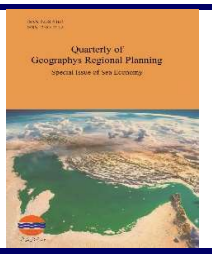
Iranian Association of Geopolitical

Geography (Regional Planning)
Autumn 2024. Vol 14. Issue 56
ISSN (Print): 2228-6462 - ISSN (Online): 2783-2112
Journal Homepage: https://www.jgeoqeshm.ir/



Research Paper

Environmental and Geographical Spaces and Their Impact on Cyber-Crimes with an Emphasis on Terrorism Against the Iranian Government

Ali Yarikhah*

1. Researcher of the specialized doctoral course in criminal law and criminology, University of Tehran, Tehran, Iran.

ARTICLEINFO

PP: 456-467

Use your device to scan and read the article online

Keywords:
Environmental Anatomy, Cyber Terrorism, Environmental Geography, Culture Building, National Security

Abstract

In general, geographers, relying on the old theory of the influence of climate, have said that the basic lines of countries are from natural data (geographical determinism). In the geographical school, the realities of social life are explained based on the influence of geographical factors. What is certain is the influence of geography on the individual and society. This influence is sometimes direct and sometimes indirect. To the extent of the growth of the human individual and the civilizational progress of society, liberation from geographical determinism is achieved to its extent. Just as this growth can be limited by the dominance of other factors such as economic, racial and environmental factors. Now, the geographical factor can form different forms as an accelerating or decelerating factor; but there are always degrees of extensive possibilities and a wide variety of choices, although what is chosen is not itself the result of absolute human choice. In today's world, the economic structure and service delivery of many countries are based on information and communication technologies, so it can be said that cyber terrorism is more dangerous than traditional terrorism. Groups opposing the Islamic Republic of Iran also use this tool in different geographical environments to harm the country's national interests. In the present study, the impact of geographical spaces on the cyber terrorism space against the Iranian government has been examined through the library study method.

Citation: Yarikhah, A. (2024). **Environmental and Geographical Spaces and Their Impact on Cyber-Crimes with an Emphasis on Terrorism Against the Iranian Government.** Geography (Regional Planning), 14 (56), 456-467
DOI: 10.22034/jgeoq.2024.485947.4158

* **Corresponding author:** Ali Yarikhah, **Email:** bebdaco@gmail.com

Extended Abstract

Introduction

Today, information technology has entered all aspects of life, regardless of geographical location, but this growth, despite its advantages, has also had negative aspects. On the one hand, computer crimes are preferred over other ways of committing crimes due to their characteristics: because the way they are committed is easy, and on the other hand, with the advancement of computer technology, the ways of committing crimes have become more technical and specialized, and the ways of dealing with them have become more difficult. One of the characteristics of information technology, especially the Internet, is the possibility of organizing and preparing an organized attack from long distances against predetermined targets, and it allows attackers to act against their targets and cause disruption. In today's world, it is seen that some terrorist acts are carried out by accessing protected information. Information terrorists cause serious security damage that can lead to acute crises. It is important to note that in new perspectives on security, the entire human community, from the individual to the largest international institutions, as well as all environmental spaces and geographical environments and different territories, can be considered a source of threats. According to Robert Mandel, from a conceptual perspective, this transformation has had three stages: the limitation of national sovereignty, the increase in global interdependence, and finally the increase in chaotic and chaotic conflicts. In the simplest conception of the consequences and results of malware disrupting the functioning of computer and telecommunications systems depends on the manufacturer or programmer of the aforementioned malware. On the other hand, some computer malware, with the help of people called intruders, have the ability to perform actions that are almost impossible in the physical world. Terrible results on computer and telecommunication systems through computer espionage, data theft, destruction of computer programs and data, destruction of computer hardware, disruption of power lines, disruption of emergency systems and in some cases, severe physical and psychological injuries to members of society. This research was conducted with the aim of investigating the impact of geographical spaces on the cyber terrorism space against the Iranian government.

Methodology

In the present research, the impact of geographical spaces on the cyber terrorism space against the Iranian government was investigated through a library study method with a descriptive-analytical approach.

Results and Conclusion

Basically, terrorist and destructive attacks at any level and format pave the way for the emergence of the target country's capabilities in defense and countering the source of the threat. As stated in the National Security Doctrine of the Islamic Republic based on the orders of the Supreme Commander of the Armed Forces, Iran will respond to any threat and aggression, and the intensity of this response will be proportional to the level of the enemy's aggression. Therefore, some American experts are fundamentally opposed to cyber attacks against Iran's military and nuclear facilities, because given the weaknesses in the defense sector of this area of conflict and the vastness of American Internet networks, it could lead to disastrous results. In addition to paying attention to cyberspace, paying special attention to the geographical territory and geographical environments to control and prevent the occurrence of cybercrimes, given the mutual influence of these environments on each other and the significant role they play in the interactions that occur in the aforementioned areas, has necessitated environmental planning and zoning and locating cybercrime distribution areas in domestic and international territories in order to carry out offense and defense, and subsequently criminalizing new methods of crime in cyberspace.

References

1. Akbari, Hossein (2011). The causes of the increasing growth of terrorism in the last half century and the strategies to combat it, International Conference of the Global Coalition Against Terrorism for a Just Peace. [In Persian]

2. Aminzadeh, Elham (2001). The difference between terrorism and achieving the right to self-determination, Strategy, No. 21, p. 148. [In Persian]

3. Aristotle, Politics, translated by Hamid Enayat, Al-Khwarizmi Publications, 1985 [In Persian]

4. Ashuri, Dariush (2005)., "Political Encyclopedia", Sohravardi, Tehran, p. 98. [In Persian]

5. Azrang, Abdolhossein, Technology and Environmental Crisis, Amirkabir Press, Tehran, 1985. [In Persian]

6. Bahram Soltani, Kambiz, Collection of Urban Planning Topics and Methods (Environment), Iranian Urban Planning and Architecture Studies and Research Center, Tehran, First Edition, 1992. [In Persian]

7. Barkhordar, Banafsheh, Understanding the Environment, Payam Noor University Press, 2008. [In Persian]

8. Bigzadeh, Sedif, Valuation of Environmental Resources, Payam Sabz Publication, No. 25, Iranian Green Space Engineers Association, Year 3, 2003. [In Persian]

9. Brown, Lester et al., A Look at the World Situation, translated by Hamid Taravati, Arvin Press, Tehran, 1996. [In Persian]

10. Clark, R. B., Sea Pollution, translated by Mohammad Ali Zahed and Zeinab Mohammadi Dashtaki, Naqsh-e-Mehr Publications, first edition, Tehran, 1990. [In Persian]

11. Cola: E., Natural Resources Economics-Environment and Policy-Making, Translated by Siavash Dehghanian and Farrokh Din-Ghazli, Ferdowsi University of Mashhad Press, Second Edition, 2006 [In Persian]

12. Dabirsiyaghi, Manouchehr, Environmental Crisis, Hadith Emrooz Publications, Qazvin, 2004. [In Persian]

13. Darreh Mir Heydar (Mohajerani), Principles and Foundations of Political Geography, p. 8, Simorgh Books, 2007 [In Persian]

14. Fawzi, Yahya (2007). Islam and Terrorism, Andishe Sazan Noor, Collection of Articles on Terrorism and International Law, Tehran. [In Persian]

