Journal of Safe City

Online ISSN: 2676-556X

Journal Homepage: www.ispdrc.ir

Research Paper

Challenges of Ensuring Cybersecurity in the Legal Systems of Iran and Iraq

Galineh Khalil Hassan[a], Masoud Raei Dehghi [b*],Alireza Ansari Mahyari [c],

[a]. *PhD student in public law,.Ph.D student in International Law, Najafabad Branch, Islamic Azad University, Najafabad , Iran*

[b]. P*rofessor Department of Law, Najafabad Branch, Islamic Azad University, Najafabad, Iran*

[c]. *Assistant Professor, Department of Law, Najafabad Branch, Islamic Azad University, Najafabad, Iran*

https://doi.org/ 10.22034/ispdrc.2025.2047872.1150

A R T I C L E I N F O

Keywords:
Cyber Threats,
Cyber Crimes,
Ensuring Cybersecurity,
Iranian law,
Iraqi law.

Received:
10 Desember 2024
Received in revised form:
8 January 2025
Accepted:
17 February 2025
pp.39-56

A B S T R A C T

In recent years, with significant advances in digital technologies and increasing dependence on cyberspace, new challenges have emerged in ensuring cybersecurity in countries. The legal systems of Iran and Iraq have also faced numerous problems in dealing with cyber threats. In both countries, the lack of a comprehensive and appropriate legal framework to counter cyber attacks was one of the biggest challenges. In Iran, despite the adoption of the Computer Crimes Law in 2009, the country still faced a lack of a comprehensive and efficient legal framework to counter complex and advanced cyber threats. In fact, many aspects of cybersecurity, including the protection of personal data, countering international cyber attacks, and rapid response to cyber crises, were not effectively foreseen in the Iranian legal system. In Iraq, too, due to political and economic crises and inadequacies in infrastructure structures, the country's efforts to establish an integrated and effective cybersecurity system did not achieve significant success. In addition, the lack of coordination between government agencies and the lack of regional and international cooperation left Iraq vulnerable to global and regional cyber threats.The method of this research is a descriptive-analytical method and analyzes the challenges and problems that Iran and Iraq have faced in ensuring cybersecurity..The results of this study showed that to address these challenges, it is necessary for both countries to undertake structural reforms in their legal and technical systems. Establishing international and regional cooperation in the field of cybersecurity is suggested as effective solutions to improve the cybersecurity situation in these two countries.If Iran and Iraq pay more attention to legal reforms and strengthening cybersecurity infrastructure, they will be able to effectively counter cyber threats.

* ***Corresponding Author: Masoud Raei Dehghi Email:masoudraei@yahoo.com***

Introduction

Cybersecurity, as one of the most important issues in today's digital world, refers to a set of measures, technologies, and processes that aim to protect information systems, networks, and data from cyber threats and unauthorized access. Given the rapid growth of information and communication technologies and the increase in cyber threats, cybersecurity has become one of the major challenges in various countries, especially Iran and Iraq. This study examines the challenges of ensuring cybersecurity in the legal systems of these two countries, and its findings have shown the existing shortcomings and issues.

Methodology

The method of conducting this research is descriptive-analytical. In this study, special attention has been paid to the formulation and effectiveness of existing laws, regulatory structure, and public education. Accurate recognition of the challenges and weaknesses of this area can help clarify the legal and executive needs to improve the current situation.

Results and discussion

According to the results of this study, the first major challenge was the lack of a comprehensive and effective legal framework to combat cyber threats. Although a computer crime law was passed in Iran, this law failed to cover all new threats such as advanced cyber attacks. On the other hand, Iraq was unable to formulate appropriate laws in this field due to political and economic crises, which has jeopardized cybersecurity in this country. The second challenge was the lack of internal coordination and cooperation among government and private institutions. In Iran, the multiplicity of relevant institutions and their overlapping duties have caused delays in responding to cyber threats. In Iraq, structural weaknesses and lack of resources have prevented effective cooperation and led to further problems in cybersecurity. In addition, the findings showed that external cyber threats exist as a serious challenge in both countries. Iran faces cyber attacks from malicious groups and international competitors, and Iraq is under constant threats due to the presence of terrorist groups. Other key challenges include weak technical infrastructure and a lack of skilled cybersecurity personnel. Both countries need specialized training in this area to increase their capabilities against cyber threats.

Conclusion

The present study showed that cybersecurity challenges in the legal systems of Iran and Iraq significantly affect the performance and response of these countries to cyber threats. Legal shortcomings, lack of coordination between different institutions, and lack of resources and technical infrastructure have always been serious obstacles in this direction. According to the findings, it seems that fundamental reforms in legal frameworks and strengthening international and regional cooperation are necessary to effectively confront cyber threats. At the same time, implementing specialized training programs and investing in cybersecurity infrastructure are of particular importance as key strategies to increase capabilities and improve responsiveness to cyber attacks. Finally, this study emphasizes the need to create an integrated and coordinated approach to strengthen cybersecurity in both countries, so that effective and constructive measures can be taken against persistent and growing global threats. Overall, paying attention to national and international needs in the field of cybersecurity can help maintain the integrity of data and critical infrastructure in Iran and Iraq.

Keywords: Cyber Threats, Cyber Crimes, Ensuring Cybersecurity, Iranian law, Iraqi law.

Funding

There is no funding support.

Authors' Contribution

Authors contributed equally to the conceptualization and writing of the article. All of the authors approved thecontent of the manuscript and agreed on all aspects of the work declaration of competing interest none.

Conflict of Interest

Authors declared no conflict of interest.

Acknowledgments

We are grateful to all the scientific consultants of this paper.

نشریه علمی شهر ایمن
شاپا الکترونیکی: 556X-2676
Journal Homepage: www.ispdrc.ir
مقاله پژوهشی

چالشهای تضمین امنیت سایبری در نظام حقوقی ایران و عراق

گلینه خلیل حسن- دانشجوی دکترا حقوق عمومی، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد ، ایران.
مسعود راعی دهقی*-استاد گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد ، ایران.
علیرضا انصاری مهیاری- استادیار گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد ، ایران.

https://doi.org/ ۱۰.۲۲۰۳۴/ispdrc.۲۰۲۵.۲۰۴۷۸۷۲.۱۱۵۰

واژگان کلیدی
امنیت سایبری، جرمهای سایبری ، تضمین امنیت سایبری، قانون ایران، قانون عراق.

چکیده
در سال‌های اخیر، با پیشرفت‌های چشمگیر در فناوری‌های دیجیتال و افزایش وابستگی به فضای مجازی، چالش‌های جدیدی در زمینه تضمین امنیت سایبری در کشورها به وجود آمد. نظام‌های حقوقی ایران و عراق نیز در مواجهه با تهدیدات سایبری با مشکلات عدیده‌ای روبه‌رو بودند. در هر دو کشور، فقدان چارچوب قانونی جامع و مناسب برای مقابله با حملات سایبری به‌عنوان یکی از بزرگ‌ترین چالش‌ها مطرح بود. در ایران، علی‌رغم تصویب قانون جرایم رایانه‌ای در سال ۱۳۸۸، این کشور همچنان با کمبود یک چارچوب قانونی جامع و کارآمد برای مقابله با تهدیدات سایبری پیچیده و پیشرفته مواجه بود. در واقع، بسیاری از ابعاد امنیت سایبری، از جمله محافظت از داده‌های شخصی، مقابله با حملات سایبری بین‌المللی و همچنین واکنش سریع به بحران‌های سایبری به‌طور مؤثر در نظام حقوقی ایران پیش‌بینی نشده بود. در عراق نیز، به دلیل بحران‌های سیاسی و اقتصادی و ناتوانی در ساختارهای زیرساختی، تلاش‌های این کشور در جهت ایجاد یک سیستم امنیتی سایبری یکپارچه و مؤثر به موفقیت چشمگیری نرسید. علاوه بر این، نبود هماهنگی میان دستگاه‌های دولتی و عدم همکاری‌های منطقه‌ای و بین‌المللی، باعث شد که عراق در برابر تهدیدات سایبری جهانی و منطقه‌ای آسیب‌پذیر باقی بماند. روش پژوهش توصیفی تحلیلی، می باشد. نتایج حاصل از این پژوهش حاکی از آن است که برای رفع این چالش‌ها، لازم است که هر دو کشور به اصلاحات ساختاری در سیستم‌های حقوقی و فنی خود بپردازند. ایجاد همکاری‌های بین‌المللی و منطقه‌ای در حوزه امنیت سایبری، به‌عنوان راهکارهای مؤثر برای بهبود وضعیت امنیت سایبری در این دو کشور پیشنهاد می شود. در صورتی که ایران و عراق به اصلاحات حقوقی و تقویت زیرساخت‌های امنیت سایبری توجه بیشتری داشته باشند، قادر خواهند بود تا با تهدیدات سایبری به‌طور مؤثری مقابله کنند.

تاریخ دریافت:
۱۴۰۳/۰۹/۲۰
تاریخ بازنگری:
۱۴۰۳/۱۰/۱۹
تاریخ پذیرش:
۱۴۰۳/۱۱/۲۹
صص: ۵۶-۳۹

*. نویسنده مسئول:رایانامه masoudraei@yahoo.com

مقدمه:

در دنیای امروز، امنیت سایبری به یکی از موضوعات حیاتی و ضروری برای حفاظت از اطلاعات حساس و زیرساخت‌های کلیدی تبدیل شده است. با توجه به وابستگی عمیق جوامع به فناوری اطلاعات و اینترنت، چالش‌های مرتبط با امنیت سایبری در کشورهایی مانند ایران و عراق به شدت احساس می‌شود. این دو کشور با تهدیدات سایبری متعددی مواجه هستند که ناشی از ناپایداری‌های سیاسی، اقتصادی و اجتماعی، همچنین ضعف‌های قانونی و اجرایی در حوزه امنیت سایبری است. بررسی این چالش‌ها و موانع می‌تواند به شناسایی نقاط ضعف موجود در نظام‌های حقوقی این کشورها کمک کند و راهکارهای مؤثری برای بهبود وضعیت ارائه دهد(افشار و همکاران،۱۳۹۳: ۳۳). چالش‌های اصلی تضمین امنیت سایبری در ایران و عراق شامل نقص‌های قانونی، عدم شفافیت در فرآیندهای اداری، کمبود نیروی انسانی متخصص و عدم همکاری‌های بین‌المللی است. در ایران، علی‌رغم وجود برخی قوانین مرتبط با امنیت سایبری، هنوز هم مشکلاتی در اجرای آن‌ها وجود دارد که مانع از حفاظت مؤثر از داده‌ها و اطلاعات می‌شود. در عراق نیز فقدان یک چارچوب قانونی جامع و مؤثر برای مقابله با تهدیدات سایبری، آسیب‌پذیری این کشور را افزایش داده است. همچنین، ناپایداری سیاسی و اجتماعی در هر دو کشور موجب می‌شود که دولت‌ها نتوانند به طور مؤثر بر روی مسائل امنیت سایبری تمرکز کنند. از جمله راهکارهای موجود برای مقابله با این چالش‌ها شامل تقویت زیرساخت‌های قانونی، تربیت نیروی انسانی متخصص و افزایش آگاهی عمومی درباره خطرات سایبری است. در ایران، تلاش‌هایی برای ارتقاء قوانین و مقررات صورت گرفته، اما نیاز به سرمایه‌گذاری بیشتر در آموزش و تربیت متخصصان احساس می‌شود. در عراق نیز باید بر روی تدوین قوانین جدید و ایجاد همکاری‌های بین‌المللی تمرکز شود تا بتوان به طور مؤثری با تهدیدات سایبری مقابله کرد. همچنین، افزایش آگاهی عمومی درباره حقوق کاربران و خطرات فضای مجازی می‌تواند به کاهش آسیب‌پذیری کمک کند. هدف این پژوهش بررسی موانع حقوقی حمایت از امنیت سایبری در نظام‌های قانونی ایران و عراق است. سوال اصلی این پژوهش این است که چه موانع حقوقی و اجرایی در نظام‌های قانونی ایران و عراق وجود دارد که مانع از تأمین امنیت سایبری مؤثر می‌شود؟ در پاسخی کوتاه به عنوان فرضیه می توان بیان نمود که موانع حقوقی شامل نقص‌های قانونی، عدم شفافیت در فرآیندهای اداری و کمبود نیروی انسانی متخصص هستند که به کاهش اثر بخشی اقدامات حمایتی در هر دو کشور ایران و عراق منجر می‌شوند.

