Examining the dimensions of cyber warfare

Behrouz nasiri*ghasem toraby**Alirezarezaei***

Abstract

Cyber threats have unique characteristics. On the one hand, these threats include a wide range of legal, technical, organizational, and cultural barriers, and on the other hand, low cost, tremendous impact, and lack of public transparency in cyberspace have led many actors to enter this field. This research examines the effects of cyberspace on the national security of the Islamic Republic of Iran in various fields, especially the political-security fields. Also, discovering the weaknesses and shortcomings in the field of cyber security with regard to the threats in the virtual space is one of the other goals of this research, which is analytical-descriptive. This basic question wants to answer how cyber threats affect the security of the Islamic Republic of Iran. The findings of the research show that the Islamic Republic of Iran is one of the most important countries targeted by cyber attacks in various fields, and from this point of view, the acceleration of infrastructure equipment and investment in the field of dealing with cyber threats, including Iran's strategic approaches are considered in this field, and in this research, more dimensions are analyzed.

Keywords: cyber space, security threats, cyber war, national security, artificial intelligence, Iran

1-Dr.Behrouz nasiri ph.D. in international relation,Hamadan Branch,IslamicAzad University,Hamadan,Iran.1364behnasiri@gmail.com

2-Dr.ghasem toraby Professor of International Relations,HamadanBranch,IslamicAzad University,Hamadan,Iran (corresponding Author)ghasemtoraby@yahoo.com

3-Dr.Alirezarezaei Associate Professor Of International Relations,Hamadan Branch,Islamic Azad University,Hamadan,Iran.alirezarezaei@gmail.com

Introduction

According to this group, today security threats are no longer solely military, but environmental issues, global poverty, migration and, more recently, cyber threats have endangered the security of states more than military threats. The discussion about cyber threats is influenced by the ongoing information revolution that results from the dynamics of the dissemination of information and communication technologies in all aspects of human life. As the dimensions of Internet services increase in various areas of human life,

especially in business and commerce,computer attackers, thieves and information spies have greatly increased the volume of threats and damage caused by this technology.Today, in addition to expanding and becoming more complex day by day, these threats directly affect the national security of governments.Traditional concepts of war based on attack and defense have been challenged and rapidly changed by the complexities of cyberspace, and this threat has changed the traditional concepts of war in a way. The cyber threat is asymmetric and therefore,there is no need for a large investment to use it or attack through it.On the contrary,defense against cyber threats must consider all aspects, the costs of which are increasing today.The foundation of any country is based on a set of vital infrastructures in the sectors of communications,defense,energy, transportation,agriculture,health and economic affairs, which are interconnected by cyberspace as a nervous system. Today, there are many terrorist acts in cyberspace targeting governments, and the characteristics of these attacks include the unknown nature and speed of the attacks, and most of these attacks are identified after they occur.Also,todiscover the weaknesses and shortcomings in the field of cyber security with regard to the threats in the cyberspace is one of the other goals of this research. It wants toanswer the basic question of how cyber threats affect the security of the Islamic Republic of Iran in a descriptive-analytical method. Thefindings of the research show that the Islamic Republic of Iran is one of themost important countries targeted by cyber attacks in various fields. From thispoint ofview, acceleration ininfrastructure equipment and investment in the field of dealing with cyber threats is considered as oneofIran's strategic approaches in this field, which is analyzed in this research.

Materials and Methods

The method of work in this research is library, descriptive-analytical. First, we study historical written works, documents, and research conducted on the effects of cyberspace and virtual networks on values at different levels, then we analyze the data from the questionnaires and streams, and finally we compile and write the research. The method of work in this research is library, descriptive-analytical. First, we study historical written works, documents, and research conducted on the effects of cyberspace and virtual networks on values at different levels, then we analyze the data from the questionnaires and streams, and finally we compile and write the research

Discussion and Results

Technology has always played a decisive role in shaping human life, but with the passage of time and the advancement of technology,the influence of

this phenomenon on human life has intensified. Many consider the Industrial Revolution in the eighteenth century to be a turning point in this direction. The consequence of the Industrial Revolution was the emergence of more complex technologies that increasingly overshadowed the developments of human societies. These technologies increased the exchanges and the relative complexity of human relationships. The characteristic of all technological revolutions is that they affect the entire sphere of human activity, in the sense that they act as the context in which human activity takes place.Since the 1970s, technological progress has accelerated at a rapid pace, to the point where it can now be said that the machine, as the infrastructure for producing weapons to ensure security,has given way to information and communication technologies,and as a result,has become central to military strategies. This situation has dangerously increased the vulnerabilities of societies and made security threats more complex than ever. In addition,it has enabled the emergence of new actors in the global arena and has strengthened the capacity of non-state actors to influence international trends and dynamics, including security, by utilizing new information and communication technologies.At the same time,alongside the real world, a virtual world has emerged in which state and non-state actors, free from the limitations of the real world, play a role. The most important feature of the new space is the uncontrollability of interactions and the changing nature of many concepts such as war and victory. Changes in the tools and methods of battle have created new forms of war, such as information warfare, in cyberspace, according to which victory no longer means achieving goals by defeating the enemy by resorting to violent means; rather,victory means achieving goals without bloodshed and conflict.

Some consider the virtual sphere to be the fifth domain of battle.Military analysts have recognized the cyber domain as a new domain in warfare whose importance is now surpassing that of other domains.The absence of international law has allowed each country to engage in virtual or cyber war against another country.

Conclusion

The purpose of a cyber attack is to access information from other countries,disrupt trade,or damage infrastructure such as water,electricity,transportation,etc. in a way that increases economic costs. In recent years,the number of cyber attacks worldwide has increased significantly. The starting point of virtual war is considered to be the Balkan War,when opposing forces tried to infiltrate each other's information. Today, the growth of computer networks is much faster than the growth of security

software related to them. There is still not enough infrastructure to prevent cyber attacks in countries' computer systems. Cyberspace has become a potential place for such crimes.Billions of dollars are transferred in cyberspace daily without the slightest security,and some of the most important government and personal information exists in cyberspace without the slightest security, increasing the risk of cyberattacks.Finally, in this research, we will examine the negative effects of cyber threats on changing the dimensions of national security and the resulting security crisis, and finally, the strategic warnings necessary to overcome this security crisis affected by cyber threats.

Bibliography

- Ahmed Jamal, A., et al., (2021). "***A review on security analysis of cyber physical systems using machine learning***". Mater. Today: Proc.
- Alkatheiri, M.S., Chauhdary, S.H., Alqarni, M.A., (2021). "***Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications***". Sustain. Energy Technol. Assess. 45, 101219.
- Alzubaidi, A., (2021). "***Cybercrime awareness among Saudi nationals: Dataset***". Data Brief 36, 106965
- **Abdullah Khani, Ali (2009), "War Battle 3, Battle in the Information Age", Abrar Contemporary Cultural and Research Institute, Tehran.[In Persian].**
- **Abdullah Khani, Ali (2003), "Security Theories: An Introduction to the Design of National Security Doctrine (1)", Volume 1, Tehran: Abrar Contemporary Cultural and Research Institute, Tehran..[In Persian].**
- **Asgarkhani, Abu Mohammad and Rahmati, Reza (2010), "Realism Theory and International Security", Foreign Policy Quarterly, Year 24, Issue.[In Persian].**
- **1.Talibpour, Atiyeh (2019), "History of Cyber Attacks in Iran and the World", Young Journalists Club News Agency, 11 February 2019.[In Persian].**
- **Beman Eghbali Zarch, Ali (2012), "Cyber Threats and Attacks against Iran", Center for Political and International Studies IPIS. .[In Persian].**
- **Bayat Kahdan, Mohammad and Jafari, Isa (2013), "Artificial in Cyber Security", 18th National Conference on Electrical, Computer and**

Mechanical Engineering, Shirvan https: / / civilica.com / doc / 1686186. .[In Persian].

- **Ebrahimian, Bahman; Toshe, Ali and Pourhadi, Ebrahim (2015), "Solutions to Counter Cyber Threats against the Islamic Republic of Iran with Emphasis on the Role of Technology and Human Resources", Defense Strategy Quarterly, Year 13, Issue 50, pp. 87-115. .[In Persian].**

- **Eslami, Masoud (2010), "The Position and Situation of Small Countries in the International System", Foreign Policy Journal, Year 4, Issue 4. .[In Persian].**

- Eriksson, J., & Giacomello, G. (2006). "The information revolution, security, and international relations: (IR) relevant theory?". ***International political science review***, 27(3), 221-244.
- Furnell, S, M, and Warren, M, J (1999), "Computer Hacking and Cyber Terrorism: the Real Threats in the New Millennium"?, ***Computers & Security***, vol.18.
- Jay Hoofnagle, Chris, (2022), "***Cybersecurity in Context, PUBLISHER***" TBD, BOOK-WEBSITE.COM
- **Hafendorn, Helga (1992), "The Security Puzzle", translated by Alireza Tayyeb, Foreign Policy Magazine, No. 4.**
- **Kazemi, Ali Asghar (2011), "International Crisis Management", Tehran, Islamic Culture Publishing House..[In Persian].**

- Krishnasamy, V., Venkatachalam, S., (2021). "***An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using index-level Boundary Pattern Convergent Encryption algorithm***". Mater. Today: Proc
- **Moradian, Omid (1402), "Artificial Intelligence in Cybersecurity", Mohsen Madhej Academy.[In Persian].**

- **Tajik, Mohammad Reza (2003), "An Introduction to National Security Strategies, Approaches and Strategies", Farhang Goftman Publishing House..[In Persian].**

- **Torabi, Ghasem (2018). "Challenges and Vulnerabilities of the Islamic Republic of Iran in Cyberspace", Strategic Studies, Year 21, No. 1.Treif, Terry et al. (2004), "Modern Security Studies", translated by Alireza**

Tayeb and Vahid Bozorgy, Tehran: Institute for Strategic Studies..[In Persian].

