Strategic Studies of International Politics
https://jpir.journals.umz.ac.ir/ E-ISSN: 2717-0551
Vol. 9, No. 2, Issue. 18, Summer 2026 *** Received: 2026/05/08 Accepted: 2026/07/12
Research paper

Cyber Espionage and the Redefinition of Security Threats in the Foreign Policy of the United States of America

Ali Zargar
Department of Criminal Law and Criminology, CT, C, Islamic Azad University, Tehran, Iran.
Email: Ali.zargar@iau.ac.ir 0009-0000-5245-7385
Roya Asiaei
Department of Criminal Law and Criminology, Ahv, C, Islamic Azad University, Ahvaz, Iran. (Corresponding Author)
Email: R.asiaee@iauctb.ac.ir 0000-0002-2343-806X
Morteza Naji Zavareh
Department of Criminal Law and Criminology, CT, C, Islamic Azad University, Tehran, Iran.
Email: Mor.Naji_Zavarei@iauctb.ac.ir 0009-0008-0585-1898

Abstract

This study examines the role of cyber espionage in redefining security threats and its impact on United States foreign policy. The central research question is how cyber espionage has transformed perceptions of security threats and reshaped U.S. foreign policy strategies. Drawing on cybersecurity theory and the securitization approach, and employing a descriptive–analytical method, the study analyzes the position of cyber espionage within the national security structure and foreign policy of the United States. The findings demonstrate that cyber espionage has evolved beyond a merely technical threat and has been redefined as a strategic threat to national security, critical infrastructure, and U.S. economic and political interests. The expansion of cyber threats and increasing involvement of state and non-state actors have encouraged U.S. foreign policy to strengthen cyber deterrence, expand international security cooperation, and enhance intelligence and surveillance capabilities. Moreover, U.S. security and intelligence institutions play a central role in managing and responding to digital espionage threats. Overall, the expansion of cyber espionage has contributed to redefining traditional concepts of security and generating new forms of transnational threats. Consequently, cyber espionage has become a major driver of transformation in U.S. security, intelligence, and diplomatic policies in the digital age.

Keywords: Cyber Espionage, National Security, United States Foreign Policy, Security Threats.

Extended Abstract

Introduction: The rapid development of information and communication technologies and the growing dependence of governments, economies, and critical infrastructure on digital networks have fundamentally transformed the nature of security threats in the international system. In this context, cyberspace has evolved from a primarily technological domain into a strategic arena for geopolitical competition, intelligence gathering, power projection, and the reconfiguration of international power relations. Among emerging cyber threats, cyber espionage has acquired particular strategic significance because it enables actors to penetrate information systems, obtain sensitive data, influence decision-making processes, and gain informational advantages without resorting to conventional military force. The United States, as a leading global power and a major technological actor, has been particularly exposed to these developments due to its extensive dependence on digital infrastructures and its central position in the global information environment. The present study argues that cyber espionage can no longer be understood merely as a technical or intelligence-related threat; rather, it has increasingly been constructed as a strategic and existential threat to U.S. national security, critical infrastructure, technological superiority, and geopolitical interests. The study therefore focuses on the mechanisms through which cyber espionage has been transformed into a prioritized security concern and examines its consequences for the evolution of U.S. foreign policy.

Research Question: Through what discursive and security mechanisms has cyber espionage contributed to the redefinition of security threats and the reconfiguration of U.S. foreign policy strategies?

Research Hypothesis: The study hypothesizes that the impact of cyber espionage on U.S. foreign policy is not determined solely by the technological characteristics of cyber threats; rather, it is primarily mediated by the process of securitization through which the U.S. government, as a securitizing actor, represents cyber espionage as a strategic and existential threat through official discourse, strategic documents, intelligence assessments, and institutional practices. The acceptance of this security narrative by relevant audiences legitimizes extraordinary measures and subsequently contributes to the redefinition of security threats and the transformation of U.S. foreign and security policies.

Methodology and Theoretical Framework: This study employs a descriptive–analytical methodology to examine the position of cyber espionage within the national security structure and foreign policy of the United States. The theoretical framework integrates two complementary approaches: cybersecurity theory and the securitization theory of the Copenhagen School. Cybersecurity theory provides an analytical basis for explaining the distinctive characteristics of cyber threats, including their transnational nature, attribution difficulties, rapid dissemination, persistent intrusion capabilities, access to strategic information, and potential impact on critical infrastructure and governmental decision-making. Securitization theory, developed within the Copenhagen School, explains how political actors transform an issue from an ordinary policy concern into an existential security threat through speech acts, official documents, strategic narratives, and political practices. Within the analytical model of this study, cyber espionage constitutes the independent variable, securitization functions as the mediating variable, and the redefinition of security threats and the transformation of U.S. foreign policy constitute the dependent variables. The analysis focuses on five core components of securitization: the securitizing actor, the referent object, the speech act, the audience, and extraordinary measures.

Research Findings: The findings demonstrate that cyber espionage has moved beyond the domain of a technical or conventional intelligence threat and has been reconstructed within U.S. national security discourse as a strategic and existential threat. The U.S. government, together with security, intelligence, military, and political institutions, has played a central role in this securitization process by portraying cyber espionage as a threat to national security, critical infrastructure, digital sovereignty, technological superiority, strategic decision-making, and the continuity of governmental functions.

Strategic documents, official statements, intelligence assessments, and institutional practices have functioned as important speech acts through which cyber espionage has been elevated to the national security agenda. At the same time, the acceptance of this security narrative by Congress, executive institutions, the media, technology companies, research institutions, the public, and international allies has facilitated the institutionalization of cybersecurity as a permanent component of U.S. security governance.

The findings further indicate that the securitization of cyber espionage has transformed the concept of deterrence in U.S. security policy. Traditional deterrence, which was primarily associated with military capabilities and conventional strategic power, has increasingly been complemented by cyber deterrence, enhanced threat-detection capabilities, rapid response mechanisms, intelligence cooperation, and strengthened protection of critical infrastructure. Moreover, cybersecurity has become an increasingly important component of U.S. foreign policy through cyber sanctions, formal attribution of cyber operations, intelligence sharing, cyber diplomacy, and expanded security cooperation with allies within NATO, the G7, and other multilateral arrangements.

The study also demonstrates that the securitization process has contributed to institutional reforms, increased investment in cyber capabilities, closer coordination among intelligence, military, governmental, and private-sector actors, and the expansion of surveillance and intelligence capacities. Consequently, the boundary between domestic and external security has become increasingly blurred, while cyberspace has emerged as a major arena of geopolitical competition and security diplomacy.

Conclusion: The study concludes that cyber espionage has become a major driver of transformation in U.S. national security and foreign policy in the digital age. Its strategic significance cannot be adequately explained by its technological characteristics or by the increasing frequency and sophistication of cyber operations alone. Rather, its political significance has been constructed through a process of securitization in which U.S. political and security actors have represented cyber espionage as an existential threat, secured audience acceptance, and thereby legitimized extraordinary security measures.

This process has expanded the referent objects of national security from territorial integrity and military capabilities to include critical infrastructure, information security, digital networks, technological superiority, the digital economy, supply chains, and strategic decision-making capabilities. As a result, U.S. foreign policy has increasingly incorporated cyber deterrence, cyber sanctions, intelligence cooperation, cyber diplomacy, and multilateral cybersecurity arrangements. Overall, the study demonstrates that cyber espionage should be understood not merely as a technological phenomenon but as a strategic factor contributing to the transformation of security concepts, institutional structures, and foreign policy instruments in the United States. The integration of cybersecurity theory with securitization theory therefore provides a more comprehensive explanation of how technological

developments are translated into security priorities and ultimately reshape the foreign policy behavior of a major international power.

Keywords: Cyber Espionage, National Security, United States Foreign Policy, Security Threats.

E-ISSN: 2717-0551 / University of Mazandaran / Quarterly of Strategic Studies of International Politics

doi 10.22080/jpir.2026.31767.1584

فصلنامه علمی مطالعات راهبردی سیاست بین الملل
سال نهم، شماره دوم (پیاپی ۱۸)، تابستان ۱۴۰۵، صص. ۱۸۷-۲۱۴
تاریخ دریافت: ۱۴۰۵/۰۲/۱۸ ـ تاریخ پذیرش: ۱۴۰۵/۰۴/۲۱

مقاله پژوهشی

جاسوسی سایبری و بازتعریف تهدیدات امنیتی در سیاست خارجی ایالات متحدهٔ آمریکا

علی زرگر
گروه حقوق کیفری و جرم‌شناسی، واحد تهران مرکز، دانشگاه آزاد اسلامی، تهران، ایران.
Email: Ali.zargar@iau.ac.ir 0009-0000-5245-7385

رویا آسیایی
گروه حقوق کیفری و جرم‌شناسی، واحد اهواز، دانشگاه آزاد اسلامی، اهواز، ایران. (نویسندهٔ مسئول)
Email: R.asiaee@iauctb.ac.ir 0000-0002-2343-806X

مرتضی ناجی زواره
گروه حقوق کیفری و جرم‌شناسی، واحد تهران مرکز، دانشگاه آزاد اسلامی، تهران، ایران.
Email: Mor.Naji_Zavarei@iauctb.ac.ir 0009-0008-0585-1898

چکیده

این پژوهش با هدف بررسی نقش جاسوسی سایبری در بازتعریف تهدیدات امنیتی و تأثیر آن بر سیاست خارجی ایالات متحده انجام شده است. پرسش اصلی پژوهش آن است که جاسوسی سایبری چگونه درک تهدیدات امنیتی را متحول و راهبردهای سیاست خارجی آمریکا را بازطراحی کرده است. پژوهش با تکیه بر چارچوب نظری امنیت سایبری و رویکرد امنیتی‌سازی و با استفاده از روش توصیفی ـ تحلیلی، جایگاه جاسوسی سایبری را در ساختار امنیت ملی و سیاست خارجی آمریکا بررسی می‌کند. یافته‌ها نشان می‌دهد جاسوسی سایبری از سطح یک تهدید صرفاً فنی فراتر رفته و به تهدیدی راهبردی علیه امنیت ملی، زیرساخت‌های حیاتی و منافع اقتصادی و سیاسی آمریکا تبدیل شده است. گسترش تهدیدات سایبری و افزایش نقش بازیگران دولتی و غیردولتی، سیاست خارجی آمریکا را به سوی تقویت بازدارندگی سایبری، توسعه همکاری‌های امنیتی بین‌المللی و ارتقای ظرفیت‌های اطلاعاتی و نظارتی سوق داده است. همچنین، نهادهای امنیتی و اطلاعاتی آمریکا نقش محوری در مدیریت و مقابله با تهدیدات ناشی از جاسوسی دیجیتال ایفا می‌کنند. در مجموع، گسترش جاسوسی سایبری به بازتعریف مفهوم سنتی امنیت و شکل‌گیری الگوهای جدید تهدیدات فراملی انجامیده و به یکی از عوامل مهم تحول در سیاست‌های امنیتی، اطلاعاتی و دیپلماتیک آمریکا در عصر دیجیتال تبدیل شده است.