از پژوهشهای موجود در زمینه موضوع این مقاله، می توان به پژوهش رسول ملکوتی و مونا خلیل زاده در سال ۱۴۰۱ در زمینه راهکار حقوقی تامین امنیت سایبری اشاره نمود، در این پژوهش بیان شده که با توجه به رشد روزافزون نرخ استفاده از فضای سایبر در دنیای کنونی، چه در سطح کلان (امور دولتی و حاکمیتی) و چه در سطح خرد (میان شهروندی)، از مهم ترین وظایف قانونگذار در این بستر، تأمین امنیت، اعم از مدنی و کیفری است. بدیهی است که ارتکاب جرم یا هرعملیات متقلبانه مادون آن، در این فضا با رشد فناوری، روزانه دستخوش تغییر می شود. گاهی، بین جرم ارتکابی و مجازات تعیین شده، تناسبی وجود ندارد، لذا فرد بزهکار، با برآورد دستاورد خود در این فضا و با علم به میزان مجازات تعیین شده، اقدام به ارتکاب جرم می کند(ملکوتی و خلیل زاده، ۱۴۰۱: ۷۱). در پژوهشی دیگر، طیبه بلوردی و مطهره طیاری پور احمدی در سال ۱۴۰۱، در پژوهش خود با عنوان اقدامات دولت در ایجاد امنیت سایبری بیان نموده اند که نتایجی به دست آمده نشان می دهد، به دلیل اثرگذاری و گستردگی زیاد و سهولت و سادگی کاربرد و تنوع ابزارها و روش ها، وقوع تهدیدات سایبری قطعی است. بایستی با فرهنگ سازی، توسعه ی زیرساخت ها، تدابیر فنی مدیریتی یک تغییر بنیادین در فضای سایبری و ارتقای امنیت آن ایجاد کرد(بلوردی و طیاری پور احمدی، ۱۴۰۱: ۶۵). همچنین لی و کرسپی در سال ۲۰۱۱ میلادی پژوهشی با عنوان اینترنت اشیا: چالشی برای معماری جدید از مشکلات به این نتیجه رسیده اند که ایده اصلی اینترنت اشیا (*IoT*) این است که اینترنت اشیاء اطراف ما را به هم متصل می کند تا ارتباطات یکپارچه و خدمات زمینه ای ارائه شده توسط آنها را فراهم کند. برنامه های بسیاری وجود دارد که به دلیل اینترنت اشیا قابل پشتیبانی هستند. توسعه چندین فناوری امکان دستیابی به چشم انداز اینترنت اشیاء را فراهم کرد. چالش‌های اصلی اینترنت اشیا شامل مسائل امنیتی و حفظ حریم خصوصی، نبود استانداردهای یکپارچه، مدیریت حجم بالای داده‌ها و هزینه‌های پیاده‌سازی است. برای غلبه بر این چالش‌ها نیاز به تدوین استانداردهای جهانی و توسعه فناوری‌های امنیتی پیشرفته است(Lee & Crespi, 2011: 54). با توجه به پیشینه های بیان شده، در زمینه تفاوت این پژوهش با موارد مذکور می توان عنوان نمود که تفاوت اصلی این پژوهش بررسی چالشهای موجود در زمینه تضمین امنیت

سایبری در دو کشور ایران و عراق می باشد، در حالی منابع عنوان شده به صورت خاص کشوری را مورد بررسی قرار نداده و تنها به مباحث فضای اینترنت و امنیت سایبری پرداخته اند که این، خود اصلی تریت تفاوت پژوهش حاضر با پژوهشهای عنوان شده می باشد.

۱- ماهیت امنیت سایبری

یکی از فعالیتهای روزانه مردم در هر زمان و مکان، استفاده نمودن از فضای مجازی می باشد. امروزه، مقوله فضای مجازی، نقش مهم و اثرگذاری را در زندگی افراد ایفا می نماید؛ گرچه استفاده نمودن از فضای مجازی دارای محاسن متعددی بوده و موجب آسانتر شدن انجام امور در زندگی مردم شده، اما کاربرد ناصحیح از آن سبب ایجاد آسیبهای روانی و جسمانی بر سلامت افراد و همچنین وجود جرایم متعدد گردیده است(حسینی و انصاری مهیاری، ۱۴۰۲: ۷۱). مبحث امنیت سایبری پایه و شالوده اصلی تکنولوژیها، فرآیندها و روشهای طراحی گردیده برای حفاظت نمودن از شبکه ها، ابزارهای دیجیتالی، داده ها و برنامه ها در برابر حمله و خسارتها و دسترسیهای غیر مجاز می باشد. مقوله امنیت سایبری به مجموعه‌ای از فناوری‌ها، فرآیندها و اقدامات گفته می‌شود که به منظور حفاظت از سیستم‌ها، شبکه‌ها، برنامه‌ها و داده‌ها در برابر حملات سایبری، دسترسی های غیرمجاز، آسیب‌ها و تخریب اطلاعات طراحی شده‌اند. این مفهوم شامل شناسایی تهدیدات، پیشگیری از حملات، واکنش به حوادث و بازیابی اطلاعات در صورت وقوع یک حمله است. امنیت سایبری به‌ویژه در دنیای دیجیتال امروز اهمیت ویژه‌ای دارد، زیرا با افزایش وابستگی به فناوری و اینترنت، خطرات مربوط به سرقت اطلاعات، نقض حریم خصوصی و آسیب‌های مالی نیز افزایش یافته است. هدف اصلی امنیت سایبری تضمین محرمانگی، صحت و دسترسی به اطلاعات و سیستم‌ها است تا سازمان‌ها و کاربران بتوانند با اطمینان بیشتری از فناوری‌های دیجیتال استفاده کنند. (نعمتی و صادقی نشاط، ۱۳۹۶: ۱۵۲). بنابراین امنیت سایبری به صورت خلاصه، به فرآیند حفاظت داده ها و اطلاعات در برابر انواع کارهای غیرمجاز شامل دسترسی، استفاده، اختلال و تخریب گفته می شود.

۲-تأمین امنیت سایبری

تأمین امنیت سایبری، فرایندی چند وجهی و پیوسته است که هدف آن حفاظت از سیستم‌ها، شبکه‌ها، دستگاه‌ها و داده‌ها در برابر حملات سایبری، دسترسی‌های غیرمجاز، سرقت، تخریب یا سوء استفاده است. این فرایند شامل مجموعه‌ای از اقدامات فنی، سازمانی و انسانی است که با هدف کاهش ریسک‌های امنیتی و تضمین محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات انجام می‌شوند(صانعی، ۱۳۹۸: ۱۹۸). تأمین امنیت سایبری نیازمند رویکردی فعال و پیشگیرانه است که شامل شناسایی و ارزیابی آسیب‌پذیری‌ها، طراحی و پیاده‌سازی کنترل‌های امنیتی مناسب، آموزش کارکنان و کاربران، نظارت مداوم بر فعالیت‌های سایبری، و پاسخگویی سریع و مؤثر به حوادث امنیتی است. همچنین، استفاده از فناوری‌های نوین مانند هوش مصنوعی و یادگیری ماشین برای شناسایی تهدیدات پیشرفته و خودکارسازی فرایندهای امنیتی نیز جزء ضروریات تأمین امنیت سایبری در دنیای امروز محسوب می‌شود(ملک، ۱۴۰۲: ۰۶). این فرایند نه تنها برای سازمان‌ها و شرکت‌ها، بلکه برای افراد عادی نیز اهمیت دارد، زیرا در دنیای امروز، اطلاعات شخصی و مالی افراد به طور مداوم در معرض خطرات سایبری قرار دارند.

۳-ضرورت تضمین امنیت سایبری

مبحث جرایم سایبری مفهومی، گسترده است که از لحاظ تحلیلی از حمله سایبری متمایز است؛ در حالی که مانند مفهوم حمله سایبری، هیچ تعریف شناخته شده جهانی از جرایم سایبری وجود ندارد ابعادی از جرایم سایبری وجود دارد که به صورت گسترده به رسمیت شناخته شده اند. بر همین اساس، جرایم سایبری طیف گستردهای از فعالیتهای غیرقانونی را در برمی گیرد و همین امر ضرورت وجود امنیت سایبری را افزایش می دهد(صادقی و همکاران، ۱۴۰۳: ۵۳).

مقوله تضمین امنیت سایبری به عنوان ضرورتی اساسی در دنیای دیجیتالی امروز، به علت افزایش یافتن تهدیدهای سایبری و پیچیدگی حملات، اهمیتی ویژه یافته است (برزگر کلاته، ۱۳۹۶: ۷۰). با گسترش فناوری اطلاعات و ارتباطات، سازمان‌ها و افراد به طور فزاینده‌ای به شبکه‌های دیجیتال وابسته گردیده و این وابستگی، آن‌ها را در معرض خطرهایی همچون نظیر سرقت اطلاعات، حملات باج‌افزاری و نفوذهای غیرمجاز قرار می دهد(جیجان السماوئلی، ۱۴۰۰: ۵۴). مقوله امنیت سایبری نه فقط برای حفاظت از داده‌های حساس و زیرساخت‌های حیاتی ضروری است، بلکه به حفظ حریم خصوصی کاربران و اعتماد عمومی به فناوری‌های دیجیتال نیز کمک می‌کند. در واقع، عدم