15. Gaetano Moscao-Boto, History of Political Beliefs and Schools, translated by Shahidzadeh, Morvarid Publications, 1984 [In Persian]

16. Hamid Hamid, Science of Social Development, Simorgh Books, 2007 [In Persian]

17. Hasan Beigi, Ebrahim (2005). Law and Security in Cyberspace, Abrar Contemporary International Studies and Research Institute, Tehran. [In Persian]

18. Hojati Ashrafi, Gholam Reza, Complete Collection of Laws and Regulations of Municipalities and Islamic Councils, Ganj Danesh Publications, Tehran, 2007. [In Persian]

19. Huggett, Peter, New Composite Geography, translated by Dr. Shapour Goodarzinezhad, Samt Publications, third edition, 2007. [In Persian]

20. Ibn Khaldun, Introduction, translated by Gonabadi, Vol. 1; and Dr. Mohammad Ali Sheikh, Research on Ibn Khaldun's Thoughts, Shahid Beheshti University Press, 1984

21. Manouchehr Mohseni, General Sociology, Tahori Library, 1987 [In Persian]

22. Maurice Duverger, Political Sociology, translated by Abul-Fadl Ghazi, Tehran University Publications, 1988 [In Persian]

23. Ministry of Interior, Organization of Municipalities and Rural Areas, Encyclopedia of Urban and Rural Management, Cultural-Information and Press Institute, first edition, 2008. [In Persian]

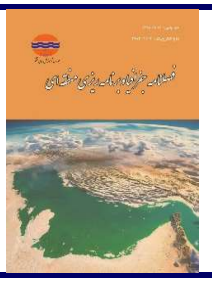
24. Montesquieu, The Spirit of Laws, Vol. 1, translated by Ali Akbar Mohtadi, Book 14, Amir Kabir Publications, 1991. [In Persian]

25. Mottalibi, Mohammad, Environment and Human Rights, Payam-e-Sabz Publication, No. 25, Iranian Association of Green Space Engineers, Year 3, 1983. [In Persian]

26. Qaderi, Ruhollah (2011). An Introduction to the Components of Terrorism Studies, International Conference of the Global Coalition Against Terrorism for a Just Peace. [In Persian]

27. Saeednia, Ahmad, Green Urban Space, Municipal Green Book, Volume 2, National Municipalities Organization Publications, 2000. [In Persian]

28. W.T. Jones, The Gods of Political Thought, Vol. 2, (Montesquieu), translated by Ali Ramin, Amir Kabir Publications, 1983 [In Persian]



فصلنامه جغرافیا (برنامه ریزی منطقه ای)

دوره ۱۴، شماره ۵۶، پاییز ۱۴۰۳

شاپا چاپی: ۶۴۶۲- ۲۲۲۸ شاپا الکترونیکی: ۲۱۱۲ -۲۷۸۳

Journal Homepage: https://www.jgeoqeshm.ir/

انجمن ژئوپلیتیک ایران

مقاله پژوهشی

فضاهای محیطی و جغرافیایی و تاثیر آن بر جرایم سایبری با تاکید بر تروریسم علیه دولت ایران

علی یاری‌خواه*- پژوهشگر دوره دکتری تخصصی حقوق جزا و جرم شناسی ، دانشگاه تهران ، تهران ، ایران.

اطلاعات مقاله

شماره صفحات: ۴۶۷-۴۵۶

از دستگاه خود برای اسکن و خواندن مقاله به صورت آنلاین استفاده کنید

واژه‌های کلیدی:

کالبدشناسی محیطی، تروریسم سایبری، جغرافیای محیطی، فرهنگ سازی، امنیت ملی

چکیده

به‌طور کلی جغرافی‌دانان با تکیه بر نظریه قدیمی تأثیر اقلیم گفته‌اند که خطوط اساسی کشورها از داده‌های طبیعی است (جبر جغرافیائی) در مکتب جغرافیایی واقعیات حیات اجتماعی به اتکاء تأثیر عوامل جغرافیایی تبیین می‌شود. آنچه مسلم است، تأثیر جغرافیا است بر فرد و جامعه. این تأثیر گاه مستقیم است و گاه غیرمستقیم. به میزان رشد فرد انسانی و پیشرفت تمدنی جامعه، رهایی از جبر جغرافیایی در حد خود انجام می‌پذیرد.همان‌گونه که این رشد تسلط عوامل دیگر چون عامل اقتصادی، نژادی و محیطی را می‌توان محدود کند. اکنون عامل جغرافیایی می‌تواند به عنوان عامل تسریع کننده یا کندکننده، اشکال مختلف را شکل دهد؛ امّا همیشه درجاتی از امکانات گسترده و تنوع وسیعی از انتخاب وجود دارد، گرچه آنچه انتخاب می‌شود نیز خود ناشی از اختیار مطلق انسان نیست. در دنیای امروز ساختار اقتصادی و خدمات رسانی بسیاری از کشورها مبتنی بر فناوری‌های اطلاعاتی و ارتباطی است، از این رو می توان گفت که تروریسم سایبری خطرناک تر از تروریسم سنتی است. گروه های مخالف جمهوری اسلامی ایران نیز از این ابزار در فضاهای محیطی جغرافیایی مختلف برای ضربه زدن به منافع ملی کشور استفاده می‌کنند. در پژوهش پیش رو از طریق روش مطالعه کتابخانه ای به بررسی تاثیر فضاهای جغرافیایی بر فضای تروریسم سایبری علیه دولت ایران پرداخته شده است.

استناد: یاری‌خواه، علی (۱۴۰۳). **فضاهای محیطی و جغرافیایی و تاثیر آن بر جرایم سایبری با تاکید بر تروریسم علیه دولت ایران.** فصلنامه جغرافیا (برنامه‌ریزی منطقه‌ای)، ۱۴ (۵۶). صص: ۴۶۷-۴۵۶

DOI: 10.22034/jgeoq.2024.485947.4158

* **نویسنده مسئول:** علی یاری‌خواه ، **پست الکترونیکی:** bebdaco@gmail.com

مقدمه

امروزه تکنولوژی اطلاعات، صرف نظر از موقعیت جغرافیایی، در تمام شئون زندگی وارد شده است، لیکن این رشد علیرغم مزایای خود، جنبه های منفی هم در برداشته است. بدین مفهوم که امکان رفتارهای ضداجتماعی و مجرمانه را به وجود آورده که پیش از این به هیچ وجه امکان پذیر نبوده است و با روند رو به رشد این جرایم روبه رو هستیم، زیرا جرایم رایانه ای به دلیل ویژگی هایی که دارند، نسبت به سایر طرق ارتکاب جرایم مرجح می باشند.

اول آنکه، شیوه ارتکاب آنها آسان است، با مبالغ اندک، خسارات هنگفتی می توانند وارد نمایند، می توان بدون حضور فیزیکی در یک حوزه قضایی معین در آن حوزه مرتکب این گونه جرایم شد، در پایان این که، در اغلب موارد غیرقانونی بودن آنها روشن نمی باشد.