کلیدواژه‌ها: جاسوسی سایبری، امنیت ملی، سیاست خارجی ایالات متحدهٔ آمریکا، تهدیدات امنیتی.

شاپای الکترونیک: ۰۵۵۱-۲۷۱۷/ دانشگاه مازندران/ فصلنامه علمی مطالعات راهبردی سیاست بین الملل

doi 10.22080/jpir.2026.31767.1584

۱. مقدمه

تحولات شتابان فناوری‌های اطلاعاتی و ارتباطی در دهه‌های اخیر، ماهیت امنیت و الگوهای سنتی تهدید در نظام بین‌الملل را با دگرگونی‌های بنیادین مواجه ساخته است. گسترش فضای سایبری و وابستگی روزافزون دولت‌ها، نهادهای اقتصادی و زیرساخت‌های حیاتی به شبکه‌های دیجیتال، سبب شده است که تهدیدات سایبری از سطح مخاطرات صرفاً فنی فراتر رفته و به یکی از مهم‌ترین چالش‌های امنیت ملی و سیاست خارجی دولت‌ها تبدیل شوند (Moulin, 2023: 6). در این میان، فضای سایبری دیگر تنها یک بستر فناورانه محسوب نمی‌شود؛ بلکه به عرصه‌ای برای رقابت ژئوپلیتیکی، اعمال قدرت، جمع‌آوری اطلاعات راهبردی و بازتعریف موازنه‌های قدرت در نظام بین‌الملل تبدیل شده است (Delerue, 2023: 22). در میان انواع تهدیدات سایبری، جاسوسی سایبری جایگاه ویژه‌ای یافته است؛ زیرا این پدیده با فراهم‌کردن امکان نفوذ به سامانه‌های اطلاعاتی، دست‌یابی به داده‌های محرمانه و اثرگذاری بر فرآیندهای تصمیم‌گیری، بدون توسل به ابزارهای نظامی متعارف، به یکی از مهم‌ترین ابزارهای رقابت میان دولت‌ها تبدیل شده است (Topor, 2024: 48; Smeets, 2023: 717). در نتیجه، جاسوسی سایبری نه‌تنها شیوه‌های سنتی جمع‌آوری اطلاعات را متحول ساخته، بلکه مرزهای میان امنیت داخلی و خارجی، امنیت نظامی و امنیت اطلاعاتی را نیز تا حد زیادی کم‌رنگ کرده و دولت‌ها را ناگزیر از بازاندیشی در مفهوم امنیت ملی کرده است.

ایالات متحدهٔ آمریکا به‌عنوان یکی از بازیگران اصلی نظام بین‌الملل و قدرت پیشرو در حوزهٔ فناوری‌های دیجیتال، بیش از بسیاری از کشورها تحت تأثیر این تحول قرار گرفته است. از یک‌سو، این کشور دارای گسترده‌ترین ظرفیت‌های اطلاعاتی و سایبری در سطح جهانی است و از سوی دیگر، به دلیل وابستگی عمیق ساختارهای حکمرانی، اقتصادی و زیرساختی خود به فضای سایبری، همواره یکی از مهم‌ترین اهداف عملیات جاسوسی سایبری محسوب می‌شود. رخدادهایی نظیر عملیات «سولاروینِدز[1]» و نفوذهای گسترده به زیرساخت‌های اطلاعاتی آمریکا نشان داده‌اند که جاسوسی سایبری صرفاً یک مسألهٔ فناورانه نیست؛ بلکه می‌تواند پیامدهای مستقیمی برای امنیت ملی، فرآیندهای تصمیم‌گیری، سیاست خارجی و جایگاه بین‌المللی این کشور به همراه داشته باشد (Edelman, 2024: 55).

1. SolarWinds

با وجود گسترش چشم‌گیر ادبیات پژوهشی در حوزهٔ امنیت سایبری، بررسی مطالعات پیشین نشان می‌دهد که بخش عمدهٔ پژوهش‌ها بر ابعاد فنی حملات سایبری، راهبردهای بازدارندگی، مسائل حقوق بین‌الملل یا رقابت‌های ژئوپلیتیکی قدرت‌های بزرگ تمرکز داشته‌اند. در مقابل، پژوهش‌هایی که به‌صورت هم‌زمان نقش جاسوسی سایبری در بازتعریف ادراک تهدیدات امنیتی و تأثیر این بازتعریف بر سیاست خارجی ایالات متحده را از منظر نظریهٔ امنیتی‌سازی بررسی کرده باشند، بسیار محدود هستند. همچنین، در بسیاری از مطالعات موجود، رابطهٔ میان ویژگی‌های ذاتی تهدیدات سایبری و فرآیند گفتمانی امنیتی‌سازی به‌صورت منسجم تبیین نشده و مشخص نشده است که چگونه دولت آمریکا از طریق اسناد راهبردی، گفتمان‌های رسمی و سیاست‌های امنیتی، جاسوسی سایبری را از یک مسألهٔ فنی به یک تهدید وجودی علیه امنیت ملی تبدیل کرده و بر مبنای آن، اقدامات و راهبردهای جدید سیاست خارجی را مشروعیت بخشیده است. این خلأ نظری و تحلیلی، ضرورت انجام پژوهشی را آشکار می‌کند که بتواند پیوند میان امنیت سایبری، فرآیند امنیتی‌سازی و تحول سیاست خارجی ایالات متحده را در قالب یک چارچوب تحلیلی واحد تبیین کند.

نوآوری پژوهش حاضر در همین چارچوب قابل تبیین است. برخلاف بخش قابل توجهی از مطالعات پیشین که یا صرفاً بر ابعاد فنی جاسوسی سایبری تمرکز کرده‌اند یا تنها به توصیف سیاست‌های امنیت سایبری آمریکا پرداخته‌اند، این پژوهش با تلفیق نظریه‌های امنیت سایبری و رویکرد امنیتی‌سازی، نشان می‌دهد که چگونه دولت ایالات متحده از طریق گفتمان‌های رسمی، اسناد راهبردی و سازوکارهای نهادی، جاسوسی سایبری را به‌عنوان یک تهدید راهبردی و وجودی بازنمایی کرده و این فرآیند چگونه به بازتعریف تهدیدات امنیتی و تحول در سیاست خارجی این کشور انجامیده است. بدین ترتیب، پژوهش حاضر علاوه بر تبیین ماهیت راهبردی جاسوسی سایبری، سازوکارهای گفتمانی و سیاسی تبدیل این پدیده به یک مسألهٔ امنیت ملی را نیز مورد تحلیل قرار می‌دهد و از این منظر، می‌کوشد خلأ موجود در ادبیات پژوهش را تا حدی برطرف سازد. بر اساس این، هدف اصلی پژوهش، بررسی نقش جاسوسی سایبری در بازتعریف تهدیدات امنیتی و تحلیل تأثیر فرآیند امنیتی‌سازی آن بر سیاست خارجی ایالات متحدهٔ آمریکا است. پرسش اصلی تحقیق آن است که جاسوسی سایبری از طریق چه سازوکارهای گفتمانی و امنیتی، موجب بازتعریف تهدیدات امنیتی و بازآرایی راهبردهای سیاست خارجی ایالات متحدهٔ آمریکا شده است؟

۲. ادبیات نظری و پیشینهٔ پژوهش

پژوهش حاضر از تلفیق دو رویکرد نظری بهره می‌گیرد. نخست، نظریه‌های امنیت سایبری که ویژگی‌های تهدیدات ناشی از فضای سایبری، پیامدهای آن برای امنیت ملی و نقش آن در تحول الگوهای قدرت و رقابت بین‌المللی را تبیین می‌کنند. دوم، نظریهٔ امنیتی‌سازی مکتب کپنهاگ که نشان می‌دهد چگونه دولت‌ها از طریق گفتمان‌های رسمی، اسناد راهبردی و کنش‌های سیاسی، یک مسأله را از حوزهٔ سیاست عادی خارج کرده و به‌عنوان تهدیدی وجودی برای امنیت ملی بازنمایی می‌کنند.

تلفیق این دو رویکرد امکان تحلیل دو بعد مکمل پدیدهٔ جاسوسی سایبری را فراهم می‌کند؛ بعد نخست، ویژگی‌ها و ظرفیت‌های واقعی این پدیده به‌عنوان یک تهدید نوظهور و بعد دوم، فرآیندی که طی آن دولت ایالات متحده این تهدید را در گفتمان امنیت ملی خود امنیتی‌سازی کرده و بر مبنای آن راهبردها و سیاست‌های جدیدی را در عرصهٔ سیاست خارجی اتخاذ کرده است. بر اساس این، چارچوب نظری پژوهش بر این فرض استوار است که تأثیر جاسوسی سایبری بر سیاست خارجی ایالات متحده صرفاً ناشی از ویژگی‌های فنی این پدیده نیست؛ بلکه نتیجهٔ تعامل میان واقعیت‌های فناورانه و فرآیندهای گفتمانی امنیتی‌سازی است. ازاین‌رو، در ادامه ابتدا مبانی نظری امنیت سایبری برای تبیین ماهیت تهدید بررسی می‌شود و سپس نظریهٔ امنیتی‌سازی به‌عنوان چارچوب تحلیل نحوهٔ بازنمایی این تهدید در سیاست امنیتی و خارجی ایالات متحده تبیین خواهد شد.

۲-۱. نظریه‌های امنیت سایبری

امنیت سایبری یکی از مهم‌ترین حوزه‌های مطالعات امنیتی معاصر است که در پاسخ به گسترش وابستگی دولت‌ها و جوامع به فناوری‌های دیجیتال شکل گرفته است. برخلاف رویکردهای سنتی که امنیت را عمدتاً در قالب تهدیدات نظامی و دفاع از تمامیت ارضی تعریف می‌کردند، نظریه‌های امنیت سایبری بر این باورند که در عصر دیجیتال، اطلاعات، شبکه‌های ارتباطی و زیرساخت‌های حیاتی نیز به عناصر بنیادین امنیت ملی تبدیل شده‌اند (Kello, 2022: 61; Segal, 2023: 55). از منظر این نظریه‌ها، فضای سایبری دارای ویژگی‌هایی مانند فراملی بودن، دشواری انتساب حملات، سرعت بالای انتشار اطلاعات و امکان فعالیت هم‌زمان بازیگران دولتی و غیردولتی است. این ویژگی‌ها موجب شده‌اند که تهدیدات سایبری، به‌ویژه جاسوسی سایبری، بتوانند بدون توسل به ابزارهای متعارف نظامی، امنیت ملی، توان اطلاعاتی و

ظرفیت تصمیم‌گیری دولت‌ها را تحت تأثیر قرار دهند (Lindsay, 2023: 403). در این چارچوب، جاسوسی سایبری صرفاً به معنای سرقت اطلاعات نیست؛ بلکه ابزاری راهبردی برای کسب برتری اطلاعاتی، افزایش قدرت تصمیم‌سازی، شناخت ظرفیت‌های رقبا و تأثیرگذاری بر موازنهٔ قدرت محسوب می‌شود (Rid, 2023: 47). ازاین‌رو، بسیاری از دولت‌ها توسعهٔ توانمندی‌های سایبری را بخشی از راهبرد کلان امنیت ملی خود تلقی و حفاظت از زیرساخت‌های دیجیتال را در کنار دفاع نظامی، به یکی از مأموریت‌های اصلی نهادهای امنیتی تبدیل کرده‌اند (Valeriano et al., 2024: 78).