تأمین امنیت مناسب می‌تواند منجر به خسارات مالی قابل توجه، آسیب به شهرت سازمان‌ها و حتی تهدید به امنیت ملی شود(*Cornish et al, 2009: 12*). بنابراین، ایجاد چارچوبی جامع جهت مدیریت نمودن تهدیدهای سایبری و اجرا نمودن سیاست‌های اثرگذار در این زمینه، برای تضمین نمودن یک عملکرد صحیح و ایمن سیستم‌های اطلاعاتی ضروری می باشد. امنیت سایبری نقش مهمی را در توسعه فناوری اطلاعات و همچنین خدمات اینترنتی ایفا می کند. تقویت امنیت سایبری و حفاظت از زیرساخت های اطلاعات برای امنیت و رشد اقتصادی هر ملتی ضروری می باشد(ملکوتی و خلیل زاده، ۱۴۰۰: ۷۶). ایمن تر نمودن فضای اینترنت و حفاظت نمودن از کاربران اینترنت جهت توسعه یافتن سرویسهای جدید و سیاست های دولتی، امری بسیار ضروری می باشد(*Andress&Winterfled, 2014: 11*). توقف جرمهای سایبری قسمتی مهم از رویکرد حفاظت از زیربنای اطلاعات و امنیت سایبری هر کشوری می باشد (زابلی زاده و وهاب پور، ۱۳۹۶: ۱۷). در سطح ملی، این مسئولیتی مشترک می باشد، که نیازمند وجود یک هماهنگی برای پیشگیری، آمادگی، پاسخگویی بین بخشهای دولتی، بخش خصوصی و شهروندان می باشد. در سطح منطقه ای و بین المللی شامل همکاری و هماهنگی بین دولت ها و سازمان های بین‌المللی مربوطه می باشد. تضمین امنیت سایبری از اهمیت بالایی برخوردار میباشد، به این علت که امروزه حیات اقتصادی، اجتماعی و حتی امنیت ملی کشورها به شدت به زیرساخت‌های دیجیتال وابسته است. با توجه به افزایش تهدیدات سایبری مانند هک، بدافزارها، و حملات فیشینگ، عدم امنیت در فضای سایبری می‌تواند منجر به سرقت اطلاعات حساس، اختلال در خدمات عمومی، و حتی تخریب زیرساخت‌های حیاتی شود(*JaBae, 2003: 84*). علاوه بر آن، با گسترش اینترنت اشیا و استفاده روزافزون از سیستم‌های هوشمند، خطرات مرتبط با امنیت سایبری پیچیده‌تر و گسترده‌تر شده‌اند. بنابراین، تضمین امنیت سایبری نه تنها برای حفاظت از داده‌های شخصی و سازمانی ضروری است، بلکه برای حفظ اعتماد عمومی به فناوری‌های دیجیتال و ایجاد یک محیط پایدار و امن برای نوآوری و توسعه اقتصادی نیز حیاتی است.(مرندی، ۱۳۹۹: ۳۳). در این راستا، تدوین و اجرای سیاست‌ها و قوانین جامع، ارتقای آگاهی عمومی و افزایش همکاری‌های بین‌المللی از ضروریات دستیابی به امنیت سایبری پایدار به شمار می‌رود.

۴- چالشهای تضمین امنیت سایبری در رویه نظری

پیشرفت انسان در زمینه های های مختلف سیاسی و اجتماعی فرصت ها و چالش های جدیدی را ایجاد نموده و یکی از این چالش ها، مبحث حملات سایبری می باشد که باتوجه به گسترش روزافزون فناوری و توسعه فضای مجازی در نقاط مختلف جهان، تهدیدی برای زندگی اشخاص محسوب می گردد. (انصاری مهیاری و محمودی، ۱۴۰۱: ۲۰). خصیصه اصلی فضای سایبری این است که با وجود تمامی فواید و آسان سازی دسترسی به اطلاعات و انجام امور، بستری امن برای افراد مجرم باشد. پیشرفت سریع و روزانه تکنولوژی های ارتباطی، علیرغم وجود مزایای فراوان، دارای معایبی نیز می باشند؛ با نگاهی به وب سایتهای مختلف می توان به این نتیجه رسید که صنعت وب روزانه در حال رشد بوده و این موضوع، فرصتی طلایی برای مجرمینی می باشد که در حال فعالیت در فضای اینترنت می باشند(الجصانی، ۱۴۰۱: ۱۴). با توجه به تحولات گسترده در حوزه تکنولوژِی و فناوری ارتباطی و اطلاعاتی در چند سال اخیر، با توجه به کارکردهای خوب و مثبت این حوزه، گاهی دیده می شود که برخی از اشخاص سودجو برای فراگیری مهارتهای حوزه سایبر درصدد سوءاستفاده نمودن از اشخاص کاربر در این فضا و ایجاد مشکلاتی برای آنها می باشند(انصاری مهیاری و همکاران، ۱۴۰۳: ۴۳). فضای سایبری، فرصتهایی جدید و پیشرفتهای را برای قانون شکنی در اختیار اشخاص قرار می دهد و ظرفیتی بالقوه برای ارتکاب جرایم را به روشهای مرسوم و جدید داشته تا اشخاص بزه کار این حوزه قادر باشند تا در فضای گسترده اینترنت هر فکر و اندیشه ای را که در ذهن دارند، عملی نمایند.

تضمین امنیت سایبری به لحاظ نظری، دارای چالشهایی می باشد که در ادامه پس از بررسی قوانین موجود در کشورهای ایران و عراق در رابطه با امنیت سایبری به آن پرداخته می شود.

۴-۱-بررسی قوانین موجود

در این قسمت، قوانین داخلی کشورهای ایران و عراق در زمینه تضمین امنیت سایبری بررسی می شوند:

۴-۱-۱-قوانین کشور ایران

در کشور ایران، قوانین و مقررات مختلفی برای امنیت سایبری تدوین شده است که برای حفاظت از داده‌ها و جلوگیری از جرایم سایبری به کار می‌روند:

الف(قانون جرایم رایانه‌ای)۱۳۸۸(

این قانون در سال ۱۳۸۸)۲۰۰۹(به تصویب مجلس شورای اسلامی رسید و در سال ۱۳۸۹ به اجرا درآمد. هدف این قانون مقابله با انواع جرایم رایانه‌ای و حفظ امنیت فضای سایبری است. این قانون شامل طیف وسیعی از جرایم از قبیل نفوذ به سیستم‌های رایانه‌ای، سرقت اطلاعات، جعل مدارک الکترونیکی و انتشار ویروس‌هاست. قانون جرایم رایانه‌ای مجازات‌های متناسب با هر نوع جرم را تعیین کرده است. این مجازات‌ها شامل حبس، جریمه نقدی یا هر دو است. محاکم عمومی و ویژه برای رسیدگی به این جرایم تعیین شده‌اند و به دادسرای جرایم رایانه‌ای تحت نظارت دادستانی کل کشور ارجاع داده می شوند)متقی و همکاران، ۴۸ :۱۳۹۲(.

ب(قانون حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی)۱۳۹۹(

این قانون در سال ۱۳۹۹ به تصویب مجلس شورای اسلامی رسید. هدف این قانون حمایت از حقوق کاربران در فضای مجازی و ساماندهی به خدمات پایه کاربردی است. حفاظت از داده‌های کاربران: این قانون به حفاظت از داده‌ها و حریم خصوصی کاربران پرداخته و الزاماتی برای آژانس‌ها و ارائه‌دهندگان خدمات آنلاین به وجود آورده است. ارائه‌دهندگان خدمات ملزم به ارائه اطلاعات دقیق و شفاف در مورد نحوه جمع‌آوری و استفاده از داده‌های کاربران هستند. این قانون مکانیزم‌های قانونی برای حل و فصل اختلافات بین کاربران و ارائه‌دهندگان خدمات را مشخص کرده است)الجصانی، ۱۴۰۱: ۱۴(.

ج(قانون شبکه ملی اطلاعات)۱۳۹۵(

این قانون در سال ۱۳۹۵ تصویب شد و به منظور ایجاد یک شبکه داخلی برای کاهش وابستگی به اینترنت جهانی طراحی گردید.این قانون به هدف فراهم کردن زیرساخت‌های لازم برای داده‌های داخلی و ایجاد امنیت بیشتر در تبادل اطلاعات در داخل کشور تصویب شده است. زیرساخت‌های شبکه: مطابق این قانون، ایجاد زیرساخت‌های امن برای تأمین داده‌ها از طریق شبکه ملی اطلاعات الزامی است.این قانون به حفظ اطلاعات و حریم خصوصی کاربران ایرانی در فضای دیجیتال تأکید دارد)مجتبی زاده، ۰۷ :۱۴۰۰(.

د)نظام‌نامه امنیت سایبری (ابلاغیه شورای عالی فضای مجازی)

این نظام‌نامه در در سال ۱۳۹۵ توسط شورای عالی فضای مجازی تهیه و ابلاغ شد. هدف از این نظام‌نامه ایجاد یک چارچوب کلی برای حفاظت از سیستم‌ها و اطلاعات در برابر تهدیدات سایبری است. نظام‌نامه به ارائه دستورالعمل‌های امنیتی برای سازمان‌ها و نهادهای دولتی و خصوصی می‌پردازد تا در برابر تهدیدات سایبری مقاوم‌سازی شوند. تأکید بر لزوم آموزش و پژوهش در زمینه امنیت سایبری برای متخصصان و کارکنان به منظور بالا بردن آگاهی و قابلیت‌ها (عیفان الشمری، ۱۴۰۲: ۸۵).

و)قانون تجارت الکترونیک (۱۳۸۲)

این قانون در سال ۱۳۸۲ به تصویب رسید و به طور رسمی در سال ۱۳۸۳ لازم‌الاجرا گردید. این قانون به هدف تنظیم و تسهیل فعالیت‌های اقتصادی در فضای مجازی و اعتبار بخشیدن به معاملات الکترونیکی طراحی شده است(انوشا و همکاران، ۱۴۰۰: ۰۳). معاملات الکترونیکی: قانون احکام و قواعد مربوط به انجام معاملات الکترونیک و چگونگی اعتبار آن‌ها را مشخص می‌کند. تدابیر امنیتی برای حفاظت از داده‌های شخصی و مالی کاربران در فرآیندهای آنلاین تعریف شده است (افشار و همکاران، ۱۳۹۳: ۳۹).

۴-۱-۲- قوانین کشور عراق

در عراق، تضمین امنیت سایبری یک موضوع پیچیده است که تحت پوشش قوانین مختلفی قرار دارد:

الف) قانون حفاظت از داده‌های شخصی (۲۰۲۱)

عراق در سال ۲۰۲۱ یک قانون حفاظت از داده‌های شخصی به تصویب رساند که به طور خاص بر امنیت اطلاعات و داده‌های شخصی افراد تمرکز دارد. این قانون با هدف حفظ حریم خصوصی و امنیت داده‌های شخصی کاربران و شرکت‌ها تدوین شده است. از آنجا که تهدیدات سایبری معمولاً در ارتباط با سرقت یا افشای اطلاعات شخصی اتفاق می‌افتد، این قانون نقش مهمی در امنیت سایبری ایفا می‌کند. این قانون شامل الزاماتی برای شرکت‌ها و سازمان‌ها در راستای حفظ و حفاظت از داده‌های شخصی، همچنین نحوه ذخیره‌سازی، پردازش و انتقال داده‌های شخصی می‌باشد. همچنین این قانون شامل جریمه‌ها

و مجازات‌هایی برای کسانی است که به صورت غیرمجاز به داده‌های شخصی دسترسی پیدا کرده و آن‌ها را افشا کنند(علاء تکلیف، ۱۴۰۲: ۳۵).

ب) قانون امنیت سایبری (۲۰۲۰)

قانون امنیت سایبری عراق که در سال ۲۰۲۰ میلادی تصویب شد، به‌طور خاص به ایجاد یک چارچوب قانونی برای حفاظت از زیرساخت‌های حیاتی در برابر تهدیدات سایبری می‌پردازد. این قانون ایجاد یک آژانس ملی برای نظارت و هماهنگی در زمینه امنیت سایبری را پیش‌بینی می‌کند.آژانس ملی امنیت سایبری: این نهاد مسئول نظارت بر تهدیدات سایبری و اجرای تدابیر پیشگیرانه است. این سازمان باید مسئول ارزیابی آسیب‌پذیری های سایبری و پیش‌بینی تهدیدات احتمالی باشد. این قانون عراق را ملزم به همکاری با دیگر کشورها در زمینه مقابله با تهدیدات سایبری و جرایم اینترنتی می‌کند (حبیب خبط، ۱۴۰۳: ۶۸).

