

Examining the threats of cyberwarfare and how it affects

Iran's national security

Received: 2025/03/16

Accepted: 2025/5/11

Behrouz Nasiri: PhD student in International Relations, Hamedan Branch, Islamic Azad University, Hamedan, Iran

E-mail: 364behnasiri@gmail.com

ORCID ID

0000-0002-6795-6782

Qasem Torabi: Associate Professor of International Relations, Hamedan Branch, Islamic Azad University, Hamedan, Iran (Corresponding Author)

E-mail: ghasemtoraby@yahoo.com

ORCID ID: 0000-0002-5359-9390

Alireza Rezaei: Associate Professor of International Relations, Hamedan Branch, Islamic Azad University, Hamedan, Iran

E-mail: alirezarezaei@gmail.com

ORCID ID: 0000-0002-2865-4343

Abstract

With the revolution in information technology in the 21st century and the emergence of new media, the concept of security has undergone tremendous changes and the effective components have also changed, and the power of governments has also faced a new challenge. The purpose of this research is to investigate 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 or shortcomings in the field of cyber security with regard to the threats in the cyberspace is one of the other goals of the current research, which wants to answer the basic question of how cyber threats affect the security of the Islamic Republic of Iran in an analytical-descriptive method. The findings of the research indicate that the Islamic Republic of Iran is one of the most important target countries for cyber attacks in various fields, and in this regard, acceleration in equipping infrastructures and investing in the field of dealing with cyber threats is one of Iran's strategic approaches in this regard. It is considered to be an area that is analyzed in more dimensions in this research.

بررسی تهدیدات جنگ سایبری و نحوه تأثیر آن بر امنیت ملی ایران

پذیرش: ۱۴۰۴/۰۳/۲۱

ارسال: ۱۴۰۳/۱۲/۲۶

چکیده:

با بروز انقلاب در فناوری اطلاعات در قرن بیست و یک و به وجود آمدن رسانه های جدید، مفهوم امنیت دستخوش تغییرات شگرفی شده و مؤلفه های اثر گذار در آن را نیز متحول کرده است و قدرت دولت ها را نیز با چالش جدیدی رو برو کرده است. هدف از این پژوهش، بررسی تا ثیرات فضای سایبری بر امنیت ملی جمهوری اسلامی ایران در حوزه های مختلف بویژه حوزه های سیاسی-امنیتی می باشد. همچنین کشف نقاط ضعف و یا کاستی های موجود در حوزه امنیت سایبری با توجه به تهدیدات موجود در فضای مجازی از دیگر اهداف پژوهش حاضر می باشد که بصورت روش تحلیلی-توصیفی به این پرسش اساسی میخواید پاسخ دهد که تهدیدات سایبری چگونه بر امنیت جمهوری اسلامی ایران تأثیر میگذارد؟ امری که یافته های تحقیق بیانگر آن است که جمهوری اسلامی ایران یکی از مهمترین کشورهای هدف حملات سایبری در حوزه های مختلف بوده و از این نظرتسریع در تجهیز زیر ساختها وسرمایه گذاری در حوزه مقابله با تهدیدات سایبری از جمله رویکردهای راهبردی ایران در این حوزه بشمار می رود که در این پژوهش به واکاوی ابعاد بیشتر آن پرداخته می شود.

کلید واژه ها: فضای سایبر، تهدیدات امنیتی، جنگ سایبری، امنیت ملی، هوش مصنوعی، ایران

بهروز نصیری

دانشجوی دکتری تخصصی روابط بین الملل، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران

کد ارکید

۰۰۰۰-۰۰۰۲-۶۷۹۵-۶۷۸۲

E-mail: 364behnasiri@gmail.com

قاسم ترابی

دانشیار روابط بین الملل، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران (نویسنده مسئول)

E-mail: ghasemtoraby@yahoo.com

کد ارکید:

۰۰۰۰-۰۰۰۲-۵۳۵۹-۹۳۹۰

علیرضا رضایی

دانشیار روابط بین الملل، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران

E-mail: alirezarezaei@gmail.com

کد ارکید:

۰۰۰۰-۰۰۰۲-۲۸۶۵-۴۳۴۳

Extended abstract

Introduction: Cyberspace has been a concern of individuals for many years, but now it has become a political, security, and economic issue for everyone. The development of this technology created the impression that cyber governance is a technical issue, not a political one. However, the reality is that developments in the international system have transformed the cyber issue from an engineering issue to an issue between different sciences and governmental and state structures, so that cyberspace is removed from the control of individuals, and actors in this field have gone beyond the borders of a country and have a direct impact on the governance space of other states. The expansion of cyberspace has led to the emergence of virtual borders, and therefore a realistic understanding of security threats depends on paying attention to software factors that are actually the intermediary between the security environment of countries and hardware, and therefore perceptions of the concept of national security in this space have been challenged. One of the main security threats in the era of communication and globalization for countries should be considered in the cyber domain, a clear example of which is the computer attack on Iran's nuclear and electronic facilities by the United States. On the other hand, cyber threats are a new phenomenon in recent decades that have emerged and grown with the evolution of information technology and the expansion of global communications through the vast Internet network worldwide in the form of various viruses, worms, crimes, hackers, and Internet attacks, so that today the challenge of cyber threats seems both important and complex. Cyber threats have unique characteristics. On the one hand, these threats include a wide range of legal, technical, organizational, and cultural obstacles, and on the other hand, low cost, tremendous impact, and lack of public transparency in cyberspace have led many players to enter this field. It seems that the low entry costs, the anonymity of individuals, the unclear geographical territory of the threat or threats in this space, the tremendous influence and general lack of transparency in cyberspace have caused strong and weak actors, including governments, organized and terrorist groups, and even individuals entering this space, to create threats such as cyberwar, cybercrime, cyberterrorism, cyberespionage, and the like. This point distinguishes cyber threats from traditional national security threats, which are largely verbal in nature and whose actors are nation-states that are identifiable in a specific geographical territory, and has caused national security in its traditional sense to be challenged and considered ineffective in this space.

In the present study, considering the capacities of cyberspace, we will examine and analyze the destructive effects that cyber threats can have on the country's national security and what important changes these threats will bring to national security. Another topic addressed in this study is the investigation of the most important cyber attacks against Iran. On the other hand, in this study, we seek to examine the hypothesis that cyber threats, due to their characteristics such as low cost, anonymity, international responsibility, and widespread impact on the target country, weaken the security of the Islamic Republic in various military, political, economic, cultural, and social dimensions. Also, considering the direct connection between artificial intelligence and cyberspace, we seek to examine the application of artificial intelligence to cybersecurity in this study.