ازسوی دیگر، با پیشرفت تکنولوژی رایانه، راه های ارتکاب جرم فنی تر و تخصصی‌تر شده و راه های مقابله با آن نیز دشوارتر می نماید. یکی از ویژگی های فناوری اطلاعات به ویژه اینترنت امکان ساماندهی و تدارک تهاجم سازمان یافته از فواصل دور علیه اهداف از پیش تعیین شده می باشد و به مهاجمان این امکان را می دهد تا علیه اهداف خود اقدام و ایجاد اختلال کنند. این فناوری علاوه بر این که موجب آشکار شدن نقاط ضعف موجود در زیرساخت های حیاتی می‌شود، با ایجاد ارتباط مخرب مانع از واکنش های دفاعی و یا ایجاد تأخیر در آن‌ها می گردد (حسن بیگی،۱۳۸۴).

در دنیای امروز دیده می‌شود که برخی اقدامات تروریستی توسط دسترسی به اطلاعات حفاظت شده صورت می پذیرد. تروریست های اطلاعاتی می توانند به صورت غیرمجاز وارد سیستم های رایانه ای امنیتی شوند، مثلا با تداخل در سیستم ناوبری هوایی باعث سقوط هواپیما شده یا باعث قطع برق سراسری یا مسموم کردن منابع غذایی شوند.

به طورکلی تروریست های اطلاعاتی آسیب های امنیتی جدی ایجاد می‌کنند که می تواند منجر به ایجاد بحران های نوع حاد گردد. بنابراین، امروزه اهمیت درک چنین فضایی در ارتباط با مفهوم امنیت ملی، از مهم ترین ادراکات ضروری برای جوامع مختلف است.

توجه به این نکته مهم است که در دیدگاه های جدید درباره امنیت، کل جامعه بشری از فرد گرفته تا بزرگترین نهادهای بین المللیو همچنین کلیه فضاهای محیطی و محیط های جغرافیایی و قلمرو های مختلف می توانند منشأ تهدیدات تلقی شوند. در پایان قرن بیستم ما به وضوح شاهد پایان جنگ سرد، انحلال نظام دو قطبی، سقوط کمونیسم و تغییر بازیگران اصلی روابط بین المللی بودیم. به اعتقاد رابرت ماندل از دیدگاه مفهومی، دگرگونی مزبور سه مرحله داشته است : تحدید حاکمیت ملی، افزایش وابستگی متقابل جهانی و بالاخره فزونی کشمکش‌های بی نظم و هرج و مرج گونه. در ساده ترین تصور از عواقب و نتایج بد افزارهای رایانه ای از قبیل: تروجان‌ها، کرم ها، ویروس های رایانه ای و غیره که به دست بزهکاران یا سود جویان تولید می شود، اختلال در عملکرد سیستم‌های رایانه ای و مخابراتی یعنی کاهش سرعت پردازش داده‌ها، بروز رفتارهای غیرعادی از برنامه ای رایانه ای و به طور کلی بستگی به تولید کننده یا برنامه نویس بد افزارهای مذکور دارد که چه نوع خساراتی را به قربانیان وارد نماید. از طرف دیگر، برخی از بدافزارهای رایانه ای به کمک افرادی به نام نفوذگران، توانایی به انجام رساندن اعمالی را دارا هستند که در دنیای فیزیکی تقریباً غیرممکن است. نتایج وحشتناک بر سیستم های رایانه ای و مخابراتی که به وسیله جاسوسی رایانه ای، سرقت داده‌ها، تخریب برنامه و داده‌های رایانه ای، تخریب سخت افزارهای رایانه ای، مختل شدن خطوط نیرو، اختلال در سیستم های اورژانسی و در برخی موارد منجر به صدمات شدید جسمانی و روانی در افراد جامعه می گردد.

امنیت و فضای شهری

امنیت مصونیت از تعرض و تصرف اجباری بدون رضایت است . امنیت در مورد افراد به این معناست که مردم هراس و بیمی نسبت به حقوق و آزادی‌های مشروع خود نداشته باشند. به هیچ وجه حقوق ایشان به مخاطره نیفتد و هیچ عاملی حقوق مشروع آنها را تهدید نکند (گروسی و دیگران، ۱۳۸۶)

فضای شهر مکان کنش‌های اجتماعی افراد در فضاهای مختلف برای گروه‌های اجتماعی است و بستر مطالعه پدیده‌ها و به عبارتی آزمایشگاه جامعه شناسی است (ربانی، ۱۳۸۵)

ارتباط بین شهر و جرم از آن رو است که ویژگی‌های فضایی محیطی می‌تواند پرورش دهنده جرائم خاصی باشد نکته اساسی آن است که شرایط عینی و کالبدی زندگی شهری می‌تواند روابط شهروندان با شهر را محدود سازد . ریشه این محدود سازی تعاملات با شهر نگرانی و ترس آنان از تعرض اعمال و رفتارهای مجرمانه است .شهروندان برای کاهش آسیب‌ها و ضررهای چنین تعرضی ترجیح می‌دهند تا حیطه بده بستان خود را با شهر محدود کنند (علیخواه و ربیعی، ۱۳۸۵)

توجه به مکان به عنوان عامل بی‌واسطه در وقوع جرم در مقایسه با عوامل فردی یا ساختاری این مکان را محقق می‌سازد تا راهکارهای عملی‌تری برای پیشگیری از جرم ارائه دهد . از سوی دیگر تحلیل فضایی جرم در شهرها به شناسایی الگوهای رفتار مجرمانه کشف کانون‌های جرم خیز و در نهایت به تغییر این شرایط و خلق فضاهای مقاوم در برابر جرم و رفع نابهنجاری‌های شهری کمک می‌کند . از این رو بررسی‌های مکانی از اهمیت بسزایی در مطالعه جرم برخوردار بوده است و ضرورت بررسی موضوع را دو چندان می‌نماید.

پیشگیری جرم از طریق طراحی محیطی

در سال ۱۹۶۹ جفری اولین کسی بود که نظریه پیشگیری از جرم از طریق طراحی محیطی را ارائه داد. به نظر جفری، جامعه شناسان به میزان قابل توجهی در عوامل اجتماعی موثر بر جرم از قبیل محرومیت ، تاثیرات فرهنگی ، خانواده و غیره اغراق کرده و به عوامل بیولوژیکی فیزیکی توجه نکرده‌اند. او بر فرصت‌هایی که محیط در اختیار مجرمین قرار می‌دهد تا جرائم گوناگون را ، ناشی از فرصت‌های محیطی می‌دانست . این نظر یه از شش جزء تشکیل شده است که عبارتند از: قلمروگرایی ، نظارت، کنترل دسترسی، تصویر محیط سخت ، آماج کردن و فعالیت‌های پشتیبانی (کلانتری و همکاران، ۱۳۸۹)

تقسیم‌بندی مقوله‌های زیست محیطی

امروزه مفاهیم محیط شناسی دامنه‌ای گسترده یافته است. به طوری که هر نوع فعالیت ذهنی و یا عینی آدمی، محیط خاص آن مقوله را مطرح می‌کنند. از آن جمله می‌توان محیط روانی، محیط اقتصادی، محیط فرهنگی، محیط سیاسی، محیط آموزشی و غیره را بر شمرد. در مفهوم کلی محیط زیست سه نوع محیط قابل تشخیص است که عبارتند از:

۱-محیط طبیعی: به چشم‌اندازهایی که به طور کامل از دخالت‌های انسان در امان مانده باشند، محیط طبیعی اطلاق می‌شود. به همین دلیل زمانی که دخالت انسانی متوقف می‌گردد، اکوسیستم نیز خود را ترمیم کرده، به تکامل طبیعی خود ادامه می‌دهد (سعیدنیا، ۱۳۸۹: ۸۲).