ج)قانون مبارزه با جرایم اینترنتی (۲۰۱۵)

عراق در سال ۲۰۱۵ قانون دیگری به نام قانون مبارزه با جرایم اینترنتی را تصویب کرد. این قانون شامل تدابیر مقابله با جرایم سایبری مختلف از جمله هک کردن سیستم‌ها، حملات دیداس[1]، سرقت داده‌ها و ایجاد نرم‌افزارهای مخرب است. این قانون شامل تعریفی جامع از انواع جرایم سایبری از جمله دسترسی غیرمجاز به داده‌ها، تغییر داده‌ها و تخریب اطلاعات است. افرادی که مرتکب جرایم سایبری می‌شوند، ممکن است با مجازات‌های سنگینی از جمله جریمه‌های مالی و حبس روبرو شوند(سبهان النویصری، ۱۴۰۳: ۶۵).

۴-۲- مقایسه تطبیقی قوانین موجود در کشور ایران و عراق در زمینه تضمین امنیت سایبری

مقایسه تطبیقی قوانین موجود در زمینه تأمین امنیت سایبری در کشورهای ایران و عراق نشان‌دهنده تلاش‌های هر دو کشور برای مقابله با تهدیدات سایبری و حفاظت از داده‌ها و اطلاعات می باشد. در ایران، قانون جرایم رایانه‌ای که در سال ۱۳۸۸ه.ش تصویب گردیده، به عنوان یکی از مهم‌ترین قوانین در این حوزه شناخته می‌شود. این قانون به جرم‌انگاری دسترسی غیرمجاز به سیستم‌های رایانه‌ای، انتشار محتویات مجرمانه و هک پرداخته و مجازات‌های مشخصی برای متخلفان تعیین نموده است(رضایی، ۱۴۰۲: ۶۳). در مقابل، عراق نیز با وجود اینکه هنوز قانون جامعی مشابه با قانون ایران ندارد، اقداماتی را برای تدوین قوانین امنیت سایبری آغاز کرده است(العتابی، ۱۴۰۱: ۷۱). در کشور ایران، آیین‌نامه امنیت فضای تولید و تبادل اطلاعاتبه عنوان یک چارچوب قانونی برای سازمان‌ها و نهادهای دولتی و خصوصی عمل می‌کند. این آیین‌نامه شامل دستورالعمل‌هایی برای حفاظت از داده‌های حساس و مدیریت ریسک‌های سایبری است. در عراق، با وجود تلاش‌ها برای ایجاد زیرساخت‌های قانونی در زمینه امنیت سایبری، هنوز هیچ آیین‌نامه مشخصی وجود ندارد که به طور جامع به این موضوع بپردازد و نیاز به تدوین چنین مستنداتی احساس می‌شود (اختری و همکاران، ۱۴۰۲: ۱۲۷).

قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای نیز در کشور ایران به حفاظت از حقوق مالکیت فکری و جلوگیری از نقض این حقوق کمک می نماید. این قانون به نوعی می‌تواند به تقویت مقوله امنیت سایبری کمک نماید، چون که حفاظت نمودن از نرم‌افزارها و داده‌ها به کاهش جرایم سایبری مرتبط با سرقت نرم‌افزارها منجر می‌شود. در کشورعراق، هرچند قوانینی برای حمایت از حقوق مالکیت فکری وجود دارد، اما اجرای مؤثر آن‌ها و آگاهی عمومی درباره این حقوق کماکان نیازمند تقویت می باشد. در زمینه تأمین امنیت سایبری، طرح صیانت که اخیراً در کشور ایران مطرح گردیده، شامل کنترل بیشتر دولت بر فضای مجازی و محدود کردن دسترسی به برخی ابزارها مانند وی.پی.و اِن[2] هاست. این طرح با انتقاداتی متعدد زیادی مواجه گردیده و نگرانی‌هایی درباره تأثیر آن بر آزادی بیان ایجاد کرده

---

[1] حملاتDDoS: مله دیداس یا DDoS مخفف عبارت Distributed Denial of Service به‌معنی «منع سرویس توزیع شده» است. حمله سایبری DDoS یکی از خطرناک‌ترین حملاتی است که هکرها و باتنت‌ها با ارسال حجم عظیمی از ترافیک (Flood of Internet Traffic) قصد ایجاد اختلال در ترافیک عادی یک سرور، شبکه و وب‌سایت یا از دسترس خارج کردن آن برای سرویس‌دهی را برعهده دارند. در حمله DDoS، یک سرور، وب‌سایت یا شبکه با ترافیک اینترنتی غیرعادی از چند منبع مواجه می‌شود که باعث اختلال در سرویس‌دهی آن خواهد شد. حملات سایبری DDoS می‌توانند از نظر پیچیدگی و اندازه متفاوت باشند و عملکرد وب‌سایت‌ها و دسترسی به آن‌ها را به‌طور قابل توجهی تحت تاثیر قرار دهند.
برای مطالعه بیشتر رجوع شود به:
https://parspack.com/blog/security/ddos-attack

[2] وی.پی.اِن(VPN): VPN مخفف عبارت Virtual Private Network است

است. کشورعراق نیز به دنبال ایجاد کنترل بر فضای مجازی می باشد، اما هنوز هیچ طرح جامع مشابهی مانند طرح صیانت کشور ایران ارائه نگردیده است)العتابی، ۸۳ :۱۴۰۱(. از نظر همکاری های بین‌المللی، کشور ایران به دلیل تحریم‌ها و محدودیت‌های سیاسی با چالش‌هایی مواجه می باشد که بر توانایی آن در همکاری با دیگر کشورها اثرگذار است. کشور عراق نیز به علت وضعیت سیاسی ناپایدار خود نتوانسته همکاری‌هایی مؤثر را با کشورهای دیگر در زمینه مقوله امنیت سایبری برقرار نماید.

۵- چالشهای حقوقی تضمین امنیت سایبری در رویه عملی

چالش‌های حقوقی در تضمین امنیت سایبری به‌ویژه در ابعاد بین‌المللی و داخلی شامل فقدان چارچوب‌های قانونی جامع و هماهنگ است که کشورهای مختلف بر سر آنها توافق ندارند. این موضوع منجر به تفسیرهای متفاوت از قوانین و عدم هم‌افزایی در هنجارها و معیارهای امنیت سایبری می شود(مرادی و همکاران، ۱۴۰۱: ۶۴). در سطح داخلی، به تضاد منافع ملی و حقوق بشر محدود می شود، جایی که نگرانی‌های امنیتی ممکن است آزادی‌های فردی را تحت فشار قرار دهد (پروانه، ۱۴۰۱: ۷۸). همچنین، عدم وجود استانداردهای مشترک و ابزارهای نظارتی کافی در بسیاری از کشورها، به چالش‌هایی در حفاظت از داده‌ها و مقابله با تهدیدات سایبری، به‌خصوص در فضای متغیر فناوری اطلاعات و ارتباطات، دامن می‌زند.

۵-۱- نقص اجرای قوانین در کشورهای ایران و عراق

نقص در اجرای قوانین امنیت سایبری در کشورهای ایران و عراق به عنوان یکی از چالش‌های مهم و اساسی در این دو کشور مطرح می باشد؛ در کشور ایران، با وجود قوانین مشخصی همانند قانون جرایم رایانه‌ای و آیین‌نامه امنیت فضای تولید و تبادل اطلاعات، مشکلاتی همانند عدم ضمانت اجرایی و کمبود نظارت بر اجرای این قوانین وجود دارد(حسینی‌امینی و محسن‌زادگان، ۱۳۹۳: ۵۳۶). به عنوان نمونه، مقامات مسئول در ایران مکرراً به عدم پاسخگویی مدیران سازمان‌ها در قبال نشت اطلاعات و نقض حریم خصوصی کاربران اشاره نموده اند. این موضوع حاکی از ضعف در سیستم‌های نظارتی و عدم احساس مسئولیت از سوی مدیران بوده که می‌تواند به تکرار حوادثی ناگوار منجر شود(شیرنسبیان، ۱۴۰۱: ۶۸). در عراق نیز، وضعیت مشابهی حاکم است. اگرچه این کشور تلاش‌هایی برای تدوین قوانین امنیت سایبری انجام داده، اما هنوز هیچ قانون جامع و مؤثری برای مقابله با تهدیدات سایبری وجود ندارد(حبیب‌خبط، ۱۴۰۳: ۱۵۴). این کمبود قانونی به همراه ناپایداری سیاسی و اجتماعی در عراق، باعث شده تا اجرای هرگونه اقدام مؤثر در زمینه امنیت سایبری با چالش‌های جدی مواجه شود. بسیاری از کارشناسان معتقدند که نبود یک چارچوب قانونی مشخص برای حفاظت از داده‌ها و اطلاعات کاربران، زمینه‌ساز افزایش حملات سایبری و نقض حریم خصوصی در این کشور است(الشمری، ۲۰۲۱: ۲۲۱). مضاف بر این موارد، در هر دو کشور، عدم وجود یک هماهنگی میان نهادهای متولی در زمینه مقوله امنیت سایبری نیز به عنوان یک مشکل جدی مطرح می باشد؛ در کشور ایران، با وجود تلاش‌هایی برای هماهنگی بین نهادهای امنیت سایبری، کماکان موازی‌کاری‌ها و ناهماهنگی‌هایی مشاهده می شود که می‌تواند بر کارایی اقدامات امنیتی اثراتی منفی بگذارد(برقعی، ۱۳۹۳: ۴۷). در کشور عراق نیز به دلیل وضعیت نابسامان سیاسی، همکاری‌های بین‌نهادهای مختلف برای تأمین امنیت سایبری به شدت محدود است (جیجان‌السماوئلی، ۱۴۰۰: ۹۸). چالش دیگری که در هر دو کشور وجود دارد، کمبود نیروی متخصص در زمینه امنیت سایبری است؛ کشورایران با وجود تلاش‌هایی برای تربیت نیروهای متخصص، هنوز با کمبود منابع انسانی ماهر مواجه است(کاویانی و میرسپاسی، ۱۴۰۰: ۱۳۱). کشور عراق نیز به دلیل شرایط اقتصادی و اجتماعی خود، نتوانسته است نیروی انسانی کافی را برای مقابله با تهدیدات سایبری تربیت نماید. این کمبود نیروهای متخصص می‌تواند به کاهش توانایی های هر دو کشور در مقابله با حملات سایبری منتج شود

که به عنوان یک شبکه خصوصی مجازی، امنیت، حریم خصوصی و آزادی شما را در سازمان هنگام فعالیت در اینترنت افزایش می‌دهد. تمامی ترافیک اطلاعات شما از طریق یک تونل مجازی رمزگذاری شده ارسال می‌شود. این رمزگذاری باعث می‌شود تا هکرها و افراد سودجو نتوانند به اطلاعات سازمانی شما دسترسی داشته باشند.

VPN یک ارتباط نقطه به نقطه را بین دستگاه شما و شبکه جهانی اینترنت برقرار می کند و به کاربر اجازه می‌دهد تا از رایانه شخصی خود، با استفاده از پروتکل‌های تونلینگ (Tunneling)، به رایانه دیگری دسترسی پیدا کند. به منظور محافظت از داده‌های سازمانی خود و جلوگیری از ردیابی اطلاعات در هنگام انتقال، ترافیک اغلب با پروتکل‌های رمزنگاری شبکه مانند SSH یا IPsec رمزگذاری می‌شود.