Objective: In the present era, cyberspace and the cyber threats present in it have become an important part of security issues, especially national and cyber security of countries and organizations, in order to prevent sabotage and threats caused by it. Therefore, the importance and complexities arising from the nature of cyber threats and their unique characteristics and manifestations have made it necessary and inevitable to recognize and deal with them in order to prevent adverse and negative effects on various areas such as national security of countries. In this regard, the nature of this space and the recognition of the conditions and requirements for countries to become a safe space against this type of threat are among the first priorities of the security sector of countries, especially the Islamic Republic of Iran, to confront external threats, especially in the sanctions environment and external interventions and pressures to affect the national security of the Islamic Republic of Iran, which is dealt with in a specialized manner in this research due to its importance and influential position.

Method: The present research, using a descriptive-analytical method and based on a qualitative study, has examined the consequences of these attacks on Iran's national security and analyzed the challenges in this area. The research findings show that weakness in institutional coordination, dependence on foreign technologies, and a national policy vacuum have increased the country's cyber vulnerability. In this regard, developing a comprehensive cybersecurity strategy, strengthening local infrastructure, developing international cooperation, and establishing a national cybersecurity coordination center have been proposed as suggested solutions. Without taking preventive and coordinated measures, cyber threats could become one of Iran's most important security challenges in the coming years.

Findings and Conclusion: What is certain is that the issue of cyber threats will never be definitively resolved. Concerns about whether we can trust the devices, networks, and information contained in them will continue and need to be managed. Whether from the perspective of officials or an ordinary user, if we look at cybersecurity problems, we realize that finding a definitive solution is very difficult. It seems that no field or profession can solve the problems of cybersecurity. Iran, like other countries, is perhaps more exposed to numerous cyber threats than they are. Most cyber attacks against the Islamic Republic of Iran occur from Western countries, especially the United States and Israel. According to the results of this study, the attacks have caused damage to the country in various dimensions. Iran ranks first among those threatened by cyber threats. On the other hand, the increase in the use of cyberspace and the expansion of technological and telecommunications infrastructures, and in general, the smartization of many businesses, offices, and government and private organizations, and the use of modern systems by users, have caused Iran to be exposed to threats much more than its neighboring countries. Therefore, it is necessary that when cyber attacks occur, the authorities take immediate action to resolve the problem by informing the community in a timely manner and employing expert experts. In any case, cyber attacks and threats cannot be prevented, but the severity of the occurrence, the increase in damages, and the creation of huge costs can be prevented. This will happen when the authorities can increase the awareness of citizens and organizations in the use of cyberspace through timely and up-to-date training and, in the event of attacks, control the situation and prevent various crises in society. Perhaps the most important solution to having a safe Internet is to implement a comprehensive national security plan in the cyber field. A plan that the National Information Network can also be a part of. This plan should address the areas of public education, strengthening defense systems, and the ability to confront and execute operations at every level against the attacker. It is also necessary to consider considerations related to passive defense in all plans related to communication networks and the requirement for executive agencies to use domestic capacity (to the extent possible). On the other hand, given the direct connection between cyber issues and artificial intelligence technology, it is necessary for the authorities to pay due and sufficient attention to this category and to make the necessary use of all the capacities and abilities of experts in this field to strengthen cyber infrastructure. On the other hand, it seems that strengthening diplomatic procedures in the form of increasing participation and activity to find ways to pursue international legal cyber attacks on Iran is an inevitable necessity. Also, efforts to participate in the management of the global In-

ternet through participation in effective and relevant forums are measures that require greater mobility and dynamism on the part of the Ministry of Foreign Affairs in this regard

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

چکیده مبسوط

مقدمه: موضوع سایبری سالهای زیادی دغدغه افراد خاص بوده اما حالا تبدیل به یک مسئله سیاسی و امنیتی و اقتصادی برای همگان شده است. توسعه این تکنولوژی این تصور را ایجاد مینمود که حکمرانی سایبری یک مساله فنی است و نه سیاسی. اما واقعیت این است که تحولات نظام بین الملل مساله سایبری را از یک موضوع مهندسی به مساله بین علوم مختلف و ساختارهای حکومتی و دولتی تبدیل نموده است به طوری که فضای سایبری را از تسلط افراد خاص خارج نموده و بازیگران این عرصه از مرزهای یک کشور فراتر رفته و بر فضای حکمرانی سایبر دولتها نیز تاثیر 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 سراسر جهان 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، تاثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران زیادی به این عرصه وارد شوند. به نظر می رسد در این میان هزینه های کم ورود، ناشناس بودن افراد، مشخص نبودن قلمرو جغرافیایی تهدیدکننده یا تهدیدکنندگان در این فضا، تاثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران قوی و ضعیف اعم از دولت ها و گروه های سازمان یافته و تروریستی و حتی افراد وارد شده به این فضا؛ تهدیدهایی همچون جنگ سایبری، جرائم سایبری، تروریسم سایبری، جاسوسی سایبری و مانند آن ها را به وجود آورند. همین نکته، تهدیدهای سایبری را از تهدیدهای سنتی امنیت ملی که تا حدود زیادی از ماهیت شفاهی برخوردارند و بازیگران آن رادولت - ملت هایی تشکیل می دهند که در یک قلمرو مشخص جغرافیایی قابل شناسایی هستند، متمایز کرده و سبب شده است امنیت ملی به مفهوم سنتی آن در این فضا به چالش کشیده شده و ناکارآمد به حساب آید. در پژوهش حاضر با توجه به ظرفیت های فضای سایبری، به بررسی واکاوی این مهم می پردازیم که تهدیدات سایبری چه تأثیرات مخربی می توانند بر امنیت ملی کشور داشته باشند و این تهدیدات، امنیت ملی را با چه تغییرات مهمی مواجه می کنند و بررسی مهم ترین حملات سایبری علیه ایران از دیدگاه مباحثی است که در این پژوهش به آن پرداخته می شود. از طرفی در این تحقیق به دنبال بررسی این فرضیه که تهدیدات سایبری به دلیل ویژگی های همچون هزینه پایین، گمنامی و داشتن مسئولیت بین المللی و تاثیرگذاری گسترده بر کشور هدف، امنیت جمهوری

اسلامی را در ابعاد مختلف نظامی، سیاسی، اقتصادی، فرهنگی و اجتماعی تضعیف می‌کنند، می‌باشیم و همچنین با توجه به ارتباط مستقیم هوش مصنوعی با فضای سایبر- در پی بررسی کاربرد هوش مصنوعی بر امنیت سایبری- در این پژوهش هستیم.