- **_____ "Cyber Attacks and the Electronic Battlefield", Ministry of Culture and Islamic Guidance website https: / / herasat.farhang.gov.ir / fa / articl / cyberattaks / cyberattaks5.[In Persian].**

- **Sayad, Mohammad Kazem; Amini, Armin and Taheri, Abolghasem (2010), "Cyber Threats and Security Measures in Cyberspace - A Study of the Approaches of the United States of America and the Islamic Republic of Iran", National Security Quarterly, Year 10, Issue 38..[In Persian].**

- **Raisi, Leila (2019), "Protecting Citizens' Rights in Cyberspace in the Third Human Rights Protocol with Emphasis on Iranian Rights", International Studies Quarterly, Year 20, Issue 3, Winter 2019.[In Persian].**

- **Eghtesadnews.com website: 1402 / 09 / 27www.eghtesadnews.com.[In Persian].**

- Nguyen, D.C.L., Golman, D.W., (2021). "***Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. Comput***". Law Secur. Rev. 40, 105521.
- Palmieri, M., Shortland, N., McGarry, P., (2021). "***Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. Comput. Hum***". Behav. 120, 106745.
- **Sadooghi, Moradali (2005), "Information Technology and National Sovereignty", Tehran, Ministry of Foreign Affairs..[In Persian].**
- **Qasemi, H. (2013), "Different Perceptions of National Security", Defense Policy Journal, Year 1, Issue 2..[In Persian].**

- **.Yazdan Fam, Mahmoud (2007), "Changes in the Theories and Concept of International Security", Strategic Studies Quarterly, No. 38,.[In Persian].**

- Yuchong, Li., Qinghui, Liu., (2021). "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments", ***journal homepage***: www.elsevier.com/locate/egyr, Energy Reports.
- Ogbanufe, O., (2021). "Enhancing end-user roles in information security: Exploring the setting, situation, and identity". ***Comput***. Secur. 108, 102340.
- Zhang, J., (2021). "Distributed network security framework of energy internet based on Internet of Things. Sustain". Energy Technol. Assess. 44, 101051. Schmitt, M. zilkowski,k.(2019)international law for cyberspace.at
- :http://www.ccdoce.org/uploads/2019/05trends-intlaw_a4_final.pdf.2019.

بررسی ابعاد جنگ سایبری

چکیده
تهدیدهای سایبری ویژگیهای منحصر به فردی دارند.ازیک سو،این تهدیدها گستره وسیعی اعم از موانع قانونی،فنی،سازمانی وفرهنگی راشامل میشوندوازسوی دیگر،هزینه کم،تأثیرگذاری شگرف وعدم شفافیت عمومی درفضای سایبری،موجب شده بازیگران زیادی به این عرصه واردشوند .هدف از این پژوهش،بررسی تاثیرات فضای سایبری بر امنیت ملی ایران درحوزه های مختلف بویژه حوزه های سیاسی-امنیتی می باشد.همچنین کشف نقاط ضعف ویاکاستی‌های موجوددرحوزه امنیت سایبری باتوجه به تهدیدات موجوددرفضای مجازی از دیگراهداف پژوهش حاضر می باشدکه بصورت روش تحلیلی-توصیفی به این پرسش اساسی میخواهدپاسخ دهد که تهدیدات سایبری چگونه برامنیت ایران تأثیر می‌گذارد؟امری که یافته های تحقیق بیانگر ان است که ایران یکی ازمهمترین کشورهای هدف حملات سایبری درحوزه های مختلف بوده واز این نظرتسریع درتجهیززیرساختهاوسرمایه گذاری درحوزه مقابله باتهدیدات سایبری ازجمله رویکردهای راهبردی ایران دراین حوزه بشمارمی رودکه دراین پژوهش به واکاوی ابعادبیشترآن پرداخته می شود

مشخصات نویسندگان:
۱-دکتربهروزنصیری،دانش آموخته دکتری تخصصی روابط بین الملل،واحدهمدان،دانشگاه آزاداسلامی،همدان،ایران
1364behnasiri@gmail.com

۲-دکترقاسم ترابی(نویسنده مسؤل)استاد روابط بین الملل،واحدهمدان،دانشگاه آزاداسلامی،همدان،ایران

ghasemtoraby@yahoo.com

۳-دکترعلیرضارضایی،دانشیارروابط بین الملل،واحدهمدان،دانشگاه آزاداسلامی،همدان،ایران

Alirezarezaei@gmail.com

واژگان کلیدی: فضای سایبر، تهدیدات امنیتی، جنگ سایبری، امنیت ملی، هوش مصنوعی، ایران

۱-مقدمه

موضوع سایبری سالهای زیادی دغدغه افرادخاص بوده اما حالا تبدیل به یک مسئله سیاسی وامنیتی و اقتصادی برای همگان شده است.توسعه این تکنولوژی این تصوررا ایجاد مینمود که حکمرانی سایبری یک مساله فنی است ونه سیاسی.اماواقعیت این است که تحولات نظام بین الملل مساله سایبری را ازیک موضوع مهندسی به مساله بین علوم مختلف وساختارهای حکومتی ودولتی تبدیل نموده است به طوری که فضای سایبری راازتسلط افرادخاص خارج نموده وبازیگران این عرصه ازمرزهای یک کشور فراتر رفته و بر فضای حکمرانی سایردولتها نیزتاثیر مستقیم می گذارند گسترش فضای سایبر باعث پیدایش مرزهای مجازی شده و از این جهت درک واقع بینانه از تهدیدات امنیتی در گرو توجه به عوامل نرم افزاری است که در واقع حلقه واسط بین محیط امنیتی کشورها و سخت افزارها قرار دارند و بدین جهت برداشت ها از مفهوم امنیت ملی در این فضا به چالش کشیده شده است. یکی از محورهای اصلی تهدید امنیتی در عصر ارتباطات و جهانی شدن برای کشورها را باید در حوزه سایبری دانست که نمونه بارز آن حمله رایانه ای به تاسیسات هسته ای و الکترونیکی ایران توسط آمریکا می باشد. از طرفی تهدیدات سایبری پدیده ای جدید در دهه های اخیر می باشد که با تحول فن آوری اطلاعات و گسترش ارتباطات جهانی از طریق شبکه وسیع اینترنت در سراسرجهان به صورت انواع ویروس ها، کرم ها، جرم ها، هکرها و حملات اینترنتی ظهور و رشد پیدا کرده است به گونه ای که امروزه چالش تهدیدهای سایبری، هم مهم و هم پیچیده به نظر می رسد. تهدیدهای سایبری ویژگیهای منحصر به فردی دارند. از یک سو، این تهدیدها گستره وسیعی اعم از موانع قانونی، فنی، سازمانی و فرهنگی را شامل میشوند و از سوی دیگر، هزینه کم، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران زیادی به این عرصه وارد شوند. به نظر می‌رسددراین میان هزینه‌های کم ورود،ناشناس بودن افراد،مشخص نبودن قلمرو جغرافیایی تهدیدکننده یا تهدیدکنندگان دراین فضا،تأثیرگذاری شگرف وعدم شفافیت عمومی درفضای سایبری،موجب شده

بازیگران قوی وضعیف اعم ازدولت‌هاوگروه‌های سازمان‌یافته وتروریستی وحتی افراد واردشده به این فضا؛تهدیدهایی همچون جنگ سایبری،جرائم سایبری،تروریسم سایبری،جاسوسی سایبری ومانندآن‌هارابه وجود آورند. همین نکته،تهدیدهای سایبری را از تهدیدهای سنتی امنیت ملی که تاحدودزیادی ازماهیت شفاهی برخوردارندو بازیگران آن رادولت –ملت‌هایی تشکیل می‌دهندکه دریک قلمرو مشخص جغرافیایی قابل‌شناسایی هستند،متمایزکرده وسبب شده است امنیت ملی به مفهوم سنتی آن دراین فضابه چالش کشیده شده وناکارآمدبه‌حساب آید.درپژوهش حاضرباتوجه به ظرفیت‌های فضای سایبری،به بررسی وواکاوی این مهم می‌پردازیم که تهدیدات سایبری چه تأثیرات مخربی می‌توانندبر امنیت ملی کشورداشته باشندواین تهدیدات،امنیت ملی راباچه تغییرات مهمی مواجه می‌کنندوبررسی مهم‌ترین حملات سایبری علیه ایران ازدیگرمباحثی است که دراین پژوهش به آن پرداخته می‌شود.از طرفی دراین تحقیق به دنبال بررسی این فرضیه که تهدیدات سایبری به دلیل ویژگی‌های همچون هزینه پایین، گمنامی واداشتن مسئولیت بین‌المللی وتأثیرگذاری گسترده بر کشورهدف،امنیت جمهوری اسلامی رادرابعادمختلف نظامی، سیاسی،اقتصادی،فرهنگی واجتماعی تضعیف می‌کنند،می‌باشیم وهمچنین با توجه به ارتباط مستقیم هوش مصنوعی با فضای سایبر– درپی بررسی کاربرد هوش مصنوعی بر امنیت سایبری–در این پژوهش هستیم.

