اما چندین عنصر را می‌توان از رویه قضایی و رویه معاهداتی استخراج کرد تا ویژگی‌های آن را به عنوان یک مفهوم و اصل شناسایی کند. (ILA 8&7 :2016) تجاربی مانند واقعه ۱۱ سپتامبر ۲۰۰۱ نشان داد که در صورت وقوع هر تهدیدی از ناحیه فضای سایبر، دو اقدام باید به سرعت انجام شود. نخست ارائه یک واکنش مثبت جهت تحدید بحران و آماده کردن فضای مناسب برای مدیریت اوضاع و دوم تهیه و اعمال سیاست‌هایی که بتواند مانع از تکرار وضعیت شود. برای توجه به تخصصی بودن هر دو فعالیت، لازم است که گروه‌های کارشناسی تحلیل راهبردی، تحلیل تاکتیکی و آسیب‌شناسی فضای مجازی، کاملاً فعال باشند و با کم‌ترین خطر و در زمان کوتاه، بیش‌ترین بهره را ببرند. (صیاد و دیگران، ۱۳۹۹: ۲۹۷) برخی از کشورها برای این موضوع حیاتی برنامه‌ریزی کرده‌اند، از آن جمله به استراتژی‌های هوانوردی کشور قطر می‌توان اشاره کرد؛ «رویکرد کلیدی مدیریت خطرات امنیت سایبری در بخش حمل‌ونقل هوایی قطر، توسعه رویکرد ۳۶۰ درجه است. یک استراتژی جامع، تا قادر به پیش‌بینی خطرات سایبری برای اکوسیستم هوانوردی باشد.»[3] این پژوهش در صدد رسیدن به پاسخ این سئوال است که دولت‌ها در مواجه با تهدیدات نوظهور و نگرانی‌های امنیتی سایبری در فرودگاه‌ها و هواپیماهای در حال پرواز چه مسئولیت‌هایی دارند؟ لذا به بررسی و تبیین وضعیت امنیت سایبری هوانوردی در حقوق بین‌الملل و مسئولیت‌های مترتب بر آن در چهار بخش با مباحث حقوق بین‌الملل هوانوردی، حقوق امنیت هوانوردی، رابطه امنیت سایبری با حقوق بین‌الملل و مسئولیت بین‌المللی دولت‌ها می‌پردازد.

1. due diligence
2. due, or merited, care
3.https://www.caa.gov.qa/ar,qa/PrintedPublications,Documents,CS,CSPS,Guidelines,Aviation , Sector, English, V1.5.pdf

۱- حقوق بین‌الملل هوانوردی

حقوق هوانوردی شاخه‌ای جدید از حقوق بین‌الملل است که بر جنبه‌های قانونی و تجاری پرواز و حمل‌ونقل هوایی مانند حقوق ترافیک هوایی، ایمنی و امنیت هوانوردی، مقررات اقتصادی شرکت‌های هواپیمایی و عملکرد فرودگاه‌ها نظارت می‌کند.[۱]

سازمان ملل متحد به‌کارگیری اصول حقوق بین‌الملل را به عنوان بخش جدایی‌ناپذیر حفظ صلح و امنیت بین‌المللی و پرهیز از موقعیت‌هایی که منجر به نقض صلح می‌شوند، تشخیص داده است.[۲] تروریسم مجازی تنها امنیت حمل‌ونقل هوایی را متأثر نمی‌کند. تروریسم مجازی به طرق گوناگون به کار گرفته می‌شود. می‌توان از آن به عنوان وسیله‌ای برای اطلاع‌رسانی کذب یا جنگ روانی از طریق منحرف کردن توجه رسانه‌ها در رابطه با تهدیدات ممکن استفاده کرد و از این‌رو، منجر به وقفه در فعالیت فرودگاه‌ها و هواپیماها شد. (نمامیان و شیرزاد، ۱۳۹۹: ۱۸۷) مانوئل گویل کارشناس برجسته در ارزیابی تهدید گفته: می‌توان به روش‌های بسیار ساده از تروریسم سایبری استفاده کرد. این نوع تروریسم به ساده‌ترین شکل خود به عنوان روشی برای جنگ دروغ پراکنی یا جنگ روانی با منحرف کردن توجه رسانه‌ای از تهدیدات ممکن به کار می‌رود که سبب اختلال در عملیات فرودگاه و ناوگان هوایی می‌شود که آن هم به نوبت خود به اکراه مسافران برای سفر هوایی ختم می‌شود و اقتصاد کشورهای وابسته به جابه‌جایی مسافران هوایی را متاثر می‌سازد. تروریسم سایبری در خطرناک‌ترین شکل خود به مرگ و میر، جراحات و خسارت شدید به فرودگاه و به هواپیماهای درحال پرواز منجر می‌شود. (آبیرانته، ۱۳۹۴: ۷۳) برای مقابله با تهدیدات سایبری و اطمینان از اینکه صنعت هوانوردی غیرنظامی در برابر حملات سایبری مقاوم و در سطح جهانی ایمن و قابل اعتماد است، در سال ۲۰۱۹، استراتژی امنیت سایبری هوانوردی[۳] ایکائو مورد تأیید قرار گرفت. در پی نتایج چهلمین نشست مجمع ایکائو، بر ضرورت انجام اقدامات بیشتر برای مقابله با تهدیدات سایبری توسط دولت‌ها و صنعت تاکید شد. سازمان‌های بین‌المللی که در رأس آنان سازمان ملل متحد وجود دارد و همچنین شورای وزرای اروپا که نقش فزاینده‌ای را در جهت تقویت و گسترش جرم‌انگاری جرایم سایبری در دهه اخیر ایفا کرده‌اند، می‌توانند با استفاده از کمیته‌های تخصصی و استفاده از متخصصان دیگر کشورها که در زمینه تروریسم سایبری و جرم‌انگاری آن پیشتاز بوده‌اند، برای تدوین کنوانسیون‌های الزام‌آور بین‌المللی در خصوص پیشگیری از تروریسم سایبری و حمایت ویژه از بزه‌دیدگان آن اقدام کنند. (قدیر و کاظمی، ۱۳۹۸: ۲۶۱) از کارانداختن ماهواره‌ها به وسیلهٔ جنگ افزارهای لیزری و یا پارازیت انداختن بر روی آن‌ها، از جمله مهم‌ترین آسیب‌پذیری است

1. http://www.aviation-safety-bureau.com

۲. ماده یک منشور سازمان ملل متحد

3. ICAO, Aviation Cybersecurity Strategy ,October 2019.

که می‌تواند آماجی برای سوءاستفاده دشمنان بالقوه باشد. اتکای بیش از حد صنعت اطلاعات به تجهیزات خارجی نارسایی و ناکافی بودن تأسیسات امنیتی، ناتوانی برای سنجش ایمنی تجهیزات وارداتی و عدم آگاهی جامعه از اهمیت ایمنی اطلاعات، دیگر تهدیدهایی است که امنیت را در جامعه به خطر می‌اندازد. (سلطانی‌نژاد و همکاران، ۱۳۹۲: ۱۰۱) قلمرو فعالیت هواپیمایی کشوری دارای یک زمینه ذاتی بین‌المللی است و حقوق بین‌الملل قواعدی دارد که روابط، اقدامات متقابل و همکاری بین کشورها را در حالی که از مرزهایشان فراتر می‌رود، قانون‌مند می‌سازد. بنابر این حقوق هوانوردی را بیشتر تحت تاثیر حقوق بین‌الملل باید دانست تا حقوق داخلی.

۱ -۱- معاهدات و مقررات هوانوردی بین‌المللی

معاهدات بین‌المللی نقش اصلی را در شکل‌گیری حقوق بین‌الملل هوانوردی دارند. منشور ملل متحد مهم‌ترین منبع حقوق بین‌الملل محسوب می‌شود و بر طبق بند ۴ ماده ۲ منشور، تمامی کشورها از «تهدید به استفاده از زور» یا «استفاده از زور»[1] یا روش دیگر (مانند حملات سایبری هوانوردی) علیه تمامیت ارضی و استقلال سیاسی سایرکشورها برحذر داشته شده‌اند و در بند ۷ نیز از دخالت در امور داخلی سایر کشورها منع شده‌اند (اصل منع مداخله).

