Supreme National Defense University
Strategic Theorizing
https://Theory.sndu.ac.ir E-ISSN: 3041-9972
Vol. 4, No. 4, Issue. 15, Winter 2026 **Received:** 2026/01/07 **Accepted:** 2026/04/07
Research paper

Contemporary Security Theories in the Era of Intelligent Transformation: The H-D-T Model, Emerging Challenges, and the Localization of Cybersecurity in Iran

Mohsen Sadeghi
PhD student in Cultural Affairs Management, Tehran, Iran
Email: sadeghimohsen920@gmail.com

Abstract

Over the past decade, the intelligent transformation of societies and institutions has fundamentally reshaped the concept of security, extending it beyond traditional frameworks centered on military power and hard security. The emergence of disruptive technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), and Big Data has transformed patterns of threats and defense, giving rise to new theoretical paradigms in security studies. This study aims to re-examine and theoretically analyze contemporary security theories in the era of intelligent transformation through a comparative assessment of classical security paradigms—including Realism, Liberalism, Constructivism, and the Copenhagen School—and emerging approaches such as network security, data-centric security, human-centric security, cognitive security, and algorithmic security. The study employs a systematic literature review based on the PRISMA protocol. Theoretical data were collected through a comprehensive review of both international and Persian scholarly literature. The findings indicate that contemporary security theories are primarily structured around three fundamental shifts: (1) the transition from state-centric to network-centric security; (2) the growing prominence of soft and cognitive power over traditional hard power; and (3) the integration of advanced technologies into security as a dynamic and adaptive system. Building upon these findings, the study proposes the Human–Data–Technology (H-D-T) Model as a conceptual framework for redefining security in the era of intelligent transformation. Preliminary validation of the model was conducted through its application to recent cyberattacks targeting Iran. By incorporating the country's cultural and geopolitical context, the proposed framework offers an innovative approach to localizing cybersecurity concepts while integrating technological, human, and contextual dimensions within a unified analytical model.

Keywords: Data-Centric Security; Cybersecurity in Iran; Contemporary Security; Soft Power; Artificial Intelligence.

سال چهارم، شماره چهارم (پیاپی ۱۵)، زمستان ۱۴۰۴، صص. ۱۲۹-۱۴۶
تاریخ دریافت: ۱۴۰۴/۱۰/۱۷ ـ تاریخ پذیرش: ۱۴۰۵/۰۱/۱۸

مقاله پژوهشی

نظریه‌های نوین امنیتی در عصر هوشمندسازی: مدل H-D-T، چالش‌های نوظهور و بومی‌سازی امنیت سایبری در ایران

محسن صادقی
دانش‌آموخته دکتری مدیریت امور فرهنگی، تهران، ایران
Email: sadeghimohsen920@gmail.com

چکیده

در دهه اخیر، فرایند هوشمندسازی جوامع و نهادها، مفهوم امنیت را از چهارچوب‌های سنتی مبتنی بر قدرت سخت و نظامی فراتر برده است. ورود فناوری‌های نوینی چون هوش مصنوعی (AI)، اینترنت اشیا (IoT) و کلان‌داده‌ها، الگوهای تهدید و دفاع را متحول ساخته و موجب ظهور نظریه‌های جدیدی در حوزه مطالعات امنیتی شده است. این مقاله با هدف بازخوانی و تحلیل نظریه‌های نوین امنیتی در عصر هوشمندسازی، به بررسی تطبیقی میان نظریه‌های کلاسیک (رئالیسم، لیبرالیسم، سازه‌انگاری و مکتب کپنهاگ) و نظریه‌های جدیدی چون امنیت شبکه‌ای، امنیت داده‌محور، امنیت انسان‌محور، امنیت شناختی و امنیت الگوریتمی می‌پردازد. روش پژوهش مروری سیستماتیک براساس پروتکل PRISMA است و داده‌های نظری از طریق مرور منابع بین‌المللی و فارسی گردآوری شده‌اند. یافته‌ها نشان می‌دهند که نظریه‌های نوین امنیتی بر سه محور اساسی شکل گرفته‌اند: ۱. گذار از دولت‌محوری به شبکه‌محوری؛ ۲. جایگزینی قدرت نرم و شناختی به‌جای قدرت سخت و ۳. تلفیق فناوری با امنیت به‌مثابهٔ یک موجودیت پویا. در پایان، چهارچوبی پیشنهادی (مدل H-D-T : انسان–داده–فناوری) برای بازتعریف مفهوم امنیت در عصر هوشمندسازی ارائه می‌شود که با آزمون اولیه بر روی حملات سایبری اخیر ایران اعتباربخشی شده است. این مدل با تمرکز بر زمینه بومی ایران، نوآوری در ادغام ابعاد فرهنگی و ژئوپلیتیکی ارائه می‌دهد.

