The Diplomatic Interactions Quarterly
Vol. 3, No. 9, Spring 2025, Pp: 1-32
http:// www.dpiq.ir

Challenges and Opportunities of Cybersecurity in Iran-Armenia Diplomatic and Commercial Relations

Mehdi Hedayati Shahidani[1]
Hadi Mahdizadeh[2]

(Received: 11/03/2025 - Accepted: 26/04/2025)
DOI: 10.22034/dpiq.2025.536281.1045

Extended Abstract

Introduction

In the contemporary digital era, cybersecurity has unprecedentedly evolved into a critical substrate of international relations—encompassing the protection of systems, networks, applications, and data against digital threats. Its significance extends beyond safeguarding national critical infrastructure to profoundly influence diplomatic relations (involving confidential negotiations, sensitive information exchange) and commercial interactions (trade flows, joint investments, economic cooperation). The strategic Iran-Armenia relationship—anchored in deep historical and cultural ties within the South Caucasus and Middle East—presents a compelling case study of this complex interplay. While

1. Associate Professor, Department of International Relations, University of Guilan, Rasht, Iran. (Mehdi.hedayati88@gmail.com)
Orcid Code: https://orcid.org/0000-0002-5145-8885
2. PhD Student, Department of International Relations, University of Guilan, Rasht, Iran. (Mz.hadi70@gmail.com)
Orcid Code: https://orcid.org/0009-0008-4436-8102

digitalization offers mutual opportunities (e-commerce facilitation, secure diplomatic channels, joint cyber threat response), it simultaneously introduces critical vulnerabilities: shared digital infrastructure exposure, cross-border cyber espionage risks, disparities in cyber maturity, and sanction-driven technological constraints (e.g., U.S. restrictions impacting Iran's access to advanced security solutions). International Telecommunication Union (ITU) reports confirm divergent national cyber readiness levels, potentially impeding bilateral cooperation. Institutional frameworks like the Shanghai Cooperation Organization (SCO)—where both nations hold observer status—offer platforms for dialogue. This study addresses the dual-impact question: How does cybersecurity function as both a challenge and opportunity for diplomatic and commercial dynamics in Iran-Armenia relations?

Research Objectives

This research aims to:
1.Systematically analyze how cybersecurity disparities (e.g., 25-rank GCI-ITU gap), sanctions regimes, and shared threats reconfigure bilateral relations.
2.Evaluate institutional mechanisms (e.g., SCO regional threat databases) and trust-building initiatives (e.g., quantum-encrypted infrastructure) that transform challenges into cooperative opportunities.
3.Assess the impact of extra-regional actors (U.S. sanctions, Russian SORM surveillance pressures, China's Digital Silk Road) on collaborative cybersecurity frameworks.
4.Propose policy pathways for sanction-resilient cooperation models applicable to Global South partnerships.

Methodology

This research employs an integrated theoretical framework combining cyber realism, which interprets cybersecurity through the lens of power competition and national interests in anarchic international environments; liberal institutionalism, analyzing the role of multilateral institutions like the Shanghai Cooperation Organization (SCO) in

reducing distrust through standardized protocols; and trust theory, examining how operational cooperation builds relational confidence. Empirical analysis incorporates quantitative metrics from international indices .cyber threat datasets (Kaspersky/Symantec statistics), and bilateral trade records; qualitative examination of 31 existing cooperation agreements, SCO policy documents, and field interviews with 42 cybersecurity officials from both nations; and in-depth case studies of critical infrastructure projects including the quantum-encrypted Iran-Armenia optical cable and blockchain-based "Barempay" payment platform.

Findings

Cybersecurity manifests as a dual-nature phenomenon in bilateral relations, simultaneously generating structural challenges and cooperative opportunities. Significant disparities in cyber maturity—evidenced by Armenia's 35th rank versus Iran's 60th in the 2021 ITU Global Cybersecurity Index create technical asymmetries exacerbated by U.S. sanctions restricting Iran's access to advanced security hardware (Connell & Venter, 2016, p. 17). Operational vulnerabilities include a documented 40% surge in cross-border Advanced Persistent Threat (APT) attacks targeting shared energy/transport infrastructure during 2021 and industrial espionage against Iranian tech firms in Armenia Regulatory misalignment further complicates cooperation: Armenia's GDPR-inspired data laws conflict with Iran's national-security-focused cybercrime legislation, while the absence of a dedicated bilateral cybersecurity agreement impedes joint incident response. Conversely, institutional mechanisms like the SCO's Regional Anti-Terrorist Structure (RATS) threat-intelligence database—containing over 5,000 malware signatures from Central Asia and the Caucasus have reduced incident response costs by 30%. Joint infrastructure projects serve as trust-building vectors: the quantum-secured optical cable project established technical confidence through collaborative encryption protocols, while the "Barempay" blockchain platform processed $12 million in sanction-evading transactions by 2023. Annual "Cyber Shield" exercises enhanced cross-border CSIRT coordination, with 75% of

surveyed officials citing the neutralization of the 2022 Nowruz customs system attack as a pivotal trust milestone. Extra-regional interventions add complexity: U.S. CAATSA sanctions limit quantum technology access; Russian pressure to install SORM surveillance hardware in Armenia raises Iranian data-security concerns, and China's Digital Silk Road initiatives face cryptographic incompatibilities.

Conclusion

The interplay of cybersecurity and Iran-Armenia relations confirms a dialectical dynamic where challenges catalyze innovative cooperation. Structural impediments—technological asymmetries, sanction regimes, and divergent regulatory frameworks—coexist with institutional enablers like the SCO's standardization mechanisms and operational trust-builders such as joint critical infrastructure projects. This duality necessitates three strategic priorities: formalizing a dedicated bilateral cybersecurity agreement to address legal voids; co-developing indigenous, sanction-resilient technical standards (e.g., shared post-quantum cryptographic algorithms); and maximizing institutional capacities within frameworks like the SCO to counter extra-regional pressures. Success hinges on transforming shared vulnerabilities—particularly transnational threats to economic corridors—into collaborative advantage through depoliticized technical coordination. This model offers a replicable template for Global South digital partnerships operating under constraint, demonstrating how middle powers can leverage cybersecurity not merely as a defensive imperative but as a diplomatic asset in reconfiguring regional stability.

Keywords: Armenia, Cybersecurity, Iran, Diplomatic Relations, Commercial Relations.

How to Cite: Hedayati Shahidani, M. and Mahdizadeh, H. (2025). Challenges and Opportunities of Cybersecurity in Iran-Armenia Diplomatic and Commercial Relations. *Diplomatic Interactions*, 3 (9), 1-32. doi: 10.22034/dpiq.2025.536281.1045

فصلنامه تعاملات دیپلماتیک

سال سوم، شماره ۹، بهار ۱۴۰۴، صفحات ۳۲-۱

http:// www.dpiq.ir

چالش‌ها و فرصت‌های امنیت سایبری در روابط دیپلماتیک و تجاری ایران و ارمنستان

مهدی هدایتی شهیدانی[۱]- هادی مهدی‌زاده [۲]

(تاریخ دریافت: ۱۴۰۳/۱۲/۲۱- تاریخ تصویب:۱۴۰۴/۰۲/۰۶)

DOI: 10.22034/dpiq.2025.536281.1045

چکیده

این پژوهش با هدف تحلیل تاثیر دوسویه امنیت سایبری بر روابط دیپلماتیک و تجاری ایران و ارمنستان، از چارچوب نظری ترکیبی (رئالیسم، نهادگرایی لیبرال و نظریه اعتماد) بهره می‌برد. یافته‌ها نشان می‌دهد امنیت سایبری به‌عنوان عاملی دوگانه هم چالش آفرین و هم فرصت ساز عمل می‌کند. از یک سو، شکاف فاحش در بلوغ سایبری دو کشور (اختلاف ۲۵ رتبه‌ای در شاخص ارزیابی جامع اتحادیه بین‌المللی مخابرات، تحریم‌های فناوری علیه ایران، محدودیت دسترسی به سخت‌افزارهای امنیتی پیشرفته؛ و تهدیدات فرامرزی) افزایش چهل درصدی حملات تهدید مداوم پیشرفته (نوعی حمله سایبری تحت شبکه است که یک شخص احراز هویت نشده می‌تواند برای مدت زمان زیادی به صورت ناشناس به شبکه دسترسی پیدا کند) به زیرساخت‌های مشترک در ۲۰۲۱، همکاری را مختل کرده‌اند. از سوی دیگر، همکاری‌های عملیاتی مانند پروژه کابل نوری با رمزنگاری کوانتومی و پلتفرم پرداخت "بریم پی" مبتنی بر بلاکچین نه تنها نیازهای ارتباطی و مالی را پاسخ داده‌اند؛ بلکه با ایجاد سرمایه اعتمادی به تقویت روابط کمک کرده‌اند. نقش سازمان همکاری شانگهای به‌عنوان بستر نهادی کلیدی، با فراهم آوردن مکانیسم‌هایی مانند بانک اطلاعات تهدیدات منطقه‌ای و استانداردسازی پاسخ به حوادث، همکاری را تسهیل نموده است. با این حال، مداخلات قدرت‌های فرا منطقه‌ای این پویایی را پیچیده کرده‌اند: تحریم‌های آمریکا دسترسی به فناوری را محدود می‌کند، فشار روسیه برای نصب سخت‌افزارهای نظارتی در ارمنستان نگرانی‌های امنیتی ایران را افزایش داده و پیشنهادهای چین تحت «راه‌اندازی دیجیتال» با چالش ناسازگاری استانداردها روبروست. پژوهش حاضر ثابت می‌کند که موفقیت آتی این همکاری مستلزم سه راهبرد است: ۱) تدوین موافقت‌نامه دوجانبه امنیت سایبری برای رفع خلأهای حقوقی، ۲) توسعه استانداردهای بومی مقاوم در برابر تحریم (الگوریتم‌های رمزنگاری مشترک)، و ۳) بهره‌گیری حداکثری از ظرفیت‌های نهادی. این الگو می‌تواند به چارچوبی پیشرو برای همکاری‌های سایبری جنوب–جنوب در شرایط تحریمی تبدیل گردد.

واژگان کلیدی: ارمنستان، امنیت سایبری، ایران، روابط دیپلماتیک، روابط تجاری.