هدف: در عصر حاضر فضای مجازی و تهدیدات سایبری موجود در بستر آن به بخش مهمی از موضوعات امنیتی بویژه امنیت ملی و سایبری کشورها و سازمانها جهت جلوگیری از خرابکاری و تهدیدات متاثر از آن تبدیل شده است. از این رو، اهمیت و پیچیدگی های ناشی از ماهیت تهدیدهای سایبری و ویژگیها و نمودهای منحصر به فرد آن، شناخت و چگونگی مقابله با آن برای جلوگیری از آثار سوء و منفی بر حوزه ای مختلف همچون امنیت ملی کشورها را به امری ضروری و اجتناب ناپذیر تبدیل کرده است. در این راستا، ماهیت شناسی این فضا و تشخیص شرایط و الزام های تبدیل شدن کشورها به فضایی امن در مقابل این دسته از تهدیدات، از نخستین اولویت های حوزه امنیتی کشورها بویژه جمهوری اسلامی ایران برای مقابله با تهدیدات خارجی بویژه در فضای تحریمی و مداخلات و فشارهای خارجی برای اثر گذاری بر امنیت ملی جمهوری اسلامی ایران بشمار می رود که بنابر اهمیت و جایگاه تاثیرگذاری آن در این پژوهش به صورت تخصصی به آن پرداخته می شود.

روش: پژوهش حاضر با استفاده از روش توصیفی-تحلیلی و بر مبنای مطالعه کیفی، به بررسی پیامدهای این حملات بر امنیت ملی ایران پرداخته و چالش های موجود در این حوزه را تحلیل کرده است. یافته های تحقیق نشان می دهد که ضعف در هماهنگی نهادی، وابستگی به فناوری های خارجی و خلأ سیاست گذاری ملی، آسیب پذیری سایبری کشور را افزایش داده است. در این راستا، تدوین راهبرد جامع امنیت سایبری، تقویت زیرساخت های بومی، توسعه همکاری های بین المللی و ایجاد مرکز ملی هماهنگی امنیت سایبری به عنوان راهکارهای پیشنهادی ارائه شده اند. بدون اتخاذ تدابیر پیشگیرانه و هماهنگ، تهدیدات سایبری می توانند به یکی از مهم ترین چالش های امنیتی ایران در سال های آینده تبدیل شوند.

یافته ها و نتیجه گیری: آنچه 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 می‌رسد که هیچ رشته یا حرفه ای نمی‌تواند 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 می‌افتد که باتوجه به نتایج این پژوهش حملات توانسته خساراتی را در ابعاد گوناگون متوجه کشور کند. ایران در بین تهدید شونده‌گان 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 نمی‌توان از حملات و تهدیدات سایبری پیشگیری نمود ولی می‌توان 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 سهمیم 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.

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

موضوع سایبری سالهای زیادی دغدغه افراد خاص بوده اما حالا تبدیل به یک مسئله سیاسی و امنیتی و اقتصادی برای همگان شده است. توسعه این تکنولوژی این تصور را ایجاد مینمود که حکمرانی سایبری یک مساله فنی است و نه سیاسی. اما واقعیت این است که تحولات نظام بین الملل مساله سایبری را از یک موضوع مهندسی به مساله بین علوم مختلف و ساختارهای حکومتی و دولتی تبدیل نموده است به طوری که فضای سایبری را از تسلط افراد خاص خارج نموده و بازیگران این عرصه از مرزهای یک کشور فراتر رفته و بر فضای حکمرانی سایر دولتها نیز تاثیر 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 سراسر جهان 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، تاثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران زیادی به این عرصه وارد شوند. به نظر می رسد در این میان هزینه های کم ورود، ناشناس بودن افراد، مشخص نبودن قلمرو جغرافیایی تهدیدکننده یا تهدیدکنندگان در این فضا، تاثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران قوی و ضعیف اعم از دولت ها و گروه های سازمان یافته و تروریستی و حتی افراد وارد شده به این فضا، تهدیدهایی همچون جنگ سایبری، جرائم سایبری، تروریسم سایبری، جاسوسی سایبری و مانند آن ها را به وجود آورند. همین نکته، تهدیدهای سایبری را از تهدیدهای سنتی امنیت ملی که تا حدود زیادی از ماهیت شفاهی برخوردارند و بازیگران آن رادولت - ملت هایی تشکیل می دهند که در یک قلمرو مشخص جغرافیایی قابل شناسایی هستند، متمایز کرده و سبب شده است امنیت ملی به مفهوم سنتی آن در این فضا به چالش کشیده شده و ناکارآمد به حساب آید. در پژوهش حاضر با توجه به ظرفیت های فضای سایبری، به بررسی واکاوی این مهم می پردازیم که تهدیدات سایبری چه تأثیرات مخربی می توانند بر امنیت ملی کشور داشته باشند و این تهدیدات، امنیت ملی را با چه تغییرات مهمی مواجه می کنند و بررسی مهم ترین حملات سایبری علیه ایران از دیگر مباحثی است که در این پژوهش به آن پرداخته می شود. از طرفی در این تحقیق به دنبال بررسی این فرضیه که تهدیدات سایبری به دلیل ویژگی های همچون هزینه پایین، گمنامی و داشتن مسئولیت بین المللی و تاثیرگذاری گسترده بر کشور هدف، امنیت جمهوری اسلامی را در ابعاد مختلف نظامی، سیاسی، اقتصادی، فرهنگی و اجتماعی تضعیف می کنند، می باشیم و همچنین با توجه به ارتباط مستقیم هوش مصنوعی با فضای سایبر - در پی بررسی کاربرد هوش مصنوعی بر امنیت سایبری - در این پژوهش هستیم.

بررسی تحقیقات سایبرپژوهشگران درحوزه تهدیدات سایبری و امنیت ملی متوجه می‌شویم که افراد زیادی در این مقوله تحقیق نموده و به نتایج گوناگون دست یافته‌اند که در ادامه به بخش کوچکی از این پژوهش‌ها اشاره خواهیم کرد: (بیات کاه‌دان، محمد، جعفری عیسی ۱۴۰۲) در مقاله [هوش مصنوعی و امنیت سایبری] با استفاده از هوش مصنوعی به تقویت امنیت سایبری و شناسایی و دفع حملات سایبری پرداخته. (رئیس، لیلیا ۱۴۲۰) در مقاله [اصیان از حقوق شهروندان در فضای سایبردر پرتونسل سوم حقوق بشر] تاکید بر حقوق ایران، آدری پاسخ به این سؤال فضای سایبر چگونه می‌تواند در صیانت از حقوق شهروندی از حیث انطباق با قوانین نسل سوم حقوق بشر مؤثر باشد. (Chris Jay Hoof ۲۰۲۲) در مقاله Cybersecurity in Context، به امنیت سایبری را به عنوان یک مشکل «شرور» تعریف می‌کند، به این معنی که امنیت سایبری فقط قابل مدیریت است، نه حل کردن. (Yuchong Li و Qinghui Liu ۲۰۲۱)، با مقاله A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments و نتیجه امنیت سایبری اطلاعات لحظه‌ای درباره آخرین داده‌های فن‌آوری اطلاعات را دنبال می‌کند. تاکنون روش‌های مختلفی برای جلوگیری از حملات سایبری و یا کاهش آسیب‌های 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 انجام شده در این باره به ویژه آنچه در داخل انجام شده است بادر نظر گرفتن یک تعداد محدودی از تأثیرات عرصه سایبری رو تهدیدات متأثر از آن بر امنیت ملی مورد بررسی و تحلیل قرار گرفته است به نوعی که در بیشتر پژوهش‌ها به دنبال ارزیابی آن و چگونگی اثرپذیری آن از محتوای فضای سایبر هستند. ارزش کاربردی مؤلفه‌های امنیت ملی در بخش‌های مختلف آنکه توجه به آن‌ها لازمه حفظ جنبه‌هایی از امنیت ملی است در این پژوهش‌ها نادیده گرفته شده است. همچنین این پژوهش‌ها در مراحل سطحی به مسئله پرداخته و به علل عمیقی که منجر به اثرگذاری تهدیدات سایبری بر حوزه‌های حساس زیرساخت‌های نظامی، هسته‌ای و صنعتی 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 و بحران امنیتی حاصل از آن و همچنین تأثیر و کاربرد هوش مصنوعی بر فضای سایبر و در نهایت هشدارهای راهبردی لازم برای غلبه بر این بحران امنیتی متأثر از تهدیدات سایبری می‌پردازیم.