شورای امنیت در قطعنامه ۲۳۴۱ (۲۰۱۷) «با تاکید مجدد بر مسئولیت اصلی خود در قبال حفظ صلح و امنیت بین‌المللی، مطابق با منشور ملل متحد، تاکید مجدد بر احترام به حاکمیت، تمامیت ارضی و استقلال سیاسی همه کشورها و تاکید مجدد بر اینکه تروریسم در همه اشکال و مظاهر آن یکی از جدی‌ترین تهدیدها برای صلح و امنیت بین‌المللی است و هرگونه اقدام تروریستی صرفنظر از انگیزهای آن‌ها، در هر زمان، هر کجا و توسط هرکس که مرتکب شده باشد، مجرمانه و غیرقابل توجیه است. قانون حقوق بین‌الملل بشردوستانه و منشور ملل متحد، با تاکید بر اینکه تروریسم نباید با هیچ دین، ملیت، تمدن یا گروه قومی مرتبط شود، تاکید می‌کند که مشارکت و همکاری فعال همه دولت‌ها و سازمان‌های بین‌المللی، منطقه‌ای و زیرمنطقه‌ای ضروری است.»[2] حوادث ۱۱ سپتامبر در هرحال خشن‌ترین، پیچیده‌ترین و مدرن‌ترین نوع ترور و تخریب بود که تاکنون در حوزه حمل‌ونقل هوایی به وقوع پیوسته است. این حادثه نشان داد حمل‌ونقل هوایی غیرنظامی یک هدف آسیب‌پذیر و بسیار جذاب برای تروریست‌ها بوده و هست. تابحال با تلاش‌های مستمر برای مقابله با این حملات و تهدیدها و حمایت از امنیت هواپیمایی کشوری و مبارزه با تروریسم، دهها کنوانسیون، پروتکل بین‌المللی، دستورالعمل و مقرره توسط سازمان‌های بین‌المللی مانند؛ سازمان ملل متحد، ایکائو، انجمن بین‌المللی حمل‌ونقل هوایی

1. Threat or use of force
2. https://undocs.org/S/RES/2341(2017(

(IATA)[1]، اتحادیه فرودگاه‌های بین‌المللی (ACI)[2]، اتحادیه اروپا، کمیسیون اروپایی، آژانس ایمنی هوانوردی اروپا (EASA)[3]، سازمان اروپایی تجهیزات هواپیمایی کشوری (EUROCAE)[4]، سازمان خدمات ناوبری هوایی غیرنظامی (CANSO)[5]، مرکز کنترل اروپا EUROCONTROL[6]، RTCA[7]، رادیو هوانوردی، (ARINC)، سازمان بین‌المللی استاندارد[8] (ISO)، انجمن بین‌المللی اتوماسیون، تدوین شده است که مورد استفاده حوزه امنیت سایبری هوانوردی می‌باشند و اهم آن‌ها به شرح زیر است:

الف) کنوانسیون‌های حقوق بین‌الملل هوایی

- کنوانسیون سرکوب تصرف غیرقانونی هواپیماها (۱۹۷۰)
- کنوانسیون سرکوب اقدامات غیرقانونی علیه ایمنی هوانوردی غیرنظامی (۱۹۷۱)
- پروتکل سرکوب اقدامات غیرقانونی خشونت در فرودگاه‌های خدمات هوانوردی غیرنظامی بین‌المللی.
- مکمل کنوانسیون سرکوب اقدامات غیرقانونی علیه ایمنی هوانوردی غیرنظامی (۱۹۷۱)
- کنوانسیون سرکوب اقدامات غیرقانونی مربوط به هوانوردی غیرنظامی بین‌المللی (۲۰۱۰)
- پروتکل تکمیلی پکن به کنوانسیون ۱۹۷۰ لاهه برای سرکوب تصرف غیرقانونی هواپیماها (۲۰۱۰)

ب) مقررات سازمان بین‌المللی هواپیمایی کشوری (ICAO)

- کتابچه امنیت هوانوردی، ضمیمه ۱۷ ایکائو
- راهنمای امنیت هوانوردی، سند ۸۹۷۳
- راهنمای امنیت مدیریت ترافیک هوایی، سند ۹۹۸۵
- سند خطرات جهانی، سند ۱۰۱۰۸
- قطعنامه مجمع عمومی ایکائو A40-10

اسناد و مقررات دیگری نیز در این حوزه وجود دارد که به علت اطاله کلام درج آن‌ها در اینجا میسر نشد.

1. International Air Transport Association
2. Airports Council International
3. European Aviation Safety Agency
4. European Organisation for Civil Aviation Equipment
5. Civil Air Navigation Services Organisation
6. European Agency for the Safety of Air Navigation
7. Radio Technical Commission for Aeronautics (RTCA(
8. International Organization for Standardization

۱- ۲- حقوق بین‌الملل عرفی

مجمع عمومی سازمان ملل متحد قطعنامه‌های متعددی تصویب و عوامل تهدیدکننده صلح و امنیت بین‌المللی را یادآور شده است؛ از آن جمله قطعنامه ۲۹۰ دسامبر ۱۹۴۹، قطعنامه ۲۲۲۵ دسامبر ۱۹۶۶، قطعنامه ۲۶۲۵ اکتبر ۱۹۷۰، قطعنامه ۳۳۱۴ دسامبر ۱۹۷۴ و قطعنامه ۳۶/۱۰۳ دسامبر ۱۹۸۱.

این قطعنامه‌ها از تمامی کشورها می‌خواهند که از به‌کارگیری هرگونه تهدید و اعمال زور چه به صورت مستقیم (قوای نظامی) و چه به صورت غیرمستقیم (جاسوسی و حملات سایبری) علیه سایر کشورها خودداری نمایند. همچنین از هرگونه اقدامات پنهان و مخفی علیه حاکمیت و استقلال سیاسی سایر کشورها خودداری و اصل عدم مداخله را رعایت نمایند. اگرچه قطعنامه‌های مجمع عمومی قدرت الزام‌آوری ندارند، لیکن ارزش قاعده‌سازی و تبدیل شدن به قاعده عرفی را دارند. همچنین اعمال یک جانبه دولت‌ها هر چند قاعده حقوقی بمعنی خاص کلمه منبع مستقل حقوق بین‌الملل عمومی محسوب نمی‌شود، اما برای عاملان آن‌ها دارای اعتبار و آثار مشخصی است. البته به شرطی که به قصد ایجاد تعهد صادر شده باشد.

۱- ۲ -۱- اصل عدم مداخله

اصل منع مداخله در امور کشورها نه تنها در بند ۷ مادۀ ۲ منشور بیان شده است، بلکه از اهم موضوعاتی است که از دیرباز به عنوان یک اصل عرفی حقوق بین‌الملل مورد قبول جامعه جهانی بوده است. حقوقدانان در تعریف مداخله بیان کرده‌اند که هرگونه ورود و دخالت در قلمرو حاکمیتی یک کشور که به قصد صدمه به منافع دولت قربانی منتج شود، مداخله محسوب می‌شود. پس حملات سایبری هوانوردی از یک کشور به تاسیسات کشور دیگر می‌تواند از مصادیق تعرض و مداخله در امور حاکمتی سایرین باشد.

۱- ۲-۲- عدم توسل به زور

اصل عدم توسل به زور مندرج در ماده ۲ بند ۴ منشور سازمان ملل متحد به کرات از سوی دولت‌ها نه به عنوان اصل عرفی، بلکه به منزله یک اصل بنیادین حقوقی نیز پذیرفته شده است. کمیسیون حقوق بین‌الملل به هنگام تدوین کنوانسیون وین حقوق معاهدات ابراز داشته که حقوق منشور راجع به ممنوعیت استفاده از زور نمونه بارز قاعده‌ای است که در حقوق بین‌الملل ویژگی قاعده آمره را دارد. (زرنشان، ۱۳۹۲: ۲۸۴) بنابراین هرگونه توسل به زور و اعمال خشونت علیه هواپیمایی کشوری بین‌المللی مغایر با بند ۴ ماده ۲ منشور ملل متحد و قواعد حقوق بین‌الملل عرفی محسوب می‌گردد.

کنوانسیون ۱۹۷۱ مونترال اعمال غیرقانونی بر ضد امنیت هواپیمایی کشوری را جرم‌انگاری نمود. براساس این کنوانسیون که در پی کنوانسیون ۱۹۷۰ لاهه تصویب شد، سایر خشونت‌های علیه هواپیما و سرنشینان آن را جرم شناخته است؛ از جمله بمب‌گذاری در هواپیما، ایجاد اختلال در سرویس‌های هوانوردی و هواپیماربایی، همچنین در بند «د» ماده یک کنوانسیون آمده است؛ «هرکس تاسیسات یا سرویس‌های هوانوردی را از بین برده یا به آن‌ها آسیب برساند یا در فعالیت آن‌ها اختلال ایجاد کند و ماهیت هر یک از اقدامات مذکور امنیت هواپیمای در حال پرواز را به خطر اندازد، مجرم شناخته می‌شود».