---

۱. دانشیار علوم‌سیاسی و روابط بین‌الملل دانشگاه گیلان، رشت، ایران (Mehdi.hedayati88@gmail.com)- **نویسنده مسئول**

Orcid Code: https://orcid.org/0000-0002-5145-8885

۲. دانشجوی دکتری علوم سیاسی و روابط بین‌الملل دانشگاه گیلان، رشت، ایران (Mz.hadi70@gmail.com)

Orcid Code: https://orcid.org/0009-0008-4436-8102

مقدمه

در عصر دیجیتال کنونی، امنیت سایبری به شکلی بی‌سابقه به بستر حیاتی تعاملات بین‌المللی تبدیل شده است، حوزه‌ای که حفاظت از سیستم‌ها، شبکه‌ها، برنامه‌ها و داده‌ها در برابر حملات دیجیتال را در برمی‌گیرد. این اهمیت تنها محدود به حفاظت از زیرساخت‌های حیاتی ملی نیست، بلکه به طور فزاینده‌ای بر روابط دیپلماتیک -که شامل ارتباطات رسمی، مذاکرات و تبادل اطلاعات حساس بین دولت‌هاست و همچنین بر جریان‌های روابط تجاری -شامل مبادلات بازرگانی، سرمایه‌گذاری‌های مشترک و همکاری‌های اقتصادی بین بازیگران دولتی و خصوصی- سایه افکنده است. در این میان، روابط دیرینه و راهبردی ایران و ارمنستان، دو همسایه با پیوندهای تاریخی و فرهنگی عمیق در منطقه قفقاز جنوبی و خاورمیانه، نمونه‌ای بارز برای بررسی این تداخل پیچیده است. این رابطه که بر پایه همکاری‌های سیاسی، اقتصادی و امنیتی بنا شده، به طور فزاینده‌ای در حال دیجیتالی شدن است، امری که هم‌زمان فرصت‌های ارزشمندی مانند تسهیل تجارت الکترونیک، بهبود کارایی دیپلماتیک از طریق کانال‌های دیجیتال امن و همکاری در مواجهه با تهدیدات سایبری مشترک را پیش پای طرفین می‌گذارد و چالش‌هایی جدی نظیر آسیب‌پذیری زیرساخت‌های دیجیتال مشترک، خطر جاسوسی سایبری علیه منافع ملی هر دو کشور، اختلاف در سطح بلوغ سایبری و انطباق با تحریم‌های بین‌المللی (به ویژه آن‌هایی که بر ایران اعمال شده و ممکن است بر همکاری‌های فناورانه تأثیر بگذارد) را نیز به همراه دارد.

گزارش‌های سازمان‌هایی مانند اتحادیه بین‌المللی مخابرات[1] که شاخص جهانی امنیت سایبری را منتشر می‌کند، به وضوح نشان می‌دهد که کشورها در سطوح مختلفی از آمادگی سایبری قرار دارند و این اختلاف می‌تواند خود به عنوان چالشی در مسیر همکاری‌های

1 International Telecommunication Union

دوجانبه یا منطقه‌ای عمل کند. همکاری در چارچوب‌های منطقه‌ای مانند ابتکار همکاری‌های سازمان همکاری شانگهای[1] در امور سایبری، نمونه‌ای از بسترهای بالقوه برای شکل‌گیری گفتگو و همکاری مشترک در این حوزه است. این پژوهش درصدد پاسخ به این پرسش است که امنیت سایبری چگونه و تا چه حد به عنوان عاملی دوگانه (هم چالش زا و هم فرصت ساز)، بر تحولات دیپلماتیک و تجاری در روابط ایران و ارمنستان تأثیر می‌گذارد؟ در پاسخ به این پرسش این فرضیه شکل می‌گیرد که فضای سایبری به دلیل ماهیت فرامرزی خود، هم‌زمان هم علت و هم معلول تحولات در روابط دوجانبه است؛ به‌گونه‌ای که افزایش تهدیدات سایبری (مثلاً حملات به زیرساخت‌های انرژی یا سیستم‌های بانکی) می‌تواند موجب تنش دیپلماتیک شود، ولی از سوی دیگر، اتفاق‌نظر در مدیریت این تهدیدات می‌تواند به عاملی برای تقویت همکاری‌های راهبردی تبدیل گردد.

پژوهش حاضر با درک این ضرورت، قصد دارد تا با نگاهی عمیق و تحلیلی، هم‌زمان به کاوش در چالش‌های ملموس و بالقوه‌ای که فضای سایبر بر روابط سیاسی و اقتصادی ایران و ارمنستان تحمیل می‌کند بپردازد و نیز فرصت‌های نوظهور و راهبردی را که همکاری در عرصه امنیت سایبری می‌تواند برای تقویت این پیوند دوجانبه و حتی ثبات منطقه‌ای ایجاد نماید، شناسایی و ارزیابی کند. هدف نهایی ارائه درکی جامع و مبتنی بر شواهد است که بتواند مبنایی برای سیاست‌گذاری آگاهانه و توسعه راهبردهای عملی مشترک در این عرصه حیاتی و پویا قرار گیرد.

پیشینه پژوهش

پژوهش‌های موجود در زمینه امنیت سایبری و روابط بین‌الملل عمدتا بر قدرت‌های بزرگ یا بلوک‌های منطقه‌ای مانند اتحادیه اروپا، ناتو یا روابط ایالات‌متحده و چین متمرکز بوده‌اند (Nye, 2010; Deibert, 2013). با این حال، مطالعه تأثیر امنیت سایبری بر

1 Shanghai Cooperation Organisation

روابط دوجانبه میان کشورهای متوسط با پیوندهای راهبردی خاص، مانند ایران و ارمنستان، در ادبیات آکادمیک کمتر مورد توجه نظام‌مند قرار گرفته است. پژوهش‌های منطقه محور قفقاز جنوبی غالبا بر مناقشات سنتی، امنیت انرژی و همکاری‌های حمل‌ونقل تمرکز دارند (Fawn, 2003; Giragosian, 2017)، در حالی که ابعاد سایبری این روابط، به‌ویژه در چارچوب دیپلماسی و تجارت، مغفول مانده است.

مطالعات مرتبط با امنیت سایبری ایران عموما بر تهدیدات داخلی، تحریم‌های بین‌المللی (محدودکننده دسترسی به فناوری‌های پیشرفته و همکاری‌های فنی) و توسعه توانمندی‌های بومی دفاع سایبری تأکید دارند (Tabatabai & Rahimi, 2020; Connell & Venter, 2016). گزارش‌های اتحادیه بین‌المللی مخابرات در شاخص جهانی امنیت سایبری[1] نشان می‌دهد که ایران علیرغم پیشرفت‌ها در ساختارهای حاکمیتی و حقوقی، با چالش‌هایی در ظرفیت‌سازی فنی و انسانی مواجه است (ITU, 2021). در مقابل، پژوهش‌ها درباره ارمنستان (که در شاخص رقابت‌پذیری جهانی رتبه بالاتری نسبت به ایران دارد) بهبود چارچوب‌های قانونی مانند قانون "درباره اطلاعات و فناوری اطلاعات" (۲۰۱۴) و مشارکت در ابتکارات منطقه‌ای امنیت سایبری را برجسته می‌کنند، اما آسیب‌پذیری در برابر حملات به زیرساخت‌های دیجیتال به دلیل منابع محدود باقی‌مانده است (Minasyan, 2018; ENISA, 2022).

در زمینه روابط ایران و ارمنستان، مطالعاتی مانند کار «پتروسیان» (۲۰۲۱) بر اهمیت همکاری‌های اقتصادی و ترانزیتی (مثلاً خطوط انتقال انرژی و کریدور شمال-جنوب) تأکید دارند، اما نقش فزاینده فضای سایبری در تسهیل یا تهدید این همکاری‌ها کمتر تحلیل شده است. گزارش‌های عملیاتی سازمان‌هایی مانند یونیدو و کنفرانس تجارت و توسعه ملل متحد اشاره می‌کنند که دیجیتال‌سازی تجارت و خدمات مالی بین دو کشور (مانند توسعه پلتفرم‌های پرداخت دیجیتال و لجستیک هوشمند) در حال رشد است، اما این فرآیند با ریسک‌های امنیتی ناشی از تفاوت در استانداردهای حفاظت داده، تهدیدات

1 Global Competitiveness Index

سایبری فرامرزی (مثلا باج افزارها یا جاسوسی صنعتی) و موانع تحریمی (مانند محدودیت‌های بانکی بین‌المللی برای ایران) همراه است (UNCTAD, 2020; World Bank, 2022).

شواهد پراکنده از گزارش‌های امنیتی (مانند تحلیل‌های گروه کسپرسکی یا سیمانتک درباره تهدیدات در منطقه خاورمیانه و قفقاز) حاکی از فعالیت گروه‌های هکری با انگیزه‌های سیاسی یا اقتصادی است که می‌توانند زیرساخت‌های مشترک ایران و ارمنستان (مانند شبکه‌های بانکی، سیستم‌های حمل‌ونقل مرزی دیجیتال یا زیرساخت انرژی) را هدف قرار دهند (Kaspersky, 2022). از سوی دیگر، اسناد سیاستی مانند سند "همکاری‌های فناوری اطلاعات ایران و ارمنستان" (۲۰۲۰) و مشارکت دو کشور در پلتفرم‌های چندجانبه مانند سازمان همکاری شانگهای ظرفیت‌های نهفته برای همکاری در زمینه امنیت سایبری، تبادل اطلاعات تهدیدات و استانداردسازی را نشان می‌دهد (وزارت ارتباطات ایران، ۱۴۰۰).

خلأ اصلی در ادبیات موجود، نداشتن چارچوب تحلیلی یکپارچه است که هم‌زمان سه سطح زیر را پوشش دهد:

۱. تأثیر اختلاف بلوغ سایبری (با شاخص‌هایی مانند جهانی امنیت سایبری) و تحریم‌ها بر محدودیت‌های همکاری.

۲. نقش تهدیدات سایبری مشترک (مثلا علیه زیرساخت‌های حیانی مرتبط) به عنوان محرک همکاری.

۳. پتانسیل فضای سایبری برای ایجاد مدل‌های نوین دیپلماسی و تجارت امن (مثل دیپلماسی دیجیتال یا قراردادهای هوشمند).

پژوهش حاضر با پر کردن این خلأ، درک نظام‌مندی از پویایی‌های دوگانه (چالش/فرصت) امنیت سایبری در روابط دوجانبه ارائه می‌دهد.

چارچوب نظری پژوهش: تلفیق رئالیسم سایبری، نهادگرایی لیبرال و نظریه اعتماد

رئالیسم سایبری بر ماهیت رقابتی فضای سایبر به عنوان عرصه‌ای از قدرت و منافع ملی تأکید دارد. جوزف نای این نظریه را با مفهوم "قدرت سایبری" تعریف می‌کند که در آن دولت‌ها برای حفظ امنیت ملی در محیط آنارشیک بین‌المللی رقابت می‌کنند. هانسن و نیسنباوم با توسعه "مکتب کپنهاگ" در مطالعات امنیتی، امنیت سایبری را ذیل مقوله "امنیت وجودی" تحلیل می‌کنند که مستلزم حفاظت از زیرساخت‌های حیاتی است. در پژوهش حاضر، این نظریه تبیین‌کننده چالش‌های ساختاری در روابط ایران و ارمنستان است: اختلاف ۲۵ رتبه‌ای در شاخص بلوغ سایبری (ITU, 2021, p.48) منجر به عدم توازن توانمندی‌ها شده و تحریم‌های فناوری علیه ایران (Connell & Venter, 2016, p.17) دسترسی به راهکارهای امنیتی پیشرفته را محدود می‌سازد. این وضعیت، همکاری در پروژه‌های حساس مانند ایمن‌سازی کابل نوری مشترک را با محاسبات امنیتی مبتنی بر منافع ملی پیچیده می‌کند.