با عنایت به این مسئله که پژوهش حاضر بر پایه‌های مکتب واقع‌گرایی متکی است و از آنجایی که مباحث مربوط به حملات سایبری ارتباط مستقیم با محیط آنارشیک نظام بین‌الملل دارد (به دلیل برتری جویی مهاجم) لذا با محور قرار دادن مفاهیم اصلی واقع‌گرایی، بحث را پیگیری می‌کنیم. برای اینکه مقوله استقرار امنیت را بر اساس این مکتب توضیح دهیم ابتدا شش مفروض اصلی مکتب رئالیسم را امتدکر می‌شویم: محیط آنارشیک نظام بین‌الملل: هیچ قدرت فائقه‌ای در نظام بین‌الملل برای منع

کردن از کاربرد زوریکی علیه دیگری وجود ندارد، دولت سالاری: دولت‌ها بازیگران اصلی سیاست بین‌المللی هستند، قدرت: ویژگی تعریف‌شده محیط بین‌الملل که دولت‌ها از آن بهره‌مندند، عقلانیت: دولت‌ها محاسبه هزینه - فایده انجام کارهای خود را قبل از انجام عمل می‌کنند، بقا: که پیش شرط دسترسی به همه اهداف ملی است و خودیاری: برای بقا می‌توان به تضمین دیگری متکی بود. البته توجه واقع‌گرایی به درس‌های تاریخ نیز راهنمای این رهیافت برای توضیح امنیت است (عسگرخانی و رحمتی، ۱۳۸۹: ۱۴۰).

۲-۲-۲- نظریه واقع‌گرایی

واقع‌گرایان معتقدند در سطح سیاست داخلی، مسئله‌ای به نام امنیت وجود نداشته و امنیت صرفاً در سطح بین‌المللی معنا می‌یابد. به بیان دیگر، امنیت ملی نزد آنان چیزی جز امنیت بین‌الملل نیست و در این راستا ناامنی و ویژگی بارز نظام بین‌الملل است (عبدالله خانی، ۱۳۸۲: ۷۰). از نظر واقع‌گرایان، عدم امنیت اصلی‌ترین مسئله، قدرت مهم‌ترین ابزار، دولت مهم‌ترین بازیگر و جنگ، بارزترین جلوه بروز ناامنی در عرصه بین‌المللی است (یزدان فام، ۱۳۸۶: ۷۳۱). بنابراین، محور تمرکز واقع‌گرایی در موضوع امنیت، نظامی است. همان‌طور که استغن‌والث تعریف می‌کند، مطالعات امنیتی، مطالعه تهدید، استفاده و کنترل نیروی نظامی است. جدای از مسائل نظامی، سایر عوامل هم در بحث امنیت می‌توانند مهم باشند؛ اما واقع‌گرایان و نوواقع‌گرایان معمولاً تنها تاجایی آن‌ها را مهم می‌شمارند که به توسعه توانایی‌های نظامی کمک کند (تریف، ۱۳۸۳: ۸۵). از نظر واقع‌گرایان، هر چیزی ممکن است بر امنیت 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 خواهند گرفت. (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 و رشد اندیشه بشردر تفسیر آن دارد. پارادایم امنیت ملی در بستر تاریخی مشخصی ظهور کرد. با تولد دولت ملی در قرن هفدهم میلادی و علاقه‌ای 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 با چشم‌پوشی از بخشی از اختیارات خود و تنفیذ آن به یک حکمران تسلیم او می‌شوند و از انتظار تأمین صلح رادارند چنین دولتی با برخورداری از پشتوانه مردمی، خود را موظف به تأمین امنیت، آن‌ها می‌بیند و بهترین و کوتاه‌ترین مسیر را در تقویت و تجهیز بنیه دفاعی کشور برای دفع تهاجمات احتمالی می‌یابد؛ به‌طوری‌که در شرایط محدودیت منابع با ارزش جهانی، هر کس که قوی‌تر است، در رقابت بر سر تصاحب این‌گونه منابع برنده خواهد شد؛ بنابراین، بازیگران صحنه جهانی هرگز خود را دور از تهدید نمی‌دانند، بلکه سایه تهدیدی دائمی را بر سر خود احساس می‌کنند. در نتیجه، هر بازیگری کسب قدرت برای دفاع از خود را شرط اولیه بقا می‌شمارد. در این دیدگاه، رابطه مفروض میان امنیت و قدرت، رابطه‌ای همیشگی و مستقیم است هر اندازه 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 دیگری رابطه‌ای معکوس برقرار است به این معنا که امنیت یکی به بهای ناامنی دیگری حاصل می‌شود. با وجود چنین رابطه‌ای میان امنیت ملت‌ها، امنیت هر واحد به صورت مجزا از دیگران تحقق می‌یابد و جمع میان امنیت ملت‌ها نه تنها 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 رانظریه پردازی 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 کند و در آستانه جنگ جهانی دوم از هم فروپاشید، سازمان ملل نیز با ظهور دو قدرت برتر، یعنی ایالات متحده آمریکا و اتحاد جماهیر شوروی و دعوی غیرقابل جمع آن‌ها برای سلطه بر جهان که به جنگ سرد انجامید، عملاً کارایی خود را از دست داد. در نتیجه 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 بود که هر کشوری برای دفع تهدیدهای احتمالی، آمادگی جنگی را ضروری و لازم می‌داند و در شرایط بحرانی، تهدید به استفاده از نیروهای نظامی به منظور تحصیل امتیاز یا عدم تمکین در مقابل خواسته حریف، به شکل یکی از ابزارهای اعمال قدرت درآمد (کاظمی، ۱۳۷۰: ۷۷). به این ترتیب، حفظ برتری تکنولوژیک در رقابت تسلیحاتی به یکی از مهم‌ترین اهداف قدرت‌های بزرگ و به تبع 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، بازگیزی نبود. انگلستان بیش از یک قرن چنین نقشی را در حوزه خلیج فارس ایفا کرد (اسلامی، ۱۳۶۹: ۵۵۲). در این دیدگاه، رابطه مفروض میان امنیت و قدرت، 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 برقرار است به این معنا که امنیت یکی به بهای ناامنی دیگری حاصل می‌شود. با وجود چنین رابطه‌ای میان امنیت ملت‌ها، امنیت هر واحد به صورت مجزا از دیگران تحقق می‌یابد و جمع میان امنیت ملت‌ها نه تنها دشوار، بلکه ناممکن است (قاسمی، ۱۳۷۲: ۵۹).