شورای امنیت سازمان ملل متحد در پی سرنگونی هواپیمای ام اچ ۱۷ مالزی[1] در تاریخ ۲۱ جولای ۲۰۱۴ برای اولین بار در حوزه هوانوردی اقدام به تصویب قطعنامه ۲۱۶۶[2] مبنی بر محکومیت سرنگونی هواپیمای مالزی، هر گونه خشونت و زور علیه ایمنی و امنیت هوانوردی را تهدید علیه صلح و امنیت بین‌المللی قلمداد نمود و مغایر قواعد بین‌المللی دانست. این اقدام شورای امنیت نقطه عطفی در حوزه حقوق بین‌الملل هوانوردی محسوب می‌شود و موجب توسعه حقوق بین‌الملل و تدوین قواعد و مقررات جدید در مفهوم عام خواهد شد.

۱ -۳- رویه‌های قضایی

در قضیه نیکاراگوئه دیوان بین‌المللی دادگستری بر اساس نظر قاضی سیت کامارا[3] در نظریه جداگانه‌ای بیان کرد؛ «در صورتی که معیار مندرج در ماده ۵۳ کنوانسیون وین در خصوص معاهدات را به کار گیریم، اصل عدم مداخله به عنوان قاعده آمره تلقی می‌شود.» (اسماعیل‌زاده و عبداللهی، ۱۳۹۹: ۷۲۴) همچنین دیوان بین‌المللی دادگستری در قضیه پالپ میلز[4] بیان کرد: «اصل پیشگیری یک قاعده عرفی است، و به همین دلیل منشأ آن در احتیاط مقتضی است که در قلمرو یک دولت لازم است.» در همین راستا، با استناد به داوری ادعاهای آلاباما، دادگاه Trail Smelter[5] اعلام کرد که هر دو داوری براساس «اصل کلی همانندی»[6] تصمیم گرفته شده‌اند، که طبق آن «یک دولت همیشه موظف است در برابر اعمال زیان‌بار افراد از داخل کشور و حوزه صلاحیت خود، علیه سایر کشورها حمایت کند.» (Dias, 2021: 35 & Coco) قواعد حقوق بین‌الملل مورد بحث در این بخش دلالت بر امکان پیگیری حقوقی هرگونه حملات سایبری خشونت بار علیه امنیت هوانوردی دارد.

1. MH17
2. S/RES/2166(2014). Para 1.
3. Judge Sette-Camara
4.Pulp Mills case (Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, I.C.J .Reports 2010
5. Trail Smelter (United States v. Canada) (1941) 3 RIAA 1911, at 1963, 196
6. same general principle

۲- حقوق امنیت هوانوردی

سه تهدید فاحش و نوظهور برای هواپیمایی کشوری؛ تروریسم زیستی، تروریسم سایبری و سوءاستفاده از موشک‌های دوشی زمین به هوا می‌باشد. (آبیرانته، ۱۳۹۴: ۶۱) امنیت سایبری در هواپیمایی در حال تبدیل شدن به موضوعی بسیارجدی است. قانون هواپیمایی اتحادیه اروپا و همچنین حقوق بین‌الملل مرتبط، با تأکید ویژه بر امنیت سایبری به عنوان موضوعی حیاتی، مدعی است، که وضع موجود، قانونی مناسب نیست و باید تغییر کند. ایجاد یک فرهنگ جامع امنیتی برای امنیت هواپیمایی موثر و طولانی مدت ضروری است.[1]

برنامه جهانی ایمنی هواپیمایی[2](GASP) استراتژی ارائه شده از اولویت بندی و بهبود مستمر ایمنی هواپیمایی را پشتیبانی می‌کند. برنامه جهانی ایمنی هواپیمایی، همراه با برنامه جهانی ناوبری هوایی[3](GANP) و سند [4](Doc 9750) چارچوبی را فراهم می‌کنند که در آن برنامه‌های ایمنی هواپیمایی منطقه‌ای و ملی تدوین و اجرا می‌شود.کارگروه امنیت هواپیمایی ایکائو بیستمین اجلاس خود را از سی‌ام مارس الی سوم آوریل ۲۰۰۹ در مونترآل برگزار کرد. یکی از مسائل بسیار مهم در این اجلاس توجه به تهدیدات جدید و نوظهور هواپیمایی کشوری بود، به نحوی که پیشرفت قابل ملاحظه‌ای در شناسایی کُنشی چالش‌ها و عدم تطابق فعالیت کشورها حاصل گردیده که موجب تقویت پیوست۱۷ (امنیت هواپیمایی) کنوانسیون هواپیمایی کشوری بین‌المللی شد. همچنین در ادامه این اجلاس، «کنفرانس هواپیمایی کشوری اروپا» [5] برگزار و بر تاثیر تهدیدات سایبری ناشی از فقدان مقرره‌های مربوطه در پیوست ۱۷ تأکید گردید.

ایکائو به منظور پیشرفت سریع در هدف اصلی خود یعنی افزایش اثربخشی امنیت هوانوردی جهانی و بهبود اجرای عملی و پایدار اقدامات پیشگیرانه امنیت هوانوردی، پنج اولویت کلیدی را شناسایی کرد، به نحوی که دولت‌ها و ذینفعان باید توجه فوری خود را در آن‌ها متمرکز کنند. (ICAO Doc10118,2017) شورای امنیت سازمان ملل متحد نیز براساس قطعنامه ۱۳۷۳ (۲۰۰۱) از کشورهای عضو خواسته است« تا راه‌هایی برای تشدید و تسریع تبادل اطلاعات عملیاتی، به ویژه در مورد اقدامات یا تحرکات افراد یا شبکه‌های تروریستی بیابند. اسناد مسافرتی جعلی یا اسناد جعلی حمل‌ونقل اسلحه، مواد منفجره یا مواد حساس؛ استفاده از فناوری‌های ارتباطی توسط گروه‌های تروریستی؛ و تهدید ناشی از در اختیار داشتن سلاح‌های کشتار جمعی توسط گروه‌های تروریستی و همچنین همکاری، به ویژه از طریق ترتیبات و توافقات دوجانبه و چند جانبه، برای جلوگیری و سرکوب حملات تروریستی، با توجه به کار سازمان‌ها، نهادها، انجمن‌های بین‌المللی،

1. Report of the Second High-level Conference on Aviation Security) Doc 10123), A40-WP/26 Outcome of the Second High-level Conference on Aviation Security (HLCAS/2)
2. Global Aviation Safety Plan (GASP) (Doc 10004(
3. Global Air Navigation Plan
4. The Global Air Navigation Plan, Doc 9750-AN/963 – 2016
5. European Civil Aviation Conference

منطقه‌ای و فرعی مربوطه.»[1] همچنین کنوانسیون (۱۹۷۱ مونترال) برای جلوگیری از اعمال غیرقانونی علیه امنیت هواپیمایی کشوری مطابق ماده ۱۱ بند یک بیان می‌دارد؛ «دول متعاهد حداکثر معاضدت قضایی را در مورد رسیدگی‌های کیفری مربوط به جرائم نسبت به یکدیگر معمول خواهند داشت. قانون قابل اجرا در کلیه موارد – قانون دولت متقاضی‌عنه ـ خواهد بود.»[2]

۲ -۱- امنیت سایبری هوانوردی[3]

امنیت سایبری و امنیت هوانوردی باید یکپارچه باشند و در سیلوهای جداگانه قرار نگیرند.[4] امنیت در لغت از ریشه «امن» به معنای «در امان بودن» و «مصون بودن» از هرگونه تعرض و در «آرامش و آسودگی» بودن از هرگونه «تهدید» و «ترس» است. (معین، ۱۳۶۳: ۳۵۴) کوفی عنان[5] دبیر کل فقید سازمان ملل متحد در جمله قابل تاملی گفت: «ما بدون امنیت از توسعه برخوردار نخواهیم شد، بدون توسعه از امنیت برخوردار نخواهیم شد و بدون رعایت حقوق بشر از هیچ کدام بهره نخواهیم برد.» (A/59/2005, Para: 17) ایکائو نیز در تعریف امنیت[6] می‌گوید: «حفاظت هواپیمایی کشوری در مقابل اقدامات مداخله غیرقانونی که این هدف به وسیله مجموعه‌ای از مقررات و منابع مادی و انسانی میسر می‌گردد.» (Annex17, 2016: 4) چشم‌انداز ایکائو برای امنیت سایبری جهانی این است که بخش هوانوردی غیرنظامی در برابر حملات سایبری مقاوم باشد و در سطح جهانی ایمن و قابل اعتماد باقی بماند و در عین حال به نوآوری و رشد ادامه دهد.[7]