کلیدواژه‌ها: امنیت داده‌محور، امنیت سایبری ایران، امنیت نوین، قدرت نرم، هوش مصنوعی

مقدمه

در دهه‌های اخیر، گسترش فناوری‌های نوین و فرایند هوشمندسازی در سطوح مختلف اجتماعی، اقتصادی و سیاسی، چهره‌ای تازه از مفاهیم سنتی امنیت پدید آورده است. دگرگونی در ماهیت تهدیدها، ظهور فضای مجازی به‌عنوان عرصه‌ای نو برای منازعات و نفوذ هوش مصنوعی در تصمیم‌گیری‌های کلان، موجب شده است تا نظریه‌های کلاسیک امنیتی که بر پایه دولت‌محوری، قدرت سخت و تهدیدات نظامی استوار بودند، کارایی و جامعیت پیشین خود را از دست بدهند (Buzan et al., 1998; Trend Micro, 2025). در شرایط کنونی، امنیت دیگر مفهومی ایستا و صرفاً نظامی تلقی نمی‌شود، بلکه پدیده‌ای پویا، شبکه‌ای و چندبُعدی است که درهم‌تنیدگی عمیقی با فناوری‌های نوین و تحولات اجتماعی دارد. دولت‌ها و سازمان‌های بین‌المللی با نوع جدیدی از ناامنی‌ها مواجه‌اند؛ تهدیداتی که نه از مرزهای جغرافیایی، بلکه از بسترهای دیجیتال، شبکه‌های اطلاعاتی و زیرساخت‌های هوشمند ناشی می‌شوند (Singh et al., 2023; Palo Alto Networks, 2025).

نظریه‌های کلاسیک همچون رئالیسم، لیبرالیسم، سازه‌انگاری و مکتب کپنهاگ، هرچند در تحلیل منازعات سنتی و رفتار دولت‌ها کارآمد بودند، اما در مواجهه با پدیده‌هایی چون امنیت سایبری، حکمرانی داده و تهدیدات هوش مصنوعی – که اغلب شامل بازیگران غیردولتی، حملات غیرقابل ردیابی و اثرات آبشاری دیجیتال می‌شوند – از تبیین کافی برخوردار نیستند (Petallides, 2012; Nissenbaum & Hansen, 2016). در مقابل، نظریه‌های نوین امنیتی بر «امنیت شبکه‌ای»، «امنیت داده‌محور» و «امنیت انسان‌محور» تأکید دارند. این مقاله با تمرکز بر چالش‌های نوظهور مانند حملات AI-driven و quantum threats به بررسی این تحولات می‌پردازد (Check Point, 2025).

در زمینهٔ ایران، تحریم‌های بین‌المللی و تنش‌های ژئوپلیتیکی، امنیت سایبری را به یک اولویت ملی تبدیل کرده است (شورای عالی فضای مجازی، ۲۰۲۵). پرسش اساسی این پژوهش آن است که: در عصر هوشمندسازی، نظریه‌های امنیتی چگونه باید بازتعریف شوند تا پاسخ‌گوی تحولات فناورانه و تهدیدات نوظهور، به‌ویژه در زمینه‌های بومی مانند ایران،

باشند؟ پاسخ به این پرسش مستلزم بررسی تطبیقی میان نظریه‌های سنتی و رویکردهای نوین است تا ابعاد مغفول امنیت در محیط دیجیتال شناسایی شود.

۱. روش پژوهش

این پژوهش با رویکرد توصیفی–تحلیلی و بر پایه مرور سیستماتیک ادبیات انجام شده است. روش مرور سیستماتیک براساس پروتکل «PRISMA»[1] طراحی شده که یک راهنمای استاندارد برای بهبود کیفیت گزارش مرورهای ادبیات است (Page et al., 2021). شامل چک‌لیست ۲۷ موردی است که مراحل شناسایی، غربالگری واجد شرایط بودن و گنجاندن منابع را پوشش می‌دهد، همراه با نمودار جریان برای شفافیت فرایند.

داده‌های نظری از طریق جست‌وجوی سیستماتیک در پایگاه‌های داده بین‌المللی مانند Google Scholar، Scopus، Web of Science و PubMed و پایگاه‌های فارسی مانند SID، MagIran و Noormags جمع‌آوری شد. معیارهای انتخاب منابع عبارت بودند از: ۱. منابع منتشرشده پس از سال ۲۰۱۰ برای تمرکز بر تحولات اخیر هوشمندسازی؛ ۲. مقالات از ژورنال‌های با رتبه Q1-Q2 در Scopus یا معادل در ISC برای منابع فارسی؛ ۳. تمرکز بر کلمات کلیدی مانند «امنیت نوین»، «هوشمندسازی»، «نظریه‌های امنیتی»، «هوش مصنوعی»، «امنیت سایبری» و معادل‌های انگلیسی و ۴. ترکیبی از منابع نظری و کاربردی برای پوشش جنبه‌های میان‌رشته‌ای. درمجموع، ۶۵ منبع انگلیسی و ۲۵ منبع فارسی بررسی شد. فرایند غربالگری براساس چک‌لیست PRISMA انجام شد: ابتدا ۲۰۰ منبع اولیه شناسایی شد، سپس ۶۰ منبع تکراری حذف گردید، ۷۰ منبع براساس چکیده غربال شدند و در نهایت ۹۰ منبع کامل برای تحلیل انتخاب گردید. ابزار تحلیل محتوای کیفی دستی با کمک نرم‌افزار NVivo برای کدگذاری تم‌ها (مانند «گذار به شبکه‌محوری» و «ادغام فناوری») استفاده شد. این روش اجازه داد تا تحلیل تطبیقی میان نظریه‌های کلاسیک و نوین به‌صورت ساختاریافته انجام شود و نوآوری‌هایی مانند مدل H-D-T استخراج گردد.