با وجود اهمیت این رویکرد، نظریه‌های امنیت سایبری عمدتاً بر ماهیت و ویژگی‌های تهدید تمرکز دارند و کمتر توضیح می‌دهند که چگونه یک تهدید فناورانه به اولویت سیاست امنیتی و خارجی دولت‌ها تبدیل می‌شود. به بیان دیگر، این نظریه‌ها وجود تهدید را تبیین می‌کنند، اما سازوکارهای سیاسی و گفتمانی تبدیل آن را به یک مسألهٔ امنیت ملی را به‌طور کامل توضیح نمی‌دهند. از همین رو، برای تحلیل نحوهٔ بازنمایی جاسوسی سایبری در سیاست خارجی ایالات متحده، بهره‌گیری از نظریهٔ امنیتی‌سازی ضروری است.

۲-۲. رویکرد امنیتی‌سازی

نظریه امنیتی‌سازی که توسط باری بوزان، اولی ویور و یاپ دویلده در چارچوب مکتب کپنهاگ توسعه یافت، یکی از تأثیرگذارترین رویکردهای مطالعات امنیتی معاصر است. این نظریه با فاصله‌گرفتن از برداشت‌های سنتی امنیت، بر این فرض استوار است که تهدیدات امنیتی صرفاً دارای ماهیتی عینی نیستند؛ بلکه در بسیاری از موارد، از طریق فرآیندهای گفتمانی، سیاسی و اجتماعی به‌عنوان «تهدید امنیتی» بازنمایی می‌شوند (Buzan & Hansen, 2020: 72). بر اساس این، امنیت نه‌فقط محصول وجود یک تهدید واقعی، بلکه نتیجهٔ فرآیندی است که طی آن یک بازیگر سیاسی می‌تواند موضوعی را به‌عنوان تهدیدی علیه بقا و امنیت جامعه معرفی کرده و پذیرش آن را از سوی مخاطبان به دست آورد. در این رویکرد، امنیتی‌سازی فرآیندی است که طی آن یک مسأله از حوزهٔ سیاست عادی خارج شده و به موضوعی مرتبط با امنیت ملی تبدیل می‌شود؛ به‌گونه‌ای که اتخاذ اقدامات استثنایی و فراتر از رویه‌های معمول سیاسی برای مقابله با آن مشروعیت می‌یابد (Wæver, 2019: 96)؛ بنابراین، در نظریهٔ امنیتی‌سازی، اهمیت اصلی نه‌صرفاً در وجود تهدید، بلکه در نحوهٔ بازنمایی و پذیرش آن به‌عنوان

یک تهدید وجودی است. بر اساس مکتب کپنهاگ، تحقق فرآیند امنیتی‌سازی مستلزم وجود پنج مؤلفهٔ اساسی است:

نخست، بازیگر امنیتی‌ساز[1]: یعنی فرد یا نهادی که موضوعی را به‌عنوان تهدید امنیتی مطرح می‌کند. در سطح دولت‌ها، این نقش معمولاً توسط رؤسای دولت، نهادهای امنیتی، وزارتخانه‌های مسؤول، شوراهای امنیت ملی یا سایر مقامات عالی‌رتبه ایفا می‌شود (Balzacq et al., 2023: 115).

دوم، ابژه مرجع[2] یعنی آن ارزش، نهاد یا موجودیتی که ادعا می‌شود در معرض تهدید قرار گرفته و حفاظت از آن ضروری است. بسته به موضوع، این ابژه می‌تواند امنیت ملی، حاکمیت، زیرساخت‌های حیاتی، اقتصاد، نظم سیاسی یا حتی هویت ملی باشد.

سوم، کنش گفتاری[3] که هستهٔ اصلی نظریهٔ امنیتی‌سازی را تشکیل می‌دهد. مطابق دیدگاه ویور، امنیتی‌سازی زمانی آغاز می‌شود که بازیگر امنیتی‌ساز، از طریق سخنرانی‌ها، اسناد رسمی، راهبردهای امنیت ملی، بیانیه‌های سیاسی یا سایر ابزارهای گفتمانی، موضوعی را به‌عنوان تهدیدی وجودی بازنمایی کند؛ بنابراین، امنیتی‌شدن یک مسأله صرفاً به دلیل وقوع آن نیست؛ بلکه به نحوهٔ بیان و صورت‌بندی آن در گفتمان رسمی بستگی دارد (Wæver, 2017: 64).

چهارم، مخاطب[4]: امنیتی‌سازی تنها زمانی موفق خواهد بود که مخاطبان، اعم از افکار عمومی، نهادهای قانون‌گذار، دستگاه‌های اجرایی یا متحدان بین‌المللی، روایت امنیتی ارائه‌شده را بپذیرند. درواقع، پذیرش مخاطبان شرط اساسی موفقیت فرآیند امنیتی‌سازی است.

پنجم، اقدامات فوق‌العاده[5]: هنگامی که یک مسأله به‌عنوان تهدیدی وجودی پذیرفته شود، دولت می‌تواند اقداماتی فراتر از رویه‌های معمول سیاست‌گذاری را برای مقابله با آن توجیه کند؛ اقداماتی مانند ایجاد نهادهای جدید، افزایش اختیارات امنیتی، توسعهٔ توانمندی‌های دفاعی، اعمال تحریم‌ها، گسترش همکاری‌های اطلاعاتی یا تصویب قوانین ویژه.

---

1. Securitizing Actor
2. Referent Object
3. Speech Act
4. Audience
5. Extraordinary Measures

کاربرد این نظریه در حوزهٔ امنیت سایبری طی سال‌های اخیر به‌طور چشم‌گیری گسترش یافته است. پژوهشگران این حوزه معتقدند که بسیاری از تهدیدات سایبری، ازجمله جاسوسی سایبری، صرفاً به دلیل ویژگی‌های فنی خود در کانون سیاست امنیتی قرار نگرفته‌اند؛ بلکه دولت‌ها با بهره‌گیری از گفتمان‌های امنیتی و اسناد راهبردی، آن‌ها را به‌عنوان تهدیدی علیه امنیت ملی و استمرار کارکرد دولت بازنمایی کرده‌اند (Hansen & Nissenbaum, 2022: 13-14). از این منظر، امنیت سایبری نه‌فقط نتیجهٔ تحول فناوری، بلکه حاصل فرآیندهای سیاسی و گفتمانی است که تهدیدات دیجیتال را به مسائل امنیت ملی تبدیل می‌کنند (Dunn Cavelty & Wenger, 2022: 153-154).

در پژوهش حاضر، نظریهٔ امنیتی‌سازی چارچوب اصلی تحلیل را تشکیل می‌دهد. بر اساس این، بررسی خواهد شد که دولت ایالات متحده چگونه در مقام بازیگر امنیتی‌ساز، از طریق اسناد راهبرد امنیت ملی، راهبرد امنیت سایبری، بیانیه‌های رسمی و مواضع مقامات ارشد به‌عنوان کنش‌های گفتاری، جاسوسی سایبری را به‌مثابه تهدیدی علیه امنیت ملی، زیرساخت‌های حیاتی و برتری راهبردی ایالات متحده (ابژه مرجع) بازنمایی کرده است؛ این بازنمایی چگونه توسط کنگره، نهادهای اجرایی، افکار عمومی و متحدان آمریکا (مخاطبان) پذیرفته شده و درنهایت چگونه به اتخاذ اقدامات فوق‌العاده نظیر توسعهٔ توان سایبری، اصلاح ساختارهای امنیتی، تشدید همکاری‌های اطلاعاتی، اعمال تحریم‌های سایبری و بازنگری در راهبردهای سیاست خارجی منجر شده است. بدین‌ترتیب، نظریه امنیتی‌سازی در این پژوهش صرفاً به‌عنوان یک چارچوب مفهومی معرفی نمی‌شود، بلکه مبنای مستقیم تحلیل داده‌ها و تفسیر یافته‌های پژوهش قرار می‌گیرد.

۳-۲. مدل تحلیلی پژوهش

بررسی نقش جاسوسی سایبری در تحول سیاست خارجی ایالات متحده مستلزم چارچوبی است که بتواند هم ویژگی‌های ذاتی این پدیده و هم فرآیند سیاسی تبدیل آن به یک مسألهٔ امنیت ملی را به‌صورت هم‌زمان تبیین کند. هر یک از دو رویکرد نظری مورد استفاده در این پژوهش، تنها بخشی از این فرآیند را توضیح می‌دهند. نظریه‌های امنیت سایبری، ماهیت، ویژگی‌ها و پیامدهای تهدیدات ناشی از فضای سایبری را تبیین می‌کنند، اما به‌تنهایی قادر به توضیح این مسأله نیستند که چرا برخی از این تهدیدات به اولویت سیاست امنیتی و خارجی دولت‌ها تبدیل می‌شوند. در مقابل، نظریهٔ امنیتی‌سازی، سازوکارهای گفتمانی و سیاسی تبدیل یک مسأله را به

تهدید امنیتی توضیح می‌دهد، اما دربارهٔ ویژگی‌های ذاتی تهدیدات سایبری توضیح مستقلی ارائه نمی‌کند. بر اساس همین، پژوهش حاضر با تلفیق این دو رویکرد، مدلی تحلیلی ارائه می‌دهد که طبق آن، جاسوسی سایبری متغیر مستقل، امنیتی‌سازی متغیر میانجی و بازتعریف تهدیدات امنیتی و تحول سیاست خارجی ایالات متحده متغیر وابسته محسوب می‌شوند.

در این چارچوب، ویژگی‌های خاص جاسوسی سایبری، ازجمله دشواری انتساب، فراملی بودن، قابلیت نفوذ به زیرساخت‌های حیاتی، دسترسی به اطلاعات راهبردی و امکان اثرگذاری بر فرآیندهای تصمیم‌گیری، زمینهٔ شکل‌گیری ادراک تهدید را فراهم می‌کند. بااین‌حال، این ویژگی‌ها به‌تنهایی برای تبدیل جاسوسی سایبری به یک مسألهٔ امنیت ملی کافی نیستند.

