Journal of Combat Medicine
2024; 7(1): 10-14
10.30491/jcm.2024.216115
Mini Review

The Role of Health in National Security and Sustainable Development Section 8: Cybersecurity and Health

Seyyed Yahya Safavi [1*]

[1] *Professor in Political Geography, Imam Hossein University, Tehran, Iran*

Received: 24 February 2024 **Accepted:** 13 April 2024

Abstract

National security is one of the most important basic components of any political system, as it is always threatened from various dimensions. Any national security issue that relies on cyberspace, including health information technology, is potentially at risk. Political elites strive to protect the country from both hard and soft threats. Cybersecurity in the health sector is strategically important and is considered a component of sustainable national security.

Keywords: Cybersecurity, Cyberspace, Information Technology.

*** Corresponding Author:** Seyyed Yahya Safavi
Address: Imam Hossein University, Tehran, Iran.
E-mail: yahyasafavi@gmail.com

نشریه بهداری رزمی دفاع مقدس و مقاومت
۱۴۰۳، دوره ۷، شماره ۱، صفحات: ۱۴-۱۰
10.30491/jcm.2024.216115
مروری کوتاه

نقش سلامت در امنیت و توسعه پایدار ملی
بخش هشتم: امنیت سایبری و سلامت

سیدیحیی صفوی[1*]

[1] استاد جغرافیای سیاسی، دانشگاه امام حسین (ع)، تهران، ایران

دریافت مقاله: ۱۴۰۲/۱۲/۰۵ **پذیرش مقاله:** ۱۴۰۳/۰۱/۲۵

چکیده

امنیت ملی از مهمترین مؤلفه‌های مبنایی هر نظام سیاسی به‌شمار می‌رود، که همواره از ابعاد مختلفی تهدید می‌شود و نخبگان سیاسی با تمرکز بر این ابعاد، سعی دارند تا کشور را از معرض تهدیدات سخت و نرم پیش‌رو عبور دهند (۱). هر موضوع مرتبط با امنیت ملی که به فضای مجازی وابسته است، از جمله فناوری اطلاعات سلامت، به‌طور بالقوه در معرض خطر است. داده‌ها، زیرساخت‌های سایبری و حتی امنیت نظامی و ملی می‌توانند با حملات عمدی، نقص‌های امنیتی سهوی و آسیب‌پذیری‌های اینترنت جهانی در معرض خطر قرار گیرند (۲). امنیت سایبری در حوزه سلامت از اهمیت راهبردی برخوردار است و از مؤلفه‌های امنیت پایدار ملی محسوب می‌شود.

کلیدواژه‌ها: امنیت، سلامت، امنیت سایبری، فضای مجازی، فناوری اطلاعات.

*** نویسنده مسئول:** سیدیحیی صفوی
آدرس: دانشگاه امام حسین (ع)، تهران، ایران.
ایمیل: yahyasafavi@gmail.com

مقدمه

تهدیدات امنیت سایبری در دنیا نظیر دسترسی غیرمجاز به شبکه یا هک کردن، فیشینگ، کلاهبرداری ایمیلی، هرزنامه‌نویسی و تروریسم سایبری، باعث وارد آوردن خسارات مادی و معنوی جبران ناپذیری به سازمان‌ها می‌شود (۳).

هدف این گفتار مصون‌سازی زیرساخت‌های سایبری و وابسته به سایبر نظام سلامت در برابر تهدیدات سایبری، از طریق کاهش آسیب‌پذیری، افزایش سطح آمادگی‌های ضروری و حفظ و تضمین تداوم کارکردهای اساسی است.

امنیت سایبری عمل محافظت از سیستم‌های حیاتی و اطلاعات حساس در برابر حملات دیجیتالی است. اقدامات مبتنی بر امنیت سایبری که با عنوان امنیت فناوری اطلاعات (IT) نیز شناخته می‌شود، برای مقابله با تهدیدات علیه سیستم‌ها و برنامه‌های مبتنی بر شبکه طراحی شده‌اند، خواه این تهدیدات از داخل یا خارج از سازمان سرچشمه بگیرند (۳). هدف از امنیت سایبری، محافظت از اطلاعات در برابر سرقت و آسیب است. بدون وجود امنیت سایبری، سازمان‌ها نمی‌توانند از خود در برابر نقض‌های داده‌ای و حمله‌های هکرها دفاع کنند و به هدفی ساده برای مجرمان سایبری تبدیل می‌شوند. مخاطرات امنیتی به‌دلیل گسترده‌تر شدن ارتباطات در مقیاس جهانی و استفاده از سرویس‌های ابری برای ذخیره‌سازی اطلاعات حساس و شخصی رو به افزایش است. امنیت سایبری به‌طورکلی شامل تغییر رویکرد امنیتی از اقدام واکنشی به اقدام پیشگیرانه است.