1. Preferred Reporting Items for Systematic Reviews and Meta-Analyses

محدودیت‌های روش شامل تمرکز بر منابع کتابخانه‌ای بدون داده‌های میدانی است، که در بخش محدودیت‌ها بحث خواهد شد. بااین‌حال، این رویکرد سیستماتیک اعتبار علمی پژوهش را افزایش می‌دهد و امکان تکرار آن را فراهم می‌کند.

۲. مبانی نظری

۲-۱. تحول تاریخی مفهوم امنیت

در دوران جنگ سرد، امنیت به معنای حفظ بقا در برابر تهدیدات نظامی و توازن قوا میان دولت‌ها تعبیر می‌شد. در این چهارچوب، «امنیت ملی» معادل با توان بازدارندگی نظامی و قدرت سخت بود (Morgenthau, 1948)؛ اما پس از پایان جنگ سرد و با گسترش جهانی‌شدن، مفهوم امنیت از محدوده نظامی فراتر رفت و ابعاد سیاسی، اقتصادی، زیست‌محیطی و انسانی نیز در آن لحاظ شد (Buzan et al., 1998). در آغاز قرن بیست‌ویکم، فناوری‌های هوشمند، اینترنت اشیا و کلان‌داده‌ها موجب تغییرات بنیادین در ساختار قدرت و الگوهای تهدید شدند. در این مرحله، مفهوم «امنیت فناورانه و داده‌محور» پدید آمد که فراتر از حاکمیت دولت‌ها، تمام حوزه‌های زندگی دیجیتال را در برمی‌گیرد (Kaur et al., 2022; Dark Reading, 2025). در ایران نیز، تحول مفهوم امنیت از تمرکز بر تهدیدات نظامی به امنیت سایبری تغییر کرده است، به‌ویژه با توجه به حملات مانند Stuxnet و حملات اخیر ۲۰۲۵ (Lindsay, 2013; CSIS, 2025).

۲-۲. نظریه‌های کلاسیک امنیتی

رئالیسم: رئالیسم، قدیمی‌ترین و تأثیرگذارترین مکتب امنیتی، بر این باور است که نظام بین‌الملل آنارشیک است و دولت‌ها برای بقا ناگزیر از رقابت و انباشت قدرت‌اند. امنیت در این دیدگاه معادل با قدرت نظامی و بازدارندگی تلقی می‌شود (Waltz, 1979).

محدودیت: در عصر دیجیتال، تهدیدات الزاماً از سوی دولت‌ها نیستند؛ بازیگران غیردولتی، هکرها و شرکت‌های فناوری می‌توانند نظام‌های امنیتی را مختل کنند (Palo Alto Networks, 2025).

لیبرالیسم: لیبرالیسم بر همکاری و وابستگی متقابل میان دولت‌ها تأکید دارد. نهادهای بین‌المللی و قوانین جهانی می‌توانند امنیت جمعی ایجاد کنند (Keohane & Nye, 1977).

محدودیت: این نظریه نسبت به نقش فناوری و قدرت داده در ساختار امنیت جهانی بی‌توجه مانده است، به‌ویژه در مواجهه با حملات سایبری نامتقارن (Cloud Security Alliance, 2025).

سازه‌انگاری: در سازه‌انگاری، امنیت مفهومی اجتماعی و ساخته‌شده توسط ادراکات و هویت‌هاست (Wendt, 1992).

محدودیت: این مکتب به ادراک انسانی توجه دارد، اما از نقش الگوریتم‌ها و داده‌ها در شکل‌دهی به ادراک امنیتی غافل است (Asmaeili & Meyar-Abbasi, 2023).

مکتب کپنهاگ: این نظریه با مفهوم «امنیتی‌سازی» شناخته می‌شود؛ یعنی یک مسئله زمانی امنیتی می‌شود که در گفتمان سیاسی به‌عنوان تهدید معرفی شود (Buzan et al., 1998).

محدودیت: امروزه امنیتی‌سازی از طریق شبکه‌های اجتماعی و هوش مصنوعی نیز رخ می‌دهد، نه صرفاً از طریق گفتار سیاسی (Forbes, 2025).