۲–مبانی نظری و پیشینه شناسی تحقیق

۲–۱–پیشینه تحقیق

بررسی تحقیقات سایرپژوهشگران درحوزه تهدیدات سایبری و امنیت ملی متوجه می‌شویم که افراد زیادی در این مقوله تحقیق نموده و به نتایج گوناگون دست‌یافته‌اند که در ادامه به بخش کوچکی از این پژوهش‌ها اشاره خواهیم کرد:(بیات کاه‌دان، محمد، جعفری عیسی۱٤۰۲)در مقاله [هوش مصنوعی و امنیت سایبری]با استفاده از هوش مصنوعی به

تقویت امنیت سایبری و شناسایی و دفع حملات سایبری پرداخته.(رئیسی ،لیلا۱٤۲۰)در مقاله [صیانت ازحقوق شهروندان درفضای سایبردرپرتونسل سوم حقوق بشرباتاکید برحقوق ایران،]درپی پاسخ به این سؤال فضای سایبر چگونه میتواند درصیانت ازحقوق شهروندی ازحیث انطباق با قوانین نسل سوم حقوق بشر مؤثر باشد.(Chris Jay Hoofnagle۲۰۲۲)درمقاله ،Cybersecurity in Contextبه امنیت سایبری را به‌عنوان یک مشکل «شرور» تعریف می‌کند، به این معنی که امنیت سایبری فقط قابل مدیریت است، نه حل کردن.(Qinghui Liu ۲۰۲۱ و Yuchong Li)،بامقاله A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments ونتیجه امنیت سایبری اطلاعات لحظه‌ای درباره آخرین داده‌های فن‌آوری اطلاعات را دنبال می‌کند. تاکنون روش‌های مختلفی برای جلوگیری از حملات سایبری و یا کاهش آسیب های ناشی از آن توسط محققان در سراسر جهان ارائه شده است. برای این منظور سازمان‌های مختلف از راه‌حل‌های مختلفی برای جلوگیری از آسیب‌های ناشی از حملات سایبری استفاده می‌کنند.اغلب مطالعات انجام‌شده در این باره به‌ویژه آنچه در داخل انجام‌شده است بادرنظر گرفتن یک تعداد محدودی از تأثیرات عرصه سایبری رو تهدیدات متأثرازآن بر امنیت ملی مورد بررسی و تحلیل قرارگرفته است به‌نوعی که دربیشتر پژوهش‌ها به دنبال ارزیابی آن وچگونگی اثرپذیری آن از محتوای فضای سایبر هستند.ارزش کاربردی مؤلفه‌های امنیت ملی دربخش‌های مختلف آنکه توجه به آن‌ها لازمه حفظ جنبه‌هایی از امنیت ملی است در این پژوهش‌ها نادیده گرفته‌شده است.همچنین این پژوهش‌ها در مراحل سطحی به مسئله پرداخته وبه علل عمیقی که منجر به اثرگذاری تهدیدات سایبری برحوزه‌های حساس زیرساخت‌های نظامی،هسته‌ای وصنعتی چندان توجهی نشده است. صحبت از مؤلفه‌های شکل‌دهنده به امنیت ملی، مبحث گسترده‌ای است که نیازمند پژوهش‌ها و تحقیقات تخصصی‌تر است. در این پژوهش به بررسی تأثیرات منفی تهدیدات سایبری در تغییر ابعاد امنیت ملی وبحران امنیتی حاصل از آن و همچنین تأثیر و کاربرد هوش مصنوعی بر فضای سایبر ودرنهایت هشدارهای راهبردی لازم برای غلبه براین بحران امنیتی متأثرازتهدیدات سایبری می‌پردازیم.

۲-۲-مبانی نظری

۲-۲-۱-چارچوب نظری تحقیق

با عنایت به این مسئله که پژوهش حاضر بر پایه‌های مکتب واقع‌گرایی متکی است و ازآنجایی‌که مباحث مربوط به حملات سایبری ارتباط مستقیم با محیط آنارشیک نظام بین‌الملل دارد (به دلیل برتری جویی مهاجم)لذابامحورقرار دادن مفاهیم اصلی واقع‌گرایی،بحث را پیگیری می‌کنیم.برای اینکه مقوله استقرار امنیت رابر اساس این مکتب توضیح دهیم ابتدا شش مفروض اصلی مکتب رئالیسم رامتذکر می‌شویم:محیط آنارشیک نظام بین‌الملل:هیچ قدرت فائقه‌ای درنظام بین‌الملل برای منع کردن از کاربردزوریکی علیه دیگری وجودندارد،دولت سالاری:دولت‌ها بازیگران اصلی سیاست بین‌المللی هستند،قدرت:ویژگی تعریف‌شده محیط بین‌الملل که دولت‌هاازآن بهره‌مندند،عقلانیت: دولت‌هامحاسبه هزینه - فایده انجام کارهای خودراقبل از انجام عمل می‌کنند،بقا:که پیش‌شرط دسترسی به همه اهداف ملی است وخودیاری:برای بقانمی‌توان به تضمین دیگری متکی بود. البته توجه واقع‌گرایی به درس‌های تاریخ نیزراهنمای این رهیافت برای توضیح امنیت است (عسگرخانی و رحمتی، ۱۳۸۹: ۱٤۰).

۲-۲-۲-نظریه واقع‌گرایی

واقع‌گرایان معتقدند در سطح سیاست داخلی،مسئله‌ای به نام امنیت وجود نداشته وامنیت صرفاًدرسطح بین‌المللی معنا می‌یابد.به‌بیان‌دیگر،امنیت ملی نزدآنان چیزی جز امنیت بین‌الملل نیست ودراین راستا ناامنی ویژگی بارزنظام بین‌الملل است (عبدالله خانی، ۱۳۸۲: ۷۰).ازنظرواقع‌گرایان،عدم امنیت اصلی‌ترین مسئله،قدرت مهم‌ترین ابزار،دولت مهم‌ترین بازیگرو جنگ،بارزترین جلوه بروزناامنی درعرصه بین‌المللی است(یزدان فام، ۱۳۸٦: ۷۳۱).بنابراین،محورتمرکزواقع‌گرایی درموضوع امنیت،نظامی است.همان‌طورکه استفن والت تعریف می‌کند،مطالعات امنیتی،مطالعه تهدید،استفاده وکنترل نیروی نظامی است.جدای ازمسائل نظامی،سایرعوامل هم دربحث امنیت می‌توانند مهم

باشند؛اماواقع‌گرایان ونوواقع‌گرایان معمولاً تنهاتاجایی آن‌هارامهم می‌شمارندکه به توسعه توانایی‌های نظامی کمک کند(تریف، ۸۵:۱۳۸۳).ازنظر واقع‌گرایان،هر چیزی ممکن است برامنیت تأثیرگذار باشد،اما موضوع امنیت هر چیزی نمی‌تواند باشد.به باور واقع‌گرایان، چون دولت‌ها بازیگران اصلی در نظام بین‌الملل می‌باشند،بنابراین آنان مرجع امنیت قرار خواهندگرفت.(عبدالله خانی، ۱۳۸۲: ۸۳).ظهور و تحول تدریجی پارادایم امنیتی و گذار از «امنیت ملی» به «امنیت بین‌المللی» و سپس به «امنیت جهانی» که هر یک بر پایه مفروضات نظری و سیاسی متفاوتی استوار هستند،پیوند نزدیکی با تطور تاریخی نظام بین‌المللی ورشداندیشه بشردرتفسیرآن دارد.پارادایم امنیت ملی دربسترتاریخی مشخصی ظهورکرد.باتولد دولت ملی در قرن هفدهم میلادی وعلاقه‌ای که به بقای خود داشت،امنیت ملی از اهمیت خاصی برخوردار شد.برای پایان دادن به جنگ همه بایکدیگر و رسیدن به آرامش داخلی شهروندان باچشم‌پوشی ازبخشی ازاختیارات خودوتنفیذآن به یک حکمران تسلیم او می‌شوندوازاوانتظارتأمین صلح رادارندچنین دولتی بابرخورداری ازپشتوانه مردمی،خودراموظف به تأمین امنیت،آن‌ها می‌بیند و بهترین وکوتاه‌ترین مسیر را در تقویت و تجهیز بنیه دفاعی کشور برای دفع تهاجمات احتمالی می‌یابد؛به‌طوری‌که در شرایط محدودیت منابع باارزش جهانی، هرکس که قوی‌تراست،در رقابت برسرتصاحب این‌گونه منابع برنده خواهدشد؛بنابراین، بازیگران صحنه جهانی هرگز خودرادور از تهدید نمی‌دانند،بلکه سایه تهدیدی دائمی رابر سر خود احساس می‌کنند.درنتیجه،هر بازیگری کسب قدرت برای دفاع از خود را شرط اولیه بقا می‌شمارد.در این دیدگاه،رابطه مفروض میان امنیت وقدرت، رابطه‌ای همیشگی و مستقیم است هراندازه بر میزان قدرت یک کشور افزوده شود،امنیت آن کشور نیز افزایش می‌یابد.دراین دیدگاه که از آن به «نگرش واقع‌گرایانه» به مفهوم امنیت نام برده می‌شود،میان امنیت یک ملت،باامنیت ملت‌های دیگری رابطه ای معکوس برقرار است به این معنا که امنیت یکی به بهای ناامنی دیگری حاصل می‌شود.باوجودچنین رابطه‌ای میان امنیت ملت‌ها،امنیت هر واحد به‌صورت مجزا از دیگران تحقق می‌یابدو جمع میان امنیت ملت‌ها نه‌تنها دشوار، بلکه ناممکن است(قاسمی، ۱۳۷۲: ۵۹).طرح اولویت منافع ملی بر منافع امنیت دسته‌جمعی ملهم از«سیاست قدرت»که