برای مطالعه بیشتر رجوع شود به:

https://respina.net/blog/what-is-vpn/

(الشوابکه، ۲۰۱۱:۸۷). در مجموع، یک بازنگری مداوم در قوانین و مقررات موجو دو اجیاد یک چارچوب جامع برای مدیریت تهدیدات سایبری در هر دو کشور احساس امری ضروری می باشد؛ این امر نه تنها به افزایش سطح امنیت سایبری کمک

خواهد، بلکه بستر را برای توسعه فناوری‌های نوین و ارتقاء کیفیت خدمات دیجیتال فراهم می‌آورد.

۵-۲-عدم وجود همکاریهای بین المللی در کشورهای ایران و عراق

عدم وجود همکاریهای بین‌المللی در زمینه تأمین امنیت سایبری در کشورهای ایران و عراق به‌عنوان دو کشور با چالش‌های مشابه، یکی از عوامل کلیدی می باشد که بر کیفیت و اثربخشی مقابله با تهدیدات سایبری اثر می‌گذارد. در کشور ایران، به‌دلیل تحریم‌های بین‌المللی و تنش‌های سیاسی، امکان همکاری با نهادهای بین‌المللی و کشورهای دیگر به شدت محدود گردیده است (بلوردی و طیاری‌پوراحمدی، ۱۴۰۱: ۶۹). این عدم دسترسی به اطلاعات و تجارب کشورهای پیشرفته در حوزه امنیت سایبری، سبب می‌شود که کشور ایران نتواند از بهترین شیوه‌ها و فناوری‌های نوین برای تقویت زیرساخت‌های خود بهره‌برداری نماید. این وضعیت نه‌تنها زمینه‌ساز ضعف در مقابله با تهدیدات سایبری می‌شود، بلکه آسیب‌پذیری‌های بیشتری را در بخش‌های مختلف کشور ایجاد می‌نماید(کتانچی و پورقهرمانی، ۱۴۰۱: ۱۴۱). در کشور عراق، عدم همکاری با نهادهای بین‌المللی نیز به چالش‌های امنیت سایبری این کشور دامن می‌زند. شرایط سیاسی ناپایدار و مشکلات اقتصادی به همراه نبود اعتماد بین‌المللی باعث می‌شود که کشور عراق نتواند به‌خوبی از تجربیات کشورهای دیگر بهره‌برداری نماید. همچنین، بدون تعاملات بین‌المللی، این کشور به‌طور موثر قادر به شناسایی و پاسخ به تهدیدات جهانی نمی باشد(زعال، ۲۰۲۳: ۶۵). به عنوان مثال، تهدید گروه‌های هکری بین‌المللی که برای اهداف سیاسی یا اقتصادی فعالیت می‌کنند، می‌تواند عواقب وخیمی برای زیرساخت‌های کشور عراق به دنبال داشته باشد، در حالی که ناتوانی در همکاری با دیگر کشورها و سازمان‌ها مانع از تقویت ظرفیت‌های دفاعی این کشور می‌شود.

همچنین عدم وجود همکاری‌های بین‌المللی در حوزه آموزش و تبادل اطلاعات نیز به صورت مستقیم بر توانمندسازی نیروی انسانی در هر دو کشور تأثیر می‌گذارد؛ در کشور ایران، برنامه‌های آموزشی مربوط به امنیت سایبری می‌تواند با مبادله تجربیات و فناوری‌ها با کشورهای پیشرو تقویت گردد، اما وجود تحریم‌ها و مشکلات سیاسی سبب می‌شود که این امکان کمتر مورد توجه قرار گیرد (اختری و همکاران، ۱۴۰۲: ۱۲۱). در کشور عراق نیز، کمبود منابع و زیرساخت‌های آموزشی، مانع از برگزاری دوره‌های تخصصی و کارگاه‌های آموزشی موثر می‌شود. عدم ایجاد شبکه‌های آموزشی بین‌المللی در این زمینه، به کمبود نیروی متخصص و کارآمد در هر دو کشور می‌انجامد(الزبیدی، ۲۰۱۷: ۵۷).

چالش دیگر، عدم وجود توافقنامه‌های حقوقی و فنی بین کشورها در زمینه امنیت سایبری می باشد؛ این کمبود باعث می شود که همکاری‌ها در زمینه تبادل اطلاعات و بهترین شیوه‌ها به شکل نامنظم و پراکنده انجام شود(محمودزاده و اسماعیلی، ۱۳۹۷: ۶۵). برای نمونه، در صورتی که کشورهای ایران یا عراق بخواهند با کشوری دیگر در زمینه مقابله با جرایم سایبری همکاری کنند، نبود چارچوب حقوقی واضح می‌تواند مانع از تبادل اطلاعات و هماهنگی‌های لازم شود. این وضعیت می‌تواند به افزایش تهدیدات سایبری و آسیب‌پذیری کاربران و زیرساخت‌ها در هر دو کشور منتج شود(الجصانی ، ۱۴۰۱: ۸۹). در نهایت، عدم وجود همکاری‌های مؤثر بین‌المللی در زمینه تأمین امنیت سایبری نه‌تنها به کاهش توانمندی‌های دفاعی کشورها منجر می‌شود، بلکه می‌تواند اثرات منفی بر توسعه اقتصادی و اجتماعی آنها نیز داشته باشد(فرشاسعید و همکاران، ۱۴۰۱: ۱۶۹). برای رفع این مشکلات، نیاز است که هر دو کشور به‌دنبال تقویت روابط بین‌المللی، به‌ویژه در زمینه تبادل اطلاعات، آموزش و ایجاد چارچوب‌های حقوقی مناسب برای همکاری در زمینه امنیت سایبری باشند(اصلانی، ۱۳۹۸: ۶۵). این اقدامات می‌توانند موجب افزایش سطح امنیت سایبری و کاهش تهدیدات در هر دو کشور شوند.

۵-۳- عدم وجود آموزشهای عمومی در کشورهای ایران و عراق

عدم وجود آموزش‌های عمومی در زمینه تأمین امنیت سایبری در کشورهای ایران و عراق، به‌عنوان یکی از چالش‌های اساسی در این دو کشور، تأثیرات منفی زیادی بر حفاظت از اطلاعات و داده‌های کاربران می‌گذارد. با افزایش روزافزون تهدیدهای سایبری، آگاهی عمومی نسبت به خطرات و نحوه مقابله با آن‌ها ضرورت بیشتری پیدا کرده است (طهماسبی وشاهمرادی، ۱۳۹۷: ۷۸). در کشور ایران، گرچه برخی برنامه‌های آموزشی

وجود دارد، اما این فعالیت‌ها به‌اندازه کافی گسترده و مؤثر نیستند و دسترسی به آن‌ها محدود است. به همین دلیل، بسیاری از کاربران هنوز از فنون پایه‌ای امنیت سایبری همانند استفاده از رمزهای عبور قوی، شناسایی ایمیل‌های فیشینگ و رفتارهای ایمن در اینترنت آگاهی ندارند (شایان، ۴۱ :۴۹۳۱). در کشور عراق، شرایط به مراتب حادتر می باشد، بسیاری از شهروندان که با استفاده از اینترنت و تکنولوژی‌های نوین در زندگی روزمره خود مشغول هستند، کمترین آگاهی را نسبت به تهدیدات سایبری و راه‌حل‌های حفاظتی دارند. این وضعیتی خطرناک است، زیرا عدم آگاهی می‌تواند باعث شود که کاربران به‌راحتی هدف حملات سایبری قرار بگیرند. فقدان برنامه‌های آموزشی جامع و مؤثر که بتواند به‌طور مستمر و در سطح وسیع اجرا شود، به این نقص دامن می‌زند و به‌خصوص در بین جوانان و کاربران تازه‌کار، خطراتی جبران‌ناپذیر را ایجاد می نماید)فکری، ۴۷ :۰۲۰۲(.

یکی از عاملهای اثرگذار در زمینه عدم اجرای آموزش‌های عمومی، عدم توجه به امنیت سایبری در آموزشهای رسمی می باشد؛ در کشور ایران، برنامه‌های آموزشی در مدارس و دانشگاه‌ها به‌ندرت به موضوع امنیت سایبری پرداخته می‌شود)عباسی و لطفی، ۹۲ :۱۹۳۱(. این کمبود در کشور عراق نیز مشهود می باشد، جایی که تنش‌های سیاسی و مشکلات اقتصادی سبب شدهاند که اولویت‌ها بر روی مسائل فوری‌تر متمرکز شود و به نیاز به آموزش در زمینه امنیت اطلاعات توجهی نشود. در نتیجه، نسل جدیدی از کاربران اینترنت به‌ویژه در مناطق دورافتاده، بدون دانش کافی نسبت به روش‌های حفاظتی در فضای مجازی وارد دنیای دیجیتال می‌شوند)عائشه، ۱۴۱ :۲۱۰۲(. مبحث دیگری که در این زمینه قابل توجه می باشد، کمبود همکاری های بین‌المللی برای بهبود وضعیت آموزش در حوزه امنیت سایبری می باشد؛ بسیاری از کشورهای پیشرفته، برنامه‌های آموزشی و منابع ارزشمندی را در سطح جهانی ارائه می‌دهند، اما به‌دلیل موانع سیاسی و اقتصادی، کشورهای ایران و عراق از این منابع محروم می باشند. عدم دسترسی به چنین مواد آموزشی و تجربیات می‌تواند سبب شود که هر دو کشور در مواجهه با تهدیدات جهانی به شدت آسیب‌پذیر شوند. این کمبود در واقع فرصتی برای ارتقاء سطح آگاهی عمومی را نیز از بین می‌برد)عبدالصادق، ۸۷ :۲۰۱۶(.

۶-بررسی خلأهای موجود در زمینه تضمین امنیت سایبری در نظام حقوقی ایران و عراق

خلأهای نظری تضمین امنیت سایبری شامل عدم قطعیت و پیش‌بینی‌ناپذیری تهدیدات سایبری، پیچیدگی در تعریف مفاهیم امنیت، و تعارض میان اهداف امنیتی و آزادی‌های فردی است. تهدیدات سایبری به سرعت تغییر می‌کنند و پیش‌بینی دقیق آن‌ها دشوار است (فرانکلین و همکاران، ۱۳۹۴: ۲۴). از سوی دیگر، تعریف امنیت تنها به محافظت از داده‌ها محدود نمی‌شود و شامل مسائل اخلاقی، اجتماعی و حفظ حریم خصوصی نیز می‌شود. علاوه بر این، توازن میان امنیت و حقوق کاربران، مانند آزادی بیان و حریم خصوصی، موضوعی دیگر می باشد که نظریه‌پردازان با آن مواجه‌اند(*Lee & Crespi, 2011: 63*). در نهایت، پیچیدگی سیستم‌های فناوری و ضرورت هماهنگی بین حوزه‌های مختلف (فنی، قانونی و انسانی) نیز بر پیچیدگی نظری امنیت سایبری می‌افزاید. در کشورهای ایران و عراق، قوانین امنیت سایبری با خلأهای مشابهی روبرو هستند که هم از نظر نظری و هم از نظر اجرایی می‌تواند مانع از تحقق یک سیستم امنیتی مؤثر شود(باقری و همکاران، ۱۴۰۳: ۱۴۶). یکی از اصلی‌ترین خلأهای اصلی در این کشورها، عدم تعادل بین امنیت و حقوق بشر است. در هر دو کشور، نگرانی‌هایی درباره نقض حریم خصوصی افراد به دلیل نظارت‌های دولتی گسترده وجود دارد. در ایران، قوانین امنیت سایبری به‌ویژه در زمینه نظارت بر اینترنت و محدود کردن دسترسی آزاد به اطلاعات، با انتقادات زیادی روبرو هستند(سلگی جالینوسی و همکاران، ۱۳۹۲: ۱۷). در کشور عراق نیز، با وجود قوانین نسبتاً جدید در زمینه امنیت سایبری، تضادهای داخلی و بین‌المللی بر اجرای آن‌ها تاثیرگذار است. از دیگر خلأهای حقوقی در این کشورها، فقدان چارچوب‌های جامع و هماهنگ بین‌المللی است که این امر باعث می‌شود قوانین ملی نتوانند به طور مؤثر در مقابله با تهدیدات سایبری جهانی عمل کنند(سبهان النویصری، ۱۴۰۳: ۷۹). همچنین، در هر دو کشور، کمبود منابع و تخصص در زمینه امنیت سایبری و مشکلات مربوط به هماهنگی بین نهادهای مختلف دولتی و خصوصی، کارایی این قوانین را کاهش می‌دهد. این مسائل نشان‌دهنده یک تناقض میان نیاز به حفاظت از امنیت سایبری و حفظ آزادی‌های فردی و حاکمیت ملی است.