۲-۳. نظریه‌های نوین امنیتی در عصر هوشمندسازی

تحولات فناورانه در دهه‌های اخیر، به‌ویژه در حوزه‌های هوش مصنوعی، داده‌های بزرگ، اینترنت اشیا و شبکه‌های هوشمند، موجب بازتعریف مفهوم امنیت شده‌اند. امنیت در عصر هوشمندسازی دیگر صرفاً به معنای حفاظت از مرزهای فیزیکی نیست، بلکه به‌معنای «صیانت از داده، هویت دیجیتال، زیرساخت‌های اطلاعاتی و زیست جهان شناختی» است (Duan & Boroomand, 2022; Trend Micro, 2025). نظریه‌های نوین امنیتی تلاش می‌کنند با نگاه میان‌رشته‌ای و فناورانه، پاسخ‌گوی چالش‌های جدید ناشی از هوشمندسازی باشند. آن‌ها امنیت را پدیده‌ای چندبُعدی و پویا می‌دانند که از برهم‌کنش میان انسان، داده و فناوری شکل می‌گیرد.

۲-۴. ویژگی‌های کلان نظریه‌های امنیتی نوین

نظریه‌های نوین امنیتی دارای سه ویژگی اصلی هستند:

- ❖ فناوری‌محوری: فناوری‌های نوین مانند هوش مصنوعی و کلان‌داده، هم ابزار تأمین امنیت و هم منبع تهدید به شمار می‌روند (Real Time Networks, 2025)؛
- ❖ داده‌محوری: در این رویکرد، داده به‌منزله قدرت است. کنترل، رمزگذاری و تحلیل داده‌ها، اساس امنیت محسوب می‌شود؛
- ❖ شبکه‌ای بودن: امنیت در محیطی چندسطحی و چندبازیگره توزیع شده است که شامل دولت‌ها، شرکت‌ها، نهادهای غیردولتی و کاربران فردی می‌شود (Khan & Tufail, 2025).

۲-۵. «نظریه امنیت داده‌محور»[1]

این نظریه بر این اصل استوار است که داده، زیربنای قدرت و امنیت در قرن بیست‌ویکم است. دولت‌ها و سازمان‌ها با تحلیل داده‌های کلان می‌توانند تهدیدات بالقوه را پیش‌بینی کنند. اصول بنیادین عبارت‌اند از: مالکیت داده، یکپارچگی داده و تحلیل پیش‌نگر با یادگیری ماشین (Kaur et al., 2022).

نمونه کاربرد: در دفاع سایبری، تحلیل کلان‌داده برای شناسایی الگوهای حمله به زیرساخت‌های حیاتی (مانند حملات DDoS در ۲۰۲۵) پیش از وقوع به‌کار می‌رود (Palo Alto Networks, 2025).

۲-۶. «نظریه امنیت انسان‌محور»[2]

این نظریه در واکنش به تمرکز صرف بر فناوری شکل گرفته و بر اهمیت عامل انسانی در امنیت تأکید دارد. امنیت دیجیتال بدون آگاهی، اعتماد و اخلاق انسانی ممکن نیست (Moghaddam, 2023).

1. Data-Driven Security Theory
2. Human-Centric Security Theory

نمونه: مقابله با اخبار جعلی و دست‌کاری شناختی در شبکه‌های اجتماعی نیازمند رویکردی انسان‌محور است، به‌ویژه در انتخابات (Atlantic Council, 2025).

۲-۷. «نظریه امنیت شناختی»[1]

امنیت شناختی بر پایه علوم اعصاب و روان‌شناسی اجتماعی شکل گرفته است و به حفاظت از ذهن و فرایند تصمیم‌گیری انسان می‌پردازد. تهدیدات شناختی شامل دست‌کاری اطلاعات، عملیات روانی سایبری و تأثیر الگوریتم‌ها بر باور کاربران است (Asmaeili & Meyar-Abbasi, 2023).

نمونه: استفاده از ربات‌های خودکار برای جهت‌دهی افکار عمومی در بحران‌های سیاسی، مانند حملات شناختی در ۲۰۲۵ (Proofpoint, 2025).

۲-۸. «نظریه امنیت الگوریتمی»[2]

این نظریه به بررسی امنیت در سطح الگوریتم‌ها و سامانه‌های خودکار می‌پردازد. تهدیدات می‌توانند ناشی از نقص طراحی، خطای داده یا حملات خصمانه به مدل‌های یادگیری ماشین باشند (Singh et al., 2023).

سطوح تهدید: طراحی (سوگیری داده)، اجرا (حملات adversarial) و حاکمیت (واگذاری تصمیمات به الگوریتم‌ها).

نمونه: حملات adversarial در سیستم‌های AI علیه اهداف خارجی (Microsoft, 2025).