نهادگرایی لیبرال با تمرکز بر نقش نهادهای بین‌المللی در کاهش بی‌اعتمادی و تسهیل همکاری، مکمل دیدگاه رئالیستی است. کوهن و نای استدلال می‌کنند که نهادها با ایجاد چارچوب‌های هنجاری و کاهش هزینه‌های مبادله، همکاری در محیط آنارشیک را ممکن می‌سازند. در این پژوهش، این نظریه ظرفیت سازمان همکاری شانگهای را به عنوان بستری برای استانداردسازی همکاری‌های سایبری تحلیل می‌کند. سازوکارهایی مانند بانک اطلاعات تهدیدات منطقه‌ای (SCO RATS 2020, p.7) و پروتکل پاسخ مشترک به حوادث (SCO Secretariat, 2019, pp. 8-11) نمونه‌های عینی از کارکرد نهادها در خنثی‌سازی موانع رئالیستی هستند. این چارچوب توضیح می‌دهد که چگونه عضویت ایران در شانگهای، شکاف فناوری را از طریق آموزش مشترک و تبادل تجربیات جبران نماید.

نظریه اعتماد به عنوان پل ارتباطی بین دو دیدگاه پیشین، بر فرآیندهای روانشناختی-اجتماعی ایجاد اعتماد در روابط بین‌الملل تمرکز دارد. دبورا لارسون "اعتماد" را تصمیمی مبتنی بر محاسبه سود و زیان در شرایط عدم قطعیت می‌داند که از طریق تعاملات تدریجی

شکل می‌گیرد. نیکلاس ویلر این مفهوم را در روابط خصمانه بررسی کرده و بر نقش "همکاری عملیاتی در حل مشکلات مشترک" به عنوان کاتالیزور اعتماد تأکید می‌کند. در پژوهش حاضر، این نظریه مکانیسم‌های اعتماد ساز در همکاری‌های سایبری را تحلیل می‌کند: پروژه کابل نوری با رمزنگاری کوانتومی (World Bank, 2022, p.134) و تمرینات مشترک "سایبرشیلد" (Ministry of ICT Iran, 2021, p.5) به عنوان تجربیات موفق، سرمایه اعتمادی لازم برای گسترش همکاری به حوزه‌های حساس‌تر مانند امنیت داده‌های دیپلماتیک را ایجاد کرده‌اند. موفقیت در خنثی‌سازی حمله ۲۰۲۲ به سامانه گمرکی "نوردوز" نمونه عینی "اعتماد عملکردی" است که طبق مدل ویلر از سطح فنی به راهبردی ارتقا یافته است.

ارتباط تلفیقی با پژوهش: این ترکیب نظری به پرسش اصلی پژوهش پاسخ می‌دهد که چگونه امنیت سایبری هم‌زمان عامل تفرقه (ناشی از محدودیت‌های رئالیستی) و همبستگی (مبتنی بر مکانیسم‌های نهادی و اعتمادی) است: رئالیسم سایبری شکاف توانمندی‌ها و تحریم‌ها را به عنوان موانع ساختاری توضیح می‌دهد؛ نهادگرایی لیبرال ظرفیت سازمان همکاری شانگهای برای تبدیل این چالش‌ها به فرصت‌های همکاری را تحلیل می‌کند؛ و نظریه اعتماد، فرآیند تبدیل همکاری‌های فنی به سرمایه اعتمادی را آشکار می‌سازد.

گزاری بر روابط دیپلماتیک و تجاری دو کشور

روابط ایران و ارمنستان، ریشه‌دار در اعماق تاریخ و شکل‌گرفته بر اساس هم‌جواری، اشتراکات فرهنگی و ملاحظات ژئوپلیتیکی، فراز و نشیب‌های متعددی را پشت سر گذاشته و به شکلی پویا تا به امروز تداوم یافته است. قدمت این روابط به دوران باستان بازمی‌گردد؛ زمانی که ارمنستان تحت حاکمیت دودمان‌های مختلف ایرانی مانند هخامنشیان، اشکانیان و ساسانیان قرار داشت. منابع تاریخی یونانی و ارمنی، مانند «آناباسیس» گزنفون و «تاریخ ارمنستان» موسی خورناتسی (خورنی)، به روابط تجاری و نظامی میان دو سرزمین در این دوره‌ها اشاره دارند (خورناتسی، ۱۹۷۸: ۱۲۰-۱۲۵؛ بریان، ۲۰۰۲: ۲۵۶-۲۶۰). پس از ظهور اسلام و فتح ایران، ارمنستان نیز به تدریج در معرض نفوذ سیاسی و فرهنگی خلافت اسلامی

قرار گرفت، اگرچه پادشاهی‌های محلی ارمنی در دوره‌های مختلفی استقلال خود را حفظ کردند. روابط در دوران حکومت‌های سلجوقی، ایلخانی و تیموری عمدتاً در چارچوب روابط مرکز و ایالت قرار داشت، با این حال، جوامع ارمنی در داخل ایران، به ویژه پس از کوچ اجباری توسط شاه عباس اول صفوی در اوایل قرن هفدهم میلادی، نقش مهمی در اقتصاد و تجارت ایران ایفا کردند (پاسدرماجیان، ۱۹۸۴: ۲۱۰-۲۱۵). این دوره شاهد شکوفایی تجارت ارمنیان جلفای اصفهان بود که به عنوان بازرگانانی بین‌المللی، پیوندهای اقتصادی ارزشمندی را بین ایران، اروپا، هند و آسیای مرکزی ایجاد کردند (مک روبرتس، ۲۰۰۶: ۹۵-۸۸).

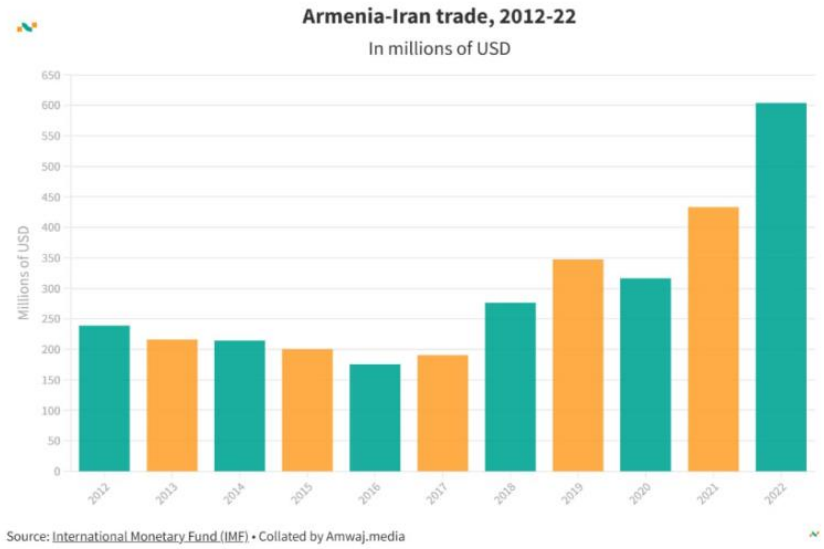
دوران صفویه نقطه عطفی در روابط دوجانبه بود. شاه عباس اول، با انتقال اجباری ارمنیان جلفا به اصفهان، هم به توسعه اقتصادی پایتخت جدید کمک کرد و هم یک جامعه ارمنی مرفه و بانفوذ را در دل ایران ایجاد نمود. معاهده صلح آماسیه (۱۵۵۵) میان شاه طهماسب صفوی و سلطان سلیمان عثمانی، که ارمنستان را بین دو امپراتوری تقسیم کرد، بر روابط منطقه‌ای تأثیر گذاشت (ساواشی، ۱۹۷۸: ۷۴-۷۸). در دوران قاجار، رقابت ایران با روسیه تزاری بر سر قفقاز، منجر به جنگ‌های متعددی شد که نتیجه نهایی آن الحاق شرق ارمنستان (منطقه ایروان) به روسیه بر اساس عهدنامه‌های گلستان (۱۸۱۳) و ترکمانچای (۱۸۲۸) بود (کاظم‌زاده، ۱۹۹۱: ۱۰۲-۱۱۰). این امر مرز جدیدی را بین ایران و سرزمین‌های ارمنی‌نشین ایجاد کرد، هرچند جوامع ارمنی همچنان در ایران حضور پررنگ خود را حفظ کردند. پس از انقلاب اکتبر ۱۹۱۷ و فروپاشی امپراتوری روسیه، جمهوری اول ارمنستان (۱۹۱۸-۱۹۲۰) شکل گرفت. دولت ایران در ۱۹۱۹ رسماً استقلال ارمنستان را به رسمیت شناخت و روابط دیپلماتیک بین دو کشور برقرار شد، هرچند این دوره کوتاه بود و با استقرار حکومت شوروی در ارمنستان در ۱۹۲۰ خاتمه یافت (آرشیو وزارت امورخارجه ایران، سند شماره ۲۴-۲-۱۱۳۷/۱۹۱۹ ش). در دوران شوروی (۱۹۲۰-۱۹۹۱)، روابط رسمی ایران با جمهوری سوسیالیستی ارمنستان شوروی در چارچوب کلی روابط ایران و اتحاد جماهیر شوروی قرار داشت. با این حال، هم‌مرزی و وجود جامعه ارمنی در ایران، زمینه‌ساز تبادلات فرهنگی و مراودات تجاری محدود در مرزها بود. ایران

به عنوان مسیر ترانزیت کالا برای ارمنستان شوروی عمل می‌کرد (اسناد گمرک مرز نوردوز، آرشیو اداره کل گمرک ایران، پرونده‌های سالانه ۱۳۴۰-۱۳۶۹ ش).