۲-محیط اجتماعی: محیط اجتماعی که در مفهوم وسیع‌تر به آن سپر اجتماعی می‌گویند، عبارت است از جامعه‌ای که انسان در آن زیست می‌کند، به اضافه نهادهای اجتماعی که امور مختلف جامعه را سازمان می‌دهند. محیط اجتماعی از خانواده شروع می‌شود و همسایگان، همکاران، جامعه شهری و روستایی را در بر می‌گیرد و دامنه آن به ملت و دولت کشیده می‌شود.

۳-محیط انسان ساخت: محیط اجتماعی یا محیط مصنوع، به آن بخش از محیط زیست اطلاق می‌شود که ساخته و پرداخته انسان باشد. محیط انسان ساخت را بر حسب زمینه بحث «محیط فرهنگ ساخت»، «محیط تفکر ساخت» و «سپر فنی» نیز می‌گویند. در این میان، به نظر می‌رسد بهترین مفهومی که می‌تواند توجه برنامه‌ریز و طراح را جلب کند، مفاهیم محیط فرهنگ ساخت و محیط تفکر ساخت باشد (بهرام سلطانی، ۱۳۷۱: ۳).

مفهوم و واژه تروریسم

برای نخستین بار واژه تروریسم به معنای "ترساندن و ترس و وحشت" و تروریسم به معنای "نظام ترس و وحشت" در فرانسه برای توصیف حکومت ترس و وحشتی که در سال های ۱۷۸۹ تا ۱۷۹۴ در آن کشور حاکم بود، به کار رفت (اکبری، ۱۳۹۰). این واژه از فرانسه به کشورهای دیگر منتقل شد. در سطح حقوق بین الملل، اصطلاح تروریسم نخستین بار در سال ۱۹۳۰ در سومین کنوانسیون بین المللی کردن حقوق جزا در بروکسل استفاده شد[1].

1- ر. ک. کنوانسیون بین المللی کردن حقوق جزا در ببروکسل، ۱۹۳۰ م.

یکی از محققان تروریسم را " استفاده از خشونت برضد اهداف غیرنظامی تصادفی، به منظور ارعاب یا ایجاد ترس فراگیر، برای دسترسی به اهداف سیاسی" تعریف می‌کند[1]. دیگری تروریسم را "تهدید، خشونت، اعمال منفرد خشونت آمیز یا مبارزه خشونت آمیز که هدف آن در وهله نخست ایجاد ترس است" [2]می داند. یکی دیگر از محققان "تروریست را کسی می داند که برای اشاعه نظریاتش از وحشت و ارعاب استفاده می کند"[3].در دانشنامه سیاسی ترور به این صورت تعریف شده است "ترور در لغت به معنای وحشت و به وحشت افکندن است و در سیاست به عمل حکومت یا گروههایی اطلاق میشود که برای حفظ قدرت یا مبارزه با دولت با اعمال خاص ایجاد وحشت می کند" (آشوری، ۱۳۸۴). فرهنگ اصطلاحی دالوز[4] نیز تروریسم را اقدام سیاسی خشونت آمیز افراد یا اقلیت‌های سازمان یافته علیه اشخاص، دارایی‌ها و نهادهایی می‌داند که برای نیل به اهدافی نظیر کسب استقلال از یک دولت، سرنگونی رژیم حاکم و مبارزه علیه برخی جنبه های سیاسی یک دولت صورت می گیرد.

حقوقدانان درباره مفهوم تروریسم می‌گویند: وقتی سخن از واژه «ترور» و «تروریسم» به میان می‌آید، ناخود آگاه آنچه به ذهن متبادر می‌شود، سوءقصد به جان مقامات سیاسی یک کشور است. هر چند این مورد از مصادیق بارز تروریسم است اما فعالیت‌های تروریستی منحصر به این مورد نیست و به طور کلی شامل تمامی اعمال خشونت‌آمیزی می‌شود که معمولاً منافع حیاتی یک کشور را هدف قرار می‌دهد و آنچه در اینگونه اعمال مجرمانه سازمان یافته و بینالمللی موضوعیت پیدا می‌کند، ایجادترس و وحشت است.

به نظر می رسد نزدیک ترین تعریف تروریسم به منافع بشر را بتوان چنین تعریف نمود که "تروریسم گونه‌ای از خشونت است که توأم با استفاده سیستماتیک یا توسل به قتل، جرح، خرابکاری برای تضییع منافع، تهدید یا ترساندن انسان ها به کار گرفته شود به نحوی که از حیث ابزار و هدف با ارزشهای الهی انسانی منافات دارد و موجب تضییع حقوق و سلب امنیت شود" (اکبری، ۱۳۹۰).

تروریسم سایبری

تروریسم سایبری یا سایبر تروریسم به معنای اقدامات برنامه‌ریزی شده با اهداف سیاسی و غیرشخصی است که علیه داده‌های ذخیره‌شده در رایانه‌ها از طریق شبکه اینترنت صورت می‌گیرد و هدف از چنین عملیاتی از بین بردن یا وارد آوردن آسیب‌های شدید و جدی به آن‌هاست. یکی از مهم‌ترین مصادیق تروریسم رایانه‌ای علیه جمهوری اسلامی ایران، طراحی و حمله ویروسی به نام «استاکس نت» به شکه‌های رایانه‌ای کشورمان بوده است. طبق گزارش نیویورک تایمز، آژانس امنیت ملی آمریکا (NSA) و واحد سایبری اسراییل «استاکس نت» را طراحی کرده‌اند.

تروریسم سایبری حاصل تلاقی تروریسم و فضای مجازی است. این واژه نخستین بار از سوی « کالین باری »5 و در دهه ۱۹۸۰ مطرح شد. اما جامعترین تعریف از این پدیده از سوی خانم « دوروتی دنینگ6 » استاد علوم رایانه‌ای دانشگاه جرج تاون ارائه شده است. وی می‌گوید: سایبر تروریسم، بیشتر به معنای حمله یا تهدید علیه رایانه‌ها، شبکه‌های رایانه ای و اطلاعات ذخیره شده در آنهاست، هنگامی که به منظور ترساندن یا مجبور کردن دولت یا اتباع آن برای پیشبرد اهداف سیاسی یا اجتماعی خاص اعمال می شود. یک حمله، برای اینکه به عنوان تروریسم سایبری شناخته شود باید به خشونت علیه اشخاص یا داراییها منجر شود یا دست کم آسیب کافی برای ایجاد ترس را باعث شود. حملاتی که منجر به مرگ یا صدمات بدنی، انفجار، سقوط هواپیما، آلودگی آب یا خسارات متعدد اقتصادی می‌شود را می توان به عنوان مصادیق تروریسم نام برد.

سایبر تروریسم به صور مختلفی واقع می‌شود که این تنوع زیاد از دو جهت است: نخست آن‌که شیوه‌های ارتکاب چنین جرمی زیاد و فضای مجازی بسیار وسیع است. دوم: ماهیت ترورها در فضای اینترنتی به نحوی است که برعکس تروریسم سنتی در فضای سه بعدی محصور نبوده و فضای گسترده مجازی تحت عنوان اینترنت را پیش رو دارد. به این ترتیب که روش‌های

1 – نشریه آزاد، «ملاحظاتی در باب تروریسم»، به نقل از یونا الکساندر، ۱۳۸۰.
2 – همان، به نقل از برایان جمکیتر.
3 – همان، به نقل از ویلیام فیتز پاتریک.