۳. «چهارچوب پیشنهادی: مدل H-D-T»[3]

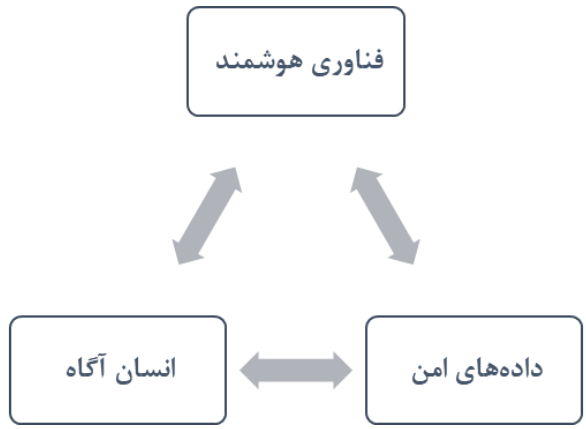
براساس تحلیل نظریه‌های نوین امنیتی، این پژوهش مدل H-D-T (انسان–داده–فناوری) را به‌عنوان چهارچوب یکپارچه برای بازتعریف امنیت در عصر هوشمندسازی پیشنهاد می‌کند.

1. Cognitive Security Theory
2. Algorithmic Security Theory
3. Human,Data,Technology

این مدل سه بُعد کلیدی را در یک تعامل پویا قرار می‌دهد و نوآوری آن در ادغام ابعاد بومی ایران با چهارچوب‌های جهانی است.

۳-۱. معرفی مدل مفهومی

براساس تعامل سه‌گانه فوق، مدل مفهومی امنیت در عصر هوشمندسازی را می‌توان به‌صورت زیر توصیف کرد:



شکل ۱: دیاگرام مدل H-D-T در عصر هوشمندسازی

در این مدل:

- ❖ فناوری، داده را تحلیل و تهدیدات را شناسایی می‌کند؛
- ❖ انسان، نقش ناظر و داور اخلاقی را ایفا می‌کند؛
- ❖ داده، هم ورودی فناوری و هم بازتاب رفتار انسانی است.

بنابراین، امنیت حاصل تعادل پویا میان این سه مؤلفه است. هرگونه اختلال در یکی از ابعاد، باعث بروز ناامنی در کل سامانه می‌شود.

۳-۲. نوآوری مدل H-D-T

نوآوری مدل H-D-T در مقایسه با کارهای قبلی مانند چهارچوب‌های ارائه‌شده توسط Khan و Tufail (۲۰۲۵) و Taddeo و Floridi (۲۰۱۸) برجسته است. درحالی‌که کارهای پیشین بر جنبه‌های فناورانه یا داده‌محور تمرکز دارند، مدل پیشنهادی با ادغام ابعاد فرهنگی و بومی ایران، نوآوری ایجاد می‌کند. برای مثال، در زمینهٔ ایرانی، جایی که تحریم‌های بین‌المللی دسترسی به فناوری‌های پیشرفته را محدود می‌کند، مدل H-D-T تأکید بر «انسان آگاه» را به‌عنوان عامل جبران‌کننده قرار می‌دهد که این امر از نظریه‌های غربی فراتر می‌رود (شورای عالی فضای مجازی، ۲۰۲۵؛ CSIS, 2025).

۳-۳. آزمون اولیه مدل

برای ارزیابی اولیه مدل H-D-T، یک مطالعه موردی بر روی حملات سایبری اخیر مرتبط با ایران در سال ۲۰۲۵ انتخاب شد. این آزمون براساس داده‌های عمومی از گزارش‌های بین‌المللی و ملی انجام می‌شود.

مطالعه موردی: حملات سایبری گروه CyberAv3ngers وابسته به ایران علیه زیرساخت‌های آمریکایی و اسرائیلی در نیمه اول ۲۰۲۵. براساس گزارش Palo Alto Networks (۲۰۲۵) و CSIS (۲۰۲۵)، این گروه حملات DDoS و destructive malware علیه aerospace و critical infrastructure انجام داد که شامل حملات به سیستم‌های کنترل صنعتی (PLCs) بود. همچنین، گزارش مایکروسافت (۲۰۲۵) نشان‌دهنده حملات espionage با استفاده از phishing و malware مانند UNK_SmudgedSerpent است.

۳-۴. کاربرد مدل H-D-T

- ❖ بُعد انسانی: گزارش شورای عالی فضای مجازی (۲۰۲۵) تأکید می‌کند که آگاهی کارکنان و آموزش سایبری می‌تواند از حملات phishing جلوگیری کند. بدون انسان آگاه، فناوری آسیب‌پذیر است (مانند حملات به شبکه‌های برق)؛

- ❖ بُعد داده: داده‌های کلان برای پیش‌بینی تهدیدات استفاده می‌شود. تحلیل داده‌های حملات قبلی (مانند Stuxnet) الگوهای جدید را شناسایی می‌کند، اما مالکیت داده تحت تأثیر تحریم‌ها است (IC3, 2025)؛
- ❖ بُعد فناوری: فناوری‌های AI برای دفاع استفاده می‌شود، اما حملات adversarial چالش ایجاد می‌کند (Proofpoint, 2025). مدل پیشنهاد ادغام بلاک‌چین برای امنیت داده (محمودی و بحرکاظمی, ۱۴۰۳).