فضای سایبر فضای غیرمادی و ناملموس است که توسط شبکه‌های رایانه‌ای به وجود آمده و دنیای مجازی را درکنار دنیای واقعی ایجاد کرده است. (فضلی، ۱۳۸۹: ۱۷) زیرساخت‌های سایبری اکنون زیربنای بسیاری از امور اساسی یک جامعه مدرن است. فضای مجازی زندگی ما را فرا گرفته است و خطرات سوءاستفاده از آن به طور عمومی شناخته شده است. شهروندان از مزایای فناوری سایبری بهره می‌برند و در عین حال از دولت‌ها انتظار دارند که از آن‌ها در برابر تهدیدات سایبری فراملی محافظت کنند. (ILA, 2016: 256) رشد فزآینده مسافرت‌های هوایی و پیشرفت‌های فناورانه ناوبری و ضرورت به روزرسانی داده‌ها درباره موقعیت هر هواپیما در

1. https://undocs.org/S/RES/1373(2001)

۲. قانون الحاق دولت ایران مصوب ۱۳۵۲

3. Aviation Cyber Security
4.https://www.icao.int/Meetings/MIDCyberSec/PublishingImages/Pages/Presentations/20CyberSecurity.pdf
5. Kofi A. Annan
6. Security. Safeguarding civil aviation against acts of unlawful interference. This objective is achieved by a combination of measures and human and material resources .
7. Aviation Cybersecurity Strategy .https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx

سیستم‌های جدید کنترل ترافیک هوایی نیازمند یک سیستم کاملاً خودکار برای جمع‌آوری داده‌ها و پردازش اطلاعات پروازی است.

اتوماسیون می‌تواند مزیتی بزرگ باشد زمانی که به درستی استفاده شود. اتوماسیون می‌تواند به کارایی و بهبود امنیت و ایمنی هوانوردی کمک کند و از خطاها جلوگیری و اعتبار سیستم مدیریت ترافیک هوایی را افزایش دهد. (آزاد، ۱۳۹۷: ۱۱۴) در عین حال حملات سایبری که زیرساخت‌های مهم ملی را مورد هدف قرار می‌دهند خطری قابل توجه، وسیع و به سرعت در حال افزایش را در فضای تهدیدات جهانی به وجود آورده است. اولین حادثه ثبت شده از یک حمله سایبری تروریستی گسترده نسبتا موفق به سیستم‌های کامپیوتری که به گردان‌های جنگ الکترونیکی طارق بن زیاد نسبت داده شده، در سال ۲۰۱۰ رخ داد. (معاونت، ۱۳۹۴: ۱۳۸) بنابراین دلایل زیادی برای رشد و ترقی اتوماسیون در سیستم‌های ترافیک هوایی وجود دارد. یکی از این دلایل، پیشرفت‌های فنآورانه ناوبری هوایی است که منجر به دقت و اعتبار بیشتر و لحظه‌ای بودن داده‌ها درباره موقعیت هر هواپیمای می‌گردد.

۲- ۲- تهدیدات سایبری هوانوردی کشوری

منظور از تهدید؛ هر چیزی که می‌تواند عمداً یا به طور تصادفی از آسیب‌پذیری سوءاستفاده کند و سرمایه‌ای را بدست آورد، آسیب برساند یا از بین ببرد. ویروسی که در سال ۲۰۰۰ توسط یک نوجوان فیلیپینی ساخته شد، از هر ۱۰ کامپیوتر کره‌زمین، به یک کامپیوتر آسیب رسانده و صدمات زیادی به پنتاگون وارد کرد. (دهقانی، ۱۳۹۷: ۱۳۲) براساس مطالعات یاتا در سال ۲۰۱۹ انتظار می‌رود؛ که هشت تهدید اصلی بر چشم‌انداز ۲۰۴۰ تسلط داشته باشد؛[1] تهدید سایبری، درون سازمانی، تروریسم، وسایل‌نقلیه بدون‌سرنشین، زنجیره تامین حمل‌ونقل هوایی، بیماری روانی، بیماری‌های بیولوژیکی و عفونی از آن جمله‌اند.

برخی از حوادث قابل توجه در حوزه هوانوردی که می‌توان از آن‌ها نام برد؛ " کشور ویتنام، ژوییه ۲۰۱۶، توسط گروه هک چینی «CN1937» مورد حمله سایبری قرار گرفت که صفحات اطلاعات پرواز و سیستم‌های صوتی را در فرودگاه‌های Noi Bai و Tan Son Nhat ربودند و منجر به از دست دادن کنترل محلی و پخش ضد ویتنامی و فیلیپینی شد." (کتانچی و پورقهرمانی، ۱۴۰۰: ۱۴۵) لئون پانتا [2] وزیر اسبق دفاع امریکا هشدار می‌دهد؛ «ایالات متحده با احتمال "حمله غافلگیرانه سایبری" روبرو است و به طور فزاینده‌ای در برابر هکرهای خارجی آسیب‌پذیر است و می‌توانند شبکه برق کشور، سیستم حمل‌ونقل، شبکه بانکی و دولت را از بین

1. Air Transport Security 2040 and Beyond, V1 2019
2. Leon E. Panetta

ببرند و نشان اتهام به سوی چین، روسیه، ایران و گروه‌های شبه نظامی است.»[1] امروزه بیشتر زیرساخت‌ها و سیستم‌های امنیتی حیاتی در فرودگاه‌ها، اغلب در بستر شبکه‌های مختلف با سایر سیستم‌های فرودگاهی اجرا می‌شوند.

این خطر وجود دارد که هواپیماها عمداً هدف قرار گیرند یا اینکه سیستم‌های کنترل ترافیک هوایی هک شوند تا اطلاعات نادرست را برای خلبانان ارسال کنند و پیامدهای بالقوه‌ی کشنده داشته باشد. آنچه واضح است، این است که این موارد نگران‌کننده و روبه‌رشد برای بخش امنیت هوانوردی وجود دارد و نیاز فوری به درک بهتر تأثیرات و خطرات واقعی است تا بتوان استراتژی‌ها و پروتکل‌های مناسب را برای به حداقل رساندن خطرات در نظر گرفت.

۳- رابطه امنیت سایبری با حقوق بین‌الملل

اگرچه فضای سایبر بعضاً در قالب کنوانسیون جرایم سایبری بوداپست در اروپا و رویه و استراتژی ملی مربوط به امنیت سایبری در بسیاری از کشورها تا حدی ساماندهی شده، ولی با عنایت به اینکه در مورد حملات سایبری هنوز هیچگونه اجماع بین‌المللی در چهارچوب معاهده حاصل نشده است و با توجه به اینکه هنوز رویه و عرفی هم در این خصوص موجود نیست، باید حملات سایبری را در چهارچوب قواعد موجود حقوق بین‌الملل ارزیابی کنیم و به نظم در آوریم. (اسماعیل‌زاده و عبداللهی، ۱۳۹۹: ۷۱۸) امنیت سایبری در حوزه کنترل ترافیک هوایی بسیار حیاتی است. ایکائو اکتبر ۲۰۱۹، در چهلمین اجلاس مجمع عمومی، قطعنامه A40-10 را در زمینه امنیت سایبری در هوانوردی غیرنظامی تصویب کرد و گامی مثبت در جهت تثبیت راهبری هوانوردی برداشت. از دولت‌ها خواسته است تا استراتژی امنیت سایبری هوانوردی را اجرا کرده و چشم‌انداز و اهداف استراتژیک خود را مشخص کنند.[2]