در گام بعد، دولت ایالات متحده به‌عنوان بازیگر امنیتی‌ساز، از طریق اسناد راهبرد امنیت ملی، راهبرد امنیت سایبری، گزارش‌های رسمی، بیانیه‌های سیاسی و مواضع مقامات ارشد، جاسوسی سایبری را به‌عنوان تهدیدی علیه امنیت ملی، زیرساخت‌های حیاتی، برتری فناورانه و جایگاه بین‌المللی آمریکا بازنمایی می‌کند. این کنش‌های گفتاری، در صورت پذیرش از سوی کنگره، نهادهای اجرایی، افکار عمومی و متحدان ایالات متحده، موجب امنیتی‌شدن جاسوسی سایبری و مشروعیت یافتن اقدامات فوق‌العاده در حوزهٔ سیاست‌گذاری امنیتی می‌شوند.

پیامد این فرآیند، بازآرایی راهبردهای امنیت ملی و سیاست خارجی ایالات متحده است. توسعهٔ توانمندی‌های سایبری، افزایش همکاری‌های اطلاعاتی و امنیتی، اعمال تحریم‌های سایبری، اصلاح ساختارهای نهادی، تقویت بازدارندگی سایبری و گسترش همکاری با متحدان، ازجمله مهم‌ترین اقداماتی هستند که در نتیجهٔ امنیتی‌شدن جاسوسی سایبری در سیاست خارجی آمریکا قابل مشاهده‌اند.

بر اساس این، فرض بنیادین پژوهش حاضر آن است که تأثیر جاسوسی سایبری بر سیاست خارجی ایالات متحده، صرفاً ناشی از ویژگی‌های فنی این پدیده نیست؛ بلکه محصول فرآیند امنیتی‌سازی آن در گفتمان رسمی و اسناد راهبردی دولت آمریکا است. ازاین‌رو، در بخش تحلیل، با استفاده از مؤلفه‌های نظریهٔ امنیتی‌سازی شامل بازیگر امنیتی‌ساز، کنش گفتاری، ابژه مرجع، مخاطب و اقدامات فوق‌العاده، نحوهٔ بازنمایی جاسوسی سایبری و آثار آن بر بازتعریف تهدیدات امنیتی و تحول سیاست خارجی ایالات متحده مورد بررسی قرار خواهد گرفت.

۴-۲. پیشینهٔ تجربی پژوهش

مرور ادبیات نشان می‌دهد که پژوهش‌های انجام‌شده در حوزهٔ جاسوسی سایبری و امنیت سایبری را می‌توان در سه دستهٔ اصلی طبقه‌بندی کرد:

دستهٔ نخست، پژوهش‌هایی هستند که بر ابعاد فنی و سازمانی جاسوسی سایبری تمرکز دارند. در این راستا، جمیری (۱۴۰۴) نشان داد که فقدان چارچوب‌های نظارتی، ضعف سواد امنیتی کاربران و بهره‌گیری مهاجمان از الگوریتم‌های هوش مصنوعی، نقش مهمی در افزایش آسیب‌پذیری‌های سایبری دارند. همچنین، ساوه‌درودی و خدادادی (۱۴۰۴) با بررسی انگیزه‌ها و آسیب‌پذیری‌های جاسوسی دیجیتال، چهار عامل اصلی شامل عوامل روان‌شناختی، اقتصادی، سایبری و ساختاری را به‌عنوان زمینه‌های مؤثر بر موفقیت عملیات جاسوسی معرفی کردند. این مطالعات، اگرچه شناخت مناسبی از عوامل ایجادکنندهٔ تهدیدات سایبری ارائه می‌کنند، اما پیامدهای این تهدیدات بر بازتعریف امنیت ملی و سیاست خارجی را مورد توجه قرار نداده‌اند.

دستهٔ دوم، پژوهش‌هایی هستند که ابعاد ژئوپلیتیکی و راهبردی امنیت سایبری را بررسی کرده‌اند. اسماعیلی و همکاران (۱۴۰۲) با تحلیل رقابت سایبری میان ایالات متحده و چین، نشان دادند که توسعهٔ قابلیت‌های سایبری چین موجب شکل‌گیری الگوهای جدید رقابت قدرت و حکمرانی سایبری شده است. همچنین، گارتزک و لیندسی[1] (۲۰۲۴) و بوکانان و رید[2] (۲۰۲۴) نتیجه گرفتند که جاسوسی سایبری به یکی از ابزارهای اصلی رقابت اطلاعاتی میان قدرت‌های بزرگ تبدیل شده و ساختار سنتی امنیت بین‌الملل را تحت تأثیر قرار داده است. این مطالعات بیشتر بر رقابت‌های ژئوپلیتیکی و کارکرد اطلاعاتی جاسوسی سایبری تمرکز داشته و کمتر به سازوکارهای ادراکی و گفتمانی تبدیل این پدیده به یک تهدید امنیتی پرداخته‌اند.

دستهٔ سوم، پژوهش‌هایی هستند که بر پیامدهای امنیتی و سیاست‌گذاری سایبری ایالات متحدهٔ آمریکا تمرکز داشته‌اند. در این زمینه، سگل[3] (۲۰۲۵) نشان داد که افزایش حملات و عملیات جاسوسی سایبری، امنیت سایبری را به یکی از اولویت‌های سیاست خارجی آمریکا تبدیل کرده و این کشور را به توسعهٔ راهبردهای بازدارندگی سایبری، سرمایه‌گذاری در فناوری‌های امنیتی و گسترش همکاری‌های بین‌المللی سوق داده است. همچنین، لیبیکی[4] (۲۰۲۵) بیان می‌کند که گسترش عملیات

1. Gartzke & Lindsay
2. Buchanan & Rid
3. Segal
4. Libicki

جاسوسی سایبری موجب تحول در راهبردهای دفاعی، اطلاعاتی و امنیتی ایالات متحده و تقویت همکاری‌های امنیتی این کشور با متحدانش شده است. با وجود اهمیت این مطالعات، تمرکز اصلی آن‌ها بر سیاست‌های بازدارندگی و مدیریت تهدیدات سایبری بوده و فرآیند شکل‌گیری و امنیتی‌شدن این تهدیدات در گفتمان رسمی آمریکا کمتر مورد توجه قرار گرفته است.

بررسی مجموع پژوهش‌های پیشین نشان می‌دهد که هرچند ابعاد فنی، ژئوپلیتیکی و راهبردی جاسوسی سایبری به‌طور گسترده مطالعه شده‌اند، اما دو خلأ اساسی همچنان باقی است. نخست، بیشتر مطالعات، جاسوسی سایبری را به‌عنوان یک تهدید عینی و فناورانه بررسی کرده‌اند و کمتر به این پرسش پرداخته‌اند که این پدیده چگونه از طریق گفتمان‌های رسمی و اسناد راهبردی ایالات متحده به یک تهدید وجودی برای امنیت ملی تبدیل شده است. دوم، ارتباط میان ویژگی‌های تهدیدات سایبری، فرآیند امنیتی‌سازی و بازتعریف سیاست خارجی آمریکا به‌صورت یک چارچوب تحلیلی منسجم تبیین نشده است. بر اساس این، پژوهش حاضر با بهره‌گیری هم‌زمان از چارچوب نظری امنیت سایبری و نظریه امنیتی‌سازی، می‌کوشد این خلأ را برطرف کند. تمرکز اصلی پژوهش نه‌صرفاً بر ماهیت فنی جاسوسی سایبری و نه‌صرفاً بر سیاست‌های امنیت سایبری ایالات متحده، بلکه بر تبیین این فرآیند است که چگونه دولت آمریکا از طریق گفتمان‌های رسمی، اسناد راهبردی و اقدامات نهادی، جاسوسی سایبری را به‌عنوان یک تهدید راهبردی و وجودی بازنمایی کرده و این بازنمایی چگونه بر بازتعریف تهدیدات امنیتی و تحول در سیاست خارجی این کشور اثر گذاشته است.

۳. بحث و بررسی؛ بازتعریف تهدیدات امنیتی در سیاست خارجی ایالات متحدهٔ آمریکا تحت تأثیر جاسوسی سایبری

۳-۱. امنیتی‌سازی جاسوسی سایبری و بازتعریف تهدیدات امنیت ملی ایالات متحدهٔ آمریکا

بر اساس نظریهٔ امنیتی‌سازی، یک تهدید صرفاً به دلیل ویژگی‌های عینی خود به مسأله‌ای امنیتی تبدیل نمی‌شود؛ بلکه زمانی امنیتی می‌شود که بازیگران امنیتی‌ساز از طریق کنش‌های گفتاری آن را به‌عنوان تهدیدی وجودی برای ابژه‌های مرجع معرفی کنند و این بازنمایی از سوی مخاطبان پذیرفته شود (Buzan & Hansen, 2020: 86). در این رابطه باید توجه داشت که در ایالات متحده، جاسوسی سایبری دقیقاً چنین مسیری را طی کرده است. اگرچه این پدیده در آغاز عمدتاً به‌عنوان مسأله‌ای فناورانه

و اطلاعاتی تلقی می‌شد، اما از اواخر دهۀ ۲۰۱۰، دولت آمریکا با اتکا به اسناد راهبرد امنیت ملی، راهبرد امنیت سایبری، گزارش‌های نهادهای اطلاعاتی و مواضع رسمی مقامات ارشد، آن را به‌عنوان تهدیدی علیه امنیت ملی، زیرساخت‌های حیاتی و برتری راهبردی ایالات متحده بازنمایی کرده است. از این منظر، دولت ایالات متحده در مقام بازیگر امنیتی‌ساز، با بهره‌گیری از کنش‌های گفتاری، زمینۀ امنیتی‌شدن جاسوسی سایبری را فراهم کرده است. در نتیجۀ این فرآیند، مفهوم امنیت ملی در ایالات متحده نیز دستخوش تحول شده است (Maurer & Morgus, 2022: 220).

از طرفی، وابستگی روزافزون نهادهای حکمرانی، زیرساخت‌های حیاتی، سامانه‌های مالی و مراکز تصمیم‌گیری به شبکه‌های دیجیتال، موجب شده است که نفوذ اطلاعاتی در فضای سایبری دیگر صرفاً یک تهدید فناورانه تلقی نشود؛ بلکه به‌عنوان تهدیدی علیه تداوم کارکرد دولت و حفظ برتری راهبردی آمریکا درک شود (Buchanan, 2022: 17). در چارچوب نظریۀ امنیتی‌سازی، ابژه مرجع در این مرحله تنها شبکه‌های رایانه‌ای نیستند؛ بلکه امنیت ملی، حاکمیت دیجیتال، زیرساخت‌های حیاتی و قابلیت تصمیم‌گیری راهبردی دولت آمریکا را نیز دربر می‌گیرند.