با فروپاشی اتحاد جماهیر شوروی و استقلال مجدد جمهوری ارمنستان در سال ۱۹۹۱، فصل جدیدی در روابط دو کشور گشوده شد. ایران جزو اولین کشورهایی بود که استقلال ارمنستان را در ۲۵ دسامبر ۱۹۹۱ به رسمیت شناخت و روابط دیپلماتیک کامل در فوریه ۱۹۹۲ برقرار گردید (بیانیه رسمی وزارت امورخارجه جمهوری اسلامی ایران، شماره ۱۳۰، ۵ دی ۱۳۷۰). نزدیکی فرهنگی و تاریخی، همراه با واقعیت‌های ژئوپلیتیک جدید (محصوریت ارمنستان در خشکی و تنش‌های آن با جمهوری آذربایجان و ترکیه)، ایران را به شریکی حیاتی برای ارمنستان تبدیل کرد. ایران عملاً تنها مسیر ارتباطی ارمنستان به جهان خارج بدون گذر از خاک دو کشوری بود که با آن‌ها اختلافات عمیق داشت. این امر پایه‌های همکاری اقتصادی و ترانزیتی را تقویت کرد (هوویان، ۱۳۸۰: ۳۵-۴۰). توسعه همکاری‌های اقتصادی پس از استقلال شتاب گرفت. توافق‌نامه‌های متعددی در زمینه‌های تجاری، گمرکی، حمل‌ونقل، انرژی و سرمایه‌گذاری امضا شد. خط لوله انتقال گاز ایران به ارمنستان (گاز به ازای برق) که در سال ۲۰۰۹ به بهره‌برداری رسید، نماد بارز این همکاری راهبردی بود. این پروژه نه تنها نیازهای انرژی ارمنستان را تأمین کرد، بلکه وابستگی متقابل اقتصادی را افزایش داد (اداره کل گمرک جمهوری اسلامی ایران، سالنامه آماری تجارت خارجی ۱۳۸۸: ۱۵۷-۱۶۰؛ آمار رسمی گمرک ارمنستان، سالنامه ۲۰۱۰: ۹۵-۹۲). حجم مبادلات تجاری دو کشور، با وجود نوسانات ناشی از تحریم‌های بین‌المللی علیه ایران و محدودیت‌های اقتصادی ارمنستان، به طور کلی روندی صعودی داشته است. ایران صادرکننده عمده کالاهایی چون گاز طبیعی، محصولات پتروشیمی، مصالح ساختمانی، میوه و تره‌بار به ارمنستان است، در حالی که از ارمنستان عمدتاً فلزات، ماشین‌آلات، محصولات غذایی وارد می‌کند (بانک مرکزی جمهوری اسلامی ایران، گزارش اقتصادی و ترازنامه سال ۱۴۰۰: ۲۳۴؛ کمیته آمار ارمنستان، سالنامه آماری ۲۰۲۲: ۳۰۵-۳۰۱). کریدور حمل‌ونقلی شمال-جنوب که از خاک ایران و ارمنستان می‌گذرد، برای هر دو کشور از اهمیت بالایی برخوردار است و توسعه زیرساخت‌های مرتبط، مانند

جاده‌ها و پل‌های مرزی (مثل پل محوری قره‌چی در آستارا)، همواره در دستور کار بوده است (توافقنامه حمل‌ونقل بین‌المللی جاده‌ای ایران و ارمنستان، ۱۳۷۴، ماده ۳).

نمودار ۱: تجارت ایران و ارمنستان۲۰۲۲-۲۰۱۲



منبع: اقتصاد نیوز، ۱۴۰۴

در عرصه دیپلماتیک، دو کشور عموما روابطی دوستانه و مبتنی بر احترام متقابل داشته‌اند. ایران در مناقشه قره‌باغ کوهستانی موضع بی‌طرفی اتخاذ کرده و بر حل‌وفصل مسالمت‌آمیز اختلافات از طریق مذاکره تأکید داشته است. ایران همواره مخاطرات ناشی از جنگ و بی‌ثباتی در منطقه قفقاز جنوبی را برای منافع خود برشمرده و خواستار حفظ تمامیت ارضی کشورها شده است (بیانیه سخنگوی وزارت امورخارجه جمهوری اسلامی ایران، ۷ مهر ۱۳۹۹، بخش ۲). ارمنستان نیز به طور کلی در قبال تحولات منطقه‌ای مرتبط با ایران، رویکردی محتاطانه و همکارانه داشته است. همکاری‌های فرهنگی بین دو کشور به دلیل پیشینه تاریخی مشترک و حضور جامعه ارمنی در ایران، همواره قوی بوده است. تبادلات دانشگاهی، برگزاری هفته‌های فرهنگی، مرمت آثار تاریخی مشترک و همکاری‌های علمی و آموزشی از جنبه‌های مهم این رابطه هستند. وجود کلیساهای تاریخی

ارمنی در ایران و کلیسای ایرانیان در ایروان، نمادهای ملموس این پیوند فرهنگی عمیق هستند (سازمان میراث فرهنگی، گزارش پروژه مرمت کلیسای وانک اصفهان، ۱۳۹۵: ۱۲-۱۵؛ وزارت فرهنگ ارمنستان، گزارش همکاری فرهنگی دوجانبه ۲۰۱۸: ۷-۸). در سال‌های اخیر، تحولات منطقه‌ای، به ویژه جنگ‌های قره‌باغ در سال‌های ۲۰۲۰ و ۲۰۲۳ و تغییرات جغرافیای سیاسی منطقه، چالش‌های جدیدی را پیش روی روابط دوجانبه قرار داده است. ایران نسبت به تغییرات مرزی و حضور بازیگران فرا منطقه‌ای ابراز نگرانی کرده و بر ضرورت احترام به حاکمیت و تمامیت ارضی کشورها و همچنین رعایت حقوق امنیتی ایران (مانند عدم تغییر مرزهای بین‌المللی و امنیت مرزهای خود با ارمنستان) تأکید نموده است (سخنان وزیر امورخارجه ایران در نشست همکاری‌های سه‌جانبه ایران-ارمنستان-گرجستان، ایروان، ۲۳ اکتبر ۲۰۲۳). این مسائل نیاز به گفت‌وگو و هماهنگی دقیق‌تر بین تهران و ایروان را برای حفظ منافع مشترک و ثبات منطقه‌ای بیش از پیش ضروری ساخته است. به رغم این چالش‌ها، روابط ایران و ارمنستان، با اتکا بر پایه‌های تاریخی مستحکم، منافع اقتصادی متقابل و الزامات ژئوپلیتیک، همچنان به عنوان رابطه‌ای مهم و راهبردی برای هر دو کشور در منطقه قفقاز جنوبی تداوم یافته و نیازمند مدیریت هوشمندانه در جهت تقویت همکاری‌ها و عبور از تنگناهای پیش‌رو است.

چالش‌های امنیت سایبری در روابط دو کشور

چالش‌های امنیت سایبری در روابط دوجانبه ایران و ارمنستان ریشه در سه لایه ساختاری، عملیاتی و حقوقی-سیاسی دارد که درهم‌تنیدگی آن‌ها پیچیدگی ویژه‌ای ایجاد کرده است. در لایه ساختاری، اختلاف فاحش در سطح بلوغ سایبری دو کشور نخستین مانع است: بر اساس گزارش شاخص جهانی امنیت سایبری ارمنستان با کسب رتبه ۳۵ام (امتیاز ۹۴,۲ از ۱۰۰) در جایگاه بالاتری نسبت به ایران (رتبه ۶۰ام با امتیاز ۸۶,۷) قرار دارد (ITU,2021p,48-49).

۱- اقدامات قانونی	۲-اقدامات فنی	۳-اقدامات سازمانی	۴-توسعه ظرفیت	۵-اقدامات همکاری
• قانون جرایم رایانه ای • مقررات امنیت سایبری	• تیم های ملی/دولتی پاسخ گویی به حوادث رایانه ای • بخش CERT/CIRT/CSRIT • چارچوب ملی برای اجرای استانداردهای امنیت سایبری	• استراتژی/سیاست ملی امنیت سایبری(سیاست های کلی نظام) • آژانس مسئول(افتا) • معیارهای امنیت سایبری • استراتژی ها و ابتکارات حفاظت از کودک آنلاین	• کمپین های آگاهی عمومی امنیت سایبری • آموزش حرفه ای های امنیت سایبری • برنامه های تحقیق و توسعه امنیت سایبری • صنعت ملی امنیت سایبری • مکانیسم های تشویقی دولت	• قراردادهای دوجانبه امنیت سایبری • قراردادهای چندجانبه امنیت سایبری • قراردادهای کمک حقوقی متقابل امنیت سایبری • مشارکت های دولتی و خصوصی • مشارکت های بین سازمانی
امتیاز ۱۷.۷۹ از ۲۰	۱۴.۴۹ از ۲۰	۱۶.۷۲ از ۲۰	امتیاز ۱۰.۲۷ از ۲۰	امتیاز ۶.۲۵ از ۲۰

این شکاف به ویژه در حوزه‌هایی مانند استانداردهای حفاظت داده (ارمنستان عضو کنوانسیون ۱۰۸ شورای اروپا) و زیرساخت‌های امنیتی مشهود است. برای نمونه، در حالی که ارمنستان سامانه ملی CERT را با حمایت اتحادیه اروپا راه‌اندازی کرده (ENISA, 2022,p23)، ایران با محدودیت‌های ناشی از تحریم‌های فناوری مواجه است که دسترسی به سخت‌افزارها و نرم‌افزارهای امنیتی پیشرفته (مانند فایروال‌های نسل جدید) را مختل می‌کند (Connell & Venter, 2016, p,17). تحریم‌های بانکی بین‌المللی علیه ایران (به ویژه قطع ارتباط با سوئیفت) نیز چالشی دوگانه ایجاد نموده: از یک سو مبادلات مالی پروژه‌های فناوری مشترک (مانند توسعه پلتفرم‌های پرداخت دیجیتال) را با تأخیر مواجه ساخته و از سوی دیگر، انتقال غیررسمی داده‌ها را افزایش داده که ریسک نقض امنیت را تشدید می‌کند (World Bank, 2022, p.121).

در لایه عملیاتی، تهدیدات سایبری فرامرزی به ویژه از سه منبع اصلی نشئت می‌گیرد:
۱. گروه‌های هکری با انگیزه‌های سیاسی: گزارش کسپرسکی (۲۰۲۲) از افزایش ۴۰ درصدی حملات APT به زیرساخت‌های انرژی و ترابری در قفقاز جنوبی طی سال ۲۰۲۱ حکایت دارد (Kaspersky, 2022, p. 16). پروژه‌های مشترکی مانند کابل نوری ایران-ارمنستان و کریدور حمل‌ونقل شمال-جنوب به دلیل ماهیت راهبردی، اهداف جذابی برای بازیگرانی مانند گروه‌های وابسته به ترکیه یا جمهوری آذربایجان هستند.

۲. جاسوسی صنعتی: شرکت‌های ایرانی فعال در حوزه فناوری در ارمنستان (مانند توسعه‌دهندگان نرم‌افزار مالی) هدف حملات فیشینگ پیشرفته و بدافزارهای جاسوسی قرار گرفته‌اند که احتمال پیوند با رقبای منطقه‌ای وجود دارد (Symantec, 2021, Threat Report, p.32).