امنیت سایبری در حوزه سلامت به‌معنای دسترسی ایمن به اطلاعات مددجویان به‌صورت محرمانه است که چالش‌های اصلی پیشرو شامل محرمانه‌بودن اطلاعات، حمله نفوذگران، ذخیره‌سازی ایمن داده‌ها و اشتراک‌گذاری ایمن داده‌ها است (۴).

سلامت الکترونیک به مفهوم ارائه خدمات بهداشتی با استفاده از فن‌آوری دیجیتال است (۵). در تعریف سازمان بهداشت جهانی «سلامت الکترونیک به معنای انتقال منابع سلامت و مراقبت‌های بهداشتی از طریق وسایل الکترونیکی است و سه حوزه اصلی آن عبارتند از: ارائه اطلاعات پزشکی به فرد متخصص از طریق اینترنت و ارتباطات راه دور، استفاده از فن‌آوری اطلاعات و تجارت الکترونیکی برای بهبود خدمات پزشکی از طریق آموزش افراد مرتبط و استفاده از تجارت الکترونیکی و کسب وکار الکترونیکی در مدیریت سامانه پزشکی» (۶).

محرمانگی اطلاعات سلامت در شرایط جاری از طریق شیوه‌های بسیار امن نظیر استفاده از ابزارهای تکنولوژیکی، رمزگذاری داده‌ها یا کنترل دسترسی به سیستم‌ها محافظت می‌شود (۷).

تهدیدات سایبری به تهدیداتی در فضای سایبری گفته می‌شود که کاربران، تجهیزات و شبکه‌ها را مورد حمله قرار می‌دهند. این تهدیدات عبارتند از: تهدیدات شبکه‌ای، تهدیدات مرتبط با برنامه‌های کاربردی، تهدیدات دسترسی از راه دور و تهدیدات دستکاری داده‌ها (۸).

پیش‌بینی و پیشگیری بحران‌های سلامت جامعه

به دلایل مختلف ممکن است پیش‌بینی بحران و نتایج محتمل آن برای سیاست‌گذاران مهیا نباشد، اما احتمال کمک سرویس‌های اطلاعاتی به سیاست‌گذاران در درک موقعیت بحرانی، غیرقطعی و غیر قابل پیش‌بینی متصور است چراکه پیچیدگی آن طیف گسترده‌ای از نتایج محتمل را در بر می‌گیرد ... از این رو، نیاز مبرم به روش جدیدی برای حمایت از سیستم اطلاعاتی برای سیاست‌گذاران درگیر بحران وجود دارد (۹). رسانه‌ها با نقش و مسئولیت خطیری که بر عهده دارند, موظفند هر لحظه افکار عمومی جهان را از شرایط حاکم بر دنیای پیرامون و اثرات بحران‌های اجتماعی ناخواسته، ازجمله در حوزه سلامت آگاه و برای پیشگیری و مقابله با بحران‌ها, راهکارهایی مناسب ارایه کنند (۱۰).

نقش رسانه ملی در مدیریت بحران

رسانه‌ها در دنیای امروز جایگاه ویژه و منحصر به فردی در مدیریت افکار عمومی دارند به طوری که نظام‌های سیاسی تلاش می‌کنند از رسانه‌ها برای هدایت و مهندسی ارزش‌ها و نگرش‌های جامع استفاده کنند. در واقع رسانه‌ها یکی از مهمترین ابزارهای مدیریت تغییر و تحولات اجتماعی به شمار می‌آیند و به واسطه این کارکرد مهم، تأثیر مستقیمی در انسجام ملی و در نهایت افزایش قدرت نرم کشورها می‌گذارند. نقش رسانه ملی بر مدیریت تغییرات اجتماعی تعیین‌کننده بوده و تأثیر مثبت دارد و با الهام از آموزه‌های اسلامی ایرانی موجب ارتقاء و افزایش قدرت نرم کشور خواهد شد (۱۱).