یکی از مهم‌ترین مصادیق این فرآیند، عملیات نفوذ زنجیرۀ تأمین موسوم به سولارویندز است. در این رخداد، مهاجمان از طریق آلوده‌سازی به‌روزرسانی نرم‌افزار شرکت ارائه‌دهندۀ خدمات فناوری اطلاعات، به شبکه‌های حساس وزارت خزانه‌داری، وزارت امنیت داخلی و سایر نهادهای فدرال دسترسی یافتند. اهمیت این رخداد صرفاً در گستردگی نفوذ نبود؛ بلکه در نحوۀ بازنمایی آن در گفتمان رسمی دولت آمریکا نهفته است. پس از افشای این عملیات، اسناد و بیانیه‌های رسمی دولت، این حمله را نه یک نقص فنی، بلکه تهدیدی علیه امنیت ملی، اعتماد عمومی به زیرساخت‌های دیجیتال و استمرار حکمرانی معرفی کردند. از منظر نظریۀ امنیتی‌سازی، این بازنمایی را می‌توان نمونه‌ای روشن از کنش گفتاری دانست که هدف آن تبدیل یک رخداد فناورانه به تهدیدی وجودی و مشروعیت‌بخشی به اقدامات امنیتی جدید بود (Weiss & Jankowski, 2023: 47-49).

از سوی دیگر، یافته‌ها نشان می‌دهد که ویژگی‌های ذاتی جاسوسی سایبری، ازجمله ناشناس بودن عاملان، دشواری انتساب حملات، تداوم نفوذ و امکان دسترسی پنهان به اطلاعات راهبردی، موجب شده است این پدیده با تهدیدات کلاسیک امنیتی تفاوت ماهوی داشته باشد (Jasper, 2022: 6). بااین‌حال، این ویژگی‌ها به‌تنهایی برای امنیتی‌شدن جاسوسی سایبری کافی نیستند. آنچه این پدیده را به مسأله‌ای امنیتی

تبدیل کرده، پذیرش روایت دولت آمریکا از سوی مخاطبان امنیتی‌سازی شامل کنگره، نهادهای اجرایی، افکار عمومی و متحدان این کشور است. این پذیرش، زمینهٔ لازم را برای خروج جاسوسی سایبری از حوزهٔ سیاست عادی و ورود آن به قلمرو سیاست‌های امنیت ملی فراهم کرده است.

در ادامهٔ این روند، دولت آمریکا مجموعه‌ای از اقدامات فوق‌العاده را برای مقابله با تهدیدات سایبری در دستور کار قرار داده است. بازنگری در سیاست‌های امنیت زنجیرهٔ تأمین نرم‌افزار، تقویت الزامات امنیتی برای زیرساخت‌های حیاتی، افزایش اختیارات نهادهای امنیت سایبری، توسعهٔ سامانه‌های شناسایی تهدید و گسترش همکاری میان نهادهای اطلاعاتی و بخش خصوصی، بخشی از اقداماتی است که پس از امنیتی‌شدن جاسوسی سایبری مشروعیت یافته‌اند. این اقدامات نشان می‌دهد که فرآیند امنیتی‌سازی صرفاً به تغییر گفتمان محدود نمانده، بلکه به تغییر در سیاست‌گذاری و ساختار حکمرانی امنیتی ایالات متحده نیز انجامیده است. نکتهٔ مهم آنکه امنیت سایبری در ایالات متحده از یک حوزهٔ تخصصی و فناورانه به یکی از ارکان اصلی سیاست امنیت ملی تبدیل شده است. در این چارچوب، نهادهایی مانند آژانس امنیت ملی، فرمان‌دهی سایبری ایالات متحده و آژانس امنیت سایبری و امنیت زیرساخت‌ها، علاوه بر ایفای نقش اجرایی، در تولید ادراک تهدید، ارائهٔ ارزیابی‌های راهبردی و شکل‌دهی به اولویت‌های امنیتی کشور نیز نقش فعالی دارند (Nocetti, 2023: 1568-1569).

بدین‌ترتیب، مرز میان سیاست امنیت داخلی و سیاست خارجی در حوزهٔ سایبری تا حد زیادی از میان برداشته شده و حکمرانی امنیتی آمریکا به سمت الگویی شبکه‌ای و چندسطحی حرکت کرده است. به‌طورکلی باید اذعان داشت که تحول جایگاه جاسوسی سایبری در سیاست امنیتی ایالات متحده، صرفاً پیامد پیشرفت فناوری یا افزایش حملات دیجیتال نبوده است؛ بلکه نتیجهٔ فرآیند امنیتی‌سازی این پدیده در گفتمان رسمی دولت آمریکا است. بازیگران امنیتی‌ساز با بهره‌گیری از اسناد راهبردی و مواضع رسمی، جاسوسی سایبری را به‌عنوان تهدیدی علیه امنیت ملی بازنمایی کرده‌اند؛ مخاطبان این روایت را پذیرفته‌اند و در نتیجه، اتخاذ اقدامات فوق‌العاده برای بازآرایی ساختار امنیتی و بازتعریف مفهوم امنیت ملی مشروعیت یافته است. این یافته‌ها مؤید آن است که نظریهٔ امنیتی‌سازی، نسبت به رویکردهای صرفاً فناورانه، قدرت تبیین بیشتری برای تحلیل تحول تهدیدات سایبری در سیاست امنیتی ایالات متحده دارد.

۲-۳. امنیتی‌سازی تهدیدات سایبری و تحول راهبردهای بازدارندگی ایالات متحده

یکی از مهم‌ترین پیامدهای فرآیند امنیتی‌سازی، خروج یک مسأله از حوزهٔ سیاست عادی و تبدیل آن به مبنایی برای اتخاذ اقدامات استثنایی در سیاست‌گذاری امنیتی است. یافته‌های این پژوهش نشان می‌دهد که جاسوسی سایبری در ایالات متحده دقیقاً چنین مسیری را طی کرده است. پس از آنکه دولت آمریکا از طریق اسناد راهبردی و مواضع رسمی، جاسوسی سایبری را به‌عنوان تهدیدی علیه امنیت ملی بازنمایی کرد؛ این گفتمان به‌تدریج از سوی کنگره، نهادهای اجرایی، افکار عمومی و متحدان آمریکا پذیرفته شد. از منظر نظریهٔ امنیتی‌سازی، این مرحله بیانگر پذیرش مخاطبان[1] است؛ مرحله‌ای که امکان مشروعیت‌بخشی به سیاست‌های جدید امنیتی را فراهم می‌کند. این تحول، مفهوم بازدارندگی را نیز در سیاست امنیتی ایالات متحده دگرگون کرده است. در الگوی سنتی، بازدارندگی عمدتاً بر قدرت نظامی، توان هسته‌ای و موازنهٔ قوا استوار بود؛ اما در عصر دیجیتال، افزایش عملیات جاسوسی سایبری، نفوذ به زیرساخت‌های حیاتی و سرقت اطلاعات راهبردی موجب شد بازدارندگی سایبری به یکی از ارکان اصلی امنیت ملی آمریکا تبدیل شود (Libicki, 2025: 112). بر اساس این، دولت آمریکا تلاش کرده است با توسعهٔ توانمندی‌های دفاع سایبری، افزایش قابلیت‌های شناسایی تهدید، تقویت ظرفیت پاسخ سریع و ارتقاء همکاری‌های اطلاعاتی، هزینهٔ عملیات جاسوسی سایبری را برای بازیگران متخاصم افزایش دهد.

یکی از مهم‌ترین مصادیق این تحول، حملهٔ سایبری به "Colonial Pipeline" در سال ۲۰۲۱ است. این حمله موجب اختلال گسترده در انتقال سوخت در بخش قابل توجهی از ایالات متحده شد و پیامدهای اقتصادی و اجتماعی قابل توجهی به همراه داشت. اهمیت این رخداد از منظر نظریهٔ امنیتی‌سازی، تنها در ابعاد فنی آن نبود؛ بلکه در نحوهٔ بازنمایی آن توسط دولت آمریکا نهفته بود. مقامات آمریکایی این حمله را تهدیدی علیه امنیت انرژی، ثبات اقتصادی و امنیت ملی معرفی کردند و بر ضرورت اتخاذ اقدامات فوری برای حفاظت از زیرساخت‌های حیاتی تأکید نمودند. بدین‌ترتیب، حملهٔ "Colonial Pipeline" به نمونه‌ای از کنش گفتاری تبدیل شد که از طریق آن، یک رخداد سایبری به تهدیدی وجودی برای امنیت ملی بازتعریف گردید. پذیرش این روایت امنیتی، زمینهٔ اجرای مجموعه‌ای از اقدامات فوق‌العاده را فراهم ساخت. دولت

1. Audience Acceptance

ایالات متحده با صدور دستورهای اجرایی، تقویت الزامات امنیت سایبری برای زیرساخت‌های حیاتی، توسعهٔ همکاری میان وزارت امنیت داخلی، آژانس امنیت سایبری و امنیت زیرساخت‌ها[1]، ادارهٔ تحقیقات فدرال[2] و بخش خصوصی و نیز افزایش سرمایه‌گذاری در سامانه‌های هشدار سریع، تلاش کرد آسیب‌پذیری زیرساخت‌های حیاتی را کاهش دهد. این اقدامات نشان می‌دهد که امنیتی‌شدن تهدیدات سایبری صرفاً به تغییر در گفتمان سیاسی محدود نمانده، بلکه به اصلاح ساختارهای نهادی و سیاست‌گذاری امنیتی نیز منجر شده است. از طرفی، فرآیند امنیتی‌سازی، بر سیاست خارجی ایالات متحده نیز تأثیر مستقیم گذاشته است. دولت آمریکا در سال‌های اخیر، امنیت سایبری را به یکی از محورهای اصلی همکاری با متحدان خود در چارچوب سازمان پیمان آتلانتیک شمالی (ناتو)، گروه هفت و سایر سازوکارهای چندجانبه تبدیل کرده است. علاوه بر این، اعمال تحریم علیه اشخاص، گروه‌ها و دولت‌هایی که به انجام عملیات جاسوسی یا حملات سایبری متهم شده‌اند، نشان می‌دهد که تهدیدات سایبری دیگر صرفاً موضوعی داخلی تلقی نمی‌شوند؛ بلکه به یکی از مؤلفه‌های تعیین‌کننده در روابط خارجی و تعاملات دیپلماتیک ایالات متحده تبدیل شده‌اند (Segal, 2025: 89-92).