افرادی مانند هانس مورگنتا آن رانظریه‌پردازی کردند،موجبات شکست نظام‌های امنیت جهانی همچون جامعه ملل را،در تأمین امنیت فراهم آورده درحالی‌که جامعه ملل نتوانست از ظهور فاشیسم و نازیسم جلوگیری کندودرآستانه جنگ جهانی دوم ازهم فروپاشید،سازمان ملل نیزباظهوردوقدرت برتر،یعنی ایالات‌متحده آمریکاواتحادجماهیر شوروی و دعوی غیرقابل‌جمع آن‌ها برای سلطه بر جهان که به جنگ سرد انجامید،عملاً کارایی خود راازدست داد. درنتیجه بار دیگر، پارادایم هابزی امنیت ملی، یعنی سیاست قدرت، در امور بین‌الملل برتری یافت. هدف اصلی کشورها نه امنیت بین‌الملل یا حکومت جهانی، بلکه بقای ملی بود (هافندرون، ۱۳۷۱: ۱۰).براساس چنین برداشتی بودکه هر کشوری برای دفع تهدیدهای احتمالی، آمادگی جنگی را ضروری و لازم می‌داند و در شرایط بحرانی، تهدید به استفاده از نیروهای نظامی به‌منظور تحصیل امتیاز یا عدم تمکین در مقابل خواسته حریف،به شکل یکی ازابزارهای اعمال قدرت درآمد(کاظمی، ۱۳۷۰: ۷۷).به‌این ترتیب،حفظ برتری تکنولوژیک دررقابت تسلیحاتی به یکی از مهم‌ترین اهداف قدرت‌های بزرگ و به‌تبع آن‌ها،قدرت‌های کوچک منطقه‌ای تبدیل شد و واگرایی از سطح کلان، به سطح خرد نیز کشیده شد؛ بنابراین، کشورهای کوچک و ضعیف، همواره ناگزیر هستند برای یافتن حامی، به جمع قدرت‌های بزرگ بروند حتی اگر این حمایت به قیمت محروم شدن کشور تحت حمایت از حقوق اساسی، استقلال و حق تعیین سرنوشت تمام می‌شد، بازگریزی نبود. انگلستان بیش از یک قرن چنین نقشی را در حوزه خلیج‌فارس ایفا کرد(اسلامی، ۱۳۶۹: ۵۵۲).دراین دیدگاه،رابطه مفروض میان امنیت وقدرت، رابطه‌ای همیشگی و مستقیم است هراندازه بر میزان قدرت یک کشور افزوده شود،امنیت آن کشور نیز افزایش می‌یابد.در این دیدگاه که از آن به«نگرش واقع‌گرایانه»به مفهوم امنیت نام برده می‌شود،میان امنیت یک ملت،با امنیت ملت‌های دیگر رابطه‌ای معکوس برقراراست به این معنا که امنیت یکی به بهای ناامنی دیگری حاصل می‌شود.باوجود چنین رابطه‌ای میان امنیت ملت‌ها،امنیت هر واحد به‌صورت مجزا از دیگران تحقق می‌یابد و جمع میان امنیت ملت‌ها نه‌تنها دشوار، بلکه ناممکن است (قاسمی، ۱۳۷۲: ۵۹).

۳-یافته ها و تجزیه‌وتحلیل داده‌ها

۳-۱-یافته های تحقیق

۳-۱-۱-تأثیر تهدیدهای سایبری بر امنیت ملی

درعصراطلاعات،مفهوم امنیت ملی گسترش‌یافته و از گردش آزاداطلاعات درسراسرجهان ازراه اینترنت متأثر می‌شود. امروزه فضای سایبر بر نحوه ادراک از جنگ و نحوه انجام گرفتن آن تأثیرگذاشته است،به‌طوری‌که دیگرنه‌فقط مرزهای جغرافیایی، بلکه انواع مرزها به‌ویژه مرزهای هویتی از سوی جنگ اطلاعاتی مورد تهدید قرار دارد(، Eriksson & Giacomello ۲۰۰۶: ۲۳۲).مبرهن است که جنگ سایبری امنیت کشورها رابه خطر انداخته ودرمواردی حتی خسارات سهمگینی رادردنیای فیزیکی به بار اورده (رئیسی.لیلا:۵۱.schmitt&ziolkowski.۲۰۱۹).برای این منظور ابتدا دامنه امنیت سایبری سپس انواع امنیت سایبری و در انتهای این مبحث تأثیر حمله سایبری بر امنیت ملی را توضیح می‌دهیم:

۳-۱-۲-دامنه امنیت سایبری

افراد دامنه وسیع «امنیت سایبری» را تشخیص می‌دهند و خود را در زمینه آن قرار می‌دهند. متخصصان امنیت سایبری –یا کسانی که در حال تحصیل به‌عنوان حرفه‌ای امنیت سایبری هستند– می‌توانند از آن برای قرار دادن کارهای تخصصی روزانه خود در ارتباط با سایر زمینه‌های تحصیلی و درک فرصت‌ها و موانعی که ممکن است از بخش‌های دیگر به وجود آید استفاده کنند. کارشناسان حوزه سایبری مهم‌ترین عناصری را که زمینه‌ی مشکلات امنیت سایبری در آن پدیدار شده و مدیریت می‌شوند را شکل می‌دهند و بررسی خواهند کرد.امنیت سایبری به ما نشان خواهد داد که چگونه چارچوب‌های اخلاقی، قانونی و اقتصادی فناوری‌ها و سیاست‌های امنیتی را قادر می‌سازند که موضوعات خاص شامل سیاست‌گذاری(در سطح ملی، بین‌المللی و سازمانی)،مدل‌های کسب‌وکار،

چارچوب‌های قانونی(شامل وظایف امنیتی، حریم خصوصی، مسائل دسترسی مجری قانون، هک کامپیوتر، جاسوسی اقتصادی/ نظامی و جنگ سایبری)، توسعه فنی استانداردها و نقش کاربران، دولت و صنعت را محدود کنند (Hoofnagle، ۲۰۲۲: ۳). امنیت هر سازمان با سه اصل آغاز می‌شود:رازداری،صداقت و در دسترس بودن.از این سه اصل به‌عنوان مثلث امنیتی یا سیا یاد می‌شود که از اولین سیستم‌های کامپیوتری به‌عنوان استاندارد برای امنیت سیستم‌ها عمل کرده است(Palmieri ۲۰۲۱: ۵).اصل محرمانه بودن بیان می‌کند که فقط منابع مجاز می‌توانند به اطلاعات و عملکردهای حساس دسترسی داشته باشند، مانند اسرار نظامی (محرمانه).اصول یکپارچگی ادعا می‌کند که فقط افراد و منابع مجاز می‌توانند اطلاعات و عملکردهای حساس را اصلاح، اضافه یا حذف کنند مانند کاربر داده‌های نادرستی را در پایگاه داده[1] وارد می‌کند.اصول در دسترس بودن ادعا می‌کند که سیستم‌ها، عملکردها و داده‌ها باید بر اساس پارامترهای توافق شده بر اساس سطح سرویس SLAدر دسترس بودن)در صورت تقاضا در دسترس باشند (Nguyen and Golman، ۲۰۲۱: ۵).بهترین روش‌های امنیت سایبری خارج از اصول ذکرشده است.

شکل ۱. مثلث امنیتی (CIA) از (Qinghui،Yuchong، ۲۰۲۱)

هر هکر پیشرفته‌ای می‌تواند این دفاع آسان را دور بزند. با رشد یک شرکت،امنیت سایبری دشوارتر می‌شود. یکی دیگر از محدودیت‌های امنیت سایبری،برخورد با

1

مشارکت‌کنندگان در حال رشد با دنیای مجازی و واقعی تبادل داده است. یکی از چالش‌های مهم در امنیت سایبری،نبود شغل واجد شرایط برای انجام کاراست.بسیاری از افراد با مهارت‌های عمومی در سطح پایین‌تر بینش امنیت سایبری قرار دارند.پوشش فضای مجازی موضوعی گسترده است.یک استراتژی جامع همه این جنبه‌ها را پوشش می‌دهد و هیچ‌یک از آن‌ها را نادیده نمی‌گیرد (Alzubaidi، ۲۰۲۱: ۸).زیرساخت‌های اصلی جهان به‌عنوان یک ترکیب فیزیکی- سایبری عمل می‌کند.ما از این ساختار فوق‌العاده مزایای زیادی می‌گیریم.بااین‌حال،استقرار یک سیستم آنلاین آسیب‌پذیری جدیدی در برابر هک و حملات سایبری ایجاد می‌کند.تصمیم‌گیرندگان سازمان باید در دستور کار خود بگنجانند که چگونه حملات ممکن است بر عملکرد آن‌ها تأثیر بگذارد. بسیاری از بهترین هکرهای جدید،امنیت برنامه‌های کاربردی وب را ضعیف‌ترین نقطه برای حمله به یک سازمان می‌دانند.امنیت برنامه با رمزگذاری عالی شروع می‌شود(Yuchong & Qinghui ۲۰۲۱: ٤).هر استراتژی باید به‌صورت سفارشی برای هر کسب‌وکار به‌طور متفاوتی طراحی و اجرا شود.به‌این‌ترتیب هک اطلاعات و نفوذ به آن کمتر انجام می‌شود.امنیت سایبری به‌طور فزاینده‌ای پیچیده می‌شود. سازمان‌ها باید «دیدگاه امنیتی» در مورد نحوه عملکرد امنیت سایبری داشته باشند.درنتیجه همیشه باید امنیت بالایی داشته باشید تا یک قدم جلوتر از هکرها باشید.با توجه به افزایش سرمایه‌گذاری‌های امنیتی، سرمایه‌گذاری در سیستم‌ها و خدمات امنیت سایبری در حال افزایش است.سه شرکت فعال در این زمینه مک آفی، سیسکو و ترندمیکرو هستند(Yuchong & Qinghui، ۲۰۲۱: ٦ وSnowe، ۲۰۲۰).

انواع حملات سایبری رایج

۱. **حملات فیشینگ (:Phishing)** حملاتی که با استفاده از ایمیل‌ها یا پیام‌های تقلبی برای سرقت اطلاعات کاربری یا مالی انجام می‌شوند.

۲. **حملات باج‌افزاری (:Ransomware)** بدافزارهایی که با رمزگذاری داده‌ها، از کاربران تقاضای پول در ازای بازگرداندن دسترسی می‌کنند.

۳. **حملات DoS و :DDoS** هدف این حملات، متوقف کردن سرویس‌های آنلاین یا سامانه های ارتباطی از طریق افزایش غیرعادی ترافیک شبکه است.

٤. **حملات :(XSS (Cross-Site Scripting** دستکاری صفحات وب برای اجرای اسکریپت های مخرب و آسیب‌رساندن به کاربران.

٥. **حملات تزریق کد (:SQL Injection)** این حملات با ارسال دستورات مخرب به پایگاه های داده، داده‌های محرمانه را سرقت یا تغییر می‌دهند.

اثرات حملات سایبری

- **اختلال در سرویس‌ها:** بسیاری از حملات سایبری منجر به اختلال در سرویس‌های حیاتی یا حتی قطع دسترسی کاربران به سامانه‌ها می‌شوند.
- **از دست رفتن اطلاعات:** یکی از پیامدهای مهم این حملات، سرقت یا تخریب اطلاعات حساس و محرمانه است.
- **خسارات اقتصادی:** حملات سایبری می‌توانند باعث ضررهای مالی گسترده برای سازمان ها و افراد شوند.
- **تضعیف اعتماد عمومی:** در صورتی که حملات موفق باشند، می‌توانند اعتماد کاربران به سرویس‌ها و امنیت آنلاین را کاهش دهند.