4 . Dalloz
5- Collin Barry
6- Durouty Dening

تکنیکی رایانه‌ای و ورود به داده‌های رایانه‌ای دست کاربر را بر انتخاب شیوه ارتکب جرم باز می‌گذارد. بر این اساس روش‌های وقوع جرم در این فضا می‌توان گسترده‌تر از روش‌های کلاسیکی در فضای فیزیکی جهان مادی باشد. نحوه ضربه‌زنی به نهادهای یک کشور توسط تروریست‌های رایانه‌ای نیز به تنوع این جرم کمک می‌کند.

در بررسی ابزارهایی که در سایبر تروریسم مورد استفاده قرار می‌گیرد، تروریست‌های فضای مجازی یا اینترنتی، به جای استفاده از سلاح‌های رایج، بمب‌ها یا سایر ابزارهای معمول از نرم‌افزارهای مخرب رایانه‌ای برای پیشبرد اهداف خود استفاده می‌کنند. ویروس‌ها کرم‌ها، تروجان‌ها، اسپم‌ها، ایمیل بمبینگ، گوگل بمبینگ، هک و نفوذ رایانه‌ای و خرابکاری یا دستکاری‌های اینترنتی و شبکه‌ای بخشی از ابزارهای تروریست‌های مجازی به شمار می‌رود. هدف تروریسم سایبری، ایجاد اختلال گسترده در بخش های کلیدی اقتصاد، ازجمله امکانات دولتی و خصوصی، بانک داری و امور مالی، حمل ونقل، تولید، پزشکی، آموزش و پرورش، دولت و به طور کلی آن دسته از تأسیسات کلان کشور که برای انجام عملیات روزانه وابسته به رایانه هستند، با نگاهی به افزایش رخدادها و حمله های سایبری علیه بیشتر کشورهای توسعه یافته و بروز خسارات شدید در زیرساخت های حیاتی، می توان به فاجعه آمیز بودن نتایج حملات تروریستی سایبری علیه سیستم ها و دارایی هایی پی برد که تأثیرات شدیدی بر امنیت فیزیکی، اقتصاد ملی یا ایمنی همگانی خواهد گذاشت.

قربانیان تروریسم سایبری همانند دیگر انواع تروریسم از گستردگی و تنوع زیادی برخوردارند. امروزه با توجه به شیوع حملات سایبری در سرتاسر جهان، لزوم توجه به بزه دیدگان تروریسم سایبری در حقوق موضوعه و اسناد بین المللی دیده می شود. گستردگی فضای سایبر و به خدمت گرفتن آن توسط اکثر افراد جامعه و زیرساخت های کشور، طیف گسترده ای از مباحث را پیرامون بزه دیدگان این پدیده و چگونگی حمایت و جبران خسارت های وارد آمده به آن ها را، چه در حقوق داخلی کشورمان و کشورهای دیگر و چه در سطح بین الملل شکل داده است. تروریسم سایبری به این دلیل که در بستر فضای مجازی به وقوع می پیوندد، همانند دیگر بزه های رایانه ای مباحث نوینی را در حوزه بزه دیده شناسی و حمایت از بزه دیدگان سایبری، ایجاد نموده است.

تروریسم سایبری و نظام بین المللی

متاسفانه در نظام بین‌الملل دادگاه یا دیوانی مستقل که بتواند به جرایم ناشی از فعالیت‌های تروریستی رسیدگی کند، وجود ندارد. دادگاه بین‌المللی کیفری نیز به عنوان یک مرجع بین‌المللی شناخته‌شده، فاقد صلاحیت رسیدگی به این نوع از جرایم است. لذا به ناچار این دسته از اعمال مجرمانه باید در دادگاه‌های ملی تحت دادرسی کشور مربوطه مورد رسیدگی قرار گیرد. به دلیل اهمیت موضوع تروریسم در به خطر انداختن جدی منافع کشورها، سیزده کنوانسیون جهانی و سه کنوانسیون منطقه‌ای، برای مقابله با این معضل جهانی به تصویب رسیده است. کنوانسیون‌های بین‌المللی در رسیدگی محاکم داخلی به این جرایم سیستم اجرایی غیرمستقیم را پیش‌بینی کرده‌اند. به این معنی که مقررات کنوانسیون‌های حقوق بین‌الملل کیفری، از طریق حقوق موضوعه ملی کشورها اجرا می‌شود و کشورهای امضاکننده سند بین‌المللی مجبور به همکاری با یکدیگر در تعقیب و به کیفر رساندن مجرمین هستند. سیستم اجرایی غیرمستقیم بر اصل «استرداد یا مجازات» تاکید دارد. منظور از این نوع سیستم آن است که کشورهای پای‌بند به کنوانسیون که در قلمروی حاکمیت آنها متهمان فعالیت‌های تروریستی قرار دارند، دو روش را پیش‌رو دارند. یا باید متهمان را محاکمه کنند و یا آنها را به کشور عضو دیگر که درخواست استرداد را دارد مسترد کنند.

مقامات ارشد امنیت ملی آمریکا چندی پیش در کنگره از «جاسوسی سایبری» سخن به میان آوردند و از آن تحت عنوان خطرناک‌ترین نوع تروریسم یاد کردند. خطری وحشتناک‌تر از عملیات‌های تروریستی انتحاری. «جیمز کلپر»، مدیر سازمان اطلاعات ملی آمریکا زمان ارایه نطق ارزیابی تهدیدات پیش‌روی ایالات متحده در کمیته منتخب سنا گفت: «بیانیه امسال ما با محوریت حملات سایبری است و باید تاکید کنم که این موضوع بسیار مهم و حایز اهمیت است.» «جان برنان»، رییس سازمان سیا هم می‌گوید: «حملات رایانه‌ای به شدت افزایش یافته است و جدیت و تنوع تهدیدات سایبری علیه ایالات متحده حتی به صورت روزانه نگران‌کننده است.» باراک اوباما، رییس‌جمهوری ایالات متحده در مصاحبه با «ای.بی.سی‌نیوز» تکرار کرد: «برخورد با حملات سایبری که امنیت ملی ایالات متحده را هدف قرار داده است، ادامه دارد. حملاتی که مسوول آن گهگاه

مجرمان اینترنتی و گهگاه دولت‌های مختلف هستند.» اما شاید باید تا حدی منصفانه‌تر به ماجرا نگاه کرد. حملات سایبری خطرناک است؛ شاید حتی خطرناک‌تر از تروریست‌های انتحاری. حملاتی که به ابزار جدید جنگ در دنیای مدرن بدل شده‌اند.