در چارچوب کنوانسیون هوانوردی بین‌المللی غیرنظامی (سند ۷۳۰۰ ایکائو)،[3] خدمات ناوبری هوایی به عنوان بخشی از تعهدات دولت ارائه می‌شود و دولت‌ها باید از منافع اساسی امنیت ملی یا سیاست دفاعی و در بسیاری موارد محافظت کنند. باید الزامات قانونی، تعهدات و رویه‌های خاص مربوط به حفاظت از زیرساخت‌های حیاتی را برآورده کند. یکپارچگی داده‌ها و تضمین اطلاعات از اهمیت ویژه‌ای برای امنیت سایبری درحوزه مدیریت ترافیک هوایی برخوردار است. بنابراین، درک الزامات برای تضمین داده‌ها و اطلاعات و همچنین اقدامات و استراتژی‌هایی که می‌توان در این زمینه انجام داد، مهم است (CANSO, 2014: ۱۳).[4]

1. https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html
2. The Scowcroft Center for Strategy and Security
3. ICAO Doc7300
4. https://www.icao.int,NACC/Documents/Meetings/2018/CSEC/D06b-Cyber Security and Risk Assessment Guide-CANSO.pdf

از آنجا که به واسطه جدید بودن پدیده، هنوز مقررات‌گذاری ویژه‌ای در خصوص استفاده از فضای سایبر به عنوان محمل اقدامات خصمانه صورت نگرفته و تلاش‌های ابتدایی در رویه‌سازی (مانند تدوین دستورالعمل تالین[1] از سوی ناتو) واجد اثر حقوقی لازم نیستند، لاجرم باید از اصول و قواعد کلی حقوق بین‌الملل بشردوستانه برای تنظیم روابط خصمانه در فضای سایبر استفاده کرد. زیرا همچنان که شرط مارتنس[2] از ابتدای قرن بیستم بیان کرده است، نبود قواعد خاص مانع از اجرای قواعد و اصول کلی عرف و حتی ندای وجدان نیست. (برادران و حبیبی، ۱۳۹۸: ۱۵۵) مساله اصلی در رابطه با جایگاه حقوقی سازمان بین‌المللی هواپیمایی کشوری در ماده ۴۴ کنوانسیون شیکاگو جا دارد، که اعلام کرده است؛ «اهداف و مقاصد ایکائو توسعه اصول و فنون ناوبری هوایی بین‌المللی و تسریع برنامه‌ریزی و توسعه ترابری هوایی بین‌المللی می‌باشد تا از میان سایر موارد نیاز مردم دنیا به ترابری هوایی بی‌خطر، منظم کارآمد و مقرون به صرفه را برطرف سازد.» هرگونه حمله سایبری و زیستی خشونت‌آمیز علیه هوانوردی بر اساس مقررات فوق نقض قواعد بین‌المللی محسوب می‌شود و به نوعی شورای امنیت با تصویب قطعنامه ۲۱۶۶[3] تاکید بر ماده ۳ مکرر[4] کنوانسیون شیکاگو دارد و بر آن صحه گذاشته است.

حملات سایبری فراتر از کنترل انحصاری سرزمینی است. اما این تهدید مستلزم اختراع مجدد حقوق بین‌الملل نیست. چارچوب تلاش سایبری پیشنهادی، مسئولیت دولت محوری در فضای سایبری را حفظ می‌کند. انتظار است این مبحث بتواند به حقوق بین‌الملل به عنوان پروژه‌ای برای تحمیل و حفظ نظم از طریق کلمات در فضای مجازی کمک کند.

۴- مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری

مسئولیت بین‌المللی به مثابه یک نهاد حقوقی بین‌المللی، عبارت است از: الزام به جبران خسارت (مادی یا معنوی) وارد بر تابعان حقوق بین‌الملل (کشورها و سازمان‌های بین‌المللی) که این خسارت باید ناشی از عمل یا خودداری از عمل غیرمشروع و مخالف حقوق بین‌الملل (عرفی یا معاهده‌ای) یکی از موضوعات یا تابعان حقوق بین‌الملل باشد. (ضیائی‌بیگدلی، ۱۳۸۸: ۴۶۹) واژه «مسئولیت بین‌المللی» روابط حقوقی جدیدی که به موجب حقوق بین‌الملل و به دلیل فعل متخلفانه بین‌المللی دولت ایجاد می‌شوند را در بر می‌گیرد. (راعی، ۱۳۹۳: ۱۷) حقوق مسئولیت بین‌المللی در زمره قواعد ثانویه حقوق بین‌الملل و یکی از زمینه‌های بنیادین این دانش بشری است. (مومنی‌راد و ستایش‌پور، ۱۳۹۸: ۶۳۶) اگرچه به‌رغم این اهمیت، به جز دو طرح (مسئولیت دولت ۲۰۰۱ و سازمان‌های بین‌المللی ۲۰۱۱)، مسئولیت هنوز فاقد کنوانسیون لازم‌الاجرا می‌باشد و این هم

1.Tallinn Manual 2.0
2.Martens Clause
3. S/RES/2166(2014 (
۴. منع توسل به زور در مقابل هواپیمای در حال پرواز (ماده ۳ مکرر کنوانسیون شیکاگو)

جنبه عرفی دارد. معهذا حقوقدانان بین‌المللی، مسؤولیت را ناشی از فعل‌ها و ترک فعل‌هایی می‌دانند که به استناد مقررات بین‌المللی، غیرقانونی تلقی می‌شوند. این شاخصه توسط دیوان دائمی بین‌المللی دادگستری، در قضیهٔ فسفات مراکش[۱]، دیوان بین المللی دادگستری در قضایایی مانند کانال کورفو[۲]، دعوای نیکاراگوئه علیه آمریکا[۳]، کابچیکوو- ناگیماروس[۴] و نیز در نظر مشورتی درباره تفسیر معاهدات صلح[۵] به نوعی مورد تاکید قرار گرفته است. (کریم‌آبادی، ۱۳۹۸: ۳۶۴) مبنای مسئولیت سازمان‌های بین‌المللی در قبال اعمال متخلفانه بین‌المللی مطابق ماده ۳ طرح مسئولیت سازمان‌های بین‌المللی، این‌چنین آمده است: «اعمال متخلفانه یک سازمان بین‌المللی موجب مسئولیت بین‌المللی آن سازمان خواهد شد» در سطح جهان، تعدادی از سازمان‌ها[۶] در حال حاضر در حال تهیه استانداردها و دستورالعمل‌هایی برای محافظت از وضعیت امنیت سایبری بخش هوانوردی هستند. این صنعت، که به ایمنی و قابلیت اطمینان خود مشهور است، به سرعت درحال پذیرش فناوری با سرعت سریع است.

ایکائو با تصویب قطعنامه امنیت سایبری (A40-10 ICAO)[۷]، برنامه اقدام امنیت سایبری هوانوردی، برای ترویج پذیرش و اجرای جهانی کنوانسیون سرکوب اقدامات غیرقانونی مربوط به هوانوردی غیرنظامی بین‌المللی (کنوانسیون پکن) و پروتکل مکمل کنوانسیون سرکوب تصرف غیرقانونی هواپیماها (پروتکل پکن)، برای مقابله با حملات سایبری علیه هوانوردی غیرنظامی، از دولت‌ها و ذینفعان صنعت می‌خواهد اقدامات مربوطه [۸] را برای مقابله با تهدیدات سایبری برای حفاظت از هوانوردی غیرنظامی انجام دهند.

شورای ایکائو برنامه اقدام امنیت سایبری[۹] (CyAP) را برای اجرای استراتژی امنیت سایبری تصویب کرد و تعهد خود را برای ایجاد یک چارچوب امنیت سایبری جهانی قوی برای تقویت ایمنی، امنیت و پایداری سیستم بین‌المللی هوانوردی غیرنظامی تقویت کرد.[۱۰] مطابق قاعده ۳۱ اصل کلی راهنمای تالین «یک سازمان بین‌المللی در قبال عملیات سایبری که یک تعهد حقوقی بین‌المللی را نقض می‌کند و قابل انتساب به سازمان است، مسئولیت حقوقی بین‌المللی دارد.» [۱۱]

---

1. Phosphates in Morocco, Preliminary Objections, P.C, I, j series /A /B.no, 74, P: 10. P.2
2. Corfu Channel (United Kingdom v. Albania ,(ICJ, Judgment of 15 December 1949, ICJ Reports 1949.
3. Case Concerning Military and Paramilitaey Activies in and Aginst Nicaragua) Nicaragua v. United States of America) Jurisdiction of the court and admissibility of the application .See at : https://www.icj-cij.org/public/files/case-related/70/070-19841126-jud-01-00-en.pdf
4. Gabeíkovo-Nagymaros Project (Hungary/Slovakia). See at :https://www.icj-cij.org/en/case/92
5. Interpretation of Peace Treaties with Bulgaria Hangars and Romania second phase, I.C.j Reports, 1950, p. 221.