حمله سایبری به هرگونه اقدام غیرمجاز اشاره دارد که با هدف آسیب‌رساندن به داده‌ها، سامانه‌ها یا زیرساخت‌های دیجیتال از طریق فضای سایبری انجام می‌شود. این حملات اغلب شامل نفوذ، تخریب، تغییر یا دسترسی غیرمجاز به اطلاعات حساس هستند. با این حال، تا زمانی که یک تعریف رسمی، روشن و مورد پذیرش جامعه بین‌المللی برای حملات سایبری ارائه نشود، پرداختن به ابعاد مختلف این موضوع و ارائه مشاوره حقوقی جامع برای مقابله با آن، بسیار چالش‌برانگیز خواهد بود.

۳-۱-۳-انواع امنیت سایبری

امنیت سایبری تضمین می‌کند که فقط افراد مجاز به آن اطلاعات دسترسی دارند(Ahmed Jamal, A., et al، ۲۰۲۱).برای حفاظت بهتر، شناخت انواع امنیت سایبری ضروری است؛امنیت شبکه:امنیت شبکه از شبکه کامپیوتری در برابر اختلالات محافظت می‌کند که می‌تواند بدافزار یا هک باشد. امنیت شبکه مجموعه‌ای از راه‌حل‌ها است که سازمان‌ها را قادر می‌سازد شبکه‌های کامپیوتری را از دسترس هکرها، مهاجمان سازمان‌یافته و بدافزارها دورنگه دارند(Zhang، ۲۰۲۱: ۸).امنیت برنامه:استفاده از سخت‌افزار و نرم‌افزار(مانندبرنامه‌های آنتی‌ویروس،رمزگذاری و فایروال‌ها)ازسیستم در برابر تهدیدات خارجی که ممکن است در توسعه برنامه‌ها اختلال ایجاد کند، محافظت می‌کند(Alkatheiri et al، ۲۰۲۱: ۳). امنیت اطلاعات:از داده‌های فیزیکی و دیجیتالی در برابر دسترسی غیرمجاز،افشا،سوءاستفاده،تغییرات غیرمجاز و حذف محافظت می‌کند(Ogbanufe،، ۲۰۲۱: ۳).

امنیت عملیاتی:شامل فرآیندها و تصمیماتی است که برای کنترل و حفاظت از داده‌ها اتخاذ می‌شود.به‌عنوان‌مثال، مجوزهای کاربر هنگام دسترسی به شبکه یا فرآیندهایی که مشخص می‌کنند چه زمانی و کجا اطلاعات ممکن است ذخیره یا به اشتراک گذاشته شوند(Ogbanufe، ۲۰۲۱: ٤).

امنیت ابری:ازاطلاعات موجود در فضای ابری (بر اساس نرم‌افزار)محافظت می‌کند و برای حذف خطرات حملات در سایت نظارت می‌کند(Venkatachalam،Krishnasamy ،، ۲۰۲۱: ۲).

آموزش کاربران:بهVenkatachalam،Krishnasamy ،جنبه‌های غیرقابل پیش‌بینی امنیت سایبری، یعنی افراد اشاره دارد. هرکسی می‌تواند به‌طور تصادفی ویروسی را وارد سیستم امنیتی کند. آموزش حذف پیوست‌های مشکوک در ایمیل،عدم اتصال به USB های ناشناس و سایر مسائل مهم باید بخشی از برنامه امنیتی شرکتی باشد (Krishnasamy، Venkatachalam، ۲۰۲۱ وYuchong، ۲۰۲۱).

انواع مختلف امنیت سایبری (Yuchong، Qinghui **2021)**

۳-۱-٤-ارتباط هوش مصنوعی با امنیت سایبری

دردنیای امروزنادیده گرفتن هوش مصنوعی در امنیت سایبری عواقب خاص خودش را دارد هوش مصنوعی به‌عنوان یک فن‌آوری نوآورانه،نقش بسزایی در تقویت امنیت سایبری ایفا می‌کند. در عصری که حملات سایبری پیچیده و پیوسته در حال افزایش هستند، هوش مصنوعی می‌تواند به‌عنوان یک ابزار قدرتمند در تشخیص،پیشگیری و مقابله با تهدیدات سایبری عمل کند. استفاده از الگوریتم‌ها و مدل‌های یادگیری ماشینی، هوش مصنوعی قادراست الگوهای ناشناخته و غیرمعمول را در ترافیک داده‌ها تشخیص دهد. این قابلیت به سازمان‌ها کمک می‌کند تا حملات را در مراحل ابتدایی تشخیص داده و به‌صورت پیشگیرانه علیه آن‌ها اقدام کنند. علاوه بر تشخیص،هوش مصنوعی می‌تواند در تقویت امنیت پاسخگویی در زمان واقعی نیز مؤثر باشد.با استفاده از سیستم‌های هوشمند،حملات ممکن است به‌طور خودکار متوقف شوند و اقدامات اصلاحی انجام شود که از مزیت زمانی برخوردار است و خسارت‌های احتمالی را کاهش می‌دهد. بهره‌برداری

از هوش مصنوعی در امنیت سایبری می‌تواند عملکرد سازمان‌ها را بهبود بخشد، هزینه‌های احتمالی حملات را کاهش دهد و حفاظت در برابر تهدیدات پیچیده را تضمین کند. با توجه به اینکه جرم‌های سایبری به‌صورت گسترده و پیچیده‌تر می‌شوند، هوش مصنوعی به‌عنوان یک ابزار قدرتمند در مبارزه با این تهدیدات بی‌نظیر است(بیات کاه‌دان و جعفری، ۱٤۰۲: ۱).با توجه به اهمیت هوش مصنوعی در امنیت سایبری، در این مقاله به شش کاربرد هوش مصنوعی با استفاده از الگوریتم یادگیری ماشین(یادگیری ماشینی[1] زیرشاخه‌ای از هوش مصنوعی است که بر توسعه الگوریتم‌ها و مدل‌های آماری تمرکز دارد که سیستم‌های رایانه‌ای را قادر می‌سازد بدون برنامه‌ریزی صریح یاد بگیرند و پیش‌بینی یا تصمیم بگیرند. این شامل ایجاد مدل‌ها و الگوریتم‌های ریاضی است که به کامپیوترها امکان می‌دهد از داده‌های زیادی یاد بگیرند و آن‌ها را تجزیه‌وتحلیل کرده تا الگوها را شناسایی کنند، بینش‌های معنی‌داری را استخراج کنند و پیش‌بینی‌ها یا تصمیم‌گیری‌های دقیق بگیرند).در امنیت سایبری می‌پردازیم:

۱- شناسایی و تشخیص حملات سایبری

هوش مصنوعی می‌تواند با استفاده از الگوریتم‌های یادگیری ماشین، تغییرات غیرعادی در ترافیک شبکه را شناسایی کند این تغییرات می‌تواند نشان‌دهنده یک حمله سایبری مانند حمله DDOS باشد.

۲- جلوگیری از حملات سایبری

هوش مصنوعی می‌تواند با استفاده از الگوریتم‌های یادگیری ماشین، آسیب‌پذیری‌های سیستم‌ها و شبکه‌های کامپیوتری را شناسایی کند، سپس می‌توان از این اطلاعات برای رفع آسیب‌پذیری‌ها و جلوگیری از حملات سایبری استفاده کرد. همچنین هوش مصنوعی می‌تواند با استفاده از الگوریتم یادگیری ماشین، حملات سایبری را پیش‌بینی کند.این الگوریتم‌ها می‌تواند بر اساس داده‌های تاریخی، احتمال وقوع یک حمله سایبری را پیش‌بینی کند، سپس می‌توان با استفاده از این اطلاعات برای اتخاذ اقدام پیشگیرانه استفاده کرد.

۳- مدیریت ریسک امنیتی

هوش مصنوعی می‌تواندبه سازمان‌ها کمک کندتا آسیب‌پذیری سیستم‌ها و شبکه‌های کامپیوتری خود را شناسایی وارزیابی کنند،سپس سازمان‌ها می‌توانند بر اساس این اطلاعات، اقدامات لازم برای کاهش ریسک امنیتی انجام دهند.

٤- تحلیل داده‌های امنیتی

هوش مصنوعی می‌تواند با استفاده از الگوریتم یادگیری ماشین، الگوها و روندهای موجود در داده‌های امنیتی را شناسایی کند. این اطلاعات می‌تواند به سازمان‌ها در شناسایی حملات سایبری،کاهش ریسک امنیتی،بهبود عملکرد امنیت سایبری کمک کند.

٥- خودکارسازی امنیت سایبری

هوش مصنوعی می‌تواند به خودکارسازی فرایند امنیت سایبری با استفاده از الگوریتم یادگیری ماشین کمک کند.برای این منظور با استفاده از این الگوریتم کارهایی مانند شناسایی حملات سایبری،مدیریت ریسک امنیتی و تحلیل داده‌ها امنیتی را خودکار کند.

٦- آموزش و آگاه‌سازی کارکنان

هوش مصنوعی می‌تواند با استفاده از الگوریتم یادگیری ماشین،محتوای آموزشی با استفاده از نیاز کارکنان تولید کند، این محتوا می‌تواندبه کارکنان در شناسایی حملات سایبری، کاهش ریسک امنیتی و بهبود عملکرد امنیت سایبری کمک کند (مرادیان، ١٤٠٢: ١-٦).