به هر ترتیب تروریسم بین المللی نمی تواند جدا از نظامی که بر جهان حاکم است مورد مطالعه قرار گیرد. استفاده از حق وتو در شورای امنیت و قصور یا تقصیر این دولت ها در ایفای تکالیفی که منشور ملل متحد بر عهده آ نها گذارده است، توطئه گری دولت های بزرگ و جانبداری های یک طرفه آن ها باعث شده است که سازمان ملل متحد در ایجاد همکاری های بین المللی و حل مشکلات جهانی با ناکامی روبرو شود. غصب حقوق ملت های مستضعف، چنان ظلم و محرومیتی بر آن ها وارد آورده است که سازمان ملل متحد قادر به جبران آن نیست. پس از وقوع حملات ۱۱ سپتامبر، غالباً نظریاتی نظیر "تروریسم جهانی مخاطره ای برای دولت های جهان در دوران فعلی به شمار می رود و می بایست به طور جدی با آن مقابله نمود" مطرح گردید. هم چنین بحث های زیادی درباره همکاری دولت های جهان برای مبارزه و مقابله با افراد و یا دول تهایی که از تروریسم حمایت می کنند صورت پذیرفت. اما تلاش کمی برای یافتن خاستگاه و ریشه های تروریسم انجام پذیرفت. یقیناً تا زمانیکه ریشه های تروریسم شناخته نشود، نقش دولتهای جهان برای مقابله و ریشه کنی با آن نیز مؤثر نخواهد افتاد. واقعیت آن است که تروریسم جدید غالباً واکنشی به گسترده شدن ساختارهای اقتصادی، ترجیحات سیاسی، نگرش های فرهنگی و کیفیت حیات اجتماعی حاکم بر غرب است. در چنین شرایطی که قدرت و ثروت به شکلی کاملاً ناعادلانه توزیع شده است موجودیت هایی که بهره کمتری از این مؤلفه ها در سطح جهان داشته اند برای جبران ضعف خود به حربه تروریسم متوسل می شوند. آن چه تنور فعالیتهای تروریستی را گرم نگه داشته، تبعیض های محسوس و معیارهای دوگانه در جامعه جهانی نسبت به برخی فرهنگ ها است که این امر خود زمینه و بستری را برای پرورش عقد هها و عقیده های تاریخی تروریست ها و انجام عملیات تروریستی و حتی انحراف افکار عمومی به سمت حمایت از عملیات تروریستی فراهم می آورد. از این دیدگاه تروریسم برآیند انباشت عقده ها و عقیده های سرکوب شده تاریخی است. لذا ناکامی ها، فشارهای اقتصادی، سلطه گری، زیر پاگذاشتن و اهانت به مقدسات یک جامعه، عقده هایی را موجب می گردد که این عقده ها در مواقع مقتضی به صورت پرخاشگری،خشونت و ترور جلوه می کند، و چنانچه فشارهای جامعه افزون گردد سبب جنگ و ستیز می گردد (قادری، ۱۳۹۰).

فرهنگ‌سازی در مقابله با تروریسم سایبری

به گفته کارشناسان مهم‌ترین اقداماتی که در رویارویی با تروریسم‌ها و جنگ‌های سایبری می‌توان انجام داد اول از همه فرهنگ‌سازی و آموزش‌های عمومی در ارتباط با نحوه تعامل کاربران با سیستم‌های رایانه‌ای است و در گام بعدی ایجاد دژهایی مستحکم است که در برابر این گونه حملات از قبل تدارک دیده شده باشند که بتوانند عملیات دفاع و پاتک را انجام دهند. شعارهایی مانند دولت الکترونیکی باید بیش از پیش در انتظار استاکس‌نت و دوکوهایی باشد که سرزده وارد مرزهای مجازی کشور ما شدند و وحشت و واهمه‌ای را برای برخی مسئولان و دست‌اندرکاران بخش‌های مختلف به وجود آوردند، اما این به معنای پاک کردن صورت مسئله و انزوای کامل از شبکه‌های جهانی و پرمخاطره‌ای همچون اینترنت نیست. بلکه کسی در این عرصه موفق‌تر است که با در نظر گرفتن تمامی چالش‌ها پا در میدان نهد و با موقعیت‌سازی برای خود بهترین دستاوردها را از آن خود کند و اجازه چپ نگاه کردن را به هیچ‌کس در میدان رقابت ندهد و این در یک کلام یعنی جامعه آرمانی و الکترونیک.

تروریسم سایبری و ابعاد تهدید امنیت ملی

تهاجمات تروریستی و تخریبی در هر سطح و قالبی زمینه‌ساز ظهور توانمندی‌های کشور هدف در دفاع و مقابله با منشأ تهدید است.با پیشرفت تکنولوژی و ورود به عصر ارتباطات، روش‌ها و ابزارهای شبکه‌های ارتباطی تغییر کرده و از شکل فیزیکی به فضای مجازی وارد شده است. مفاهیم دیجیتالی، الکترونیکی و سایبری به قدری در جوامع ورود پیدا کرده‌اند که دنیا را در آستانه تبدیل همه سطوح ارتباط به فضای غیر فیزیکی پیش برده‌اند. اما در این میان به همان اندازه که ورود به دنیای مجازی ارائه خدمات، برقراری ارتباطات و کارکردها را سرعت و سهولت بخشیده است، تهدیدها، آسیب‌ها و جرائم مرتبط و جدیدی نیز تولید شده است. کلاهبرداری‌های مالی، نفوذهای اطلاعاتی و خرابکاری در تأسیسات و سخت‌افزارها نمونه‌ای از تهدیدهای در این زمینه است که باعث شده مقدمات برقراری و ارتقای امنیت در این حوزه فراهم شود.

امروزه سازمان‌های ارائه‌دهنده خدمات، سیستم‌های مالی و بانکداری، شبکه‌های ارتباطات اجتماعی، روزنامه‌نگاری و حتی پلیس، سازمان‌ها و تشکیلات امنیتی با طبقه‌بندی‌های حفاظتی به فضاهای مجازی ورود پیدا کرده و از این عرصه برای تسهیل ارتباطات و کارکردها بهره می‌گیرند. با توجه به این کارکردهای کلان، مسئله امنیت در فضای مجازی به قدری از اهمیت رسیده که اساساً تبلیغات نرم‌افزاری حتی در حوزه‌ها و کاربردهای اجتماعی به جنبه‌ها و تضمین‌های امنیتی نیز می‌پردازند و مفاهیم کنترل امنیت در فناوری اطلاعات یکی از ارکان اساسی و حفاظتی سازمان‌ها و دستگاه‌های اداری را تشکیل داده است.

برای نمونه ضربه‌های سخت‌افزاری به تجهیزات از طریق نفوذ ویروس‌های رایانه‌ای یکی از تهدیدهای جدی حوزه فضای مجازی است. این تهدید که معمولاً در شکلی کلان صورت می‌گیرد در برخی موارد با ریشه‌های سیاسی و نشأت‌گرفته از مخاصمات بین‌المللی ایجاد شده و هدف‌گذاری خود را سیستم‌های امنیتی و حفاظتی و دستگاه‌ها و تکنولوژی‌های دارای طبقه‌بندی حفاظتی قرار می‌دهند و به نوعی به دنبال جلوگیری از تولید و پیشرفت ساختارهای تکنولوژیکی یا ضربه به مراکز حساس و دارای اهمیت امنیتی است و از این رو محیط تهدیدآفرین علیه امنیت ملی کشورها را دیگر نمی‌توان فقط در محدوده جهان واقعی ترسیم کرد.

تهدیدات و تهاجمات گفته شده در حوزه مناقشات سیاسی و امنیتی که اهداف خرابکاری، ضربه و اخلال در ساختار و تشکیلات کشور هدف را دنبال می‌کند ضمن تعریف در قالبی نوین از تقسیم‌بندی انواع تروریسم، با نام تروریسم سایبری، عمدتاً در دو گروه طبقه‌بندی می‌شوند. نوع اول مربوط به کنشگرانی است که به یک دولت وابسته‌اند و از طرف تشکیلات نظامی، امنیتی یا شرکت‌های وابسته به کشور مذکور تغذیه و هدایت می‌گردند و نوع دوم را نیز گروه‌هایی تشکیل می‌دهند که ممکن است ارتباط مستقیم با دولتی خاص نداشته باشند، ولی در راستای اهداف سیاسی خود از این روش برای خرابکاری استفاده نمایند.