۶. اسامی سازمان‌ها در بند ۱-۲ مقاله ذکر شده‌اند.

7. ICAO ,A40-WP/3951 EX/161 30/7/2019
8. https://www.icao.int/cybersecurity/Pages/Resources.aspx
9. Cybersecurity Action Plan
10. https://www.icao.int/cybersecurity/Pages/Cybersecurity-Action-Plan.aspx
11. Rule 31 Tallinn Manual 2.0

بنابراین شروط تحقق و احراز مسئولیت بین‌المللی؛ اول نقض تعهد بین‌المللی است و دوم اثبات انتساب رفتار مورد بحث به دولت یا سازمان بین‌المللی می‌باشد.[1] لذا دولت‌ها و ایکائو به عنوان سازمان بین‌المللی تخصصی هوانوردی مسئول اتخاذ تدابیر احتیاطی و پیشگیری از عملیات سایبری علیه هوانوردی غیرنظامی هستند.

۴ - ۱- تعهدات سایبری هوانوردی

به منظور حفاظت از زیرساخت‌ها، هرچند ما درعمل با یک حمله سایبری جدی روبه‌رو نشده‌ایم، ولی انگیزه‌ها و توانمندی‌های وسیعی برای بهره‌برداری از آسیب‌پذیری زیرساخت‌ها وجود دارد که تدبیری همه جانبه برای محافظت از زیرساخت‌ها را ضروری می‌سازد. (سلطانی‌نژاد و همکاران، ۱۳۹۲: ۱۰۷) براساس نظر دیوان بین‌المللی دادگستری و اصل کانال کورفو؛ وظیفه جلوگیری از اعمال سایبری بر خلاف حقوق سایر کشورها اولین تعهد حفاظتی است، که کاربرد آن در فضای سایبری در میان دولت‌ها و مفسران مورد حمایت قرار گرفته است، اصل "به خوبی شناخته شده" کانال کورفو از دولت‌ها می‌خواهد "آگاهانه اجازه ندهند که قلمرویشان را در اختیار بگیرند" و برای اعمال مغایر با حقوق سایر کشورها استفاده شود. این وظیفه نتیجه طبیعی حقوق حاکمیتی دولت‌ها بر قلمرو خود است. اگرچه در اصل یک وظیفه پیش‌گیرانه است، اما تعهد تنها زمانی نقض می‌شود که ضرر تحقق یابد. (Dias &Coco , 2021: 14) مطابق قاعده ۳۰ اصل کلی راهنمای تالین[2] در خصوص نقض تعهدات بین‌المللی «جامعه به عنوان یک کل هر کشوری ممکن است به مسئولیت دولتی استناد کند که عملیات سایبری را انجام داده است که تعهدات erga omnes را که به کلیت جامعه بین‌المللی مدیون است، نقض کرده است.»

وضعیت موجود جامعه بین‌المللی ایجاب می‌کند که اعضای سازمان‌های بین‌المللی به سویی رهنمون شوند که فیلیپ جسوپ[3] آن را به عنوان تئوری «منافع مشترک» و « حس مسئولیت برای نیل به سعادت و رفاه مشترک» معرفی نموده است. (والتیکوس، ۱۳۷۶: ۱۹۱) لذا ضرورت داشتن هدف مشترک در برگیرنده و تضمین‌کننده منافع جامعه بین‌المللی است.

مهم‌ترین موضوع در امنیت سایبری جمهوری اسلامی ایران، فقدان یک استراتژی منسجم و پس از آن نبود فرماندهی واحد در شناسایی، ارزیابی و پاسخگویی به حملات سایبری است. (مرکز پژوهش‌های مجلس، ۱۴۰۰: ۲) در حالیکه ایران به عنوان عضو ایکائو و متعهد به اجرای مقررات کنوانسیون شیکاگو، باید راهبردهای لازم را اتخاذ و برنامه امنیت ملی هوانوردی را تدوین و پیاده سازی نماید.

---

۱. ماده ۲ طرح مسئولیت دولت

2.Tallinn Manual 2.0
3. Phlip Jessup

براساس سند پیشگیری و مقابله با حوادث فضای مجازی مصوب چهل‌وچهارمین جلسه شورای عالی فضای مجازی، حوزه امنیت سایبری سه متولی دارد و صیانت از زیرساخت‌های حیاتی در برابر حملات اینترنتی و دفاع در برابر هرگونه حمله به کمیسیون عالی امنیت مرکز ملی فضای مجازی سپرده شده است. ولی مشاهده می‌شود مصوبات این مراکز براساس ماده۲۹ قانون برنامه ششم برای دستگاه‌ها الزام‌آور نیست. لذا با توجه به اهمیت امنیت سایبری هوانوردی و نقشی که شورای عالی امنیت ملی در امور هوانوردی برای خود متصور و تنظیم کننده روابط دستگاه‌ها و ارگان‌های نظامی و غیرنظامی (کشوری) است، باید به این مهم ورود و مقررات لازم را تدوین، ابلاغ و نظارت نماید.

۴ – ۲- انتساب[1] حملات سایبری به دولت‌ها

برخلاف حریم هوایی ملی، عملیات سایبری در حریم هوایی بین‌المللی به طور کلی مجاز است. طبق قاعده۵۶ اصول راهنمای تالین، که بیان می‌دارد: «با توجه به محدودیت‌های موجود در قوانین بین‌المللی، یک کشور می‌تواند عملیات سایبری را در حریم هوایی بین‌المللی انجام دهد». (Tallinn Manual 2.0, 2017: 30) علاوه بر این، هنگام انجام عملیات سایبری در فضای هوایی بین‌المللی، دولت‌ها فقط توسط قوانین بین‌المللی مانند ممنوعیت مداخله و استفاده از زور یا رژیم‌های ناوبری پذیرفته‌شده مانند پرواز بر فراز مناطق بین‌المللی محدود می‌شوند. حملات سایبری ریشه در اقدامات جاسوسی دارد و جاسوسی را می‌توان به عنوان ابزاری برای اجرای سیاست و همچنین وسیله‌ای برای آسیب‌زدن به دیگران تعریف کرد.

باراک اوباما، رئیس جمهور آمریکا، قانونی را امضا کرده است که براساس آن تحریم‌های جدید متوجه ملت‌ها و افرادی می‌شود که در حملات سایبری علیه شهروندان آمریکایی، شرکت‌ها و یا بخش‌های مختلف دولت فدرال آمریکا مشارکت داشته باشند. تحریم‌های جدید شامل قطع دسترسی و یا اعمال محدودیت بر منابع مالی افراد و یا سازمان‌هایی است که به نوعی در حملات سایبری علیه زیرساخت‌های آمریکا مشارکت دارند و یا از نظر این کشور باعث وارد کردن ضرر و زیان به تأسیسات زیرساخت این کشور شده‌اند. این زیرساخت‌ها گستره وسیعی از برنامه اتمی، بخش تأسیسات آب و یا سامان‌های مالی را دربرمی گیرد. البته کارشناسان سایبری آمریکایی، همواره از روسیه و ایران به عنوان یک تهدید جدی علیه امنیت سایبری خود نام برده‌اند (پایسا، ۱۳۹۴: ۱۹). حملات سایبری در حال گسترش است و جستجوگرهای زنده روزانه بیش از ۶ میلیون حمله سایبری را ثبت می‌کنند. (Liu, 2017: 191)

1. attribution

با احراز متخلفانه‌بودن حملات سایبری، در خصوص انتساب به دولت‌ها محاکم بین‌المللی با دقت نظر بالایی عمل کرده‌اند. دیوان بین‌المللی دادگستری نیز در چندین مورد به این دو عنصر اشاره کرده است. در قضیه (کارکنان دیپلماتیک و کنسولی امریکا در تهران)، دیوان اظهار داشت که برای احراز مسئولیت ایران: نخست باید احراز کرد که مورد بحث تا چه حد از نظر حقوقی به دولت ایران قابل انتساب است دیگر آنکه باید مغایرت یا عدم مغایرت آن رفتارها و اعمال با تعهدات ایران به موجب معاهدات لازم‌الاجرا یا به موجب هر یک از قواعد حقوق بین‌الملل قابل اعمال مدنظر قرار گیرد. همچنین دیوان در مورد مسئولیت ناشی از رفتار مستقل، می‌توان به پرونده کانال کورفو اشاره کرد که در آن یوگسلاوی و آلبانی افعال متخلفانه‌ای را مرتکب شده‌اند که موجب ورود خسارت به کشتی‌های بریتانیایی شده است.[1]