۶-۱- کشور ایران

امنیت سایبری به یکی از مهم‌ترین چالش‌های کشورهای مختلف تبدیل شده است. در این راستا، هر کشور باید چارچوب‌های حقوقی و اجرایی خاص خود را برای مقابله با تهدیدات سایبری ایجاد کند(گوئو، ۱۳۹۲: ۵۴). بزرگ‌ترین خلأ حقوقی در کشور ایران، ضعف و نقص‌های موجود در چارچوب قانونی است. قانون جرائم رایانه‌ای مصوب ۱۳۸۸، در حالی که برخی از جنبه‌های جرائم سایبری را مورد پوشش قرار داده، اما در بسیاری از موارد از قبیل حفاظت از حریم خصوصی و داده‌های شخصی، خلأهای جدی دارد؛ این قانون نتوانسته است به‌روز رسانی‌های لازم را بر اساس تحولات نوین دنیای فناوری انجام دهد و به همین دلیل، امکان استفاده از این قانون به‌عنوان ابزاری مؤثر برای مبارزه با مقوله حملات و جنگهای سایبری وجود ندارد (کریمی قهرودی و همکاران، ۱۴۰۱: ۷۸). از دیگر خلأهای حقوقی، ناهماهنگی در اجرای قوانین و عدم وحدت رویه در رسیدگی به پرونده‌های سایبری است. به‌عنوان مثال، در مواردی که چند نهاد مسئول هستند، مانند پلیس فتا و قوه قضائیه، معمولاً اختلاف نظرهایی وجود دارد که بر سرنوشت پرونده‌ها تأثیر منفی گذاشته و منجر به تأخیر در دادرسی می شود. این مسئله به عدم اعتماد مردم به نهادهای قضائی و امنیتی منجر گردیده و شکایات متعددی از جانب آسیب‌دیدگان ناشی از جرائم سایبری مطرح شده است(قاسمی، ۱۳۹۱: ۱۱۹). عدم وجود محاکم تخصصی برای رسیدگی به جرائم سایبری در کشور ایران، یکی دیگر از خلأهای حقوقی است. در حال حاضر، قضات عموماً در زمینهٔ امور سایبری آموزش‌های کافی دیده‌اند و این باعث می‌شود که احکام صادره ممکن است از لحاظ علمی و قانونی ضعیف باشند. فقدان تخصص در قضات باعث می‌شود که بسیاری از پرونده‌های پیچیده قابلیت بررسی صحیح نداشته باشند و به نتیجه مطلوب نرسند(سلگی و همکاران، ۱۴۰۰: ۳۳۱). وجود ضعفهای متعدد در حفاظت از داده‌های شخصی و نقص قوانین مرتبط با حفاظت از داده‌های شخصی، چالشی جدی در ایران به حساب می‌آید. در حال حاضر، هیچ قانون جامع و مشخصی در زمینه حفاظت از اطلاعات شخصی وجود ندارد و این موضوع، منجر به نقض مکرر حریم خصوصی افراد و افشای اطلاعات حساس می‌شود(خلیلی پوررکن‌آبادی و نورعلی وند، ۱۳۹۱: ۱۷۶). عدم شفافیت در نحوه جمع‌آوری، ذخیره و پردازش داده‌ها و همچنین عدم وجود مجازات‌های مناسب برای نقض این قوانین، به تشدید این مشکل کمک کرده است.

قوانین موجود در ایران در زمینه امنیت سایبری نشانگر توجه جدی قانون‌گذاران به تهدیدات موجود و ضرورت مقابله با آن‌هاست. با این حال، برخی نقاط ضعف نیز در این قوانین وجود دارد:

-کمبود بروزرسانی: با توجه به سرعت تغییرات تکنولوژی اطلاعات، برخی قوانین مانند «قانون جرایم رایانه‌ای» و «قانون تجارت الکترونیک» نیاز به بازنگری و به‌روزرسانی دارند تا با منافع و خلأهای نوظهور فضای مجازی همگام شوند(مرادی و همکاران، ۱۴۰۱: ۵۴).

- عدم نگرش یکپارچه: برخی قوانین به صورت پراکنده و بدون نگرش یکپارچه تدوین شده‌اند و این موضوع می‌تواند باعث سردرگمی در اجرا و نظارت شود(فضلی‌نژاد، ۱۴۰۲: ۰۶)؛

-مکانیسم‌های اجرایی و نظارتی: با وجود وجود قوانین، اجرای مؤثر و نظارت بر آن‌ها به طور کافی انجام نمی‌شود. ایجاد نهادهای قوی‌تر برای نظارت و اجرای این قوانین ضروری است؛

-آگاهی عمومی: لازم است برنامه‌های آموزشی و آگاهی‌بخشی به مناطق مختلف جامعه به منظور آشنایی با حقوق و مسئولیت‌های کاربران ایجاد شود(غفاری مهرجردی، ۱۴۰۲: ۳۶).

با تقویت این نقاط ضعف و به‌روزرسانی قوانین، کشور ایران می تواند به تأمین امنیت سایبری و حفاظت از حریم خصوصی شهروندانش بهتر عمل کند.

۶-۲-کشور عراق

در کشور عراق، یکی از بزرگ‌ترین خلأهای حقوقی، عدم وجود قوانین جامع و مدرن در زمینه امنیت سایبری است. قانون مبارزه با جرائم سایبری ۲۰۱۵ در عراق، به‌طور کلی مشکلات و چالش‌های مهم‌تری را برای کاربران و سیستم‌های اطلاعاتی ایجاد کرده و بسیاری از جوانب لازم را پوشش نداده است. این قانون نتوانسته است به‌طور کامل تهدیدات سایبری موجود را شناسایی و رفع کند و غالباً به‌دلیل استفاده از زبان مبهم و نامشخص، دچار ابهاماتی در تفسیر و اجرا می‌شود(الشوابکه، ۲۰۱۱: ۳۳). خلأ دیگری که کشور عراق با آن مواجه است، وجود نقصهای متعدد وضعف در نهادهای نظارتی است. این کشور به نهادهای مستقل و مجهز نیاز دارد که بتوانند به‌طور مؤثر بر اجرای قوانین سایبری نظارت کنند و در صورت تخلف، واکنش‌های مناسبی انجام دهند. با وجود برخی نهادها، همچنان کمبود امکانات و آموزش‌های لازم برای کارکنان این نهادها

احساس می‌شود و غالباً نهادها توانایی شناسایی و مقابله با تهدیدات سایبری را ندارند(الفرمان، ۵۶ :۷۱۰۲). در حالی که عراق قوانین و مقرراتی را برای تقویت امنیت سایبری ایجاد کرده است، این کشور با خلأهای زیادی در زمینه اجرای این قوانین روبرو است. مواردی همچون: کمبود منابع مالی و انسانی: عراق هنوز از کمبود نیروی متخصص در زمینه امنیت سایبری رنج می‌برد؛ زیرساخت‌های ضعیف: بسیاری از زیرساخت‌های فناوری اطلاعات در عراق هنوز با مشکلاتی مانند کندی سرعت اینترنت و ضعف در سیستم‌های نظارتی مواجه هستند؛ تهدیدات خارجی: به دلیل موقعیت جغرافیایی و سیاسی عراق، تهدیدات سایبری از کشورهای دیگر و گروه‌های تروریستی یکی از مهم‌ترین خلأها به شمار می‌آید)المشد،۱۲۱ :۷۱۰۲(. قوانین و سیاست‌های عراق در زمینه امنیت سایبری در حال تکامل و پیشرفت هستند. با وجود خلأهای اجرایی، این کشور تلاش دارد تا از طریق همکاری‌های بین‌المللی و تقویت زیرساخت‌ها، امنیت سایبری خود را ارتقا دهد. این اقدامات می‌توانند به تدریج موجب افزایش اعتماد عمومی به فضای آنلاین و کاهش تهدیدات سایبری در این کشور شوند.

نتیجه گیری

تضمین امنیت سایبری یکی از اولویت‌های اصلی دولت‌ها در عصر دیجیتال به شمار می‌آید. با این حال، چالش‌های نظری و عملی متعددی در این زمینه وجود دارد که دستیابی به یک نظام بین‌المللی و داخلی کارآمد را دشوار می‌سازد. این چالش‌ها نه تنها به تضعیف هنجارهای امنیتی می‌انجامد بلکه می‌تواند بر حقوق بشر و آزادی‌های فردی نیز تأثیرات منفی بگذارد. چالش‌های تضمین امنیت سایبری در نظام حقوقی کشورهای ایران و عراق ناشی از مجموعه‌ای از عوامل ساختاری و قانونی بوده که بر کارایی و اثربخشی سیستم‌های نظارتی و حقوقی این دو کشور تأثیر می‌گذارد. یکی از مهم‌ترین مشکلات، عدم وجود یک نهاد نظارتی متمرکز است که به‌عنوان مرجع اصلی در حوزه امنیت سایبری فعالیت کند. در کشور ایران، نهادهای مختلفی مانند پلیس فتا و وزارت اطلاعات وظایف مربوط به امنیت سایبری را بر عهده دارند، اما عدم هماهنگی بین آن‌ها و پراکندگی مسئولیت‌ها موجب ایجاد سردرگمی، تعارض و در نهایت ناکارآمدی می‌شود. این وضعیت، امنیت داده‌ها و حریم خصوصی شهروندان را به چالش می‌کشد و در صورت بروز تخلفات، به درخواست‌ها و پیگیری‌های قانونی به‌طور مؤثری پاسخ داده نمی‌شود. در عراق نیز شرایط مشابه‌ای حاکم است، زیرا مسئولیت‌های مقابله با جرائم سایبری در بین نهادهای مختلف نظیر وزارت کشور و قوه قضائیه تقسیم شده و این موضوع به غیاب یک رویکرد یکپارچه و هماهنگ منجر شده است. در زمینه چالشهای نظری می توان عنوان نمود که در بسیاری از کشورها، به‌ویژه در ایران و عراق، فعالیت‌های دولتی برای حفظ امنیت سایبری غالباً با نقض حقوق بشر همراه است. قوانین سخت‌گیرانه و نظارت‌های گسترده بر اطلاعات، به‌ویژه در دوران‌های بحرانی، می‌تواند به سرکوب آزادی‌های فردی و حریم خصوصی منجر شود. این تضاد میان امنیت و حقوق فردی یکی از اصلی‌ترین چالش‌های نظری در زمینه امنیت سایبری است. قوانین موجود در حوزه امنیت سایبری به‌دلیل نبود نهاد نظارتی یا سیستم قانونی جامع و کارآمد، قادر به پاسخگویی به چالش‌های نوظهور تکنولوژیکی و تهدیدات جدید نیستند و این امر به ناامنی و سوءاستفاده‌های سایبری دامن می‌زند. از جهتی دیگر، عدم آگاهی عمومی نسبت به تهدیدات و چگونگی حفاظت از داده‌ها نیز به مشکلات موجود دامن می‌زند. شهروندان ممکن است اطلاعات کافی درباره حقوق خود و سازوکارهای قانونی موجود نداشته باشند که این امر می‌تواند به نقض حقوق آن‌ها منجر شود. در بسیاری از کشورها، به‌ویژه در ایران و عراق، فعالیت‌های دولتی برای حفظ امنیت سایبری غالباً با نقض حقوق بشر همراه است. قوانین سخت‌گیرانه و نظارت‌های گسترده بر اطلاعات، به‌ویژه در دوران‌های بحرانی، می‌تواند به سرکوب آزادی‌های فردی و حریم خصوصی منجر شود. این تضاد میان امنیت و حقوق فردی یکی از اصلی‌ترین چالش‌های نظری در زمینه امنیت سایبری است. کشورهای مختلف به دلیل فرهنگ‌های حقوقی متفاوت و تعاریف متناقض از جرایم سایبری، نمی‌توانند به یک توافق جهانی دست یابند. این عدم توافق نه تنها به دشواری در اجرای قوانین می‌انجامد بلکه مانع از همکاری‌های بین‌المللی ضروری برای مقابله با تهدیدات سایبری است. در زمینه چالشهای عملی نیز می توان عنوان نمود کشورهای ایران و عراق با زیرساخت‌های فناوری ضعیف مواجه‌اند که مانع از پیاده‌سازی مؤثر قوانین امنیت سایبری می شود. عدم دسترسی به فناوری‌های پیشرفته و متخصصان توانمند در این زمینه می‌تواند تأثیر منفی بر عملکرد آن‌ها داشته