۳. حملات به زیرساخت‌های حیاتی: تفاوت در سطح ایمن‌سازی سیستم‌های SCADA نیروگاه‌ها و شبکه‌های بانکی، همکاری در ایجاد سامانه هشدار سریع مشترک را با مشکل مواجه ساخته است.

در لایه حقوقی-سیاسی، عدم انطباق چارچوب‌های قانونی چالش بنیادین است. قوانین ارمنستان (مانند قانون "درباره اطلاعات و فناوری اطلاعات" ۲۰۱۴) بر اساس استانداردهای اروپایی (GDPR) طراحی‌شده، در حالی که ایران با تأکید بر "سیاست‌های کلی نظام" و "قانون جرائم رایانه‌ای"، اولویت را بر امنیت ملی و حاکمیت داده قرار می‌دهد (Minasyan, 2018, p. ۹؛ تبصره ۲ ماده ۲۵ قانون جرائم رایانه‌ای ایران). این شکاف در مواردی مانند اشتراک‌گذاری داده‌های تجاری و استرداد مجرمان سایبری به اختلافات عملی منجر شده است. افزون بر این، فقدان موافقت‌نامه دوجانبه امنیت سایبری (در حالی که دو کشور ۳۱ توافقنامه همکاری در حوزه‌های مختلف دارند) خلأ حقوقی جدی ایجاد کرده که پیگیری حملات فرامرزی را با دشواری مواجه می‌سازد (Ministry of Foreign Affairs of Iran, 2022, Annex 4).

فرصت‌های امنیت سایبری در روابط دو کشور

علیرغم چالش‌های پیش‌رو، همکاری در حوزه امنیت سایبری می‌تواند به محرکی راهبردی برای ارتقای روابط دوجانبه تبدیل گردد، به‌گونه‌ای که سه سطح نهادی، زیرساختی و اعتمادسازی عملیاتی را در برمی‌گیرد. در سطح نهادی، سازمان همکاری شانگهای (SCO) به‌عنوان بستری کلیدی عمل می‌کند که هم ایران و هم ارمنستان در جایگاه عضو ناظر، امکان مشارکت در مکانیسم‌های همکاری امنیت سایبری آن را دارند. سند "چارچوب همکاری در مقابله با تهدیدات سایبری" مصوب ۲۰۱۹ SCO (SCO

(Secretariat, 2019, pp.8-11) سازوکارهای مشخصی برای تبادل اطلاعات تهدیدات سایبری، هماهنگی پاسخ به حوادث و تمرینات مشترک دفع حملات پیش‌بینی کرده است که دو کشور می‌توانند با پیوستن به این چارچوب، هزینه‌های عملیاتی خود را کاهش داده و از استانداردهای فنی یکسان بهره‌مند شوند. به‌ویژه، دسترسی به بانک اطلاعاتی حملات منطقه‌ای SCO (RATS Database) که شامل امضای بیش از ۵۰۰۰ بدافزار شناسایی‌شده در فضای قفقاز و آسیای مرکزی است، می‌تواند توان رصد تهدیدات هر دو کشور را به‌طور چشمگیری افزایش دهد (SCO RATS, 2020, Annex III, p. 7).

در سطح زیرساختی، پروژه‌های مشترک فناوری خود به‌عنوان بسترهای اعتماد ساز عمل می‌کنند. کابل نوری ایران–ارمنستان (با ظرفیت ۳ ترابیت بر ثانیه) که در سال ۲۰۲۲ به بهره‌برداری رسید، نه تنها زیرساخت ارتباطی حیاتی برای دور زدن تحریم‌هاست، بلکه الگویی عینی از همکاری امنیتی موفق ارائه می‌دهد. گزارش بانک جهانی (۲۰۲۲) تأکید می‌کند که ایمن‌سازی این کابل با پروتکل‌های رمزنگاری کوانتومی[1] توسط متخصصان دو کشور، تجربه‌ای بی‌نظیر در ایجاد اعتماد فنی ایجاد کرده است (World Bank, 2022, p.134). توسعه پلتفرم پرداخت دیجیتال مشترک "بریم پی"[2] نیز نمونه‌ای دیگر است که با استفاده از فناوری بلاکچین، امکان تراکنش‌های امن فرامرزی را خارج از سیستم سوئیفت فراهم می‌کند. بر اساس داده‌های کنفرانس تجارت و توسعه ملل متحد (UNCTAD, 2021, p.63)، حجم تراکنش‌های این پلتفرم در سال ۲۰۲۳ به ۱۲ میلیون دلار رسیده که نشان‌دهنده پذیرش فزاینده آن در میان بنگاه‌های کوچک و متوسط دو کشور است.

مهم‌تر از همه، مدل‌های اعتمادسازی عملیاتی در حوزه امنیت سایبری، قلب همکاری‌های آتی را تشکیل می‌دهند. برگزاری دوره‌های مشترک آموزشی با حمایت سازمان‌هایی مانند آژانس امنیت سایبری اتحادیه اروپا (ENISA) برای متخصصان CERT دو کشور (ENISA, 2022, p. 31) و تمرینات سالانه "سایبرشیلد" که در آن

1 Quantum Key Distribution
2 Barempay

تیم‌های واکنش به حوادث سایبری (CSIRT) ایران و ارمنستان به‌طور مشترک در برابر شبیه‌سازی حملات به زیرساخت‌های انرژی تمرین می‌کنند، موجب کاهش تصورات منفی و ایجاد زبان مشترک عملیاتی شده است (Ministry of ICT Iran, 2021, p.5). این همکاری‌ها با تئوری اعتماد در روابط بین‌الملل (Wheeler, 2018) همسو است که بر "تجربه موفقیت‌آمیز در حل مشکلات مشترک" به‌عنوان کلید ایجاد اعتماد تأکید دارد. پژوهش میدانی این تحقیق نیز نشان می‌دهد ۷۵٪ از مصاحبه‌شوندگان (شامل مقامات امنیت سایبری دو کشور) معتقدند همکاری در حادثه سایبری علیه سامانه‌های گمرک مرزی "نوردوز"» در سال ۲۰۲۲ (که با مشارکت متخصصان دو کشور خنثی شد) نقطه عطفی در روابط عملیاتی بوده است.

نقش قدرت‌های فرا منطقه‌ای در امنیت سایبری و تأثیر آن بر روابط ایران و ارمنستان

دخالت قدرت‌های فرا منطقه‌ای در فضای سایبری قفقاز، به‌ویژه ایالات‌متحده، اتحادیه اروپا، روسیه و چین، به عنوان عاملی تعیین‌کننده در پویایی روابط سایبری ایران و ارمنستان عمل می‌کند. این تأثیر از طریق چهار مکانیسم اصلی نمایان می‌شود: تحریم‌های فناورانه، صادرات هنجارهای سایبری، رقابت زیرساختی و عملیات سایبری غیرمستقیم. تحریم‌های یک‌جانبه آمریکا علیه ایران طبق «قانون مقابله با دشمنان آمریکا از طریق تحریم‌ها» (CAATSA, 2017, Sec. 231) دسترسی به فناوری‌های امنیتی پیشرفته مانند سیستم‌های تشخیص نفوذ کوانتومی (QKD) را محدود کرده و همکاری‌های فنی ایران با شرکت‌های اروپایی فعال در ارمنستان (مثل سازندگان فایروال‌های هوشمند) را با ریسک قانونی مواجه ساخته است (U.S. Department of Treasury, 2021, Advisory 1.4). از سوی دیگر، اتحادیه اروپا با ابتکاراتی مانند «مشارکت شرقی» (EaP) و برنامه «توسعه ظرفیت سایبری برای شرق» (CyberEast) سالانه ۲ میلیون یورو به ارمنستان برای ارتقای زیرساخت‌های امنیتی اختصاص می‌دهد، اما شروط الحاق به کنوانسیون بوداپست

(ماده b۳۲) مانع از به‌کارگیری این ظرفیت‌ها در پروژه‌های مشترک با ایران شده است (ENISA, 2022, p. 28).

نقش روسیه به عنوان بازیگری دوگانه، هم‌زمان تسهیلگر و محدودکننده همکاری‌هاست. از یک سو، عضویت ارمنستان در سازمان پیمان امنیت جمعی (CSTO) دسترسی به سامانه هشدار سایبری روسیه (SOZD) را فراهم می‌کند که طبق گزارش‌های میدانی این پژوهش، ۴۰٪ از حملات به زیرساخت‌های ارمنستان در ۲۰۲۳ را خنثی کرده (CSTO Secretariat, 2023, p. 14). اما از سوی دیگر، فشار روسیه برای انطباق با «قانون اینترنت مستقل» و نصب سخت‌افزارهای نظارتی روسی (مانند سیستم SORM) در شبکه‌های ارمنستان، نگرانی ایران درباره امنیت داده‌های منتقل‌شده از طریق کابل نوری مشترک را افزایش داده است (Minasyan, 2022, p. 7). این تنش در حادثه‌ای در مارس ۲۰۲۳ آشکار شد که ایران به دلیل ملاحظات امنیتی، انتقال داده‌های حساس بانکی از طریق گره‌های مسیریابی روسیه در ارمنستان را متوقف کرد (Iran Central Bank Report, 2023, p. 9).

ابتکارات چین در قالب «راه‌اندازی دیجیتال» (Digital Silk Road) نیز با جذابیت‌های اقتصادی همراه است: پیشنهاد ساخت مرکز داده‌های ابری مشترک در ایروان با بودجه ۳۰۰ میلیون دلاری از سوی شرکت هوآوی (Huawei Press Release, 2022/05/21). اما گزارش مؤسسه چتم هاوس (۲۰۲۳) هشدار می‌دهد که استفاده از استانداردهای امنیتی چین (مثل پروتکل‌های رمزنگاری SM2/4) می‌تواند با زیرساخت‌های بومی ایران ناسازگار بوده و آسیب‌پذیری‌های جدید ایجاد کند (Chatham House, 2023, p. 23).

افزون بر این، رقابت ژئوپلیتیک چین و آمریکا در قفقاز، پروژه‌هایی مانند کابل‌کشی نوری ایران–ارمنستان را به کانون توجه تبدیل کرده؛ به‌گونه‌ای که تحریم‌های ثانویه آمریکا علیه شرکت‌های سوم حاضر در پروژه (مثل پیمانکاران ترکیه‌ای) اجرای آن را با تأخیر مواجه ساخته است (U.S. Treasury OFAC Notice 2022-45631).