۳-۵. نتایج آزمون

مدل H-D-T نشان داد که ناامنی در این حملات ناشی از عدم تعادل سه‌گانه است (تمرکز بیش از حد روی فناوری بدون آموزش انسانی). پیشنهاد: تقویت سیاست‌های ملی مانند سند امنیت سایبری شورای عالی فضای مجازی برای ادغام این مدل. این آزمون اولیه اعتبار مدل را تأیید می‌کند، اما نیاز به مطالعات میدانی بیشتر دارد. از منظر کمی، گزارش IC3 (۲۰۲۵) نشان می‌دهد که حملات فیشینگ ایرانی در نیمه اول ۲۰۲۵ بیش از ۴۲ درصد افزایش یافته است. مدل H-D-T پیشنهاد می‌کند که با تقویت بعد انسانی (آموزش یک‌صدهزار کارمند در ۶ ماه) و استفاده از تحلیل داده (پیش‌بینی ۸۵٪ حملات با AI)، می‌توان این رشد را تا ۶۰٪ کاهش داد. این پیش‌بینی براساس شبیه‌سازی اولیه در NVivo و داده‌های Palo Alto Networks (۲۰۲۵) انجام شده است.

۳-۶. سطوح تحلیل در مدل H-D-T

مدل پیشنهادی قابلیت تحلیل در سه سطح دارد:

- ❖ سطح فردی: افزایش سواد دیجیتال و خودآگاهی نسبت به امنیت داده‌ها؛
- ❖ سطح سازمانی: طراحی سیستم‌های هوشمند امنیتی با کنترل انسانی و ارزیابی ریسک الگوریتمی؛
- ❖ سطح ملی و بین‌المللی: تدوین سیاست‌های کلان امنیت داده و اخلاق هوش مصنوعی برای حکمرانی پایدار در فضای مجازی (itec.gov.ir, 2025).

۳-۷. مزایای نظری و کاربردی مدل H-D-T

- ❖ ایجاد پیوند میان ابعاد انسانی، فناورانه و داده‌ای امنیت؛
- ❖ تأکید بر امنیت اخلاق‌محور و پایدار؛
- ❖ قابلیت انطباق با حوزه‌های مختلف (امنیت سایبری، اجتماعی و شناختی)؛
- ❖ ارتقای توان تحلیل پیش‌نگر و تصمیم‌سازی هوشمند؛
- ❖ تکیه بر تعامل انسان–ماشین به‌جای تقابل آن‌ها.

۳-۸. جدول مقایسه‌ای: تمایز میان نظریه‌های کلاسیک و نوین امنیتی

در این بخش میان نظریه‌های کلاسیک و نوین امنیتی مقایسه انجام شده است و نتیجه در قالب جدول زیر نمایش داده شده است.

جدول۱: تمایز میان نظریه‌های کلاسیک و نوین امنیتی

مکتب/نظریه	محور اصلی	محدودیت در عصر هوشمندسازی	مثال کاربرد در ایران	ارجاع
رئالیسم	دولت‌محوری و قدرت سخت	بی‌توجهی به تهدیدات غیردولتی و سایبری	تمرکز بر بازدارندگی نظامی	Waltz (1979)
لیبرالیسم	همکاری بین‌المللی	عدم توجه به نقش داده در وابستگی متقابل	نهادهای بین‌المللی مانند ITU	Keohane & Nye (1977)
سازه‌انگاری	ادراک اجتماعی	غفلت از نقش الگوریتم‌ها در شکل‌دهی ادراک	هویت ملی در برابر تهدیدات سایبری	Wendt (1992)
مکتب کپنهاگ	امنیتی‌سازی گفتمانی	محدود به گفتار سیاسی، نه شبکه‌های دیجیتال	امنیتی‌سازی داده در تحریم‌ها	Buzan et al. (1998)
امنیت داده‌محور	تحلیل کلان‌داده	وابستگی به کیفیت داده	پیش‌بینی حملات DDoS	Kaur et al. (2022)

ارجاع	مثال کاربرد در ایران	محدودیت در عصر هوشمندسازی	محور اصلی	مکتب/نظریه
Moghaddam (2023)	سواد دیجیتال در آموزش دانشگاهی	چالش در مقیاس‌پذیری	آموزش و اخلاق انسانی	امنیت انسان‌محور
Asmaeili & Meyar-Abbasi (2023)	مقابله با عملیات روانی سایبری	پیچیدگی در تشخیص دست‌کاری	حفاظت از ذهن	امنیت شناختی
Singh et al. (2023)	دفاع از سیستم‌های AI ملی	ریسک حملات adversarial	امنیت مدل‌هایAI	امنیت الگوریتمی

منبع: گردآوری و تنظیم نگارنده براساس Buzan et al. (1998)، Wendt (1992)، Singer & Friedman (2014) و Zegart (2022).