۴- ۲- ۱- انتساب حملات سایبری به دولت با معیار کنترل کلی[2]

دیوان بین المللی دادگستری نیز اعلام کرده است تا جایی که به تعیین نوع مخاصمه مربوط است، معیار کنترل کلی "می‌تواند قابل اعمال و مناسب باشد." (Rep, 2007: para. 404 ICJ) به طور کلی استفاده از معیار کنترل کلی در زمینه انتساب حملات سایبری به دولت، مورد توافق گروه متخصصان بین‌المللی است که راهنمای تالین در مورد حقوق بین‌الملل قابل اعمال در جنگ‌های سایبری را تهیه کرده‌اند و هرچند در بین حقوقدانان بین‌المللی همچنان در خصوص قابلیت اعمال این قاعده برای تبیین مسئولیت بین‌المللی دولت اختلاف نظر وجود دارد اما با توجه به رای ذکر شده دیوان بین‌المللی دادگستری، می‌توان گفت این معیار در خصوص تعیین نوع مخاصمه حتماً قابل استفاده است. (برادران و حبیبی، ۱۳۹۸: ۱۴۵)

اصولا دولت‌ها اعمال خود را از طریق اشخاصی مثل ارگان‌ها و نمایندگان خود محقق می‌سازند. لذا قابلیت انتساب، یکی از ارکان تحقق مسئولیت ناشی از نقض تعهدات بین‌المللی تلقی می‌شود. بنابراین کنترل کلی حملات سایبری شامل کنترل یک دولت بر تمام کارکردهای گروه‌های تحت امر است و ضابطهٔ کنترل کلی، ارتباط بین ارکان دولت و مسئولیت بین‌المللی آن دولت را گسترش می‌دهد.

۴- ۲- ۲- انتساب حملات سایبری به دولت با معیار کنترل مؤثر[3]

براساس این فرضیه، افعال جاسوسان را می‌توان قابل انتساب به دولت دانست، ولی باید آن را با معیار کنترل مؤثر سنجید. دیوان بین‌المللی دادگستری در قضیه فعالیت‌های نظامیان و شبه

1. ICJ Reports ,194904 ,23
2. Overall Control
3. Effective control

نظامیان آمریکایی در نیکاراگوئه معیار کنترل مؤثر را مورد پذیرش قرار داد (ICJ Reports, 1986: para. 115) اگرچه مطابق قاعده ۳۰ اصل کلی راهنمای تالین «احتیاط مقتضی»[1] یک شرط اساسی حقوق بین‌الملل نیست، بلکه استانداردی است که دولت‌ها باید برای جلوگیری از استفاده از قلمرو خود برای ایجاد آسیب فرامرزی اعمال کنند. (Manual 2.0, 2017: Tallinn 30) گاهی اوقات از اصل احتیاط لازم به عنوان «تعهد به هوشیاری»[2]، «تعهد به پیشگیری»[3] یا «وظیفه پیشگیری»[4] نیز یاد می‌شود.

ظهور چندجانبه‌گرایی در قرن بیستم منجر به افزایش روزافزون حقوق و مسئولیت‌ها برای سازمان‌های بین‌المللی شده است و این امر به نوبه خود منجر به ایجاد «تعهدات مراقبت مقتضی»[5] و مثبت و منفی شده است. (ILA, 2016: 39) قاعده هفتم اصول کلی راهنمای تالین نیز در خصوص رعایت اصل احتیاط مقتضی آورده است؛ «اصل احتیاط مقتضی از هر دولت می‌خواهد که تمام اقداماتی را که در شرایط موجود امکان‌پذیر است برای پایان دادن به عملیات سایبری که بر حق سایر کشورها تأثیر می‌گذارد و عواقب نامطلوب جدی برای آن‌ها ایجاد می‌کند، اتخاذ کند.» (Manual 2.0 ,2017: 14 Tallinn)

براساس حقوق مسئولیت دولت، رفتار اشخاص و نهادهای خصوصی بطور معمول به دولت منتسب نیست. منظور از کنترل مؤثر هم این است که یک دولت نسبت به حملات سایبری، در جریان یک عملیات خاص که به نقض‌های ادعایی منجر شود و دخالت مستقیم داشته باشد، مسئولیت دارد.

بنابراین، مسئولیت دولت‌ها در هر دو وضعیت (کنترل کلی و کنترل مؤثر)، براساس اصل مسئولیت مستقل و مطابق قواعد معمول انتساب و براساس رفتار و تعهدات‌شان ارزیابی می‌شود.

بحث و نتیجه‌گیری

انگیزه و توانمندی وسیعی برای اخلال در هوانوردی و نابودی زیرساخت‌ها وجود دارد که تدبیری همه جانبه برای محافظت از آن‌ها را ضروری می‌سازد. این مقاله بطور خلاصه حملات سایبری هوانوردی را تعریف و ماهیت تهدیداتی که برای صنعت هوانوردی و جامعه ایجاد دغدغه می‌شود را توصیف نمود، همچنین به تشریح اسناد حقوقی بین‌المللی که برای رسیدگی به حملات سایبری در دسترس هستند، پرداخت و چالش‌های پیش روی هوانوردی از طریق فضای سایبری و

1. Due Diligence
2. obligation of vigilance
3. obligation of prevention
4. duty of prevention
5. due diligence obligations

تحریم‌های احتمالی سیستم‌های ناوبری ماهواره‌ای توسط صاحبان فناوری ماهواره‌ای را منعکس کرد.

– اکوسیستم هوانوردی نقش بسیار مهمی در اقتصاد جهانی دارد و خدمات حمل‌ونقل هوایی امن لازمه تجارت، گردشگری و پیوندهای سیاسی و فرهنگی بین کشورها می‌باشد، لذا بایستی صنعت هوانوردی در برابر فضای مجازی و به اشتراک‌گذاری اطلاعات، که متکی به روابط خصوصی و عمومی است، بسیار مقاوم گردد.

– اگرچه استفاده از سامانه‌های ماهواره‌ای(جی‌پی‌اس) امریکا و (گلوناس) روسیه یا (گالیله) اروپا برای هدایت هواپیماها، صنعت هوانوردی ایران را در حال حاضر منتفع نموده است، اما در صورت ادامه تنش‌های فعلی با امریکا و اروپا، ایران با چالش‌های سیاسی و حقوقی جدی روبه‌رو می‌شود. زیرا تعهد این دو کشور به ایکائو براساس نامه بوده‌است و هیچ تعهد الزام‌آور و تضمینی در ادامه بهره‌برداری و جلوگیری از جعل و حملات سایبری در حقوق بین‌الملل وجود ندارد. ضمن اینکه شورای عالی فضایی کشور بیش از ۱۰سال تشکیل نشده و چشم‌اندازی نیز قابل تصور نیست. لذا ضرورت پیشگیری و رعایت اصل احتیاط شرط عبور از بحران‌های آتی می‌باشد.

– استفاده هکرها از فضای ناامن سایبری و بی‌تفاوتی و یا مساعدت دولت‌ها زمینه را برای تهدیدات امنیتی ازجمله خرابکاری، اخلال، ترور، جاسوسی و دیگر جرائم مرتبط در هوانوردی، امکان حملات سایبری علیه هوانوردی غیرنظامی از کشوری علیه سیستم‌های عمومی و خصوصی کشور دیگر را فراهم نموده و می‌طلبد با معاضدت‌های قضایی سریع مجرمان بین‌المللی مورد پیگرد قرار گیرند.

– نگرانی‌های امنیتی سایبری مختلفی در فرودگاه‌ها وجود دارد و ضرورت «هوشمندسازی» فرودگاه‌ها به دلیل افزایش اتصال سیستم‌ها و فرآیندها، به طور جدی احساس می‌شود.