جمهوری اسلامی ایران نیز به دلیل تراکم گروه‌های تروریستی معاند در محیط پیرامونی خود و نقش فزاینده تهدیدات کنشگران دولتی در هدایت و حمایت اطلاعاتی، مالی و سخت‌افزاری از گروه‌های ضدانقلاب، با پدیده تروریسم سایبری به میزان قابل توجهی روبه‌روست که این مسئله ضرورت شناخت و رصد و مقابله با این نوع جدید از تروریسم را بیش از پیش نشان می‌دهد.

تروریسم سایبری در ایران

جمهوری اسلامی ایران همانگونه که در عرصه تروریسم فیزیکی به عنوان بزرگترین قربانی تروریسم بر پایه آمار و مستندات مطرح می‌باشد، در صحنه تروریسم سایبری نیز آمار بالایی از تهاجمات متوجه نظام اسلامی است. باراک اوباما رئیس جمهور آمریکا در اولین ماه‌های ورود به جایگاه ریاست جمهوری دستوری مبنی بر حمله سایبری به جمهوری اسلامی را صادر کرد که بعدها به شکلی هدفمند در قالب یک گزارش توسط روزنامه نیویورک‌تایمز افشا شد. دستور اوباما نشان از تغییر روش و سیاست ایالات متحده آمریکا در رویارویی با ایران داشت و گویای این واقعیت بود که بعد از دولت جمهوری‌خواه جرج بوش جریان‌های حاکم بر کشور آمریکا تمایل بیشتری به استفاده از عرصه سایبری و در امان ماندن از هزینه‌های خشونت فیزیکی در افکار عمومی دارند. البته برای اثبات هدایت و حمایت دولتی از تروریسم سایبری علیه جمهوری اسلامی ایران، نیاز نیست حتماً به اسناد و مدارک رسانه‌های غربی در این خصوص مراجعه کرد، بلکه شکل و حجم حملات و اقدامات خود گویای این مسئله می‌باشد.

نمونه‌های این موضوع را می‌توان در بررسی بدافزارهای خرابکار و جاسوسی مشاهده کرد. در این سیستم‌ها گاهی ما با وجود بیش از ۱۵هزار خط کُد برنامه‌نویسی روبه‌رو می‌شویم که یقیناً از حد و اندازه حملات انفرادی یا حتی گروهی خارج بوده و پشتیبانی اطلاعاتی و تکنولوژیکی قدرت‌های بزرگ و صاحب تکنولوژی از قبیل آمریکا را می‌طلبد. حتی این مهم نیز وجود دارد که در این عرصه خود دولت‌ها غیر از آمریت در حملات، نقش عامل را نیز بر عهده می‌گیرند و در برخی از موارد حاضر نیستند این ابزار یا علم را به هر دلیلی در دست گروه‌های مزدور قرار دهند. زیرا از یکسو ذات چنین تروریسمی نیز به دلیل پایین بودن هزینه‌های سیاسی و حقوقی آن نیازی به برون‌سپاری دولت‌ها برای پنهان‌سازی نقش مستقیم ندارد؛ به عبارت دقیق‌تر عدم امکان تشخیص دقیق مهاجمان و هویت واقعی آنها و مشکل بودن ارزیابی زمان و محل حملات و همچنین ضربه به زیرساخت‌های کشور هدف، از قبیل سیستم‌های مالی و بانکداری، کارخانجات و حتی شبکه‌های خدمت‌رسانی شهری از دلایل

تمایل دولت‌ها در مدیریت و اجرای مستقیم این نوع هجمه‌ها است. از سوی دیگر نیز می‌توان به ارزش علمی و تکنولوژیکی این پدیده را درنظر گرفت که با برون سپاری آن به گروه‌ها و سازمان‌ها مزدور حتی می‌تواند در شرایطی مخل امنیت خود کشورهای صادر کننده و منافع آنها باشد!

برای ذکر نمونه‌های آشکار شده در این عرصه باید به حملات صورت گرفته علیه تاسیسات هسته‌ای، زیرساخت‌های نفت و گاز و صنایع دفاعی ایران اشاره کرد. از ویژگی‌های این حملات می‌شود به تعدد و اجرای سریالی آنها اشاره کرد؛ زیرا با توجه به ویژگی‌های عرصه نرم‌افزار و ویروس‌های رایانه‌ای هر بار در مقایسه با دفعات قبل، حملات از شدت و توانمندی بالاتر و پیچیده‌تری برخوردار شده، زیرا ویروس‌های رایانه‌ای در هر نوبت با بهره‌گیری از سابقه نفوذهای گذشته با شناخت بیشتری طراحی و تولید می‌شوند و منطبق‌تر با ایرادات سیستم‌های امنیتی هدف، کار می‌کنند.

به عنوان مثال بدافزار «استاکس‌نت» که برای حمله به تاسیسات هسته‌ای ایران تولید و نفوذ داده شد، به گونه‌ای طراحی شده بود که قابلیت شناسایی و تخریب تجهیزات سیستم‌های هسته‌ای از قبیل سانتریفیوژها را داشت. بعد از آن نسل دومی از ویروس‌ها نفوذ داده شدند که زیرساخت‌های حیاتی صنعتی را هدف قرار می‌دادند و نسل سوم که آخرین حمله اعلام‌شده علیه جمهوری اسلامی ایران است، نرم‌افزاری به نام «شعله» بود که نزدیک به ۴۰ برابر استاکس‌نت قدرت داشت و در اولویت اول مأموریتش برای جمع‌آوری و ارسال اطلاعات یا همان جاسوسی سایبری طراحی شده بود؛ اما ساختار پیچیده این بدافزار به آن اجازه می‌داد با دریافت دستورات جدید وارد مرحله تخریب شود! این تخریب‌ها نیز در صورت موفقیت می‌توانست بدون کمک به یک عامل خارجی، برای استفاده از ظرفیت کاهش ضریب امنیتی کشور، به تنهایی خسارات جانی و مالی ایجاد نماید. به عنوان مثال با ضربه به شبکه توزیع و انتقال انرژی الکتریکی در مرحله اول کشور را به خاموشی‌های منطقه‌ای کلان یا به عبارت دیگر روشنایی‌های جزیره‌ای بدل کرده و غیر از ایجاد تهدید امنیت ملی، فعالیت تجهیزات حیاتی کشور از قبیل پزشکی و بیمارستانی را مختل نموده و خسارات جانی و مالی بر جای گذارد؛ مواردی که قطعاً در طراحی دستاوردهای مأموریت این گونه ویروس‌های رایانه‌ای دیده شده است!

مسئله ورود مستقیم دولت‌ها در حوزه حملات سایبری سبب شده که در عین برانگیختگی واکنش‌های متقابل از سوی کشورهای هدف و همچنین برخورداری از جنبه‌های دیگر مانند جاسوسی، این اقدامات در حوزه مطالعات امنیت بعضاً به نام‌هایی همچون جنگ سایبری یا جنگ الکترونیک نیز خوانده شود. اما این تعریف هیچ‌گاه از بار تروریستی آن کم نکرده و همانطور که گفته شد ویرانی‌های حاصل از حملات سایبری با ضربه به زیرساخت‌های کشور در پاره‌ای از موارد خسارات جانی و مالی را نیز در پی داشته است.