مشارکت اجتماعی و فرهنگی در ارتقای امنیت سایبری در سلامت

مشارکت اجتماعی و فرهنگی می‌تواند به عنوان عاملی اساسی در توسعه پایدار شهرهای جدید و ارتقاء امنیت اجتماعی مورد توجه و بحث و بررسی علمی قرار گیرد (۱۲). به‌موازات گسترش فعالیت‌ها و ارتباطات در فضای سایبر، بخشی از بزهکاران نیز فعالیت‌های مجرمانه خود را به فضای سایبر منتقل، یا از رهگذر چنین فضایی مرتکب جرم می‌شوند و امنیت این فضا را در معرض خطر قرار می‌دهند (۱۳).

بعضی از راهبردهای ارتقای امنیت سایبری که در حوزه سلامت کاربرد دارند:

- پیشگیری اجتماعی از جرایم سایبری در حوزه های سلامت و امنیت؛
- ارتقای فرهنگ و سواد سلامت جامعه بطور عام و فرهنگ و سواد سلامت دیژیتال بطور خاص؛
- استفاده از GIS در مدیریت بحران جامعه در مرحله‌های پیشگیری، آمادگی، مقابله و بازتوانی؛

- پیشگیری وضعی از جرایم در فضای سایبری نظیر دستورالعمل‌های قانونی برای نحوهٔ ارائه خدمات توسط ارائه‌دهندگان خدمات شبکه‌ای؛
- پیشگیری اجتماعی از جرایم در فضای سایبری (رفع انگیزه‌های مجرمانه و منحرفانه،که به‌عهده کارکردهای پیشگیرانه‌ای است که از آن‌ها به عنوان پیشگیری اجتماعی یاد می‌شود) (سیدعباس جزایری و همکاران).

راهبردهای ارتقای امنیت سایبری در حوزه سلامت

حکمرانی الکترونیک در نظام سلامت ملی شامل مشارکت اجتماعی، آگاهی‌بخشی عمومی و حرفه‌ای، توسعه زیرساخت‌های قانونی، سرمایه‌گذاری در حوزه‌های مختلف مرتبط، اعتماد اجتماعی و طراحی راهبردی فراگیر می‌باشد. قابلیت‌های اصلی این راهبرد شامل مدیریت سلامت الکترونیک، بهبود کارایی، دسترسی بهینه به خدمات، ادارهٔ الکترونیک و بهبود اثربخشی است. شفافیت، مسئولیت‌پذیری و نبود تبعیض در ارائهٔ خدمات بهداشتی– درمانی از اصول اساسی آن است (۱۴). موانع این مدل شامل کمبود بودجهٔ تخصیصی، حمایت نکردن، نداشتن مشارکت فراگیر، نبود زیرساخت‌های مناسب فناوری اطلاعات، آماده‌نبودن بستر فرهنگی، آموزش ناکافی و امنیت کم سایبری است. در ادامه، نتایج و پیامدهای این مدل، شامل پیامدهای فردی، سازمانی و اجتماعی شناسایی شدند و در نهایت مدل نهایی ارائه شد. مدل ارائه شده در این پژوهش می‌تواند نقشه راه مناسبی برای توسعهٔ حکمرانی الکترونیک در حوزهٔ سلامت کشور باشد. با گسترش روزافزون فناوری, نقش و اهمیت اطلاعات سلامت افزایش یافته است.

امنیت سایبری یک مؤلفه مهم در زیرساخت‌های کشور است. موفقیت در امنیت فضای سایبری به توانایی یک کشور در محافظت از اطلاعات اختصاصی و داده‌های خود در مقابل افراد، نهادها و کشورهایی که قصد سوءاستفاده از آن را دارند، بستگی دارد. امنیت سایبری در ایجاد وضعیت مناسب در مقابل حملات خرابکارانه و جلوگیری از حملات با هدف از کار انداختن یا اخلال در عملیات دستگاه یا سیستم، مفید می‌باشد. رویکرد توسعه امنیت سایبری، در نهایت موجب توسعه امنیت ملی خواهد شد (۸). در یک مطالعه اخیر چهار راهبرد: محافظه‌کارانه، تهاجمی، تدافعی و رقابتی برای مدیریت فضای مجازی با رویکرد مشارکت سیاسی تعریف شده است. در این مطالعه راهبردهای تهاجمی و رقابتی بهترین راهبردها برای مدیریت فضای مجازی با رویکرد مشارکت سیاسی معرفی شده‌اند (۱۵).