– آینده هوانوردی از آن سیستم‌های هوشمند است و اتوماسیون باعث تخصیص جدید وظایف تصمیم‌گیری بین انسان و ماشین خواهد شد. وظایفی که قبلاً توسط انسان انجام می‌گرفت؛ مثل جداسازی پروازها و کنترل ترافیک هوایی، هدایت هواپیماها و ماشین‌های پرنده قرار است تا حدی به سیستم واگذار شود. لذا مشارکت واقعی انسان باید مورد بازنگری قرار گیرد و تعامل انسان و ماشین مجددا مهندسی شود. این امر مستلزم بازنگری در تخصیص وظایف، نقش‌ها و مسئولیت‌ها در چارچوب سیستم‌ها و رژیم‌های پیچیده حقوقی– فنی است.

– حملات سایبری هوانوردی تهدیدکننده صلح و امنیت بین‌المللی هستند. اسناد بین‌المللی درباره جرایم سایبری هوانوردی در سطح فراملی اقدامات کافی را به منظور پیشگیری از تروریسم سایبری ترتیب نداده‌اند و تعریف رابطه عناصر «مسئولیت بین‌المللی دولت‌ها» در فضای ایجاد شده

نامشخص است و تعریف قواعد الزام‌آور منطبق با اصول حقوق بین‌الملل و منشور ملل متحد خواستهٔ جهانی می‌باشد.

تشکر و قدردانی

نویسنده از همه عزیزانی که در انتشار این پژوهش همکاری داشتند، کمال امتنان را دارد.

منابع

کتب فارسی:

- آبیراتنه، رووانتیسا ایندرانات رامیا (۱۳۹۴). حقوق امنیت هواپیمایی. ترجمه نامیان. نشرمیزان.
- آزاد، محسن (۱۳۹۷). عوامل انسانی در هوانوردی. چاپ اول. کارگاه هفت‌هنر.
- راعی، مسعود (۱۳۹۳). مسئولیت بین‌المللی دولت در قبال رفتار افراد و گروه‌ها در پرتو رویه قضایی. قم؛ موسسه آموزشی و پژوهشی امام‌خمینی.
- زرنشان، شهرام (۱۳۹۲). شکل‌گیری و شناسایی حقوق بین‌الملل عرفی. گنج‌دانش.
- ضیائی‌بیگدلی، محمدرضا (۱۳۸۸). حقوق بین‌الملل عمومی. گنج‌دانش.چاپ سی‌هشتم.
- فضلی، مهدی (۱۳۸۹). مسئولیت کیفری در فضای سایبر، جلد اول. خرسندی.
- مرکز پژوهش‌های مجلس (۱۴۰۰). اولین چالش سایبری دولت بایدن؛ اختلال سایبری در شبکه سوخت آمریکا. معاونت مطالعات سیاسی، شماره مسلسل: ۲۶۰۱۷۵۵۸
- معاونت پژوهش (۱۳۹۴). حفاظت سایبری از زیرساخت‌های حیاتی. انتشارات دانشکده اطلاعات.
- موسوی، سیدفضل الله (۱۳۹۶). جستارهایی در حقوق بین‌الملل. انتشارات خرسندی.

مقالات:

- اسماعیل‌زاده، پرستو؛ عبداللهی، محسن (۱۳۹۹). حملات سایبری و نقض اصل عدم مداخله، فصلنامه مطالعات حقوق عمومی. ۵۰ (۲): ۷۳۶ـ ۷۱۱
https://jplsq.ut.ac.ir/article_73962.pdf
- برادران، نازنین؛ حبیبی، همایون (۱۳۹۸). قابلیت اعمال قواعد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری. فصلنامه مطالعات حقوق عمومی. ۴۹ (۱): ۱۵۸- ۱۳۹
https://jplsq.ut.ac.ir/article.pdf
- ترابی، قاسم؛ طاهری‌زاده، محمدناصر (۱۴۰۰). انقلاب سایبری و تحول مفهوم جنگ اطلاعاتی در عرصه روابط بین‌الملل. فصلنامه مطالعات بین‌المللی. ۴ (۶۸): ۶۶- ۴۷
https://www.isjq.ir/article_132334.pdf
- دهقانی، علی‌اصغر (۱۳۹۶). بازدارندگی سایبری در امنیت نوین جهانی: تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا. مجله رهیافت بین‌الملل. ۸ (۴): ۱۴۷- ۱۲۱
https://piaj.sbu.ac.ir/article_99570.pdf
- صیاد، محمدکاظم و دیگران (۱۳۹۹). تهدیدهای سایبری و اقدامات امنیتی در فضای مجازی؛ بررسی رویکردهای ایالات متحده و جمهوری اسلامی ایران. فصلنامه امنیت ملی. ۱۰ (۳۸): ۳۳۰- ۲۹۳

https://ns.sndu.ac.ir/article_1258.pdf

- قدیر، محسن؛ کاظمی، حسین (۱۳۹۸). بررسی تطبیقی حقوق کیفری ایران با اسناد بین‌المللی در زمینه مقابله و پیشگیری از وقوع تروریسم سایبری. مجله حقوقی بین‌المللی. ۶۰ : ۲۶۹- ۲۳۷

http://www.cilamag.ir/article_39721.pdf

- کتانچی، الناز؛ پورقهرمانی، بابک (۱۴۰۰). چالش‌های امنیت سایبری در کشورهای «آسه آن». فصلنامه مطالعات بین‌المللی. ۱۸ (۱): ۱۵۶- ۱۳۹

https://www.isjq.ir/article_126626.pdf

- کریم آبادی، محمدصادق (۱۳۹۸).جایگاه حقوقی دکترین دولت‌ها در تفسیر معاهدات بین‌المللی، فصلنامه بین‌المللی علمی– حقوقی قانون یار. ۳(۹): ۳۷۰- ۳۴۳

http://ensani.ir/file/download/article/1563693763-10125-9-16.pdf

- کیهانلو، فاطمه؛ وحید رضادوست (۱۳۹۴). حملات سایبر به مثابه توسل به زور در سیاق منشور سازمان ملل متحد. فصلنامه تحقیقات حقوقی. ۶۹ : ۲۰۸- ۱۹۳

https://lawresearchmagazine.sbu.ac.ir/article_56270.pdf

- نمامیان، پیمان؛ شیرزاد، امید (۱۳۹۹). جرم‌انگاری رفتارهای غیرقانونی علیه امنیت هواپیمایی کشوری در قلمرو کنوانسیون ۲۰۱۰ پکن. مطالعات بین‌المللی پلیس.۴۱: ۲۰۹- ۱۸۲

http://journals.police.ir/article_94739.pdf

- والتیکوس، نیکلاس (۱۳۷۶). سازمان‌های بین‌المللی و حقوق بین‌الملل، ترجمهٔ مرتضی نجفی اسفاد، مجله دیدگاه‌های حقوقی قضایی. ۵: ۲۰۰- ۱۸۷

http://ensani.ir/file/download/article/20100913180832-.pdf

English Resources:

-Coco, Antonio & Talita de Souza Dias (2021 .(Cyber Due Diligence: A Patchwork of Protective Obligations in International Law ,EJIL, Vol. XX 1–35, www .doi. org

-Holt, T. B., Moallemi, M., Weiland, L ,.Earnhardt, M & ,. McMullen, (2016 .(Aircraft cyber security and information exchange safety analysis for the department of commerce. Embry-Riddle Aeronautical University ,www .commons .erau.edu/publication

-Liu ,I. Yuying (2017 .(State Responsibility and Cyberattacks Defining Due Diligence Obligations ,IV Indonesian Journal of International & Comparative Law 191-260, www. ijil. Org

Documents:

-Aviation Cyber Security Guidelines) 2019 .(Civil Aviation Authority and Ministry of Transport & Communications Qatar .www. caa. gov. qa/ar,qa/PrintedPublications .

-CANSO Cyber Security and Risk Assessment Guide (2014 , (www. canso. org

-ICAO, Annex17, 2016

-ICAO ,A40-WP/3951 EX/161 30/7/2019

-ICAO ,Doc10118

-ICAO ,Doc9849, 2017

-Tallinn Manual 2 .0 on the International Law Applicable to Cyber Operations) 2017 , (Cambridge University Press ,https: //cambridge . org

Cases:

-Pulp Mills, Judgment, ICJ Reports (2010), para. 101 www. mjilonline. org/due-diligence-and-the-gray-zones-of-international-cyberspace-laws.

-Trail Smelter (United States v. Canada) (1941) 3 RIAA 1911, at 1963 ,196

Websites:

-www.atlanticcouncil.org

-www.icao .int/Aviation Cybersecurity Strategy, October 2019

-www.icao. int/cybersecurity/Pages/Resources. Aspx

-www.icao.int/cybersecurity/Pages/default.aspx