۳- یافته‌ها و تجزیه و تحلیل داده‌ها

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

در عصر اطلاعات، مفهوم امنیت ملی گسترش یافته و از گردش آزاد اطلاعات در سراسر جهان از راه اینترنت متأثر می‌شود. امروزه فضای سایبر بر نحوه ادراک از جنگ و نحوه انجام گرفتن آن تأثیر گذاشته است، به طوری که دیگر نه فقط مرزهای جغرافیایی، بلکه انواع مرزها به ویژه مرزهای هویتی از سوی جنگ اطلاعاتی مورد تهدید قرار دارد (Eriksson & Giacomello, ۲۰۰۶: ۲۳۲). مبرهن است که جنگ سایبری امنیت کشورها را به خطر انداخته و در مواردی حتی خسارات سهمگینی را در دنیای فیزیکی به بار آورده (رئیس، لیلیا: ۵۱. schmitt&zolowski, 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:

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 سیایاد 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^۱ وارد می‌کند. اصول در دسترس بودن ادعا می‌کند که سیستم‌ها، عملکردها و داده‌ها باید بر اساس پارامترهای توافق شده بر اساس سطح سرویس SLA در دسترس بودن در صورت تقاضا در دسترس باشند (Nguyen and Golman, ۲۰۲۱: ۵). بهترین روش‌های امنیت سایبری خارج از اصول ذکر شده 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 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 کار است. 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. با این حال، 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: ۴). هر استراتژی باید به‌صورت سفارشی برای هر کسب‌وکار به‌طور متفاوتی طراحی و اجرا شود. به این ترتیب 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. در نتیجه 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: ۶ و Snowe, ۲۰۲۰).

۳-۱-۳- انواع امنیت سایبری

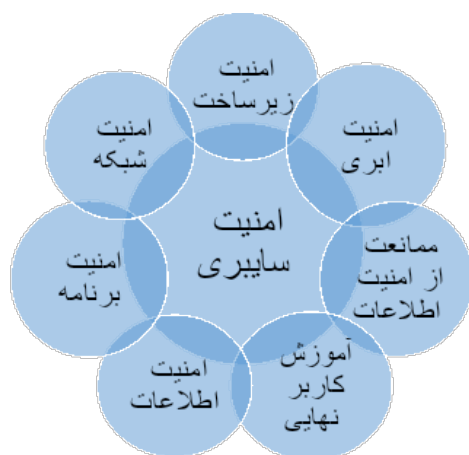
امنیت سایبری تضمین می‌کند که فقط افراد مجاز به آن اطلاعات دسترسی دارند (Ahmed Ja- al, A., et al, ۲۰۲۱). برای حفاظت بهتر، شناخت انواع امنیت سایبری ضروری است؛ امنیت شبکه؛ امنیت شبکه از شبکه کامپیوتری در برابر اختلالات محافظت می‌کند که می‌تواند بدافزار یا هک باشد. امنیت شبکه مجموعه‌ای از راه‌حل‌ها است که 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 (مانند برنامه‌های آنتی‌ویروس، رمزگذاری و فایروال‌ها) از سیستم 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، افشاء، 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. به‌عنوان مثال، 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: ۴).

امنیت ابری؛ از اطلاعات موجود در فضای ابری (بر اساس نرم‌افزار) محافظت می‌کند و برای حذف خطرات

حملات در سایت نظارت می‌کند (Venkatachalam, Krishnasamy, ۲۰۲۱: ۲).

آموزش کاربران به Venkatachalam, 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 (Venkatachalam, Krishnasamy, ۲۰۲۱ و Yuchong, ۲۰۲۱).



انواع مختلف امنیت سایبری (Yuchong, 2021 Qinghui)

۳-۱-۴- تأثیر حمله سایبری بر امنیت ملی

حمله‌های سایبری با کمترین هزینه، خسارت‌های هنگفتی به زیرساخت‌ها و تأسیسات حساس وارد می‌کند. ایجاد اختلال در سامانه‌های اطلاعاتی و ارتباطی، بهره‌برداری کارآمد را ناممکن می‌سازد. به‌کارگیری شیوه‌های جنگ اطلاعاتی، بر هم خوردن ثبات سیاسی دولت‌ها را موجب می‌شود و کشور هدف حمله را با بحران امنیتی و مشروعیتی مواجه می‌سازد که نمونه آن را پس از انتخابات سال ۱۳۸۸ شاهد بودیم. نبرد اطلاعاتی یکی از شیوه‌های جنگ روانی است که با رشد فناوری‌های ارتباطی و ورود شبکه‌های خبری متکی بر ماهواره و اینترنت و ابزارهای الکترونیکی وارد فضای جدیدی شده و تحولات زیادی را تجربه نمود. درواقع نبرد اطلاعاتی، عملیاتی است که منجر به حصول برتری اطلاعاتی با تأثیرگذاری بر روی اطلاعات دشمن، فرایند پردازش اطلاعات، سامانه‌های اطلاعاتی و شبکه‌های سایبری می‌شود (صدوقی، ۱۳۸۴: ۱۲۹). بسیاری از محققان معتقدند که ابزارهای حمله سایبری نسبت به سایر ابزارهای جنگی، بیشتر در دسترس است زیرا هزینه استفاده از آن کمتر و روش‌های به‌کارگیری