باشد. همچنین کشورهای جمله ایران و عراق با زیرساخت‌های فناوری ضعیف مواجه‌اند که مانع از پیاده‌سازی مؤثر قوانین امنیت سایبری می‌شود. عدم دسترسی به فناوری‌های پیشرفته و متخصصان توانمند در این زمینه می‌تواند تأثیر منفی بر عملکرد آن‌ها داشته باشد. همچنین فقدان همکاری‌های مؤثر میان کشورها و سازمان‌های بین‌المللی در زمینه امنیت سایبری، یکی دیگر از چالش‌هاست. کشورها معمولاً اطلاعات و منابع خود را به اشتراک نمی‌گذارند و این امر می‌تواند به افزایش تهدیدات سایبری و آسیب‌پذیری‌ها منجر شود. بر همین اساس، رفع چالش‌های موجود در زمینه امنیت سایبری در هر دو کشور به‌وضوح نیازمند یک برنامه‌ریزی جامع و استراتژیک است. اصلاحات ساختاری و حقوقی در راستای ایجاد نهادهای نظارتی مؤثر، به‌روزرسانی قوانین و افزایش آگاهی عمومی می‌تواند به شکل قابل توجهی به بهبود وضعیت امنیت سایبری در کشورهای ایران و عراق کمک کند. هر دو کشور نیازمند توسعه و تقویت سیستم‌های قانونی و اجرایی خود برای تضمین امنیت سایبری هستند. پیشنهاد می‌شود که ایران و عراق برای ایجاد هماهنگی و همکاری در زمینه امنیت سایبری با دیگر کشورها و سازمان‌های بین‌المللی مشارکت کنند. همچنین، افزایش آگاهی عمومی و آموزش متخصصان در حوزه امنیت سایبری و تدوین استراتژی‌های جامع حمایتی از اولویت‌های اصلی به شمار می‌روند. این اقدامات می‌توانند به نحو مؤثری در بهبود وضعیت امنیت سایبری در این دو کشور مؤثر باشند. در نهایت، این تلاش‌ها نه تنها به حفاظت از حقوق شهروندان کمک می‌کند، بلکه باعث افزایش اعتماد عمومی به نهادهای حقوقی و امنیتی خواهد شد و زمینه لازم برای توسعه فضای دیجیتال ایمن‌تر را فراهم می‌آورد. در پایان با توجه به چالش‌های متعددی که ایران و عراق در زمینه امنیت سایبری با آن‌ها مواجه هستند، ارائه راهکارهای علمی و عملی در این زمینه می‌تواند به تقویت وضعیت امنیتی هر دو کشور کمک کند، از جمله ایجاد و تقویت زیرساخت‌های فناوری اطلاعات و ارتباطات با استفاده از تجهیزات و نرم‌افزارهای امنیتی پیشرفته مانند سیستم‌های تشخیص نفوذ می‌تواند به بهبود وضعیت امنیت سایبری کمک کند؛ همچنین تشویق ایجاد دانشکده ها و موسسات تخصصی در زمینه حوزه امنیت سایبری برای رفع نیازهای و افزایش دادن آگاهی‌های عمومی از خطرات و تهدیدات امنیت سایبری و ارتقا و حمایت از توانمندیهای داخلی)فنی، سازمانی و انسانی(از طریق تهیه برنامه‌های درسی، برنامه‌ها و ابتکارات آموزشی و دانشگاهی، سازماندهی رویدادهای مرتبط با امنیت سایبری و تشویق و هدایت نمودن نوآوری‌ها و تحقیقات علمی در زمینه مقوله امنیت سایبری محلی نیز از دیگر راهکارهای بسیار موثر در زمینه تضمین امنیت سایبری در حقوق دو کشور می باشد.

منابع فارسی

۱. اختری، محمد؛ کرامتی، محمدعلی؛ و امین موسوی، سید عبدالله. (۱۴۰۲). ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساخت های حیاتی کشور. *آینده پژوهی دفاعی*، ۰۸(۲۹): ۱۰۱- ۱۳۴.

۲. اصلانی، حمیدرضا. (۱۳۹۸). *حقوق فناوری ارتباطات*. تهران: انتشارات میزان.

۳. افشار، احمد؛ ترمه چی، عاطفه؛ گلشن، عارفه؛ آقائیان، آزاده؛ و شهریاری، حمیدرضا. (۱۳۹۳). مروری بر امنیت سایبری سیستم های کنترل صنعتی. *مجله کنترل*،(۰۸)۰۱: ۳۱-۴۵.

۴. انوشا، سهیل؛ نیکجو، مهنوش؛ روح اله کولیوند. (۱۴۰۰). استراتژی امنیت سایبری. *سومین همایش ملی تحقیقات میان رشته ای علوم مهندسی و مدیریت*، تهران، ۰۱-۳۶.

۵. انصاری مهیاری، علیرضا؛ محمودی، هادی. (۱۴۰۱). بررسی راه کارهای تقلیل حملات سایبری از منظر حقوق بین الملل بشردوستانه. *فصلنامه مطالعات حقوقی فضای مجازی*،(۰۱) ۰۳: ۱۸-۳۶.

۶. انصاری مهیاری، علیرضا؛ حسینی، زهرا سادات؛ و رادمان، احمد. (۱۴۰۳). بررسی جایگاه فضای دیپ وب و دارک وب در حقوق بین الملل. *فصلنامه مطالعات حقوقی فضای مجازی*،(۰۲)۰۳: ۴۱-۵۳.

۷. العتابی،(۱۴۰۱). جرم شریک در جرایم سایبری در حقوق عراق و مصر. پایان نامه کارشناسی ارشد، رشته حقوق کیفری، استاد راهنما: عادل ساریخانی، دانشگاه قم.

۸. باقری، مسعود؛ موحدی صفت، محمدرضا؛ دوستی مطلق، نصب الله؛ عباس، علی. (۱۴۰۳). ارائه الگوی ساختار حاکمیتی امنیت سایبری عراق. *فصلنامه علمی مطالعات مدیریت راهبردی دفاع ملی*،(۰۸) ۳۰: ۱۴۱-۱۸۷.

۹. برقعی، سید مهدی. (۱۳۹۳). مروری بر امنیت سایبری؛ درس هایی برای جمهوری اسلامی ایران. *مطالعات انقلاب اسلامی*، ۱۱(۳۸): ۳۰-۵۴.

۱۰. برزگر کلاته، علیرضا. (۱۳۹۶). جرایم علیه حریم خصوصی شهروندان در فضای سایبری. پایان نامه کارشناسی ارشد، رشته حقوق جزا، استاد راهنما: علی مزیدی شرف اباد، دانشگاه آزاد اسلامی واحد یزد.

۱۱. بلوردی، طیبه؛ طیاری‌پوراحمدی، مطهره. (۱۴۰۱). اقدامات دولت در ایجاد امنیت سایبری. *دستاوردهای نوین در حقوق عمومی* ۰۱(۰۴): ۷۶ - ۶۴.

۱۲. پروانه، امیرحسین. (۱۴۰۱). شناسایی چالش‌های رسیدگی به تروریسم سایبری در حوزه قضایی. پایان نامه کارشناسی ارشد، رشته حقوق جزا، استاد راهنما: حسام قبانچی، دانشگاه فردوسی مشهد.

۱۳. رضایی، فرامرز. (۱۴۰۲). جایگاه و مسئولیت سازمان پدافند غیرعامل در تأمین امنیت ملی جمهوری اسلامی ایران. پایان نامه کارشناسی ارشد، رشته حقوق عمومی، استاد راهنما: صمد قائم پناه، دانشگاه آزاد اسلامی واحد ملارد.

۱۴. سلگی جالینوسی، احمد؛ ابراهیمی، شهروز؛ و قنواتی، طیبه. (۱۳۹۲). جایگاه فضای سایبر و تهدیدهای سایبری در استراتژی امنیت ملی ایالات متحده آمریکا. *فصلنامه دانش سیاسی و بین الملل*، (۰۲)۰۱: ۱۴-۳۶.

۱۵. حسینی، زهرا سادات؛ انصاری مهیاری، علیرضا. (۱۴۰۲). کنترل فضای مجازی در راستای حفظ حق بر سلامت اشخاص. فصلنامه تحقیقات حقوق خصوصی و کیفری، ۵۶: ۷۱-۸۷.

۱۶. حسینی‌امینی، حسن؛ محسن‌زادگان، امیر. (۱۳۹۳). فضای سایبر، قدرت هوشمند با رویکرد پدافند غیر عامل. *مجموعه مقالات همایش ملی پدافند غیر عامل و علوم انسانی*، ۵۳۱- ۵۵۸.

۱۷. خلیلی پوررکن‌آبادی، علی؛ نورعلی وند، یاسر. (۱۳۹۱). تهدیدات سایبری و تأثیر آن بر امنیت ملی. *فصلنامه مطالعات راهبردی*، ۱۵: ۱۶۹-۱۷۸.

۱۸. زابلی زاده، اردشیر؛ وهاب پور، پیمان. (۱۳۹۷). قدرت بازدارندگی در فضای سایبر. *فصلنامه رسانه و فرهنگ*، ۱: ۱۴-۳۶.