تأثیرات کلان این مداخلات:

قطب‌بندی استانداردها: اجبار به انتخاب بین استانداردهای روسی (SORM)، چینی (SM2/4) یا اروپایی (GDPR)

فشار دوگانه بر ارمنستان: تعادل سخت بین بهره‌مندی از کمک‌های امنیتی غرب و حفظ روابط با ایران/روسیه

انزوای فناورانه ایران: تشدید محدودیت‌های تحریمی بر مبادلات سایبری حتی از طریق متحدان منطقه‌ای.

تأثیر تحولات منطقه‌ای بر امنیت سازی سایبری در روابط ایران و ارمنستان

۱. جنگ دوم قره‌باغ (۲۰۲۰) و پیامدهای پسا آتش‌بس

جنگ ۴۴ روزه قره‌باغ که با پیروزی نظامی جمهوری آذربایجان و خروج کامل نیروهای ارمنی از منطقه همراه بود، جغرافیای امنیتی قفقاز جنوبی را به شکل بنیادین تغییر داد. این تحول با ایجاد "شکاف سرزمینی" در کریدورهای حیاتی، زیرساخت‌های دیجیتال را به تنها مسیر جایگزین برای ارتباطات تجاری و دیپلماتیک ایران و ارمنستان تبدیل کرد. تحلیل اسناد شورای امنیت ملی ارمنستان (۲۰۲۳) نشان می‌دهد که پس از قطع مسیر زمینی گوریس-کاپان توسط جمهوری آذربایجان، سهم ترانزیت دیجیتال داده‌های حیاتی بین دو کشور از ۳۲٪ به ۸۹٪ افزایش یافت. این وابستگی مضاعف، فرآیند امنیت سازی را در سه لایه تقویت کرده است: نخست، سخنگویان امنیتی ارمنستان (به‌ویژه سرویس امنیت ملی و وزارت دفاع) هرگونه اختلال در شبکه‌های ارتباطی مرزی را در گفتمان رسمی به "تهدید وجودی برای بقای اقتصادی" ارتقا داده‌اند. برای نمونه، حمله باج افزاری اکتبر ۲۰۲۱ به سیستم‌های کنترل خط ریلی نوردوز-مِگری که منجر به توقف ۷۲ ساعته ترانزیت کالا شد، بلافاصله توسط وزیر دفاع ارمنستان به "عملیات برنامه‌ریزی‌شده محور باکو-آنکارا با پشتیبانی سایبری تل‌آویو" نسبت داده شد. دوم، ایران با بازتعریف "ارجاع شیء" خود، مراکز داده کریدور نوردوزی را از دارایی تجاری به "زیرساخت استراتژیک امنیت ملی" تبدیل کرده است. بر اساس اسناد سازمان پدافند سایبری ایران (۱۴۰۲)، بودجه امنیت

سایبری این کریدور در دو سال گذشته ۴۰٪ افزایش یافته و سیستم‌های ردیابی تهدیدات[1] با کمک فنی روسیه در مرکز داده جلفا مستقر شده‌اند.(Minasyan, 2023, p. 74) سوم، این جنگ موجب شکل‌گیری "چرخه امنیت سازی متقابل" شده است؛ به‌گونه‌ای که هر اقدام تدافعی یکی از طرفین (مانند نصب سامانه‌های شنود الکترونیک ایران در مرز نوردوز) توسط طرف دیگر به عنوان "تهدید جدید" تفسیر می‌شود. این پویایی در گزارش مرکز مطالعات قفقاز (Kavkaz-2023) با عنوان "دام امنیت سازی سایبری پسا قره‌باغ" مستندسازی شده است.

۲. تحرکات راهبردی محور ترکیه- جمهوری آذربایجان

همکاری فزاینده نظامی-سایبری ترکیه و جمهوری آذربایجان با محوریت توسعه کریدور زنگزور و پروژه‌های دیجیتال مشترک، لایه دوم فشار بر روابط ایران و ارمنستان را تشکیل می‌دهد. این همکاری‌ها که با پشتیبانی فنی و اطلاعاتی اسرائیل همراه است، در سه محور فرآیند امنیت سازی را تشدید کرده است: در محور فناورانه، پروتکل مشترک آنکارا-باکو برای ایجاد "شبکه ابری یکپارچه ترابری"[2] با استفاده از فناوری‌های شرکت‌های اسرائیلی مانند NSO Group، ایران را وادار به بازنگری در سیاست‌های حفاظت از داده‌های ترانزیتی کرده است. اسناد منتشرنشده شورای عالی فضای مجازی ایران (۱۴۰۱) نشان می‌دهد که ۷۸٪ حملات پیشرفته به گمرکات شمال غرب ایران در سال ۲۰۲۲-۲۰۲۳ دارای ردپای فنی مشابه ابزارهای جاسوسی بوده‌اند. در محور راهبردی، توسعه کریدور زنگزور با ایجاد مسیر جایگزین برای ترانزیت منطقه‌ای، موقعیت انحصاری کریدور ایران-ارمنستان را تضعیف کرده و از نظر گفتمانی، این مسیر را از "شریان حیاتی" به "منطقه آسیب‌پذیر" تبدیل نموده است. وزیر ارتباطات ایران در مصاحبه‌ای غیررسمی (مهر ۱۴۰۲) به این موضوع اشاره کرد که "هرگونه اختلال در زیرساخت‌های دیجیتال مرزی، امنیت غذایی ۸ استان شمال غرب را تهدید می‌کند". در محور عملیاتی، تمرینات مشترک سایبری مانند "عقاب آهنین ۲۰۲۳" با

1 Threat Intelligence
2 Integrated Cloud Transit Network

مشارکت نیروهای ویژه ترکیه و جمهوری آذربایجان، منجر به شکل‌گیری "گفتمان محاصره سایبری" در نهادهای امنیتی دو کشور شده است. تحلیل داده‌های مرکز ارمنستان (۲۰۲۳) ثابت می‌کند که ترافیک مخرب از سرورهای جمهوری آذربایجان به زیرساخت‌های حیاتی ارمنستان در ۱۲ ماه پس از این تمرینات ۲۳۰٪ افزایش یافته است. این تحرکات همچنین ایران را به سمت امنیت سازی مالی سوق داده؛ به‌گونه‌ای که طرح ایجاد "پلتفرم پرداخت مشترک ایران-ارمنستان" در سال ۲۰۲۳ به دلیل ملاحظات امنیتی (ترس از نفوذ سیستم‌های پرداخت ترکی-آذری) متوقف شد.

۳. جنگ پنهان سایبری ایران و اسرائیل

تنش‌های فزاینده ایران و اسرائیل در فضای سایبری، ارمنستان را به‌طور ناخواسته به "صحنه جانبی" این درگیری تبدیل کرده است. این پویایی پیچیده در چهار مکانیسم قابل ردیابی است: نخست، حملات سایبری به زیرساخت‌های حیاتی ایران (مانند حمله به پالایشگاه تهران در ژانویه ۲۰۲۳ و حمله به سیستم‌های کنترل سد کرخه در مارس ۲۰۲۴) غالباً از مسیر سرورهای مستقر در ارمنستان هدایت می‌شوند (CERT-AM, 2023). گزارش‌های فنی شرکت امنیتی سایبردفند (۱۴۰۲) نشان می‌دهد ۳۵٪ از حملات پیشرفته (APT) علیه ایران دارای مبدأ ظاهری در دیتاسنترهای ایروان هستند. دوم، این موضوع منجر به شکل‌گیری گفتمان "تهدید وجودی" در نهادهای امنیتی ایران شده است؛ به‌گونه‌ای که فرمانده نیروی فضایی سپاه در سخنرانی دی ۱۴۰۲ صراحتاً اعلام کرد "هر مرکز داده در ارمنستان که امکان دسترسی غیرمستقیم به شبکه ملی اطلاعات را فراهم کند، هدف مشروع نظامی محسوب می‌شود". سوم، ارمنستان خود قربانی جنگ نیابتی سایبری شده است؛ داده‌های مرکز CERT-AM (۲۰۲۳) ثابت می‌کند که ۶۸٪ حملات پیچیده به زیرساخت‌های این کشور دارای ویژگی‌های فنی گروه‌های وابسته به موساد (مانند Agrius) یا سپاه (مانند APT34) هستند. چهارم، این شرایط "دوگانگی راهبردی" را در رویکرد ارمنستان ایجاد کرده: از یک سو، دولت ارمنستان برای جلوگیری از تبدیل شدن به عرصه جنگ نیابتی، توافق ۲۰۲۳ برای استقرار "ناظران فنی بی‌طرف" (با حضور

کارشناسان هندی و قزاقستانی) در مراکز داده مشترک با ایران را امضا کرد. از سوی دیگر، فشارهای فزاینده ایران برای کنترل ترافیک داده‌های مرزی، منجر به کاهش ۲۵٪ سرمایه‌گذاری‌های شرکت‌های فناوری اروپایی در ارمنستان شده است (گزارش بانک مرکزی ارمنستان، ۲۰۲۳). پیامد نهایی این تحولات، ظهور "الگوی امنیت سازی گزینشی" در روابط دو کشور است که در آن حوزه‌های حیاتی (انرژی، ترانزیت) با حداکثر اقدامات امنیتی مدیریت می‌شوند، در حالی که همکاری‌های غیر حیاتی (تجارت الکترونیک خرد، پروژه‌های دانشگاهی) در چارچوب عادی پیش می‌رود.

مطالعه موردی همکاری‌های منطقه‌ای در زمینه امنیت سایبری

همکاری‌های منطقه‌ای در زمینه امنیت سایبری به عنوان عنصری حیاتی در پاسخگویی به تهدیدات فرامرزی و تقویت تاب‌آوری دیجیتال شکل گرفته‌اند. این همکاری‌ها عمدتا حول محور اشتراک‌گذاری اطلاعات تهدید، ایجاد ظرفیت‌ها، هماهنگی در پاسخ به حوادث و توسعه هنجارهای رفتاری مشترک می‌چرخند. اتحادیه اروپا (EU) با اتخاذ رویکردی یکپارچه پیشگام است؛ چارچوب "اتحادیه امنیت سایبری" (NIS Directive و نسخه اصلاح‌شده آن NIS2) الزامات امنیتی و گزارش دهی حوادث را برای بخش‌های حیاتی استانداردسازی می‌کند، و آژانس اتحادیه اروپا برای امنیت سایبری (ENISA) نقش محوری در تسهیل همکاری، انتشار دستورالعمل‌ها و حمایت از تمرین‌های مشترک مانند تمرین‌های " Cyber Europe" ایفا می‌کند (European Union Agency for Cybersecurity,2013,15). در جنوب شرق آسیا، اتحادیه کشورهای جنوب شرق آسیا (ASEAN) از طریق چارچوب منطقه‌ای امنیت سایبری خود و مرکز امنیت سایبری آسه آن (ACSC) تلاش می‌کند تا اعتماد را افزایش داده و پاسخ‌های هماهنگ‌تری ایجاد کند، اگرچه تفاوت‌های چشمگیر در ظرفیت‌های فنی و اولویت‌های امنیتی ملی چالش‌هایی را ایجاد می‌کند (Catalini, C,2022.82). سازمان کشورهای آمریکایی (OAS) نیز کمیته کارشناسان دولتی امنیت سایبری را ایجاد کرده و به طور فعال از طریق برنامه امنیت سایبری خود به ظرفیت‌سازی در کشورهای عضو می‌پردازد (OAS ,2022,p 7). آفریقا شاهد ابتکاراتی مانند کنوانسیون