آن ساده‌تر است (عبدالله خانی، ۱۳۸۹: ۹۶). هدف اکثر کشورها از تشکیل ارتش سایبری، گرفتن امتیاز در خصوص منافع مشخص و مقابله با انواع تهدیدها در حوزه سایبری است، زیرا بسیاری از تروریست‌ها با به‌کارگیری امکانات قابل‌توجه این ابزارها می‌توانند مخاطرات زیادی را برای دولت‌ها ایجاد نمایند (صدوقی، ۱۳۸۴؛ Gray and Head، 1999؛ Furnell and Warren، 2010؛ Geers، 2009؛ ۲۰۰۹؛ ابراهیمیان و همکاران، ۱۳۹۴) اندیشکده مرکز عربی پژوهش و مطالعات سیاسی دوحه در گزارشی راهبردی به بررسی جنگ‌های مدرن سایبری و ابعاد و پیامدهای آن پرداخت و نوشت: در سال‌های اخیر مفهوم فضای سایبری به‌مثابه میدان جنگ دچار تحولات چشمگیری شده است که مهم‌ترین آن تأثیر مخرب مدنظر دولت‌ها، گروه‌ها و افراد از انجام این حملات است. مهم‌ترین نوع این نوع حمله هک کردن است که یکی از نگران‌کننده‌ترین موارد برای دولت‌ها و افراد به‌شمار می‌رود. ریشه اصلی این نگرانی حضور احزاب مختلف در این مسئله و سخت بودن ردیابی منشأ آن است. یکی دیگر از دلایل همچنین به مشخص کردن پایگاه حمله و ارزیابی هزینه تأثیرات آن باز می‌شود. فضای گسترده وب اکنون به محلی برای تنش، از جمله جاسوسی، ورود بدون مجوزو کنترل پایگاه‌های داده‌ای تبدیل شده که ممکن است امنیت ملی برخی کشورها را تحت‌الشعاع قرار دهد. به دلیل وقوع چنین پیشرفت‌هایی بیشتر دولت‌ها مسئله فضای سایبری را در اولویت خود قرار داده‌اند و بر بسط سازوکارهای جلوگیری‌کننده تمرکز نموده‌اند. مشکل بتوان تعداد اعضای گروه انانیموس (هک‌های گمنام) را که به نمادی برای هکرها تبدیل شده برآورد کرد. اعضای گروه انانیموس (هک‌های گمنام) ارتشی در فضای سایبری هستند که در اتاق‌های گفتگوی خصوصی با هم ملاقات می‌کنند. آن‌ها در مناطق مختلف جهان فعالیت دارند و اولویت‌هایشان مخصوص به خودشان است. آن‌ها رهبری ندارند و گاه از این شعار استفاده می‌کنند «ما گمنام هستیم. ما یک لژیونیم. ما نمی‌بخشیم. فراموش نمی‌کنیم. منتظر ما باشید». این شعار در انتهای نوشته‌ها یا ویدئوهایی که خطاب به خاطیان آزادی بیان و یا محدودکنندگان دسترسی به اینترنت منتشر می‌شود وجود دارد. هدف این گروه افشای فساد دولتی است که به همه دولت‌ها اعمال می‌شود. آن‌ها نماینده یک پدیده بین‌قاره‌ای هستند که جنبش اعتراضی قرن ۲۱ را نشان می‌دهند. حوزه فعالیت و واکنش آن‌ها فضای مجازی است. (سایت وزارت ارشاد) گروه‌های تروریستی از اینترنت برای اهداف گوناگونی همچون اطلاع‌رسانی، تبلیغات، جذب نیروی انسانی و جمع‌آوری اطلاعات استفاده می‌کنند. شبکه اطلاع‌رسانی رایانه‌ای برای تروریست‌های اطلاع‌رسان، مطلوب به نظر می‌رسد؛ چراکه به دلیل متمرکز نبودن، کنترل یا محدودسازی آن دشوار است و امکان دستیابی را برای هر شخصی ممکن می‌سازد. با این حال، از فضای مجازی به طریق دیگری هم می‌توان به‌عنوان یک ابزار مستقیم برای حمله و یا به‌عنوان یک سلاح مستقیم استفاده کرد. یک راه استفاده از فضای سایبری، حملات سایبری به‌وسیله سایت‌های اینترنتی است؛ به واسطه تعریف تروریسم در کنوانسیون بین‌المللی، سرکوب تأمین مالی تروریسم الزامی شمرده می‌شود. تروریسم سایبری؛ یعنی استفاده از شبکه‌ای رایانه‌ای برای ایجاد صدمات جانی یا خرابکاری در زیرساخت‌های بحرانی کشور به طریقی که منجر به صدمات جانی شود. از نظر این افراد نتیجه این اقدامات یعنی صدمات جانی و مالی حتماً باید تحقق یابد. برخی از انواع شبکه‌هایی که ممکن است مورد هدف حملات تروریسم سایبری قرار بگیرند عبارت‌اند از شبکه‌های دولتی، پلیس و آتش‌نشانی، شبکه‌های تحت تملک خصوصی یا دولتی که برای کنترل خدمات شهری همگانی به کار می‌روند، شبکه‌های فراهم‌کننده خدمات زیرساخت، آب، برق؛ بنابراین بی‌هیچ تردیدی باید گفت فضای سایبری یک میدان جنگ جدید است که در آن بسته‌های شبکه می‌توانند تقریباً بلافاصله در سراسر جهان ارسال شوند تا سیستم‌های فیزیکی، از جمله

دارایی‌های زیرساختی حیاتی در حوزه‌های فیزیکی و قلمرو سایبری را تحت تأثیر قرار دهند (هوشیار، ۱۴۰۰: کد خبر: ۳۱۶۴۵۴۸).

۳-۱-۵- ارتباط هوش مصنوعی با امنیت سایبری

دردنیای امروز نادیده گرفتن هوش مصنوعی در امنیت سایبری عواقب خاص خودش را دارد. هوش مصنوعی به عنوان یک فن آوری نوآورانه، نقش بسزایی در تقویت امنیت سایبری ایفا می‌کند. در عصری که حملات سایبری پیچیده و پیوسته در حال افزایش هستند، هوش مصنوعی می‌تواند به عنوان یک ابزار قدرتمند در تشخیص، پیشگیری و مقابله با تهدیدات سایبری عمل کند. استفاده از الگوریتم‌ها و مدل‌های یادگیری ماشینی، هوش مصنوعی قادر است 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 به صورت 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 به طور 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 به صورت گسترده و پیچیده‌تر می‌شوند، هوش مصنوعی به عنوان یک ابزار قدرتمند در مبارزه با این تهدیدات بی‌نظیر است (بیات کاه‌دان و جعفری، ۱۴۰۲: 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)^۱ 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 تجزیه و تحلیل 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 می‌تواند به سازمان‌ها کمک کند تا آسیب‌پذیری سیستم‌ها و شبکه‌های کامپیوتری خود را شناسایی و ارزیابی کنند، سپس سازمان‌ها می‌توانند بر اساس این اطلاعات، اقدامات لازم برای کاهش ریسک امنیتی انجام دهند.

۴- 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.

۵- 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.

۶- آموزش و آگاه‌سازی کارکنان

هوش مصنوعی می‌تواند با استفاده از الگوریتم یادگیری ماشین، محتوای آموزشی با استفاده از نیاز کارکنان تولید کند، این محتوا می‌تواند به کارکنان در شناسایی حملات سایبری، کاهش ریسک امنیتی و بهبود عملکرد امنیت سایبری کمک کند (مرادیان، ۱۴۰۲: ۱-۶).