٣-١-٦-چالش‌ها و آسیب‌پذیری‌های ایران در فضای سایبر

البته چالش‌های فضای سایبرتنهابه جمهوری اسلامی ایران اختصاص نداردوهمه کشورهادرسطوح مختلفی باآن مواجه هستند.برای مثال درراهبردسایبری وزارت دفاع آمریکابروجود چنین چالشی تأکید شده و راهکارهایی برای پوشش آن ارائه شده است. در ادامه به بررسی مهم‌ترین چالش‌های ایران در حوزه سایبری می‌پردازیم:

١- کاربر بودن فضای سایبر

کاربربودن به میزان استفاده افرادازنرم‌افزارهاو سخت‌افزارها ودر کل به میزان حضور افراد در فضای سایبر گفته می‌شود. کاربر بودن در کشورهای مختلف وجود دارد به این

مفهوم که افراد سایر کشورها نیز به‌مراتب بیشتر از افراد کشور ما از فضای سایبر استفاده می‌کنند. در حقیقت بیشتر کشورها در محیطی فعالیت می‌کنند که کوچک‌ترین نقشی در ایجاد و مدیریت کلان آن ندارند. اغلب کشورها نگرانی امنیتی جدی در این خصوص دارند. حتی کشورهای اروپایی نیز از اینکه اکثر سرورها در آمریکا قرار دارد ابراز نگرانی کرده‌اند و خواهان انتقال بخشی از آن به اروپا هستند؛ بنابراین اغلب کشورها ازجمله ایران به دنبال داشتن اینترنت ملی و با نام شبکه ملی اطلاعات هستند. نگرانی ایران نیز منجر به اقداماتی چون فیلتر برخی شبکه‌های اجتماعی خارجی و راه‌اندازی شبکه ملی اطلاعات شده است.بااین‌حال،چندان مشخص نیست که این‌گونه اقدامات تا چه میزان می‌تواند آسیب‌پذیری‌ها را کاهش داده و هم‌زمان مانع استفاده از فرصت‌ها نیز نشود. در معنای دیگر کاربر بودن می‌توان به استفاده گسترده اززنرم‌افزارها و سخت‌افزارهای خارجی اشاره دارد. ایران یکی از وابسته‌ترین کشورها به نرم‌افزارها و سخت‌افزارهای خارجی است به‌نحوی که اکثر گوشی‌ها و کامپیوترها،فلش‌ها و سی‌دی‌ها و حتی لوازم خانگی دیجیتال وارداتی است و ممکن است به بدافزارها جاسوسی آلوده باشند. تحقیقات شرکت کسپرسکی بیانگر آن است که نیمی از موبایل‌های کاربران ایرانی آلوده به بدافزارهاست.براین اساس، کاربر بودن جمهوری اسلامی ایران در فضای سایبری،از جدی‌ترین آسیب‌پذیری‌های کشور است که باید برنامه‌ای بلندمدت و چندجانبه برای آن داشت. استفاده از بخش خصوصی و حمایت از آن در تولید استارت آپ‌های ایرانی، همچنین آموزش و تربیت نخبگان سایبری در حوزه‌های مرتبط می‌تواند از اقدامات اساسی در حوزه فضای سایبر باشد.

۲- ضعف اعتماد به دولت

از دیگر چالش‌های جمهوری اسلامی ایران در فضای سایبر، ضعف اعتماد عمومی به دولت در این عرصه است که بیشتر در استفاده از شبکه‌های اجتماعی داخلی و استفاده از فیلترشکن‌ها تجلی‌یافته است.مهم‌ترین نگرانی در این زمینه استفاده از شبکه‌های اجتماعی خارجی مانند تلگرام است که امکان رصد روندها و رویدادهای داخلی و شناخت ارزش‌ها،باورها و خواسته‌های عمومی مردم ایران را برای سایر کشورها فراهم نموده

است.همچنین شبکه‌های اجتماعی محل مناسبی برای اطلاع از تحولات اجتماعی،ارزشی،دینی و فرهنگی یک جامعه را بیان می‌کنند.استفاده گسترده از این شبکه‌ها علاوه بر ایجاد فرصت می‌تواند زمینه آسیب‌پذیری کشور را نیز فراهم کند. به همین منظور،حاکمیت به دنبال فیلتر تلگرام نه‌تنها نتوانست از میزان استفاده از آن بکاهد بلکه موجب افزایش استفاده چند برابری از فیلترشکن‌ها شده است.درایران موبایل‌های هوشمند حداقل یک فیلترشکن فعال نصب‌شده دارند که موجب رصد اطلاعات داخلی توسط بازیگران خارجی می‌شود؛بنابراین باید راهی پیدا کرد که ضمن استفاده از فرصت‌ها،با تهدیدها نیز مقابله شود.ارتقای اعتماد در روابط دولت و جامعه شرط اساسی رسیدن به این هدف است. در حقیقت تاز مانی که بی‌اعتمادی بر این رابطه حاکم باشد، سیاست‌های محدودکننده نه‌تنها کارآمد نیست بلکه بر مشکلات خواهد افزود.

۳- نداشتن راهبرد جامع و کارآمد

نداشتن راهبرد جامع و کارآمد از مهم‌ترین چالش‌های کشور در حوزه سایبری است. البته این موضوع به معنای این نیست که ایران اسناد سایبری ندارد بلکه مسئله نبود زمینه لازم در کشور برای تدوین و مهم‌تر از آن،اجرای راهبرد سایبری جامع و کارآمد است. ضعف اصلی به ورود دیرهنگام ایران در تمامی ابعاد و سطوح به فضای سایبر و همگام نبودن دولت و جامعه با انقلاب سایبری برمی‌گردد. درواقع دولت و جامعه ایرانی در مورد ورود تکنولوژی‌های جدید نیز باوجود داشتن قوانین و مقررات کافی در این حوزه، در اجرای قوانین و مقررات با مشکل مواجه است که موجب جزیره‌ای عمل کردن نهادهای متولی در حوزه سایبر می‌گردد که آسیب‌پذیری بزرگی را وارد می‌کند. در این شرایط، کشور نیازمند راهبرد جامع و کارآمد است که باید مبتنی بر برنامه‌ای بلندمدت و جامع بر محور شناخت فضای سایبر، شناخت فرصت‌ها و تهدیدها و طرح‌ریزی برای همه بخش‌ها ازجمله خصوصی و دولتی باشد؛

٤- همگام نبودن با فضای انقلاب سایبری

مشکل بعدی، همگام نبودن ساختار اداری و اجرایی، مدیران و کارکنان دولتی و بخش خصوصی و مهم‌تر از آن نیروهای نظامی و دفاعی کشور با انقلاب سایبری است. مسئله

اصلی در این زمینه، ساختار مدیریتی کشوراست که بر مدار مدیریت سنتی می‌چرخد. درحالی‌که کشورهای پیشرفته،ساختارهای سیاسی، نظامی و امنیتی خود را در راستای همراه شدن با انقلاب سایبری قرار داده‌اند.موضوع دیگر جذب نیروهای کارآمد و آموزش کارکنان برای همراهی با انقلاب سایبری است؛بنابراین در ایران نیز بهتراست با آموزش کارکنان دولتی به‌ویژه در مراکز سیاسی،نظامی و امنیتی علاوه بر بهره‌برداری بهتر از فضای سایبری بتوان ساختارهای اداری و سیاسی را نیز به‌روز و کارآمد نمود(ترابی، ۱۳۹۷: ۱۷۳).

۳-۱-۷-رایج‌ترین حملات سایبری بر علیه ایران

در سال ۲۰۱۹ تقریباً هر ١٤ ثانیه،یک شرکت با باج‌افزار تهدید می‌شد.اندازه و پیچیدگی حملات بسیار افزایش‌یافته و اهمیت تقویت نیروی دفاعی سایبری دوچندان شده است؛به دلیل اهمیت این موضوع سازمان‌های Europol،FBI و Hewlett Packard Enterprise در مبارزه با جرائم سایبری با یکدیگر متحد شده‌اند. در کشور ما نیز در چند سال گذشته تعداد حملات سایبری به سازمان‌های دولتی و به‌ویژه هسته‌ای بسیار گسترده شده است. مهم‌ترین حملاتی که صورت گرفت، ویروس شعله «فلیم»، ویروس «استاکس‌نت» و «اکتبر سرخ» بوده است.در ژوئن ۲۰۱۰ تأسیسات هسته‌ای ایران در نطنز توسط یک بدافزار به نام «استاکس نت» مورد حمله سایبری واقع شد. طبق گزارش‌ها، «استاکس‌نت» که با مشارکت آمریکا و اسرائیل طراحی‌شده بود، نزدیک به هزار گریزانه تأسیسات اتمی ایران را نابود کرده و باعث شد برنامه اتمی ایران دو سال عقب بیفتد. این ویروس رایانه‌ای طراحی‌شده بود تا نزدیک به ٦٠ هزار رایانه را آلوده کند اما دولت ایران اظهار داشت که این ویروس نتوانسته آسیب چندانی وارد کند. ایران به راه‌حلی برای مقابله با این ویروس دست‌یافت که این باعث بهتر شدن وضعیت دفاع سایبری و پیشرفت آن شد. در حمله سایبری «اکتبر سرخ» که در روسیه و قسمت‌هایی از آسیای میانه اتفاق افتاد،حمله‌ای گسترده برای جاسوسی و جمع‌آوری اطلاعات طراحی‌شده بود.تأسیسات دیپلماتیک و هسته‌ای و بانک‌ها ازجمله مواردی بودند که اسیر بدافزار شده و ویروس‌ها و کرم‌های اینترنتی را وارد سیستم‌های امنیتی کردند. در این عملیات که به نام «روکرا» نیز