۱۹. سلگی، رضا؛ خداوردی، حسن؛ و پوستینچی، زهره. (۱۴۰۰). چالشهای نوین امنیتی دولت ملت در فضای سایبر با تاکید بر جمهوری اسلامی ایران. *فصلنامه علمی (مقاله علمی پژوهشی)جامعه شناسی سیاسی ایران*، ۰۴: ۳۲۶-۳۵۰.

۲۰. شیرنسبیان، شهره بانو. (۱۴۰۱). سیاست جنایی ایران در عرصه مبارزه با جرایم ضد امنیت ملی در فضای سایبری باتاکید برررویکرد پیشگیرانه دراین جرایم. استاد راهنما غلامرضا عبدلی، پایان نامه کارشناسی ارشد، رشته حقوق کیفری، دانشگاه آزاد اسلامی واحد شاهرود.

۲۱. شایان، علی. (۱۳۹۴). *مجموعه مقاله های همایش بررسی جنبه های حقوقی ارتباطات*. تهران: انتشارات سلسبیل.

۲۲. صادقی، تاج محمد؛ رئیسی، لیلا؛ انصاری مهیاری، علیرضا. (۱۴۰۳). راهبرد سازمانهای بین المللی و منطقهای در مواجهه با حملات سایبری. *فصلنامه علمی حقوقی فضای مجازی*، (۰۳)۱۱: ۵۰-۶۵.

۲۳. صانعی، علی. (۱۳۹۸). امنیت سایبری در آمریکا، ساختارها و روندها. *سیاست خارجی*، ۳۳(۱۲۹): ۱۹۱ - ۲۲۸.

۲۴. طهماسبی، جواد؛ شاهمرادی، خیرالله. (۱۳۹۷). چالش ها و خلأهای موجود در فرایند رسیدگی به جرایم سایبری. *مجله حقوقی دادگستری*، ۱۰۴: ۶۳-۸۹.

۲۵. عباسی، محمدعابد؛ لطفی، مرتضی. (۱۳۹۱). فضای سایبری و امنیت ملی جمهوری اسلامی ایران. *دانش انتظامی سمنان*، ۰۲(۰۵): ۲۳-۴۸.

۲۶. غفاری مهرجردی، غفار. (۱۴۰۲). تضمین امنیت سایبری از مجرای هنجارهای سخت و نرم حقوق بین الملل. استاد راهنما: پوریا عسکری. پایان نامه کارشناسی ارشد، رشته حقوق کیفری، دانشگاه تربیت مدرس تهران.

۲۷. فرشاسعید، پرویز؛ جلالی، محمود؛ و گودرزی، مهناز. (۱۴۰۱). ضرورت همکاری دولت ها در تقویت امنیت سایبری. *مطالعات بین المللی*، ۱۹(۷۴): ۱۶۳ - ۱۷۸.

۲۸. فرانکلین، کرامر؛ استار، استیوارت؛ و ونتز، لری. (۱۳۹۴). *قدرت سایبری و امنیت ملی*. ترجمه: معاونت پژوهش و تولید علم، تهران: مؤسسه چاپ و انتشارات دانشکده اطلاعات.

۲۹. فضلی‌نژاد، مینو. (۱۴۰۲). بررسی چالشهای حقوقی و امنیت اجتماعی در فضای سایبر. *چهارمین کنفرانس ملی پدافند سایبری*، ۰۱-۲۵.

۳۰. قاسمی، علی. (۱۳۹۱). حملات سایبری و حقوق بین الملل. *مجله حقوقی دادگستری*، ۷۸: ۱۱۰-۱۲۵.

۳۱. کاویانی، حسن؛ میرسپاسی، حسن. (۱۴۰۰). طراحی مدل قابلیت های سازمانی در حوزه امنیت سایبری. *مطالعات راهبردی بسیج*، ۲۵(۹۲): ۱۲۱ - ۱۵۱.

۳۲. کتانچی، الناز؛ پورقهرمانی، بابک. (۱۴۰۱). چالش های امنیت سایبری در کشورهای «آسه آن». *مطالعات بین المللی*، ۱۸(۶۹): ۱۳۹ - ۱۵۶.

۳۳. کریمی قهرودی، محمدرضا؛ محمدی، حافظ؛ و سعادتمند، امیر مسعود. (۱۴۰۱). ارائه مدلی برای ارزیابی امنیت سایبری جمهوری اسلامی ایران. *فصلنامه علمی امنیت ملی*، ۱۲(۴۵)، ۶۹-۱۰۰.

۳۴. گوئو، چن بائو(۱۳۹۲). *رسانه سلطه، سلطه رسانه*. ترجمه فری ده پیشوایی، تهران: کتاب نشر.

۳۵. متقی، افشین؛ زادگان، امیرحسین؛ امینی، حسن. (۱۳۹۲). *فضای سایبر، ژئوپلیتیک و قدرت هوشمند از منظر پدافند غیرعامل*. تهران: سازمان انتشارات جهاد دانشگاهی.

۳۶. مجتبی زاده، نیما. (۱۴۰۰). بررسی چالش های امنیتی در فضای سایبری. *فصلنامه تخصصی آرمان پردازش*، ۰۲: ۰۱-۱۰.

۳۷. محمودزاده، ابراهیم؛ اسماعیلی، کیوان. (۱۳۹۷). الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح. *فصلنامهٔ امنیت ملی*، ۰۸(۳۰): ۶۱-۸۰.

۳۸. مرادی، صادق؛ شکرچی زاده، محسن؛ نقش، امیررضا؛ و مسعود، غلامحسین. (۱۴۰۱). تهدیدات و جرایم سایبری علیه امنیت و چالش های پیش رو. *فقه جزای تطبیقی*، ۰۱: ۴۷-۷۰.

۳۹. مرندی، فرنوش. (۱۳۹۹). نقش سازمان های غیردولتی در تأمین امنیت سایبری در حقوق بین الملل. استاد راهنما: آرامش شهبازی، استاد مشاور: همایون حبیبی، رشته رشته حقوق بین الملل عمومی، پایان نامه کارشناسی ارشد، تهران: دانشگاه علامه طباطبایی.

۴۰. ملکوتی، رسول؛ خلیل زاده، مونا. (۱۴۰۰). راهکار حقوقی تأمین امنیت سایبری. *مجله رسانه*، (۰۱) ۱۲۶: ۶۹-۹۷.

۴۱. ملک، هادی. (۱۴۰۲). تامین امنیت سایبری در ایران: چالشها و راهکارها. چهارمین کنفرانس ملی پدافند سایبری. ایران: تهران، ۰۱-۲۰.

۴۲. نعمتی، نبی اله؛ صادقی نشاط، امیر. (۱۳۹۶). بررسی مسئولیت مدنی ناشی از نقض داده در تهدیدات سایبری، فصلنامه پژوهش های حفاظتی-امنیتی دانشگاه امام حسین، ۲۳: ۱۴۷-۱۶۹.

منابع عربی:

۴۳. الجصانی، امین عباس عبدالرضا. (۱۴۰۱). استراتژی عراق و امارات برای امنیت الکترونیکی (مطالعه تطبیقی). استاد راهنما: محمد هادی معینی، پایان نامه کارشناسی ارشد، رشته حقوق، قم: دانشگاه ادیان و مذاهب.

۴۴. الزبیدی، فوزی حسن. (۲۰۱۷). *مبادیء تقییم البیئة الاستراتیجیة للدولة مرجع علمی لتخطیط سیاسات الامن القومی*. بیروت: الدار العربیة للعلوم ناشرون.

۴۵. الشوابکه، محمد امین. (۲۰۱۱). *جرائم الحاسوب والانترنت*، ط۴، عمان، الأردن: دار الثقافة للنشر.

۴۶. الشمری، مصطفی إبراهیم سلمان. (۲۰۲۱). الامن السیبرانی واثره فی الامن الوطنی العراقی. *مجلة العلوم القانونیة والسیاسیة*، جامعة دیالی، ۱۰(۰۱): ۲۱۴-۲۳۶.

۴۷. الفرمان، محمود احمد. (۲۰۱۷). *الجرائم الالکترونیة*. عمان، الأردن: دار وائل للطباعة.

۴۸. المشد، احمد. (۲۰۱۷). *القرصنة الالکترونیة وامن المعلومات*. القاهرة: مؤسسة الامة العربیة للنشر.

۴۹. جیجان‌السماوئلی، احسان علی. (۱۴۰۰). شورای عالی فضای مجازی در ایران و امکان محقق شدن آن در عراق. استاد راهنما سید علی رضا طباطبائی، پایان نامه کارشناسی ارشد، رشته حقوق، قم: دانشگاه ادیان و مذاهب

۵۰. حبیب‌خبط، ابراهیم. (۱۴۰۳). مبنای حقوقی جرایم امنیت اطلاعات بین حقوق ایران و عراق (مطالعه تطبیقی). استاد راهنما: محسن قدیر استاد مشاور: عادل ساریخانی، رساله دکتری تخصصی، رشته جزا و جرم شناسی، قم: جامعه المصطفی العالمیه.

۵۱. زعال، سعید. (۲۰۲۳). جرائم الإرهاب السیبرانی. *مجلة الاندلس للعلوم الإنسانیة*، ۷۳(۱۵): ۴۷-۷۴.

۵۲. سبهان النویصری، حیدر جبر. (۱۴۰۳). نقش هوش مصنوعی در مبارزه با جرایم سایبری در حقوق عراق و ایران. پایان نامه کارشناسی ارشد، رشته حقوق جزا، استاد راهنما: حجت اله فتحی. قم: دانشگاه ادیان و مذاهب.

۵۳. عائشه، بن عمور. (۲۰۱۲). نطاق الجریمة الالکترونیة. *جامعة تسلیت*، الجزائر، مجلة المعیار، ۱۲(۱۲): ۱۳۱-۱۵۶.

۵۴. عبدالصادق، عادل. (۲۰۱۶). *الفضاء الالیکترونی والعلاقات الدولیة: دراسة فی النظریة والتطبیق*. القاهرة: المکتبة الاکادیمیة.

۵۵. علاء تکلیف، حیدر. (۱۴۰۲). نقش امنیت سایبری در چشم انداز استراتژیک امنیت ملی عراق. استاد راهنما محمد جواد نوروزی، پایان نامه کارشناسی ارشد، رشته حقوق، قم: جامعه المصطفی العالمیه.

۵۶. عیفان الشمری، نجاح ناصر. (۱۴۰۲). جرایم سایبری تأثیرگذار بر جامعه بین‌المللی مقایسه‌ای بین قوانین عراق و ایران. استاد راهنما محمدعلی کفائی فر. پایان نامه کارشناسی ارشد، رشته حقوق جزا، قم: دانشگاه ادیان و مذاهب.

۵۷. فکری، ایمن عبد الله. (۲۰۲۰). الجرائم المعلوماتیة، دراسة مقارنة، فی التشریعات العربیة والأجنبیة، کلیة الحقوق، جامعة الفیوم.

منابع انگلیسی:

58. Andress. J. Winterfled. S. (2014). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioner*. USA, Elsevier.
59. Cornish. P. Hughes. R. Livingstone. D. (2009). *Cyberspace and the national security of the United Kingdom Chatham House Report.* http://www.chathamhouse.org.uk/files/13679_r0309cyberspace.pdf.
60. JaBae.Y. (2003) Information Technology and The Empowerment of New Actors in International Relations. *Journal of International and Area Studies*,Volume.10,Number 2
61. Lee. G. Crespi. N. (2011). *the Internet of Things: Challenge for a New Architecture from Problem*. Prague. Telecom Institute.