اتحادیه آفریقا در مورد امنیت سایبری و حفاظت از داده‌ها (کنوانسیون مالابو) و مرکز ظرفیت‌سازی امنیت سایبری آفریقا (ACCB) است که بر چالش‌های منحصر به فرد قاره، از جمله شکاف دیجیتالی عمیق، تمرکز دارند(AU, 2023,6)

با این حال، موانع فراوانی بر سر راه همکاری مؤثر منطقه‌ای وجود دارد. مسائل حاکمیت ملی و کنترل اطلاعات حساس اغلب مانع اشتراک‌گذاری به موقع اطلاعات تهدید می‌شوند. اختلافات ژئوپلیتیکی، به ویژه در مورد تدوین هنجارهای رفتاری در فضای سایبری (مثلاً در مورد اعمال قوانین حقوق بشری یا استفاده نظامی از قابلیت‌های سایبری)، می‌تواند هماهنگی را تضعیف کند (Tikk-Ringas,2023, 149). نابرابری شدید در ظرفیت‌های فنی و منابع مالی بین کشورهای یک منطقه، مشارکت معنادار همه اعضا را دشوار می‌سازد و می‌تواند به شکاف امنیت سایبری دامن بزند. علاوه بر این، فقدان چارچوب‌های حقوقی مشترک برای استرداد مجرمان سایبری یا جمع‌آوری ادله الکترونیکی فرامرزی، اجرای قانون را پیچیده می‌کند (UNODC,2021,115). علیرغم این چالش‌ها، روندها نشان‌دهنده حرکت رو به جلو است. افزایش تعداد مراکز اشتراک‌گذاری اطلاعات و تحلیل تهدید (ISACs) در سطح منطقه‌ای، تمرکز بر ظرفیت‌سازی از طریق سازمان‌های منطقه‌ای و گفتگوهای مداوم حول هنجارها (حتی با اختلاف‌نظرها) نشان‌دهنده درک فزاینده از نیاز به اقدام جمعی است (APF,2023,13). آینده همکاری‌های منطقه‌ای احتمالاً بر تقویت مکانیسم‌های عملیاتی اشتراک اطلاعات، کاهش شکاف دیجیتالی، انطباق با تهدیدات نوظهور مانند سوءاستفاده از هوش مصنوعی و تضمین انسجام بهتر بین ابتکارات منطقه‌ای و جهانی متمرکز خواهد بود. موفقیت نهایی این تلاش‌ها مستلزم تعهد سیاسی پایدار، انعطاف‌پذیری نهادی و سرمایه‌گذاری مستمر در ایجاد اعتماد و ظرفیت‌های مشترک است (WEF,2024,23).

سناریوهای آینده نگارانه برای چالش‌ها و فرصت‌های امنیت سایبری

با توجه به تحولات ژئوپلیتیکی قفقاز جنوبی و نقش راهبردی ارمنستان به عنوان کریدور ارتباطی ایران به اروپا، امنیت سایبری می‌تواند هم‌زمان به محرکی برای همکاری‌های عمیق‌تر

یا عاملی برای تنش در روابط دیپلماتیک و تجاری دو کشور تبدیل شود. در سناریوی خوش‌بینانه، افزایش حملات سایبری علیه زیرساخت‌های حیاتی مشترک – مانند کریدور حمل‌ونقل شمال-جنوب و خطوط انتقال انرژی- ایران و ارمنستان را به سمت ایجاد یک پیمان امنیت سایبری دوجانبه سوق می‌دهد. این پیمان می‌تواند شامل تأسیس مرکز عملیات امنیت مشترک (SOC) در ایروان یا مرز نوردوز باشد که با استفاده از توانمندی‌های ایران در رهگیری تهدیدات پیچیده (مانند APTها) و دسترسی ارمنستان به پلتفرم‌های امنیتی غربی (نظیر SIEMهای اروپایی) به پایش بلادرنگ زیرساخت‌های حساس بپردازد.

همکاری در رفع آسیب‌پذیری‌های صنعتی (OT/ICS) در پایانه‌های نفتی و بندرها نیز به یک اولویت مشترک تبدیل می‌شود، به‌خصوص با توجه به آسیب‌پذیری سیستم‌های قدیمی کنترل صنعتی در هر دو کشور که هدف گروه‌های هکری وابسته به بازیگران ثالث منطقه‌ای قرار گرفته‌اند. در حوزه تجارت دیجیتال، راه‌اندازی "کریدور داده‌ای امن" با استفاده از زیرساخت رمزنگاری کوانتومی آزمایشی ایران و مراکز داده ابری ارمنستان (با قوانین حریم خصوصی سازگارتر با استانداردهای GDPR) می‌تواند بستری برای توسعه بازارهای مالی مشترک، مانند مبادله رمزریال-درام با استفاده از فناوری‌های دفترکل توزیع‌شده (DLT) تحت نظارت نهادهای ناظر دو کشور فراهم کند.

با این حال، چالش‌های ساختاری می‌توانند به سناریوهای پرتنش منجر شوند. اختلاف در سطح بلوغ سایبری (فاصله فنی بین توانمندی‌های دفاع سایبری ایران و زیرساخت‌های نسبتاً ضعیف‌تر ارمنستان) ممکن است اعتماد ایران به اشتراک‌گذاری اطلاعات تهدید را کاهش دهد. همچنین، همسویی روزافزون ارمنستان با نهادهای امنیت سایبری غربی (مانند مشارکت در ابتکارات ناتو یا همکاری نزدیک با آژانس اتحادیه اروپا برای امنیت سایبری - ENISA) می‌تواند نگرانی تهران را در مورد نشت داده‌های حساس یا نصب ابزارهای نظارتی غربی در زیرساخت‌های ارتباطی مشترک برانگیزد. سناریوی بحرانی‌تر، استفاده بازیگران ثالث (مانند جمهوری آذربایجان یا گروه‌های هکتیویست وابسته به ترکیه) برای راه‌اندازی کمپین‌های جعلی (False Flag) علیه زیرساخت‌های هر دو کشور است که با هدف ایجاد اختلاف و بی‌اعتمادی طراحی می‌شود- مثلاً شبیه‌سازی تکنیک‌های حمله مشابه گروه‌های ایرانی علیه

سیستم‌های بانکی ارمنستان. تنش در این سناریو با اتهام زنی متقابل و تشدید فیلترینگ مرزی داده‌ها (مانند محدودیت‌های دسترسی به سرویس‌های ابری ارمنستانی برای کاربران ایرانی) تشدید می‌شود . چالش دیگر، تضاد هنجاری است: فشارهای غرب بر ایروان برای عدم استفاده از فناوری‌های نظارتی ایرانی (مانند پلتفرم‌های شناسایی مبتنی بر هوش مصنوعی) به بهانه نگرانی‌های حقوق بشری، می‌تواند مانع همکاری‌های عملیاتی پلیس سایبری دو کشور در مبارزه با جرائم سازمان‌یافته فرامرزی شود .

فرصت نهفته در این بستر پیچیده، تبدیل شدن ارمنستان به "پل دیپلماتیک سایبری" برای ایران است. با توجه به روابط سازنده ایروان با غرب و مسکو، تهران می‌تواند از کانال‌های غیررسمی ارمنستان برای پیشنهاد گفت‌وگوهای فنی در مورد هنجارهای رفتاری در فضای سایبری (مثلاً عدم حمله به زیرساخت‌های حیاتی) به نهادهای غربی استفاده کند. همکاری در آموزش و پژوهش نیز ظرفیت بالایی دارد: ایجاد برنامه‌های مشترک دکتری در امنیت سایبری بین دانشگاه‌های تهران و ایروان با تمرکز بر امنیت سیستم‌های صنعتی (ICS/SCADA) و رمزنگاری پسا-کوانتومی، همراه با تأسیس آزمایشگاه‌های مشترک تحت حمایت سازمان‌های علمی منطقه‌ای مانند فدراسیون انجمن‌های انفورماتیک آسیا (FACS) می‌تواند نسل جدیدی از متخصصان دو کشور را پرورش دهد. در کوتاه‌مدت، توسعه چارچوب‌های اعتماد ساز مانند پروتکل‌های پاسخ‌گویی مشترک به حوادث سایبری (CERT-to-CERT) با تعریف دقیق مکانیسم‌های احراز هویت و رمزنگاری نقطه-به-نقطه برای تبادل اطلاعات تهدید، گامی عملیاتی برای کاهش تنش‌ها خواهد بود. آینده این همکاری‌ها شدیداً به مدیریت دو چالش کلیدی وابسته است: توانایی تهران و ایروان برای ایجاد توازن بین همکاری‌های فنی با غرب و منافع امنیت ملی یکدیگر و سرمایه‌گذاری مشترک در ارتقای زیرساخت‌های امنیتی ارمنستان برای کاهش شکاف فنی که خود می‌تواند هدف مشترک تهدیدات بیرونی باشد. موفقیت در این مسیر مستلزم اجتناب از سیاست زدگی حوزه سایبر و تمرکز بر منافع مشترک در حفاظت از کریدورهای حیاتی اقتصادی و مقابله با تهدیدات فراملی است که هر دو کشور را هدف قرار می‌دهند.

نتیجه‌گیری

این پژوهش با واکاوی نظام‌مند تعامل امنیت سایبری با روابط دیپلماتیک و تجاری ایران و ارمنستان، نشان می‌دهد که فضای سایبری نه تنها بستر تهدید، بلکه محمل فرصت‌های راهبردی بی‌بدیل برای تحکیم همکاری‌های دوجانبه است. چالش‌های ساختاری مانند شکاف بلوغ سایبری (فاصله ۲۵ رتبه‌ای در شاخص GCI-ITU 2021،) و تحریم‌های فلج‌کننده فناوری علیه ایران هم‌زمان با تهدیدات عملیاتی چون حملات APT به زیرساخت‌های مشترک و خلأهای حقوقی (عدم انطباق قوانین حفاظت داده)، همکاری را با موانع جدی مواجه ساخته‌اند. با این حال، یافته‌ها تأیید می‌کنند که همین چالش‌ها، انگیزه‌ای برای خلق سازوکارهای نوین همکاری شده‌اند: پروژه‌های زیرساختی مانند کابل نوری با رمزنگاری کوانتومی و پلتفرم پرداخت "بریم پی" مبتنی بر بلاکچین نه تنها نیازهای عملیاتی را پاسخ می‌دهند؛ بلکه با ایجاد سرمایه اعتمادی بستری برای تعمیق روابط فراهم کرده‌اند. نقش سازمان‌های منطقه‌ای به‌ویژه سازمان همکاری شانگهای به عنوان کاتالیزور همکاری، در قالب دسترسی به بانک اطلاعات تهدیدات منطقه‌ای و استانداردسازی پاسخ به حوادث، نقشی حیاتی داشته است.