از منظر نظریهٔ امنیتی‌سازی، این اقدامات را می‌توان مصادیقی از انتقال یک مسأله از حوزهٔ سیاست عادی به قلمرو امنیت ملی دانست. هنگامی که جاسوسی سایبری به‌عنوان تهدیدی علیه بقا و منافع حیاتی ایالات متحده بازنمایی و این روایت از سوی مخاطبان پذیرفته شد، اتخاذ اقداماتی مانند توسعهٔ بازدارندگی سایبری، افزایش بودجهٔ امنیت سایبری، اصلاح قوانین، تشدید همکاری‌های اطلاعاتی و اعمال تحریم‌های بین‌المللی مشروعیت یافت؛ بنابراین بازدارندگی سایبری در ایالات متحده نه‌صرفاً محصول پیشرفت فناوری، بلکه نتیجهٔ فرآیند امنیتی‌سازی تهدیدات دیجیتال است؛ بنابراین باید توجه داشت که تحول راهبردهای بازدارندگی آمریکا در فضای سایبری را نمی‌توان صرفاً با افزایش حملات دیجیتال توضیح داد. آنچه این تحول را امکان‌پذیر کرده، فرآیند امنیتی‌سازی جاسوسی سایبری است که از طریق کنش‌های گفتاری دولت، پذیرش مخاطبان و اجرای اقدامات فوق‌العاده، امنیت سایبری را به یکی از ارکان اصلی سیاست امنیت ملی و سیاست خارجی ایالات متحده تبدیل کرده است.

1. CISA
2. FBI

۳-۳. بازیگران امنیتی‌ساز و نهادینه‌شدن امنیت سایبری در ایالات متحدهٔ آمریکا

یکی از ارکان اساسی نظریهٔ امنیتی‌سازی، وجود بازیگر امنیتی‌ساز است؛ یعنی بازیگری که از طریق گفتمان رسمی، اسناد راهبردی و تصمیمات سیاسی، موضوعی را به‌عنوان تهدیدی علیه بقا و امنیت ملی معرفی می‌کند. یافته‌های این پژوهش نشان می‌دهد که در ایالات متحده، فرآیند امنیتی‌سازی جاسوسی سایبری صرفاً توسط رئیس‌جمهور یا دولت انجام نمی‌شود؛ بلکه مجموعه‌ای از نهادهای امنیتی، اطلاعاتی، نظامی و سیاسی در شکل‌دهی، بازنمایی و تثبیت این گفتمان نقش دارند. همین ویژگی موجب شده است که امنیت سایبری در آمریکا از سطح یک مسألهٔ فنی فراتر رفته و به بخشی نهادینه از سیاست امنیت ملی تبدیل شود (Singer & Friedman, 2022: 288).

در رأس این فرآیند، شورای امنیت ملی ایالات متحده[1] قرار دارد که با تدوین راهبردهای امنیت ملی و هماهنگی میان دستگاه‌های اجرایی، نقش مهمی در صورت‌بندی تهدیدات سایبری ایفا می‌کند. یافته‌های پژوهش نشان می‌دهد که در اسناد منتشرشده توسط این شورا، جاسوسی سایبری به‌طور مستمر به‌عنوان تهدیدی علیه امنیت ملی، برتری فناورانه، زیرساخت‌های حیاتی و رقابت راهبردی ایالات متحده بازنمایی شده است. از منظر نظریهٔ امنیتی‌سازی، این اسناد را می‌توان مهم‌ترین کنش‌های گفتاری رسمی دولت آمریکا دانست که زمینهٔ امنیتی‌شدن تهدیدات سایبری را فراهم کرده‌اند (Lanoszka, 2023: 816-817).

در کنار شورای امنیت ملی، فرمان‌دهی سایبری ایالات متحده[2] نیز نقش تعیین‌کننده‌ای در نهادینه‌شدن امنیت سایبری دارد. این نهاد علاوه بر اجرای عملیات دفاعی و تهاجمی در فضای سایبری، با انتشار ارزیابی‌های امنیتی، ارائهٔ هشدارهای راهبردی و مشارکت در تدوین سیاست‌های ملی، در شکل‌دهی به ادراک تهدید نقش فعالی ایفا می‌کند. یافته‌ها نشان می‌دهد که فرمان‌دهی سایبری تنها یک بازیگر نظامی نیست؛ بلکه یکی از مهم‌ترین بازیگران امنیتی‌ساز در حوزهٔ سایبری محسوب می‌شود؛ زیرا از طریق تولید دانش امنیتی و تبیین مخاطرات دیجیتال، فرآیند امنیتی‌سازی را تقویت می‌کند. آژانس امنیت ملی نیز به‌عنوان یکی از مهم‌ترین نهادهای اطلاعاتی آمریکا، نقش برجسته‌ای در شناسایی عملیات جاسوسی سایبری، تحلیل الگوهای تهدید و ارائهٔ گزارش‌های اطلاعاتی دارد. این گزارش‌ها که مبنای بسیاری از تصمیمات

1. National Security Council
2. U.S. Cyber Command

امنیتی دولت قرار می‌گیرند، نه‌تنها اطلاعات فنی دربارهٔ تهدیدات ارائه می‌کنند، بلکه در بازنمایی جاسوسی سایبری به‌عنوان تهدیدی علیه منافع حیاتی ایالات متحده نیز مؤثرند. از این منظر، فعالیت‌های اطلاعاتی NSA بخشی از فرآیند امنیتی‌سازی محسوب می‌شود؛ زیرا زمینهٔ لازم را برای مشروعیت‌بخشی به سیاست‌های امنیتی دولت فراهم می‌کند (Klimburg, 2022: 101).

علاوه بر این، آژانس امنیت سایبری و امنیت زیرساخت‌ها نقش ویژه‌ای در پیوند میان دولت، بخش خصوصی و زیرساخت‌های حیاتی ایفا می‌کند. یافته‌های پژوهش نشان می‌دهد که این نهاد با انتشار هشدارهای امنیتی، تدوین دستورالعمل‌های حفاظتی، ارزیابی آسیب‌پذیری‌ها و هماهنگی میان نهادهای عمومی و خصوصی، در افزایش آگاهی عمومی نسبت به مخاطرات جاسوسی سایبری نقش اساسی دارد. از منظر نظریهٔ امنیتی‌سازی، آژانس امنیت سایبری و امنیت زیرساخت‌ها یکی از مهم‌ترین نهادهایی است که در اقناع مخاطبان و تثبیت گفتمان امنیتی دولت مشارکت می‌کند. ادارهٔ تحقیقات فدرال نیز از طریق شناسایی، پیگیری و انتساب عملیات جاسوسی سایبری، نقش مهمی در تکمیل فرآیند امنیتی‌سازی ایفا می‌کند. یکی از ویژگی‌های فضای سایبری، دشواری انتساب حملات به عاملان مشخص است؛ ازاین‌رو، زمانی که ادارهٔ تحقیقات فدرال در گزارش‌های رسمی یا بیانیه‌های عمومی، مسؤولیت یک عملیات سایبری را به دولت یا گروهی خاص نسبت می‌دهد، در عمل روایت امنیتی دولت را تقویت کرده و زمینه را برای واکنش‌های سیاسی، دیپلماتیک و حقوقی فراهم می‌کند (Maurer & Morgus, 2022: 228-229).

موفقیت فرآیند امنیتی‌سازی بدون پذیرش مخاطبان امکان‌پذیر نیست. در ایالات متحده، کنگره، رسانه‌های جریان اصلی، شرکت‌های بزرگ فناوری، مراکز پژوهشی و افکار عمومی، مهم‌ترین مخاطبان این فرآیند به‌شمار می‌روند. بررسی اسناد و سیاست‌های سال‌های اخیر نشان می‌دهد که این بازیگران، روایت دولت دربارهٔ تهدیدات ناشی از جاسوسی سایبری را تا حد زیادی پذیرفته‌اند و همین امر موجب افزایش بودجهٔ امنیت سایبری، تصویب قوانین جدید، توسعهٔ ساختارهای نهادی و گسترش همکاری میان دولت و بخش خصوصی شده است (Whyte, 2023: 990-991)؛ بنابراین باید توجه داشت که امنیتی‌سازی جاسوسی سایبری در ایالات متحده، حاصل عملکرد یک نهاد واحد نیست؛ بلکه نتیجهٔ تعامل شبکه‌ای از بازیگران سیاسی، اطلاعاتی، نظامی و اجرایی است که از طریق کنش‌های گفتاری، تولید دانش امنیتی، اقناع مخاطبان و اجرای سیاست‌های امنیتی، جاسوسی سایبری را به یکی از مهم‌ترین

تهدیدات امنیت ملی و سیاست خارجی آمریکا تبدیل کرده‌اند. این امر بیانگر آن است که امنیت سایبری در ایالات متحده به مرحلهٔ نهادینه‌شدن امنیتی رسیده و به یکی از ارکان ثابت حکمرانی امنیتی این کشور تبدیل شده است.

۴-۳. پیامدهای امنیتی‌سازی جاسوسی سایبری در بازتعریف سیاست خارجی ایالات متحدهٔ آمریکا

امنیتی‌سازی زمانی کامل می‌شود که بازنمایی یک پدیده به‌عنوان تهدیدی وجودی، صرفاً در سطح گفتمان باقی نماند و به تغییر در الگوهای تصمیم‌گیری، راهبردهای امنیتی و جهت‌گیری‌های سیاست خارجی منجر شود. در مورد ایالات متحده، جاسوسی سایبری چنین مسیری را طی کرده است. بازنمایی مستمر این پدیده در اسناد راهبردی و گفتمان رسمی دولت، موجب شد امنیت سایبری از یک موضوع تخصصی و فناورانه به یکی از مؤلفه‌های بنیادین سیاست خارجی و امنیت ملی آمریکا تبدیل شود (Libicki, 2024: 13).

این تحول، مفهوم امنیت را نیز دستخوش بازتعریف کرده است. در برداشت‌های سنتی، امنیت ملی عمدتاً بر حفاظت از مرزهای سرزمینی، توان نظامی و بازدارندگی کلاسیک استوار بود؛ اما وابستگی گسترده ساختارهای حکمرانی، اقتصاد، انرژی، ارتباطات و زیرساخت‌های حیاتی به فناوری‌های دیجیتال، سبب شد تهدیدات سایبری در کنار تهدیدات نظامی، جایگاهی محوری در محاسبات امنیتی ایالات متحده پیدا کنند. در نتیجه، امنیت ملی دیگر صرفاً به حفاظت از قلمرو جغرافیایی محدود نیست؛ بلکه حفاظت از داده‌ها، شبکه‌های ارتباطی، زیرساخت‌های دیجیتال و برتری فناورانه نیز به بخشی از منافع حیاتی دولت تبدیل شده است (Jensen et al., 2022: 235-236).