نتیجه‌گیری

باوجود تلاش‌ها و پیشرفت‌ها و دستاوردهای قابل ملاحظه، زیرساخت‌های فناوری اطلاعات، متناسب با نیازهای ملی و متناسب با ضرورت‌های امنیت سایبری در سطح ملی نیست. راهبرد امنیت سایبری در حوزه سلامت، یک فرآیند مداوم ، بسیار مهم و ضروری است که با امنیت پایدار ملی گره خورده‌است. مهمترین راهبرد آن تغییر رویکرد امنیتی از اقدام واکنشی به اقدام پیشگیرانه است. برقراری حکمرانی الکترونیک در نظام سلامت کشور با سیاست گذاری عالمانه، اختصاص منابع و اعتبارات کافی و تخصیص کارآمد آن‌ها، اعمال مدیریت صحیح و برنامه‌ریزی مناسب از راهبردهای اصولی برقراری امنیت سایبری سلامت با رویکرد امنیت ملی است. شناسایی ضعف‌ها و ارزیابی قوت‌ها برای پیشرفت، پیش‌بینی اتفاقات احتمالی، آزمایش‌ها و تمرین‌ها و شبیه‌سازی اتفاقات احتمالی برای افزایش آمادگی برای مقابله درصورت بروز یک تهدید جدید، مورد تأکید است.

تضاد منافع: بدین وسیله نویسنده تصریح می‌نماید که هیچ‌گونه تضاد منافعی در مطالعه حاضر وجود ندارد.

منابع

1. Dabirian F, Eftekhari A. Determining the system of national security dimensions in the Islamic Republic of Iran. Journal of National Security. 2024;14(52):9-46. [In Persian]
2. Golestan Governorate and the Iranian Passive Defense Organization: Cybersecurity; 2022. [In Persian]
3. Bijani S, Talebi M, Entezari MH, Salehesfahani M. Cyber Security maturity conceptual model of major telecom (mobile) operators. National Security. 2023;13(48):137-54. [In Persian]
4. Narimani K, Ahmadi M, Farhangi P. Cyber Security Challenges of the Health Section: A Review Study. Journal of Combat Medicine. 2023;6(1):11-7. [In Persian] doi:10.30491/jcm.2024.430809.1020
5. Pournaghi SM, Bayat M, Farjami Y. A novel and secure model for sharing protected health record (PHR) based on blockchain and attribute based encryption. Electronic and Cyber Defense. 2020;8(1):101-24. [In Persian]
6. Rezaei M, Dorri Nogoorani S. Management of Electronic Health Records with Preservation of Privacy using the Blockchain Technology. Biannual Journal Monadi for Cyberspace Security (AFTA). 2022;11(1):48-58. [In Persian]
7. Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal. 2021;22(2):177-83. doi:10.1016/j.eij.2020.07.003
8. Anousha S, Nikjou M. Cybersecurity Strategy. 3rd Interdisciplinary Research Conference in Engineering and Management Sciences; 2022. [In Persian]
9. Aqili SH, Ramezani M. The role of intelligence services in managing international crises. National Security. 2023;13(48):63-86. [In Persian]
10. Nejatbakhsh Esfahani A, Bagheri A. The role of mass media in crisis prevention. Communication

Research. 2009;15(56):137-59. [In Persian] doi:10.22082/cr.2008.23969
11. Keyghobadi A, Jafary AA. Analyzing and explaining the role of IRIB in managing social change. National Security. 2023;13(48):155-78. [In Persian]
12. Moradpour F, Mohseni R, Rahimi M. Investigating the role of citizens' social and cultural participation in the sustainable development of new cities with emphasis on reducing social harms. National Security. 2024;14(52):69-96. [In Persian]
13. Jazayeri SA, Nematollahi M, Amirian Farsani A. Prevention of cybercrimes and its governing restrictions. Qanon Yar. 2017;3(12):24-9. [In Persian]
14. Loghman Estarki S. The design of E-Governance pattern in health system (Case study: Ministry of Health and Medical Education of Iran). Science and Technology Policy Letters. 2023;13(2):5-21. [In Persian]
15. Kazemizad Haidar Baghi A, Ahmadi Sefidan H, Javanpour Heravi A, Shakeri E. Providing an appropriate strategy for cyberspace management with a political participation approach. National Security. 2024;13(50):41-84. [In Persian]