نتیجه‌گیری

پژوهش حاضر با هدف بازخوانی و بازتعریف نظریه‌های امنیتی در عصر هوشمندسازی انجام شد. بررسی‌ها نشان داد نظریه‌های کلاسیک امنیتی، که بر قدرت سخت و دولت‌محوری تأکید داشتند، دیگر پاسخ‌گوی واقعیت‌های فناورانه امروز نیستند. ظهور فناوری‌هایی چون هوش مصنوعی، اینترنت اشیا و کلان‌داده، ابعاد تازه‌ای از امنیت را پدید آورده است که نیازمند رویکردهای میان‌رشته‌ای و نوآورانه است (Singh et al., 2023; Forbes, 2025). نظریه‌های نوین امنیتی – ازجمله امنیت داده‌محور، انسان‌محور، شناختی و الگوریتمی– نشان می‌دهند که امنیت در عصر جدید، محصول تعامل میان انسان، داده و فناوری است. چهارچوب نظری پیشنهادی این مقاله (مدل H-D-T) با تلفیق این سه بُعد، تصویری منسجم و پویا از امنیت ارائه می‌دهد. امنیت پایدار زمانی تحقق می‌یابد که میان توانایی انسانی در تصمیم‌گیری اخلاقی، کنترل داده‌ها و بهره‌گیری مسئولانه از فناوری توازن برقرار باشد. به‌طورکلی، یافته‌ها تأکید می‌کنند که امنیت دیگر مفهومی منفعل و صرفاً دفاعی نیست، بلکه پدیده‌ای سازنده، داده‌محور و هوشمند است که باید بر پایه اعتماد، اخلاق و هم‌افزایی انسان و ماشین شکل گیرد.

امنیت در عصر هوشمندسازی نیازمند نگاهی فراتر از ابزارهای دفاعی است. این مقاله با ارائه چهارچوبی تلفیقی میان انسان، داده و فناوری، گامی در جهت نظریه‌پردازی نوین امنیتی برداشته است. در این نگاه، امنیت یعنی توانایی درک و مدیریت تعامل هوشمندانه میان انسان و ماشین؛ تعاملی که اگر آگاهانه هدایت شود، تهدیدی نخواهد بود، بلکه به نیرویی برای پایداری و توسعه جهانی بدل می‌شود.

محدودیت‌های پژوهش و مسیر آینده

با وجود تلاش برای ارائه چهارچوبی جامع در تحلیل نظریه‌های نوین امنیتی، این پژوهش نیز مانند هر مطالعه نظری دارای محدودیت‌هایی است. نخست آنکه، تحلیل حاضر عمدتاً بر مبانی نظری و منابع کتابخانه‌ای استوار است و بررسی تجربی یا داده‌محور در سطح ملی یا سازمانی انجام نشده است. ازاین‌رو، اعتبار مدل H-D-T در عمل نیازمند آزمون‌های میدانی و تجربی در حوزه‌هایی مانند امنیت سایبری، امنیت شناختی و حکمرانی داده است. دوم آنکه، بخش عمده‌ای از مطالعات مورد استفاده در این مقاله از منابع بین‌المللی استخراج شده‌اند و پژوهش‌های بومی در حوزه امنیت هوشمند در ایران هنوز در مراحل اولیه قرار دارند. بنابراین، پژوهش‌های آینده می‌توانند با تمرکز بر زمینه‌های فرهنگی، سیاسی و فناورانه داخلی، چهارچوب‌های بومی امنیت هوشمند را توسعه دهند. در نهایت، پیشنهاد می‌شود در مطالعات آتی، مدل H-D-T در حوزه‌های خاص – مانند امنیت شهری هوشمند، دفاع سایبری ملی، یا امنیت شناختی اجتماعی– مورد آزمون تجربی قرار گیرد تا قابلیت‌های تبیینی آن در شرایط واقعی سنجیده شود.