در چارچوب نظریه امنیتی‌سازی، این تحول نشان‌دهندهٔ تغییر در ابژه مرجع است. اگر در گذشته تمامیت ارضی و بقای دولت مهم‌ترین ابژه‌های مرجع محسوب می‌شدند، اکنون امنیت زیرساخت‌های حیاتی، امنیت اطلاعات، اقتصاد دیجیتال، زنجیره‌های تأمین فناوری و قابلیت تصمیم‌گیری راهبردی نیز در زمرهٔ ارزش‌هایی قرار گرفته‌اند که دولت ایالات متحده حفاظت از آن‌ها را ضرورتی امنیتی تلقی می‌کند. این تغییر، بیانگر گسترش دامنهٔ مفهوم امنیت در عصر دیجیتال است و پیامد دیگر این فرآیند، بازآرایی ابزارهای سیاست خارجی ایالات متحده است. امنیتی‌شدن جاسوسی سایبری موجب شده است ابزارهای سنتی دیپلماسی با سازوکارهای نوینی مانند بازدارندگی سایبری، تحریم‌های دیجیتال، انتساب رسمی حملات سایبری، همکاری اطلاعاتی با

متحدان، تبادل داده‌های امنیتی و دیپلماسی سایبری تکمیل شوند. به این ترتیب، فضای سایبری نه‌تنها به عرصه‌ای برای رقابت اطلاعاتی، بلکه به یکی از حوزه‌های اصلی اعمال قدرت و مدیریت روابط خارجی تبدیل شده است (Brands & Gaddis, 2023: 35-37).

این روند همچنین جایگاه همکاری‌های بین‌المللی را در سیاست خارجی آمریکا دگرگون کرده است. در سال‌های اخیر، امنیت سایبری به یکی از محورهای ثابت همکاری با متحدان در چارچوب ناتو، گروه هفت و سایر ترتیبات چندجانبه تبدیل شده است. توسعهٔ سازوکارهای مشترک برای تبادل اطلاعات، هماهنگی در انتساب حملات سایبری، حفاظت از زیرساخت‌های حیاتی و مقابله با عملیات جاسوسی دیجیتال، نشان می‌دهد که تهدیدات سایبری دیگر صرفاً در سطح ملی مدیریت نمی‌شوند؛ بلکه مستلزم همکاری‌های گستردهٔ بین‌المللی هستند. از این منظر، امنیتی‌شدن جاسوسی سایبری به تقویت دیپلماسی امنیتی و شکل‌گیری الگوهای جدید حکمرانی سایبری انجامیده است (Taddeo, 2022: 6).

از سوی دیگر، امنیتی‌شدن جاسوسی سایبری موجب تغییر در الگوی تخصیص منابع و سازمان‌دهی ساختارهای حکمرانی نیز شده است. افزایش سرمایه‌گذاری در فناوری‌های دفاع سایبری، توسعهٔ توانمندی‌های اطلاعاتی، ایجاد سازوکارهای هماهنگی میان نهادهای نظامی، اطلاعاتی و غیرنظامی و گسترش همکاری میان دولت و بخش خصوصی، همگی بیانگر آن است که سیاست امنیتی ایالات متحده به‌صورت فزاینده‌ای بر مدیریت مخاطرات سایبری متمرکز شده است. این اقدامات، مصادیق روشنی از اقدامات فوق‌العاده در نظریهٔ امنیتی‌سازی هستند که پس از پذیرش گفتمان امنیتی، مشروعیت سیاسی و حقوقی یافته‌اند (Valeriano et al., 2024: 146).

در این میان، نقش کنش‌های گفتاری دولت همچنان تعیین‌کننده باقی مانده است. تکرار مداوم مفاهیمی مانند «تهدید علیه امنیت ملی»، «حفاظت از زیرساخت‌های حیاتی»، «رقابت راهبردی در فضای سایبری» و «دفاع از برتری فناورانهٔ آمریکا» در راهبردهای امنیت ملی، اسناد امنیت سایبری و اظهارات مقامات ارشد، نشان می‌دهد که دولت ایالات متحده از زبان امنیت برای تثبیت جایگاه جاسوسی سایبری در دستور کار سیاست داخلی و خارجی خود بهره گرفته است. این امر با مبانی نظری مکتب کپنهاگ همخوانی دارد؛ زیرا امنیتی‌شدن یک مسأله، بیش از آنکه محصول ویژگی‌های ذاتی آن باشد، نتیجهٔ نحوهٔ بازنمایی آن در گفتمان رسمی است (Kello, 2022: 194). در مجموع، تحلیل حاضر نشان می‌دهد که تأثیر جاسوسی سایبری بر سیاست خارجی

ایالات متحده را نمی‌توان صرفاً با افزایش تعداد حملات یا پیچیدگی فناوری‌های دیجیتال تبیین کرد. عامل تعیین‌کننده، فرآیند امنیتی‌سازی این پدیده در گفتمان رسمی دولت آمریکا است. دولت با بهره‌گیری از اسناد راهبردی، بیانیه‌های سیاسی و سیاست‌های نهادی، جاسوسی سایبری را به‌عنوان تهدیدی علیه امنیت ملی و منافع حیاتی کشور بازنمایی کرده و از طریق جلب پذیرش نهادهای سیاسی، افکار عمومی و متحدان، زمینهٔ مشروعیت‌بخشی به اقدامات فوق‌العاده را فراهم ساخته است. پیامد این فرآیند، بازتعریف مفهوم امنیت، تحول در ابزارهای سیاست خارجی، تقویت بازدارندگی سایبری و شکل‌گیری الگوی جدیدی از حکمرانی امنیتی در ایالات متحده بوده است. ازاین‌رو، نظریهٔ امنیتی‌سازی نسبت به رویکردهای صرفاً فناورانه، تبیین جامع‌تر و منسجم‌تری از رابطهٔ میان جاسوسی سایبری و تحول سیاست خارجی ایالات متحده ارائه می‌دهد.

شکل ۱. مدل مفهومی تأثیر جاسوسی سایبری بر بازتعریف تهدیدات امنیتی در سیاست خارجی ایالات متحدهٔ آمریکا (طراحی: نویسندگان)

شکل شمارهٔ ۱ که مدل مفهومی تأثیر جاسوسی سایبری بر بازتعریف تهدیدات امنیتی در سیاست خارجی ایالات متحدهٔ آمریکا است، نشان می‌دهد که چگونه گسترش جاسوسی سایبری به‌عنوان یکی از مهم‌ترین تحولات عصر دیجیتال، موجب تغییر در درک تهدیدات امنیتی و در نتیجه بازتعریف سیاست خارجی ایالات متحدهٔ آمریکا شده است. در این مدل، «جاسوسی سایبری» به‌عنوان متغیر اصلی و محرک اولیه در نظر گرفته شده که با ایجاد چالش‌های جدید امنیتی، سایر مؤلفه‌های نظام امنیتی و سیاست خارجی آمریکا را تحت تأثیر قرار می‌دهد.

نخستین مؤلفه در این مدل، گسترش عملیات جاسوسی سایبری و افزایش تهدیدات دیجیتال است. توسعهٔ فناوری‌های اطلاعاتی، وابستگی گستردهٔ ساختارهای دولتی و اقتصادی به شبکه‌های دیجیتال و افزایش رقابت اطلاعاتی میان قدرت‌های جهانی، موجب شده است فضای سایبری به یکی از مهم‌ترین عرصه‌های رقابت امنیتی تبدیل شود. در چنین شرایطی، نفوذ به شبکه‌های اطلاعاتی، سرقت داده‌های راهبردی و دسترسی غیرمجاز به زیرساخت‌های حیاتی می‌تواند پیامدهایی گسترده برای امنیت ملی کشورها داشته باشد. پیامد مستقیم این وضعیت، تحول در مفهوم امنیت ملی است. در مدل مفهومی پژوهش، تهدیدات سایبری موجب شده‌اند امنیت از چارچوب سنتی و نظامی‌محور فاصله گرفته و به مفهومی چندبعدی تبدیل شود. در این رویکرد جدید، امنیت اطلاعات، حفاظت از زیرساخت‌های دیجیتال، مدیریت داده‌ها و مقابله با نفوذ سایبری به بخش مهمی از امنیت ملی تبدیل شده‌اند. به عبارت دیگر، مرز میان امنیت نظامی، اقتصادی، اطلاعاتی و فناورانه تا حد زیادی کم‌رنگ شده و تهدیدات سایبری می‌توانند هم‌زمان چندین حوزهٔ امنیتی را تحت تأثیر قرار دهند.

در مرحلهٔ بعد، این تحول مفهومی موجب فعال‌تر شدن نهادهای امنیتی و اطلاعاتی آمریکا در حوزهٔ سایبری شده است. سازمان‌هایی مانند آژانس امنیت ملی، فرمان‌دهی سایبری آمریکا، ادارهٔ سایبری پلیس فدرال و آژانس امنیت سایبری و امنیت زیرساخت‌ها نقش مهمی در شناسایی، پیشگیری و مقابله با تهدیدات سایبری ایفا می‌کنند. در این مدل، این نهادها به‌عنوان سازوکارهای اجرایی و نهادی مدیریت تهدیدات سایبری عمل می‌کنند و با ایجاد هماهنگی میان حوزه‌های اطلاعاتی، امنیتی و فناورانه، ظرفیت دفاع سایبری آمریکا را تقویت می‌کنند.

درنهایت، مجموع این تحولات به بازتعریف سیاست خارجی ایالات متحدهٔ آمریکا منجر می‌شود. افزایش تهدیدات سایبری باعث شده است که امنیت سایبری به یکی از مؤلفه‌های مهم در سیاست خارجی این کشور تبدیل شود. در این چارچوب، آمریکا

تلاش می‌کند از طریق توسعهٔ راهبردهای بازدارندگی سایبری، تقویت همکاری‌های امنیتی با متحدان، افزایش تبادل اطلاعات و ارتقاء توانایی‌های فناوری، جایگاه راهبردی خود را در فضای سایبری حفظ کند. به بیان دیگر، فضای سایبری به یکی از عرصه‌های اصلی رقابت ژئوپلیتیکی و دیپلماسی امنیتی آمریکا تبدیل شده است. به‌طورکلی، مدل مفهومی پژوهش نشان می‌دهد که جاسوسی سایبری صرفاً یک پدیدهٔ فنی یا فناورانه نیست؛ بلکه عاملی راهبردی در تحول ساختارهای امنیتی و سیاست خارجی ایالات متحدهٔ آمریکا محسوب می‌شود. این مدل رابطه‌ای زنجیره‌ای میان گسترش تهدیدات سایبری، تحول مفهوم امنیت، فعال‌شدن نهادهای امنیتی و در نهایت بازتعریف سیاست خارجی آمریکا را ترسیم می‌کند و نشان می‌دهد که چگونه تحولات فناوری می‌توانند ساختارهای سنتی امنیت و سیاست را در نظام بین‌الملل دگرگون کنند.