۳-۱-۶- چالش‌ها و آسیب‌پذیری‌های جمهوری اسلامی ایران در فضای سایبر

البته چالش‌های فضای سایبر تنها به جمهوری اسلامی ایران اختصاص ندارد و همه کشورهای در سطوح مختلفی با آن مواجه هستند. برای مثال در راهبرد سایبری وزارت دفاع آمریکا وجود چنین چالشی تأکید شده و راهکارهایی برای پوشش آن ارائه شده است. در ادامه به بررسی مهم‌ترین چالش‌های ایران در حوزه سایبری می‌پردازیم:

۱- کاربر بودن فضای سایبر

کاربر بودن به میزان استفاده افراد از نرم‌افزارها و سخت‌افزارها و در 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 به مراتب 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 از جمله 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. با این حال، چندان مشخص نیست که این گونه 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 از نرم‌افزارها و سخت‌افزارهای خارجی اشاره دارد. ایران یکی از وابسته‌ترین کشورها به نرم‌افزارها و سخت‌افزارهای خارجی است به نحوی 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. بر این 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 استارت‌آپ‌های 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 فیلتر شکن‌ها تجلی یافته 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 نه تنها نتوانست از میزان استفاده از آن بکاهد بلکه موجب افزایش استفاده چند برابری از فیلتر شکن‌ها شده است. در ایران موبایل‌های هوشمند حداقل یک فیلتر شکن فعال نصب شده 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 تازمانی که بی‌اعتمادی بر این رابطه حاکم باشد، سیاست‌های محدودکننده نه تنها 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 دیر هنگام 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 با وجود 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 از جمله خصوصی و دولتی باشد؛

۴- 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 کشور است که بر مدار مدیریت سنتی می‌چرخد. در حالی که 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 بهتر است 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 ۱۴ ثانیه، یک شرکت با باج‌افزار تهدید می‌شد. اندازه و پیچیدگی حملات بسیار افزایش یافته و اهمیت تقویت نیروی دفاعی سایبری دوچندان شده است. به دلیل اهمیت این موضوع سازمان‌های FBI، Europol 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 «استاکس‌نت» مورد حمله سایبری واقع شد. طبق گزارش‌ها، «استاکس‌نت» که با مشارکت آمریکا و اسرائیل طراحی شده بود، نزدیک به هزار گریزانه تأسیسات اتمی ایران را نابود کرده و باعث شد برنامه اتمی ایران دو سال عقب بیفتد. این ویروس رایانه‌ای طراحی شده بود تا نزدیک به ۶۰ 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 طراحی شده بود. تأسیسات دیپلماتیک و هسته‌ای و بانک‌ها از جمله 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 ۲۰۰۶ 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: ۷۲۴۱۳۸۸) 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 ۱۴۰۱) که بخش عمده فعالیت‌های شهرداری را تحت تأثیر قرار داده است. هدف قرار دادن سامانه وزارت فرهنگ و ارشاد اسلامی در فروردین ۱۴۰۱ حملاتی که روند فعالیتی برخط وزارت مذکور را با مشکلات زیاد مواجه نمود. یکی از مهم‌ترین حملات در پاییز سال ۱۴۰۰ 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 ۱۴۰۲ 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، ۱۴۰۲ کد خبر: ۶۱۶۴۶۲) 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 قابل توجه 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 ۷۱۳۳ میلیارد دلار می‌باشد.

ب: ۶۸ درصد از مدیران و رهبران کسب‌وکارها، خطر حملات سایبری را به‌طور جدی 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. ۴۳ 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 از هم‌گسیختگی ظرفیت‌های فرماندهی و کنترل در فضای مجازی می‌تواند برای نتیجه برخورد، بسیار تعیین‌کننده باشد. از این‌رو، در جنگ‌های نوین دیگر نمی‌توان ادعا کرد که پیروزی به این بستگی دارد که کدام یک از طرفین بیشترین مقدار سرمایه، نفرات و فن‌آوری را دارند، بلکه مهم این است که کدام یک 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؛ به روزرسانی سیستم عامل و غیره اشاره نمود (اقبال زارچ، مرکز مطالعات سیاسی و بین المللی)

۴- تجزیه و تحلیل یافته ها

۴-۱- تأثیر تهدیدات سایبری بر امنیت جمهوری اسلامی ایران

ایران نیز مانند سایر کشورها چه بسا بیش از آنان در معرض تهدیدات سایبری فراوانی است به طوری که بیشترین حملات سایبری علیه جمهوری اسلامی ایران و از سوی کشورهای غربی به خصوص آمریکا و اسرائیل اتفاق می افتد. ایران در بین 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 می نماید، از این نظر ایران رتبه چهارم در جهان را داراست. بیشترین حملات سایبری در ایران برای ایجاد آشوب و بحران داخلی صورت می گیرد. افزایش استفاده از فضای مجازی و گسترش زیرساخت های فن آوری و مخابراتی و به طور کلی هوشمندسازی بسیاری از مشاغل و ادارات و سازمان های دولتی و خصوصی و به کارگیری سیستم های نوین توسط کاربران موجب شده است ایران به مراتب بیشتر از کشورهای همسایه خود در معرض تهدید قرار بگیرد. بیشترین هدف حملات سایبری در بخش نظامی، تأسیسات هسته ای و آسیب به زیرساخت های حیاتی کشور صورت می گیرد که می تواند موجب سردرگمی افراد و ایجاد بحران اجتماعی در کشور شود. نمونه این حملات، حمله به سامانه سوخت در سال ۱۴۰۰ است که هزینه های مالی فراوانی به کشور وارد نمود و باعث ایجاد تنش های روانی زیادی در بین عموم مردم گردید اما مسئولین امر با اطلاع رسانی به موقع در جامعه و به کارگیری متخصصان خبره سریعاً اقدام به برطرف کردن مشکل نمودند. 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 حکومت ها بتوانند با آموزش به موقع و به روز، آگاهی شهروندان و سازمان ها را در استفاده از فضای مجازی افزایش دهند و در صورت وقوع حملات اوضاع را کنترل نموده و از ایجاد بحران های مختلف در جامعه پیشگیری کنند. به اعتقاد تاجیک ۱۳۸۲ تهدیدهای امنیتی متأثر از فضای مجازی در ایران عبارتند از:

۱. اقدام های مخل امنیت و برانداز گروه های مسلح و غیرمسلح؛
۲. گسترش نابسامانی های اجتماعی از قبیل مواد مخدر، فساد اخلاقی، جرائم اجتماعی، سرقت و...؛
۳. شکاف بین اقلیت های قومی، مذهبی، زبانی با نظام و افزایش گرایش های تجزیه طلبانه قومی؛
۴. اقدام های تروریستی، خرابکاری و هکتیویسم؛
۵. آماده سازی افکار عمومی جهان علیه جمهوری اسلامی ایران در زمینه پرونده هسته ای و

تشدید اقدام‌ها و تحریم‌ها علیه ایران؛

۶. اقدام سرویس‌های اطلاعاتی بیگانه به عملیات جاسوسی اینترنتی علیه جمهوری اسلامی ایران (صیاد و همکاران، ۱۳۹۹: ۳۱۶).