نتیجه گیری

اساساً تهاجمات تروریستی و تخریبی در هر سطح و قالبی زمینه‌ساز ظهور توانمندی‌های کشور هدف در دفاع و مقابله با منشأ تهدید است. همانطور که در دکترین امنیت ملی جمهوری اسلامی مبتنی بر فرامین مقام معظم فرماندهی کل قوا بیان شده، ایران به هر گونه تهدید و تهاجم واکنش نشان داده و شدت این واکنش نیز متناسب با سطح تهاجم دشمن خواهد بود. لذا برخی از کارشناسان آمریکایی اصولاً مخالف شدید حملات سایبری علیه تأسیسات نظامی و هسته‌ای ایران هستند، زیرا که به اعتقاد آنها چنین اقداماتی در نهایت منجر به واکنش متقابل جمهوری اسلامی خواهد شد و با توجه به ضعف‌های موجود در حوزه دفاعی این عرصه از مخاصمات و گستردگی شبکه‌های اینترنتی آمریکا، می‌تواند نتایج فاجعه‌باری رقم بزند.

در کنار توجه به فضای سایبر ، توجه ویژه به قلمرو جغرافیایی و محیط های جغرافیایی جهت کنترل و پیشگیری از وقوع جرایم سایبری با توجه به تاثیر متقابل این محیط ها بر همدگیر و نقش به سزایی که در فعل و انفعالات رخ داده در حوزه های مزبور بر عهده دارند ، باعث ضرورت برنامه ریزی محیطی و پهنه بندی و مکانیابی مناطق توزیع جرایم سایبری در قلمرو های دخلی و بین المللی به منظور انجام آفند و پدافند و متعاقبا جرم انگاری درخصوص روش های نوین ججرم در فضای سایبر ، گردیده است.

منابع

۱. ارسطو، سیاست، ترجمه حمید عنایت، انتشارات خوارزمی، ۱۳۶۴
۲. اکبری، حسین (۱۳۹۰). علل رشد رو به تزاید تروریسم در نیم قرن اخیر و راهکارهای مقابله با آن، کنفرانس بین المللی ائتلاف جهانی علیه تروریسم برای صلح عادلانه.
۳. امین زاده، الهام (۱۳۸۰). تفاوت تروریسم و دستیابی به حق تعیین سرنوشت، راهبرد، شماره ۲۱، ص ۱۴۸.
ابن خلدون، مقدمه، ترجمه گنابادی، ج ۱، ؛ و دکتر محمد علی شیخ، پژوهشی در اندیشه‌های ابن خلدون، انتشارات دانشگاه شهید بهشتی، ۱۳۶۳
٤. آذرنگ، عبدالحسین، تکنولوژی و بحران محیط زیست، انتشارات امیرکبیر، تهران، ۱۳۶۴.
٥. آشوری، داریوش (۱۳۸۴)، "دانشنامه سیاسی"، سهروردی، تهران، ص ۹۸.
٦. براون، لستر و همکاران، نگاهی به وضعیت جهان، ترجمه حمید طراوتی، نشر آروین، تهران، ۱۳۷۵.
۷. برخوردار، بنفشه، شناخت محیط زیست، انتشارات دانشگاه پیام نور، ۱۳۸۷.
۸. بهرام‌سلطانی، کامبیز، مجموعه مباحث و روش‌های شهرسازی (محیط زیست)، مرکز مطالعات و تحقیقات شهرسازی و معماری ایران، تهران، چاپ اول، ۱۳۷۱.
۹. بیگ‌زاده، صدیف، ارزش‌گذاری منابع زیست محیطی، نشریه پیام سبز، شماره ۲۵، انجمن مهندسین فضای سبز ایران، سال سوم، ۱۳۸۲.
۱۰. حجتی‌اشرفی، غلامرضا، مجموعه کامل قوانین و مقررات مُحشای شهرداری و شوراهای اسلامی، انتشارات گنج دانش، تهران، ۱۳۸۶.
۱۱. حسن بیگی، ابراهیم (۱۳۸۴). حقوق و امنیت در فضای سایبر، مؤسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر تهران.
۱۲. حمید حمید، علم تحولات جامعه، کتابهای سیمرغ، ۱۳۵۶
۱۳. دبیرسیاقی، منوچهر، بحران محیط زیست، انتشارات حدیث امروز، قزوین، ۱۳۸۳.
۱٤. درّه میر حیدر(مهاجرانی)، اصول و مبانی جغرافیای سیاسی، ص ۸، کتابهای سیمرغ، ۱۳۵۶
۱٥. سعیدنیا، احمد، فضای‌سبزشهری، کتاب سبز شهرداری، جلددوم، انتشارات‌سازمان شهرداری‌های‌کشور، ۱۳۷۹.
۱٦. فوزی، یحیی (۱۳۸۶). اسلام و تروریسم، اندیشه سازان نور، مجموعه مقالات تروریسم و حقوق بین الملل، تهران .
۱۷. قادری، روح الله (۱۳۹۰). درآمدی بر مؤلفه های تروریسم شناسی، کنفرانس بین المللی ائتلاف جهانی علیه تروریسم برای صلح عادلانه.
۱۸. کلارک، آر. بی، آلودگی دریا، ترجمه محمدعلی زاهد و زینب محمدی دشتکی، انتشارات نقش مهر، چاپ اول، تهران، ۱۳۷۹.
۱۹. گائتانو موسکاوبوتو، تاریخ عقاید و مکتبهای سیاسی، ترجمه شهیدزاده، انتشارات مروارید، ۱۳۶۳
۲۰. کولا: ای، اقتصاد منابع طبیعی- محیط زیست و سیاست‌گذاری‌ها، ترجمه سیاوش دهقانیان و فرخ دین‌قزلی، انتشارات دانشگاه فردوسی مشهد، چاپ دوم، ۱۳۸۵
۲۱. مطلبی، محمد، محیط زیست و حقوق بشر، نشریه پیام سبز، شماره ۲۵، انجمن مهندسین فضای سبز ایران، سال سوم، ۱۳۸۲.
۲۲. منتسکیو، روح القوانین، ج ۱، ترجمه علی اکبر مهتدی، کتاب چهاردهم، انتشارات امیرکبیر، ۱۳۷۰.
۲۳. موریس دوورژه، جامعه‌شناسی سیاسی، ترجمه ابو الفضل قاضی، انتشارات دانشگاه تهران، ۱۳۶۷
۲٤. منوچهر محسنی، جامعه‌شناسی عمومی، کتابخانه طهوری، ۱۳۶۶
۲٥. و.ت.جونز، خداوندان اندیشه سیاسی، ج ۲، (منتسکیو)، ترجمه علی رامین، انتشارات امیرکبیر، ۱۳۶۲
۲٦. وزارت کشور، سازمان شهرداری‌ها و دهیاری‌های کشور، دانشنامه مدیریت شهری و روستایی، مؤسسه فرهنگی- اطلاع‌رسانی و مطبوعاتی، چاپ اول، ۱۳۸۷.
۲۷. هاگت، پیتر، جغرافیا ترکیبی نو، ترجمه دکتر شاپور گودرزی‌نژاد، انتشارات سمت، چاپ سوم، ۱۳۷۶.