۴. بحث و نتیجه‌گیری

پژوهش حاضر با هدف بررسی نقش جاسوسی سایبری در بازتعریف تهدیدات امنیتی و تحول سیاست خارجی ایالات متحدهٔ آمریکا انجام شد. پرسش اصلی بر این محور استوار بود که گسترش جاسوسی سایبری چگونه درک آمریکا از امنیت، تهدیدات راهبردی و الگوهای سیاست خارجی را دگرگون ساخته و نهادهای امنیتی و اطلاعاتی این کشور چه نقشی در مدیریت این روند ایفا کرده‌اند. در این رابطه، یافته‌ها نشان داد که ایالات متحده، جاسوسی سایبری را از سطح یک تهدید فناورانه یا جرم سایبری فراتر برده و آن را در چارچوب تهدیدات راهبردی علیه امنیت ملی، زیرساخت‌های حیاتی و منافع ژئوپلیتیکی خود بازتعریف کرده است. این امر موجب شده است فضای سایبری به یکی از کانون‌های اصلی رقابت قدرت‌های بزرگ در نظام بین‌الملل تبدیل شود و سیاست خارجی آمریکا به‌طور فزاینده‌ای تحت تأثیر ملاحظات امنیت دیجیتال قرار گیرد.

همچنین، در سطح تحلیلی، مشخص شد که افزایش وابستگی ساختارهای حکمرانی و اقتصاد آمریکا به شبکه‌های داده‌محور، مرز میان امنیت داخلی و خارجی را تا حد زیادی تضعیف کرده است. در نتیجه، تهدیدات سایبری به‌واسطهٔ ماهیت فراملی و غیرمتمرکز خود، قابلیت اثرگذاری هم‌زمان بر حوزه‌های نظامی، اقتصادی و سیاسی را یافته‌اند و همین ویژگی، آمریکا را به سمت رویکردهای چندلایهٔ امنیتی سوق داده است. در این چارچوب، امنیت سایبری به بخشی از منطق حفظ قدرت اطلاعاتی و مزیت راهبردی این کشور تبدیل شده است.

از منظر سیاست خارجی، نتایج نشان داد که آمریکا در واکنش به این تهدیدات، به‌طور هم‌زمان سه مسیر را دنبال کرده است: تقویت راهبردهای بازدارندگی سایبری، گسترش همکاری‌های امنیتی بین‌المللی و ارتقاء ظرفیت‌های اطلاعاتی و نظارتی. نمونهٔ عملی این روند را می‌توان در ائتلاف سایبری ناتو مشاهده کرد که در آن ایالات متحده نقش محوری در هماهنگی استانداردهای دفاع سایبری و تبادل اطلاعات تهدیدات با متحدان اروپایی ایفا کرده است. تحلیل این نمونه نشان می‌دهد که سیاست خارجی آمریکا در حوزهٔ سایبری، از الگوی صرفاً ملی به سمت شبکه‌ای از ائتلاف‌های امنیت دیجیتال حرکت کرده است که هدف آن افزایش هزینهٔ اقدامات نفوذی برای بازیگران رقیب است.

در حوزهٔ نهادی نیز یافته‌ها بیانگر آن است که نهادهای امنیتی و اطلاعاتی آمریکا به بازیگران مرکزی در مدیریت تهدیدات سایبری تبدیل شده‌اند. ساختارهایی مانند آژانس امنیت ملی، فرمان‌دهی سایبری و آژانس امنیت سایبری و زیرساخت‌ها، نه‌تنها در سطح دفاعی، بلکه در سطح جمع‌آوری اطلاعات، عملیات پیش‌دستانه و تحلیل تهدیدات نقش فعال دارند. نمونهٔ بارز این مسأله، واکنش نهادی آمریکا به حملهٔ زنجیرهٔ تأمین «سولارویندز» است که منجر به بازطراحی سیاست‌های امنیت نرم‌افزار و تقویت هماهنگی میان نهادهای فدرال شد. این تجربه نشان داد که مدیریت تهدیدات سایبری بدون انسجام نهادی و اشتراک‌گذاری سریع اطلاعات، امکان‌پذیر نیست. همچنین مشخص شد که دولت آمریکا با برجسته‌سازی تهدیدات سایبری در اسناد راهبردی، فرآیند امنیتی‌سازی را به‌عنوان ابزار سیاست‌گذاری دنبال کرده است.

این روند زمینه را برای افزایش اختیارات نهادهای امنیتی و مشروعیت‌بخشی به توسعهٔ زیرساخت‌های نظارتی و تهاجمی در فضای دیجیتال فراهم کرده است. درنهایت، می‌توان جمع‌بندی کرد که جاسوسی سایبری به یکی از متغیرهای اثرگذار در تحول سیاست خارجی و امنیت ملی ایالات متحده تبدیل شده است. این پدیده نه‌تنها ساختار سنتی تهدیدات را دگرگون کرده، بلکه منطق سیاست‌گذاری امنیتی آمریکا را به سمت وابستگی عمیق‌تر به فناوری، اطلاعات و شبکه‌های همکاری بین‌المللی سوق داده است. در این چارچوب، امنیت سایبری به یکی از مؤلفه‌های اصلی قدرت در نظام بین‌الملل تبدیل شده و نقش تعیین‌کننده‌ای در بازآرایی الگوهای رقابت ژئوپلیتیکی ایفا می‌کند.

فهرست منابع

الف- فارسی

- اسماعیلی، مصطفی؛ رکنی، امیرعباس و حسینی، سید رضا. (۱۴۰۲). ژئوپلیتیک سایبری در گذرگاه قدرت: تحلیل هژمونی سایبری ایالات متحدهٔ آمریکا در تقابل با چین. روابط خارجی، (۶۰)، ۳۹۶-۲۶۷.
- جمیری، روح‌الله. (۱۴۰۴). بررسی تهدیدات امنیتی ناشی از ترکیب هوش مصنوعی و شبکه‌های اجتماعی در جاسوسی سایبری. مطالعات حفاظت و امنیت انتظامی، ۲۰(۷۵)، ۷۵-۶۱.
- ساوه درودی، مصطفی و خدادادی، رضا. (۱۴۰۴). انگیزه‌ها و آسیب‌پذیری‌ها در عصر جاسوسی دیجیتال. امنیت پژوهی، (۹۰)، ۴۶-۲۹.

ب- انگلیسی

- Allison, G. (2022). Cyber rivalry and strategic instability in U.S.–China relations. The Washington Quarterly, 45(3), 77-94.
- Balzacq, T., Leonard, S., & Ruzicka, J. (2016). ‘Securitization’ revisited: Theory and cases. London: SAGE Publications.
- Buzan, B., & Hansen, L. (2020). The evolution of international security studies. Cambridge: Cambridge University Press.
- Buzan, B. (2018). People, states and fear: An agenda for international security studies in the post-Cold War era (2nd ed.). Colchester: ECPR Press.
- Delerue, F. (2023). Cyber operations and international law in the 21st century. Cambridge: Cambridge University Press.
- Dunn Cavelty, M., & Wenger, A. (2022). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. London: Taylor & Francis.
- Edelman, R. D. (2024). Rethinking cyber warfare: The international relations of digital disruption. London: Oxford University Press.
- Eriksson, J., & Giacomello, G. (2022). Cyber deterrence and international politics: Emerging strategies and challenges. Fletcher Forum of World Affairs, 46(2), 51–70.
- Hansen, L., & Nissenbaum, H. (2022). Digital disaster, cyber security, and the Copenhagen School. Oxford: Oxford University Press.
- Healey, J. (2023). The implications of offensive cyber operations for U.S. grand strategy. Strategic Studies Quarterly, 17(2), 66-89.
- Jasper, S. (2022). Cybersecurity and the protection of critical infrastructure in the United States. Homeland Security Affairs, 18(4), 1-19.
- Jensen, B., Valeriano, B., & Maness, R. (2022). Cyber strategy and statecraft in the information age. Oxford: Oxford University Press.
- Kello, L. (2022). Digital power, cyber strategy, and the transformation of international security. Oxford: Oxford University Press.
- Klimburg, A. (2022). Strategic instability in cyberspace and the future of deterrence. Survival, 64(3), 95-118.

- Lanoszka, A. (2023). Cyber conflict, NATO, and collective defense in the digital era. International Politics, 60(5), 812-830.
- Libicki, M. (2025). Cyber deterrence and the changing nature of digital conflict. London: Routledge.
- Lindsay, J. R., & Gartzke, E. (2024). Cross-domain deterrence and cyber espionage in international politics. Cambridge: MIT Press.
- Lindsay, J. R. (2023). Cyber conflict and international security in the digital era. Annual Review of Political Science, 26, 397-418.
- Maurer, T., & Morgus, R. (2022). Consensus, conflict, and cybersecurity norms in international politics. Global Governance, 28(2), 215-233.
- Moulin, T. (2023). Cyber-espionage in international law: Silence speaks. Manchester: Manchester University Press.
- Nocetti, J. (2023). Cyber power and digital sovereignty in contemporary geopolitics. International Affairs, 99(4), 1561-1579.
- Pytlak, A., & Mitchell, A. (2022). Cybersecurity and strategic competition in the twenty-first century. Contemporary Security Policy, 43(3), 401-420.
- Rid, T., & Buchanan, B. (2024). Cyber espionage and the transformation of intelligence in the digital age. Cambridge: MIT Press.
- Rid, T. (2023). Active measures, cyber espionage, and geopolitical competition in the digital age. London: Routledge.
- Segal, A. (2025). Cybersecurity and U.S. foreign policy in the era of great power competition. London: Routledge.
- Segal, A. (2023). The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. New York: PublicAffairs.
- Smeets, M. (2023). Cyber command and the institutionalization of offensive cyber power. Journal of Strategic Studies, 46(4), 711-734.
- Taddeo, M. (2022). Cybersecurity, ethics, and national security in the age of artificial intelligence. Philosophy & Technology, 35(2), 1-18.
- Topor, L. (2024). Cyber sovereignty: International security, mass communication, and the future of the internet. New York: Springer Nature.
- Valeriano, B., Jensen, B., & Maness, R. (2024). Cyber coercion, espionage, and the evolution of state power. International Security, 48(3), 95–128. Cambridge, MA: MIT Press.
- Wæver, O. (2019). Securitization and desecuritization. New York: Columbia University Press.
- Wæver, O. (2017). The theory act of securitization: A realist constructivist approach. London: Palgrave Macmillan.
- Whyte, C. (2023). Intelligence agencies and cyber threat attribution in U.S. national security policy. Intelligence and National Security, 38(7), 987-1004.
- Weiss, A., & Jankowski, D. (2023). Cyber threats, intelligence institutions, and U.S. national security strategy. International Journal of Cyber Warfare and Terrorism, 13(2), 44-61.