۵- نتیجه‌گیری و پیشنهادات

آنچه 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 می‌رسد که هیچ رشته یا حرفه ای نمی‌تواند 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 می‌افتد که باتوجه به نتایج این پژوهش حملات توانسته خساراتی رادارابعادگونگون متوجه کشور کند. ایران در بین تهدید شونده‌گان 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 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 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 بحرانهایی 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 سهمیم 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.

۱. ابراهیمیان، بهمن؛ توشه، علی و پورهادی، ابراهیم (۱۳۹۴)، «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.
۲. اسلامی، مسعود (۱۳۶۹)، «جایگاه و موقعیت کشورهای کوچک در نظام بین‌المللی»، مجله سیاست خارجی، سال ۴، شماره ۴.
۳. بمان اقبالی زارچ، علی (۱۴۰۱)، «تهدیدات و حملات سایبری بر علیه ایران»، مرکز مطالعات PIS، سیاسی و بین‌المللی.
۴. بیات کاه‌دان، محمد و جعفری، عیسی (۱۴۰۲)، «مصنوعی در امنیت سایبری» هجدهمین <https://civilica.com/doc/1686186> کنفرانس ملی مهندسی برق، کامپیوتر و مکانیک، شیروان.
۵. تاجیک، محمدرضا (۱۳۸۲)، «مقدمه‌ای بر استراتژی‌های امنیت ملی ج.ا.ا. رهیافت‌ها و راهبردها»، نشر فرهنگ گفتمان.
۶. ترابی، قاسم (۱۳۹۷)، «چالش‌ها و آسیب‌پذیری‌های جمهوری اسلامی ایران در فضای سایبر»، مطالعات راهبردی، سال ۲۱، شماره ۱.
۷. تریف، تری و دیگران (۱۳۸۳)، «مطالعات امنیتی نوین»، مترجمین علیرضا طیب و وحید بزرگی، تهران: پژوهشکده مطالعات راهبردی.
۸. «حملات سایبری و میدان جنگ الکترونیک»، سایت وزارت فرهنگ و ارشاد اسلامی <https://herasat.farhang.gov.ir/fa/articel/cyberattaks/cyberattaks5>
۹. صیاد، محمدکاظم؛ امینی، آرمین و طاهری، ابوالقاسم (۱۳۹۹)، «تهدیدهای سایبری و اقدامات امنیتی در فضای مجازی- بررسی رویکردهای ایالات متحده آمریکا و جمهوری اسلامی ایران»، فصلنامه علمی امنیت ملی، سال ۱۰، شماره ۳۸.
۱۰. عبدالله خانی، علی (۱۳۸۹)، «جنگ نبرد ۳، نبرد در عصر اطلاعات»، موسسه فرهنگی مطالعاتی و تحقیقات بین‌المللی ابرار معاصر تهران.
۱۱. عبدالله خانی، علی (۱۳۸۲)، «نظریه‌های امنیت: مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی (۱)»، جلد اول، تهران: مؤسسه فرهنگی مطالعات و تحقیقات ابرار معاصر تهران.
۱۲. عسگرخانی، ابومحمد و رحمتی، رضا (۱۳۸۹)، «نظریه واقع‌گرایی و امنیت بین‌الملل» فصلنامه سیاست خارجی، سال ۲۴، شماره ۱.
۱۳. طالب‌پور، عطیه (۱۳۹۸)، «تاریخچه حملات سایبری در ایران و جهان»، خبرگزاری باشگاه خبرنگاران جوان، ۲۱ بهمن ۱۳۹۸.
۱۴. رئیس‌ی، لیلیا (۱۴۰۲) «صیانت از حقوق شهروندان در فضای سایبر در پرتو نسل سوم حقوق بشر با تأکید بر حقوق ایران»، فصلنامه مطالعات بین‌الملل، سال ۲۰، شماره ۳، زمستان ۱۴۰۲

www.eghtesadnews.com سایت خبری اقتصاد نیوز به نشانی: ۲۷/۰۹/۱۴۰۲

۱۶. صدوقی، مرادعلی (۱۳۸۴)، «تکنولوژی اطلاعاتی و حاکمیت ملی»، تهران، وزارت امور خارجه.

۱۷. قاسمی، ح (۱۳۷۲)، «برداشت‌های متفاوت از امنیت ملی»، مجله سیاست دفاعی، سال اول، شماره ۲.

۱۸. کاظمی، علی اصغر (۱۳۷۰)، «مدیریت بحران‌های بین‌المللی»، تهران، دفتر نشر فرهنگ اسلامی.

۱۹. مرادیان، امید (۱۴۰۲)، «هوش مصنوعی در امنیت سایبری»، آکادمی محسن مدحج.

۲۰. هافندورن، هلگا (۱۳۷۱)، «معمای امنیت»، ترجمه علیرضا طیب، مجله سیاست خارجی، شماره ۴.

۲۱. هوشیار، مرتضی (۱۴۰۰)، «جنگ سایبری از منظر حقوق بین»، سایت خبرگزاری صداوسیما، ۲۶ تیر ۱۴۰۰، کد خبر: ۳۱۶۴۵۴۸.

۲۲. یزدان فام، محمود (۱۳۸۶)، «دگرگونی در نظریه‌ها و مفهوم امنیت بین‌الملل»، فصلنامه مطالعات راهبردی، شماره ۳۸.

ب- انگلیسی

23. Ahmed Jamal, A., et al., (2021). "A review on security analysis of cyber physical systems using machine learning". Mater. Today: Proc.

24. Alkathiri, 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.

25. Alzubaidi, A., (2021). "Cybercrime awareness among Saudi nationals: Dataset". Data Brief 36, 106965.

26. Eriksson, J., & Giacomello, G. (2006). "The information revolution, security, and international relations: (IR) relevant theory?". International political science review, 27(3), 221-244.

27. Furnell, S, M, and Warren, M, J (1999), "Computer Hacking and Cyber Terrorism: the Real Threats in the New Millennium"?, Computers & Security, vol.18.

28. Jay Hoofnagle, Chris, (2022), "Cybersecurity in Context, PUBLISH-ER" TBD, BOOK-WEBSITE.COM

29. 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
30. 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.
31. Palmieri, M., Shortland, N., McGarry, P., (2021). "Personality and on-line deviance: The role of reinforcement sensitivity theory in cybercrime. Comput. Hum". Behav. 120, 106745.
32. 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.
33. Ogbanufe, O., (2021). "Enhancing end-user roles in information security: Exploring the setting, situation, and identity". Comput. Secur. 108, 102340.
34. 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
35. http://www.ccdoce.org/uploads/2019/05trends-intlaw_a4_final.pdf.2019.