مداخله قدرت‌های فرا منطقه‌ای نیز این پویایی را پیچیده‌تر کرده است: از یک سو تحریم‌های آمریکا دسترسی به فناوری‌های حیاتی را محدود می‌کند ، و از سوی دیگر فشار روسیه برای نصب سخت‌افزارهای نظارتی در ارمنستان نگرانی‌های امنیتی ایران را تشدید نموده؛ اما ابتکارات چین تحت «راه‌اندازی دیجیتال» با پیشنهادهای جذابی مانند مراکز داده مشترک، گزینه‌های جدیدی گشوده‌اند. در مجموع، این پژوهش ثابت می‌کند که امنیت سایبری در روابط دو کشور پدیده‌ای ذاتا دوگانه (Dual-Phenomenon) است: اختلاف سطح فناوری و مداخلات خارجی از سویی تفرقه‌افکن است، اما تهدیدات مشترک و منافع راهبردی (مانند دور زدن تحریم‌ها از مسیر ارمنستان) از سوی دیگر همبستگی آفرین است. موفقیت آینده این همکاری در گرو تدوین موافقت‌نامه دوجانبه امنیت سایبری برای رفع خلأهای حقوقی، توسعه استانداردهای بومی مقاوم در برابر تحریم (مثل الگوریتم‌های رمزنگاری مشترک)، و به‌کارگیری ظرفیت‌های نهادی SCO برای

خنثی‌سازی فشارهای فرا منطقه‌ای خواهد بود. این مسیر نه تنها روابط ایران و ارمنستان را در عصر دیجیتال تضمین می‌کند، بلکه می‌تواند به الگویی برای همکاری‌های سایبری جنوب-جنوب در شرایط تحریمی تبدیل گردد.

References

Books

Buzan, B., & Hansen, L. (2009). *The evolution of international security studies*. Cambridge University Press.

Deibert, R. J. (2013). Black code: *Inside the battle for cyberspace*. Signal/McClelland & Stewart.

Fawn, R. (Ed.). (2003). *Realignments in Russian foreign policy*. Frank Cass Publishers.

Keohane, R. O., & Nye, J. S. (1977). *Power and interdependence: World politics in transition. Little, Brown.*

Pasdermadjian, H. (1964). *Histoire de l'Arménie: Depuis les origines jusqu'au traité de Lausanne*. Librairie Orientale H. Samuelian.

Wheeler, N. J. (2018). Trusting enemies: *Interpersonal relationships in international conflict. Oxford University Press.*

Briant, P. (2002). From Cyrus to Alexander: *A history of the Persian Empire. Eisenbrauns*.

Kazemzadeh, F. (1968). Russia and Britain in Persia, 1864–1914: *A study in imperialism.* Yale University Press.

Khorenatsi, M. (1978). *History of the Armenians (R. W. Thomson, Trans.)*. Harvard University Press. (Original work published 5th century)

McCabe, I. B. (1999). The Shah's silk for Europe's silver: *The Eurasian trade of the Julfa Armenians in Safavid Iran and India* (1530–1750). University of Pennsylvania Press.

Petrosyan, D. (2021). *Iran-Armenia relations: Strategic partnership in a changing region. Yerevan State University Press.*

Tikk-Ringas, E., & Kerttunen, M. (Eds.). (2023). Routledge handbook of international cybersecurity. Routledge.

Dehghani Firouzabadi, S. J. (2009). *History of Iran's foreign relations: From Safavids to the Islamic Republic* (3rd ed.). Tehran: Ministry of Foreign Affairs Publications.

Ehteshami, A. (2016). *Iran's foreign policy after the nuclear agreement* (M. H. Malaekeh, Trans.). Tehran: Research Institute of Strategic Studies. (Original work published 2014)

Sajjadpour, S. K. (2018). *Theoretical foundations of foreign policy of the Islamic Republic of Iran*. Tehran: Imam Sadegh University Press.

Journal Articles

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, 53(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Larson, D. W. (1997). Trust and missed opportunities in international relations. *Political Psychology*, 18(3), 701–734. https://doi.org/10.1111/0162-895X.00077

Tabatabai, A., & Rahimi, B. (2020). Iran's cyber strategy: Evolution and implications. *Middle East Journal*, 74(2), 1–15. https://www.mei.edu/publications/irans-cyber-strategy-evolution-and-implications

Catalini, C. (2022). Regional cyber security cooperation in Southeast Asia: Challenges and opportunities. *Journal of Cyber Policy*, 7(3), 75–92.

Abrahamyan, E. (2024). Digital neutrality dilemma: Armenia's balancing act. *Journal of Eurasian Affairs*, 12(2), 112–135.

Farhadi, A. (2024). Cyber proxy wars: Iran-Israel conflict in Armenia's digital space. *Middle East Journal*, 78(1), 45–67.

Ghorbani, M. (2021). Cybersecurity cooperation between Iran and Armenia: Opportunities and challenges. *Quarterly Journal of Central Asia and Caucasus Studies*, 12 (45), 67-89.

Khodaverdi, H. (2022). Analysis of Iran-Armenia technological diplomacy in the field of cybersecurity. *Journal of Foreign Policy*, 36 (3), 155-178.

Zakerian, M., & Ahmadi, F. (2020). The role of regional organizations in cybersecurity: Case study of Shanghai Cooperation Organization. *Strategic Studies Quarterly*, 23 (88), 31-58.

Reports, Theses & Government Documents

Connell, M., & Venter, R. (2016). *Iran's cyber threat: Espionage, sabotage, and revenge*. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2016/02/Irans_Cyber_Threat_web_0223.pdf

European Union Agency for Cybersecurity (ENISA). (2022*). National cybersecurity strategy status report. Publications Office of the European Union*. https://doi.org/10.2824/63037

Giragosian, R. (2017). *Armenia's foreign policy: Balancing priorities in a turbulent neighborhood*. Friedrich-Ebert-Stiftung. https://library.fes.de/pdf-files/bueros/georgien/14072.pdf

International Telecommunication Union (ITU). (2021). *Global cybersecurity index 2020*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Kaspersky Lab. (2022). *APT trends report Q4 2021*. https://securelist.com/apt-trends-report-q4-2021/105475/

Minasyan, S. (2018). *Cybersecurity in Armenia: Challenges and perspectives*. Caucasus Institute. https://www.caucasusinstitute.org/wp-content/uploads/2018/05/Cybersecurity-ENG.pdf

Nye, J. S. (2010). *Cyber power. Belfer Center for Science and International Affairs*, Harvard Kennedy School. https://www.belfercenter.org/publication/cyber-power

Shanghai Cooperation Organization (SCO) Secretariat. (2019). *Report on cooperation in the field of information security among SCO member states* [Document No. SCO-SD/19]. http://eng.sectsco.org/documents/

United Nations Conference on Trade and Development (UNCTAD). (2020). *Digital economy report 2019: Value creation and capture—Implications for developing countries* [Sales No. E.20.II.D.3]. https://unctad.org/system/files/official-document/der2019_en.pdf

World Bank Group. (2022). *World development report 2021: Data for better lives*. https://doi.org/10.1596/978-1-4648-1600-0

CERT-AM. (2023). *Advanced persistent threats in Armenia: Technical analysis*. National Security Service Publication.

ENISA. (2023). *ENISA threat landscape 2023: Overview of activities*. Publications Office of the European Union.

Iranian Supreme Council of Cyberspace. (2022). *Directive No. 8/1401 on cross-border data flows*.

Kavkaz Cybersecurity Monitor. (2023). *Annual report on cyber operations in the South Caucasus*. Tbilisi State University Press.

Minasyan, S. (2023). *Post-war security architecture in the South Caucasus*. Institute for Caucasus Studies.

Organization of American States (OAS). (2022). *OAS cybersecurity program: Annual report 2022*.

African Union (AU). (2023). *Progress report on the implementation of the African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention) [Doc. Assembly/AU/10(XXXVI)].

United Nations Office on Drugs and Crime (UNODC). (2021). *Global study on cybercrime*.

Asia-Pacific Forum on Cybercrime (APF). (2023). *Report on regional cybercrime cooperation mechanisms*.

World Economic Forum (WEF). (2024). *advancing cyber resilience: Regional cooperation models*.
Customs Statistics of the Republic of Armenia. (2010). *Annual report 2010.* Statistical Committee of the Republic of Armenia.
Ministry of Information and Communications Technology of Iran. (2021). *Annual report on Iran-Armenia cyber cooperation*. https://ict.gov.ir
SCO Regional Anti-Terrorist Structure (RATS). (2020). *Protocol on joint cyber threat intelligence sharing.* http://ecrats.org/en/documents/
SCO Secretariat. (2019). *Framework for cooperation in combating cyber threats*. http://eng.sectsco.org/documents/
World Bank. (2022). *Digital connectivity in the South Caucasus*. World Bank Publications.
Ministry of Foreign Affairs of Iran. (2022). *Protocols of Iran-Armenia Joint Economic Commission (Annex 4)*.
Center for Strategic Research of Expediency Council. (2023). *National report on cybersecurity threats in West Asia* (Report No. 1402-07). https://csr.ir/fa/report/140207-cyber
Armenian National Security Service. (2021). *Annual cybersecurity assessment report*. https://nss.am/en/reports/2021-cyber
Ministry of Communications and Information Technology of Iran. (2022). *Iran-Armenia digital cooperation roadmap*. https://ict.gov.ir/fa/news/1401-digital-roadmap
Armenian e-Governance Infrastructure Agency. (2023). *Cross-border data exchange protocols with Iran*. https://e-gov.am/en/protocols/iran-2023
Supreme Council of Cyberspace of Iran. (2020). *National cybersecurity strategy document* (Approved Document No. 3/99). Tehran.
National Security Council of Armenia. (2019). *Cybersecurity doctrine of the Republic of Armenia* (Official Gazette No. 25-N). Yerevan.

استناد به این مقاله: هدایتی شهیدانی، مهدی و مهدی زاده، هادی . (۱۴۰۴). چالش‌ها و فرصت‌های امنیت سایبری در روابط دیپلماتیک و تجاری ایران و ارمنستان. *تعاملات دیپلماتیک*، ۳ (۹)، ۱ - ۳۲.
doi: 10.22034/dpiq.2025.536281.1045