مشهور است هکرها ایمیل‌هایی حاوی فایل‌های آلوده اکسل یا Word ارسال کرده که محتوایشان می‌توانسته برای قربانیان جالب باشد. بدافزار «شعله» نیز قطعه پیچیده‌ای از یک بدافزار کامپیوتر است که رایانه‌های با سیستم‌عامل ویندوز را مورد حمله قرار می‌دهد. این بدافزار از سال ۲۰۰٦ شروع به فعالیت کرده و برای جاسوسی اینترنتی و تخریب اطلاعات مهم در کشورهای خاورمیانه و اروپای شرقی استفاده می‌شود. این بدافزار که به ویروس «فلیم» هم معروف است، اولین بار در سال ۲۰۰۷ میلادی توسط آنتی‌ویروس‌های Prevx شناسایی شد. بررسی‌های اولیه نشان می‌داد که به ترتیب کشورهای ایران با آلودگی ۱۸۹ رایانه، اسرائیل با ۹۸ رایانه و سودان با ۳۲ رایانه را تحت تأثیر آلودگی‌های رایانه‌ای قرار داده است.(طالب‌پور، ۱۳۹۸، کد خبر: ۷۲٤۱۳۸۸) در سال‌های اخیر دامنه حملات به دیگر بخش‌های مهم زیرساختاری و مدیریتی ایران افزایش چشمگیر داشته است که چند نمونه مهم آن به شرح ذیل می‌باشد:

حمله به سامانه شهرداری تهران به‌عنوان آخرین نمونه در ماه جاری (تیر ۱٤۰۱) که بخش عمده فعالیت‌های شهرداری را تحت تأثیر قرار داده است.هدف قرار دادن سامانه وزارت فرهنگ و ارشاد اسلامی در فروردین ۱٤۰۱ حملاتی که روند فعالیتی برخط وزارت مذکور را با مشکلات زیاد مواجه نمود. یکی از مهم‌ترین حملات در پاییز سال ۱٤۰۰ در سامانه سوخت و جایگاه‌های توزیع فراورده‌های نفتی صورت پذیرفت که مشکلات مهمی را در سطح ملی برای شهروندان و شرکت ملی نفت ایجاد نمود. سایت مرکز آمار ایران طی یک حمله سایبری در خردادماه سال ۱۳۹۵ از دسترس خارج شد. این در حالی بود که چند روز پس‌ازاین نیز طی حمله‌ای سایت سازمان ثبت اسناد کشور هم از دسترس خارج شده و در همان سال اطلاعات حدود ۲۰ میلیون از مشترکان ایرانسل نیز به سرقت رفت. پس از استاکس‌نت، در سال ۱۳۹۱ سیستم‌های نفتی و هسته‌ای ایران مورد حمله قرار گرفت که قصد این حمله دزدی و تخریب اطلاعات بیان گردید. در ۲۷ آذر ۱٤۰۲ گروه هکری گنجشک درنده مدعی شد حمله سایبری علیه سیستم ملی تأمین سوخت ایران انجام دادیم و اکثر پمپ‌های سوخت آن را از کار انداختیم. (اقتصاد نیوز، ۱٤۰۲ کد خبر: ٦۱٦٤٦۲) حملات سایبری به زیرساخت‌های ایران همواره ادامه داشته که

حمله به زیرساخت دوربین‌های زندان اوین و نیز زیرساخت هواپیمایی ماهان از دیگر نمونه‌های بارز می‌باشد. مجموعه‌ای حملات سایبری که در ساختار تولیدی صنایع دفاعی کشور صورت پذیرفته که هرکدام موجب خسارات قابل‌توجه مالی و نرم‌افزاری شده است.

چند آمار مهم در حوزه امنیت سایبری به شرح زیر است:

الف: در سال ۲۰۲۲ بودجه جهانی برای امنیت سایبری به رقم ۷/۱۳۳ میلیارد دلار می‌باشد.

ب: ٦٨ درصد از مدیران و رهبران کسب‌وکارها، خطر حملات سایبری را به‌طورجدی احساس می‌کنند و ۷۱ درصد از حملات صورت گرفته با اهداف مالی و ۲۵ درصد از آن‌ها با هدف جاسوسی انجام گرفته است.

ج: ۵۰ درصد از بنگاه‌های بزرگ (با بیش از ۱۰ هزار کارمند) سالانه حدود ۱ میلیون دلار و یا بیشتر برای امنیت سایبری خود هزینه می‌کنند. ٤٣ درصد از آن‌ها بالای ۲۵۰ هزار دلار و تنها ۷ درصد از آن‌ها پایین‌تر از این رقم هزینه می‌کنند. نرخ بیکاری در میان متخصصان امنیت سایبری حدود صفر است و حدود ۵۰۰ هزار متخصص امنیت اطلاعات در جهان مشغول کار هستند. با توجه به تغییر شیوه‌ها و روش‌های درگیری می‌توان گفت که امروزه افزایش توانمندی ملی برای مقابله با ابهام، پیچیدگی و پویایی تهدیدات امنیتی، مهم‌ترین راهکار برای حفظ منافع در فضای سایبر می‌باشد. هم‌چنین امروزه سرنوشت جنگ‌ها را دیگر تخریب‌ها، انفجارها و عملیات فرسایشی تعیین نمی‌کنند، بلکه ازهم‌گسیختگی ظرفیت‌های فرماندهی و کنترل در فضای مجازی می‌تواند برای نتیجه برخوردها، بسیار تعیین‌کننده باشد. ازاین‌رو، در جنگ‌های نوین دیگر نمی‌توان ادعا کرد که پیروزی به این بستگی دارد که کدام‌یک از طرفین بیشترین مقدار سرمایه، نفرات و فن‌آوری را دارند، بلکه مهم این است که کدام‌یک از طرفین بهترین اطلاعات را در اختیار دارند و کلام آخر اینکه از مهم‌ترین راه‌های پیشگیری از حملات سایبری می‌توان به کاهش انتقال داده‌ها؛ دانلود دقیق؛ بهبود امنیت رمز عبور؛ به‌روزرسانی سیستم‌عامل و غیره اشاره نمود (اقبالی زارچ، مرکز مطالعات سیاسی و بین‌المللی)

٤-تجزیه و تحلیل یافته ها

٤-١-تأثیر تهدیدات سایبری بر امنیت جمهوری اسلامی ایران

ایران نیزمانندسایرکشورهاچه‌بسابیش ازآنان درمعرض تهدیدات سایبری فراوانی است به‌طوری‌که بیشترین حملات سایبری علیه جمهوری اسلامی ایران واز سوی کشورهای غربی به‌خصوص آمریکاواسرائیل اتفاق می‌افتد.ایران دربین تهدیدشوندگان سایبری رتبه نخست را دارد. همچنین از نظر دفاع سایبری نیز ایران یکی از قدرتمندترین کشورهایی است که تهدیدات سایبری را رصد نموده و خنثی می‌نماید، از این نظر ایران رتبه چهارم در جهان را داراست. بیشترین حملات سایبری در ایران برای ایجاد آشوب و بحران داخلی صورت می‌گیرد. افزایش استفاده از فضای مجازی و گسترش زیرساخت‌های فن‌آوری و مخابراتی و به‌طورکلی هوشمندسازی بسیاری از مشاغل و ادارات و سازمان‌های دولتی و خصوصی و به‌کارگیری سیستم‌های نوین توسط کاربران موجب شده است ایران به‌مراتب بیشتر از کشورهای همسایه خود در معرض تهدید قرار بگیرد. بیشترین هدف حملات سایبری در بخش نظامی، تأسیسات هسته‌ای و آسیب به زیرساخت‌های حیاتی کشور صورت می‌گیرد که می‌تواند موجب سردرگمی افراد و ایجاد بحران اجتماعی در کشور شود. نمونه این حملات، حمله به سامانه سوخت در سال ١٤٠٠ است که هزینه‌های مالی فراوانی به کشور وارد نمود و باعث ایجاد تنش‌های روانی زیادی در بین عموم مردم گردید اما مسئولین امر با اطلاع‌رسانی به‌موقع در جامعه و به‌کارگیری متخصصان خبره سریعاً اقدام به برطرف کردن مشکل نمودند. به‌هرحال نمی‌توان از حملات و تهدیدات سایبری پیشگیری نمود ولی می‌توان از شدت وقوع، افزایش خسارات و ایجاد هزینه‌های هنگفت جلوگیری نمود و این امر زمانی اتفاق خواهد افتاد که حکومت‌ها بتوانند با آموزش به‌موقع و به‌روز، آگاهی شهروندان و سازمان‌ها را در استفاده از فضای مجازی افزایش دهند و در صورت وقوع حملات اوضاع را کنترل نموده و از ایجاد بحران‌های

مختلف در جامعه پیشگیری کنند. به اعتقاد تاجیک ۱۳۸۲ تهدیدهای امنیتی متأثر از فضای مجازی در ایران عبارت‌اند از:

۱. اقدام‌های مخل امنیت و برانداز گروه‌های مسلح و غیرمسلح؛
۲. گسترش نابسامانی‌های اجتماعی از قبیل مواد مخدر، فساد اخلاقی، جرائم اجتماعی، سرقت و...؛
۳. شکاف بین اقلیت‌های قومی، مذهبی، زبانی با نظام و افزایش گرایش‌های تجزیه‌طلبانه قومی؛
٤. اقدام‌های تروریستی، خرابکاری و هکتیویسم؛
۵. آماده‌سازی افکار عمومی جهان علیه جمهوری اسلامی ایران در زمینه پرونده هسته‌ای و تشدید اقدام‌ها و تحریم‌ها علیه ایران؛
٦. اقدام سرویس‌های اطلاعاتی بیگانه به عملیات جاسوسی اینترنتی علیه جمهوری اسلامی ایران (صیاد و همکاران، ۳۱٦:۱۳۹۹).