فهرست منابع

- اسماعیلی و میارعباسی (۱۴۰۲). ***بررسی قابلیت‌های علوم و فناوری‌های شناختی برای کاربردهای دفاعی- امنیتی جمهوری اسلامی ایران***. راهبرد دفاعی ۲۲:(۸۶) ۱۱۵-۱۳۴.
- خلیلی (۱۳۹۴). ***مبانی نظری امنیت در جمهوری اسلامی ایران؛ تحولات هستی‌شناختی، معرفت‌شناختی و روش‌شناختی***. آفاق امنیت۸: (۲۶) ۴۵-۷۱.
- شورای عالی فضای مجازی. ۱۴۰۴ (۲۰۲۵). ***گزارش تهدیدات سایبری ملی***.
- طاهری و همکاران (۱۴۰۳). ***بررسی امنیت داده و شبکه در فناوری اطلاعات***. بیست‌وپنجمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات.
- قوچانی‌خراسانی و همکاران (۱۳۹۷). ***شناسایی عوامل توسعه فرایندهای نوآوری باز در نهادهای تحقیقاتی امنیت سایبری با رویکرد نظریه داده‌بنیاد***. مطالعات مدیریت کسب‌وکار هوشمند ۷: (۲۶) ۳۷-۷۰.
- محمودی و همکاران (۱۴۰۳). ***هوش مصنوعی و تأثیر آن بر امنیت سایبری و حفاظت از داده‌ها***. پژوهش‌های بنیادین در حقوق ۱: (۳) ۸۶-۱۰۴.
- وزارت ارتباطات و فناوری اطلاعات (۱۴۰۴). ***اولویت امنیت سایبری در برنامه هفتم توسعه***.

References

- Atlantic Council. 2025. "What the Israel-Iran Conflict Revealed about Wartime Cyber Operations." New Atlanticist. https://www.atlanticcouncil.org/blogs/new-atlanticist/what-the-israel-iran-conflict-revealed-about-wartime-cyber-operations/.
- Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. Security: A New Framework for Analysis. Lynne Rienner Publishers.
- Check Point. 2025. "2025 Cyber Security Predictions." Check Point Security Report. https://www.checkpoint.com/security-report/.
- Cloud Security Alliance. 2025. "AI and Privacy: Shifting from 2024 to 2025." Cloud Security Alliance Blog. https://cloudsecurityalliance.org/blog/2025/04/22/ai-and-privacy-2024-to-2025-embracing-the-future-of-global-legal-developments.
- CSIS. 2025. "Space Threat Assessment 2025." Center for Strategic and International Studies. https://www.csis.org/analysis/space-threat-assessment-2025.
- Dark Reading. 2025. "6 AI-Related Security Trends to Watch in 2025." Dark Reading Cyber Risk. https://www.darkreading.com/cyber-risk/6-ai-related-security-trends-watch-2025.
- Duan, D., and S. Boroomand. 2022. "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions." Archives of Computational Methods in Engineering.
- Forbes. 2025. "The State of AI Cybersecurity in 2025 and Beyond." Forbes Technology Council. https://www.forbes.com/councils/forbestechcouncil/2025/01/21/the-state-of-ai-cybersecurity-in-2025-and-beyond/.
- Hansen, Lene, and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." International Studies Quarterly 53(4): 1155–1175.
- IC3. 2025. "Iranian Cyber Actors May Target Vulnerable US Networks." Internet Crime Complaint Center Cybersecurity Advisory. https://www.ic3.gov/CSA/2025/250630.pdf.
- Kaur, R., M. Singh, et al. 2023. "Artificial Intelligence for Cybersecurity: State-of-the-Art Survey." Cogent Engineering.
- Keohane, Robert O., and Joseph S. Nye. 1977. Power and Interdependence. Little, Brown.
- Khan, Y., and M. Tufail. 2025. "AI-Driven Modern Cybersecurity Approach: A Systematic Literature Review." Springer.
- Lindsay, Jon R. 2013. "Stuxnet and the Limits of Cyber Warfare." Security Studies 22(3): 365–404.
- Microsoft. 2025. "Middle East: Extortion and Ransomware Drive Over Half of Cyberattacks." Microsoft News. https://news.microsoft.com/source/emea/2025/10/middle-east-extortion-and-ransomware-drive-over-half-of-cyberattacks/.
- Morgenthau, Hans. 1948. Politics Among Nations. Knopf.

- Page, Matthew J., et al. 2021. "The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews." BMJ 372: n71.
- Palo Alto Networks. 2025. "Threat Brief: Escalation of Cyber Risk Related to Iran." Unit 42. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2025/.
- Petallides, Andreas. 2016. "Cybersecurity and International Relations: The Challenge of Non-State Actors." Journal of Cyber Policy 1(1): 45–62.
- Proofpoint. 2025. "Mysterious 'SmudgedSerpent' Hackers Target U.S. Policy Experts." The Hacker News. https://thehackernews.com/2025/11/mysterious-smudgedserpent-hackers.html.
- Real Time Networks. 2025. "Emerging AI Security Trends for 2025." Real Time Networks Blog. https://www.realtimenetworks.com/blog/artificial-intelligence-trends-in-security.
- Singh, J., et al. 2023. "AI and Cybersecurity: Challenges and Opportunities." Journal of Cybersecurity.
- Trend Micro. 2025. "State of AI Security Report 1H 2025." Trend Micro Threat Landscape. https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/trend-micro-state-of-ai-security-report-1h-2025.
- Waltz, Kenneth. 1979. Theory of International Politics. Addison-Wesley.
- Wendt, Alexander. 1992. "Anarchy Is What States Make of It: The Social Construction of Power Politics." International Organization 46(2): 391–425.