۵-نتیجه‌گیری و پیشنهادات

انچه مسلم هست مساله تهدیدات سایبری هرگز به طور قطعی حل نخواهد شد. نگرانی در مورد اینکه آیا می‌توانیم به دستگاه‌ها، شبکه‌ها و اطلاعات موجود در آنها اعتماد کنیم ادامه خواهد داشت و نیاز به مدیریت دارد. چه از دیدگاه مسولین و چه از دید یک کاربر معمولی اگر به مشکلات امنیت سایبری نگاه شود، متوجه میشویم پیدا کردن راه حل قطعی بسیار دشوار است. به نظر می رسد که هیچ رشته یا حرفه ای نمی تواند مشکلات امنیت سایبری را برطرف کند ایران نیز مانند سایر کشورها چه بسا بیش از آنان در معرض تهدیدات سایبری فراوانی است به طوریکه بیشترین حملات سایبری علیه جمهوری اسلامی ایران و از سوی کشورهای غربی به خصوص آمریکا و اسرائیل اتفاق می افتد که باتوجه به نتایج این پژوهش حملات توانسته خساراتی رادرابعادگوناگون متوجه کشور کند.. ایران در بین تهدید شوندگان سایبری رتبه نخست را دارد.از طرفی افزایش استفاده از فضای مجازی و گسترش زیرساختهای فناوری و مخابراتی و به طور کلی هوشمندسازی

بسیاری از مشاغل و ادارات و سازمانهای دولتی و خصوصی و بکارگیری سیستمهای نوین توسط کاربران موجب شده است ایران به مراتب بیشتر از کشورهای همسایه خود در معرض تهدید قرار بگیرد. لذا لازم است هنگام حملات سایبری مسئولین امر با اطلاع رسانی به موقع در جامعه و بکارگیری متخصصان خبره سریعاً اقدام به برطرف کردن مشکل نمایند. به هر حال نمی توان از حملات و تهدیدات سایبری پیشگیری نمود ولی می توان از شدت وقوع، افزایش خسارات و ایجاد هزینه های هنگفت جلوگیری نمود و این امر زمانی اتفاق خواهد افتاد که مسئولین بتوانند با آموزش به موقع و به روز، آگاهی شهروندان و سازمانها را در استفاده از فضای مجازی افزایش دهند و در صورت وقوع حملات اوضاع را کنترل نموده و از ایجاد بحرانهای مختلف در جامعه پیشگیری کنند. شاید اصلی‌ترین راهکار برای داشتن اینترنتی ایمن، اجرای یک طرح جامع امنیت ملی در حوزه سایبری باشد. طرحی که شبکه ملی اطلاعات هم می‌تواند از اجزای آن باشد. در این طرح می‌بایست به حوزه‌های آموزش عمومی، تقویت سیستم‌های دفاعی و توان مقابله و اجرای عملیات در هر سطح علیه مهاجم موردتوجه قرار گیرد. همچنین نیاز است ملاحظات مربوط به پدافند غیرعامل در همه طرح‌های مربوط به شبکه‌های ارتباطی و الزام دستگاه‌های اجرایی به استفاده از توان داخلی (تا حد امکان) مدنظر باشد. از طرفی با توجه به ارتباط مستقیم مباحث سایبری با فناوری هوش مصنوعی لازم است مسئولین امر توجه لازم و کافی به این مقوله داشته باشند و از تمام ظرفیت‌ها و توانایی‌های متخصصین این امر جهت تقویت زیرساخت‌های سایبری، استفاده لازم را به کار بگیرند.

از سوی دیگر به نظر می‌رسد تقویت رویه‌های دیپلماتیک در قالب افزایش مشارکت و فعالیت برای یافتن راه‌های پیگیری حقوقی بین‌المللی حملات سایبری به ایران ضرورتی اجتناب‌ناپذیر است. همچنین تلاش برای سهیم شدن در مدیریت اینترنت جهانی از طریق حضور در مجامع مؤثر و مرتبط، اقداماتی است که نیازمند تحرک و پویایی بیشتر وزارت امور خارجه در این راستا می‌باشد.

کتاب نامه

- ابراهیمیان، بهمن؛ توشه، علی و پورهادی، ابراهیم (۱۳۹٤)، «راهکارهای مقابله با تهدیدهای سایبری علیه جمهوری اسلامی ایران با تأکید بر نقش فن‌آوری و منابع انسانی»، ***فصلنامه راهبرد دفاعی***، سال سیزدهم، شماره ۵۰، ص ۸۷-۱۱۵.
- اسلامی، مسعود (۱۳٦۹)، «جایگاه و موقعیت کشورهای کوچک در نظام بین‌المللی»، ***مجله سیاست خارجی***، سال ٤، شماره ٤.
- بمان اقبالی زارچ، علی (۱٤۰۱)، «تهدیدات و حملات سایبری بر علیه ایران»، ***مرکز مطالعات سیاسی و بین‌المللی IPIS***.
- بیات کاه‌دان، محمد و جعفری، عیسی (۱٤۰۲)، «مصنوعی در امنیت سایبری» *هجدهمین کنفرانس ملی مهندسی برق، کامپیوتر و مکانیک*، شیروان https://civilica.com/doc/1686186.
- تاجیک، محمدرضا (۱۳۸۲)، «***مقدمه‌ای بر استراتژی‌های امنیت ملی ج.ا.ا رهیافت‌ها و راهبردها***»، نشر فرهنگ گفتمان.
- ترابی، قاسم (۱۳۹۷). «چالش‌ها و آسیب‌پذیری‌های جمهوری اسلامی ایران در فضای سایبر»، ***مطالعات راهبردی***، سال ۲۱، شماره ۱.
- تریف، تری و دیگران (۱۳۸۳)، «***مطالعات امنیتی نوین***»، مترجمین علیرضا طیب ووحید بزرگی، تهران: پژوهشکده مطالعات راهبردی.
- _____ «حملات سایبری و میدان جنگ الکترونیک»، ***سایت وزارت فرهنگ و ارشاد اسلامی*** https://herasat.farhang.gov.ir/fa/articl/cyberattaks/cyberattaks5
- صیاد، محمدکاظم؛ امینی، آرمین و طاهری، ابوالقاسم (۱۳۹۹)، «تهدیدهای سایبری و اقدامات امنیتی در فضای مجازی- بررسی رویکردهای ایالات‌متحده آمریکا و جمهوری اسلامی ایران»، ***فصلنامه علمی امنیت ملی***، سال ۱۰، شماره ۳۸.
- عبدالله خانی، علی (۱۳۸۹)، «***جنگ نبرد ۳، نبرد در عصر اطلاعات***»، موسسه فرهنگی مطالعاتی و تحقیقات بین‌المللی ابرار معاصر تهران.

- عبدالله خانی، علی (۱۳۸۲)، «***نظریه‌های امنیت: مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی(۱)***»، جلد اول، تهران: مؤسسه فرهنگی مطالعات و تحقیقات ابرار معاصر تهران.
- عسگرخانی، ابومحمد و رحمتی، رضا (۱۳۸۹)، «نظریه واقع‌گرایی و امنیت بین‌الملل» ***فصلنامه سیاست خارجی***، سال ۲٤،شماره ۱.
- طالب‌پور، عطیه (۱۳۹۸)، «تاریخچه حملات سایبری در ایران و جهان»، ***خبرگزاری باشگاه خبرنگاران جوان***، ۲۱ بهمن ۱۳۹۸.
- رئیسی،لیلا(۱٤۰۲)«صیانت ازحقوق شهروندان درفضای سایبردرپرتونسل سوم حقوق بشرباتاکید برحقوق ایران»،فصلنامه مطالعات بین الملل،سال۲۰،شماره ۳،زمستان۱٤۰۲
- سایت خبری اقتصاد نیوز به نشانی:www.eghtesadnews.com۲۷/۰۹/۱٤۰۲
- صدوقی، مرادعلی (۱۳۸٤)، «***تکنولوژی اطلاعاتی و حاکمیت ملی***»، تهران، وزارت امور خارجه.
- قاسمی، ح (۱۳۷۲)، «برداشت‌های متفاوت از امنیت ملی»، ***مجله سیاست دفاعی***، سال اول، شماره ۲.
- کاظمی، علی‌اصغر (۱۳۷۰)، «***مدیریت بحران‌های بین‌المللی***»، تهران، دفتر نشر فرهنگ اسلامی.
- مرادیان، امید (۱٤۰۲)، «***هوش مصنوعی در امنیت سایبری***»، آکادمی محسن مدحج.
- هافندورن، هلگا (۱۳۷۱)، «معمای امنیت»، ترجمه علیرضا طیب، ***مجله سیاست خارجی***، شماره ٤.

- یزدان فام، محمود (۱۳۸٦)، «دگرگونی در نظریه‌ها و مفهوم امنیت بین‌الملل»، **فصلنامه مطالعات راهبردی**، شماره ۳۸،

- Ahmed Jamal, A., et al., (2021). "***A review on security analysis of cyber physical systems using machine learning***". Mater. Today: Proc.
- Alkatheiri, M.S., Chauhdary, S.H., Alqarni, M.A., (2021). "***Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications***". Sustain. Energy Technol. Assess. 45, 101219.

- Alzubaidi, A., (2021). "***Cybercrime awareness among Saudi nationals: Dataset***". Data Brief 36, 106965.
- Eriksson, J., & Giacomello, G. (2006). "The information revolution, security, and international relations: (IR) relevant theory?". ***International political science review,*** 27(3), 221-244.
- Furnell, S, M, and Warren, M, J (1999), "Computer Hacking and Cyber Terrorism: the Real Threats in the New Millennium"?, ***Computers & Security,*** vol.18.
- Jay Hoofnagle, Chris, (2022), "***Cybersecurity in Context, PUBLISHER***" TBD, BOOK-WEBSITE.COM
- Krishnasamy, V., Venkatachalam, S., (2021). "***An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using index-level Boundary Pattern Convergent Encryption algorithm***". Mater. Today: Proc
- Nguyen, D.C.L., Golman, D.W., (2021). "***Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. Comput***". Law Secur. Rev. 40, 105521.
- Palmieri, M., Shortland, N., McGarry, P., (2021). "***Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. Comput. Hum***". Behav. 120, 106745.
- Yuchong, Li., Qinghui, Liu., (2021). "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments", ***journal homepage***: www.elsevier.com/locate/egyr, Energy Reports.
- Ogbanufe, O., (2021). "Enhancing end-user roles in information security: Exploring the setting, situation, and identity". ***Comput***. Secur. 108, 102340.
- Zhang, J., (2021). "Distributed network security framework of energy internet based on Internet of Things. Sustain". Energy Technol. Assess. 44, 101051. Schmitt, M. zilkowski,k.(2019)international law for cyberspace.at
- :http://www.ccdoce.org/uploads/2019/05trends-intlaw_a4_final.pdf.2019.