Original Article

Bio-Cyber Threats and Crimes, the Challenges of the Fourth Industrial Revolution

Abbas Amiri[1], Mohsen Shekarchizadeh[2*], Ahmad Reza Shekarchizadeh Esfahani[3], Gholam Hossein Masoud[4]

1. Ph.D. Student, Department of Law, Najafabad Branch, Islamic Azad University, Najafabad, Iran.
2. Assistant Professor, Department of Law, Najafabad Branch, Islamic Azad University, Najafabad, Iran. (Corresponding Author) Email: Mohsen.Shekarchi@gmail.com
3. Assistant Professor, Department of Law, Najafabad Branch, Islamic Azad University, Najafabad, Iran.
4. Assistant Professor, Department of Law, Najafabad Branch, Islamic Azad University, Najafabad, Iran.

Received: 28 Jun 2021 Accepted: 19 Sep 2021

Abstract

Background and Aim: The distance between the dramatic changes in scientific findings in the world, known as the Industrial Revolution, is decreasing, and with a deeper solidarity in the cyber and biological sectors, the Fourth Industrial Revolution is at the peak of its evolution. The present study with a descriptive-analytical method, in search of understanding this increasing correlation and its consequences, tries to examine security threats in the bio-cyber sector, turning cyberspace into an undeniable platform in various fields of biological sciences and introduce this increasingly dependent situation as a serious challenge to science and technology at the peak of the Fourth Industrial Revolution.

Materials and Methods: This research is of theoretical type and the research method is descriptive-analytical. The method of data collection is library and has been done by referring to documents, books and articles.

Ethical Considerations: In order to organize this research, while respecting the authenticity of the texts, honesty and fidelity have been observed.

Findings: With the advent of computers in the field of information and the admirable advancement in the field of artificial intelligence, as much as information storage and processing has become easier, information theft and misuse of data has also been facilitated. Unauthorized intrusion or access by hackers for various purposes indicates the fact that the vulnerabilities and the possibility of its occurrence are very high and the title of winning and losing governments in the field of bio-cyber according to the ability to protect such data will become a reality in the not too distant future.

Conclusion: Bio-Cyber threats and crimes can play a crucial role in the vital substructures of any society. Bio-cybercrime is considered as a serious threat to the social order in this sector. Therefore, bio-cyber security is of great importance while maintaining security between new biological technologies such as artificial biology as well as DNA and cyberspace.

Keywords: Bio-Cyber Security; The Fourth Industrial Revolution; Bio-Cyber Threats; Artificial Biology; Artificial Intelligence

Please cite this article as: Amiri A, Shekarchizadeh M, Shekarchizadeh Esfahani AR, Masoud GH-H. Bio-Cyber Threats and Crimes, the Challenges of the Fourth Industrial Revolution. *Bioethics Journal*, Special Issue on Ethical & Legal Reflections 2021; 81-97.

مقاله پژوهشی

تهدیدات و جرائم بیوسایبری، چالش‌های انقلاب صنعتی چهارم

عباس امیری[۱]، محسن شکرچی‌زاده*[۲]، احمدرضا شکرچی‌زاده اصفهانی[۳]، غلامحسین مسعود[۴]

۱. دانشجوی دکتری رشته حقوق، گروه حقوق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران.

۲. استادیار، گروه حقوق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران. (نویسنده مسؤول) Email: Mohsen.Shekarchi@gmail.com

۳. استادیار، گروه حقوق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران.

۴. استادیار، گروه حقوق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران.

دریافت: ۱۴۰۰/۴/۷ پذیرش: ۱۴۰۰/۶/۲۸

چکیده

زمینه و هدف: فاصله دگرگونی و تحولات شگرف یافته‌های علمی در جهان، با عنوان انقلاب صنعتی رو به کاهش است و با همبستگی عمیق‌تر در بخش‌های سایبری و بیولوژیکی، انقلاب صنعتی چهارم نیز در اوج تحولات خود قرار گرفته است. پژوهش حاضر با روش توصیفی ـ تحلیلی به دنبال درک این همبستگی رو به افزایش و پیامدهای آن، تلاش می‌کند تا با بررسی تهدیدها علیه امنیت در بخش بیوسایبری، تبدیل فضای سایبر به عنوان بستری غیر قابل انکار در بخش‌های مختلف علوم بیولوژیکی، این وضعیت در حال وابستگی روزافزون را به عنوان یک چالش جدی در مسیر علم و فناوری در اوج قله انقلاب صنعتی چهارم معرفی کند.

مواد و روش‌ها: این تحقیق از نوع نظری است؛ روش تحقیق به صورت توصیفی ـ تحلیلی می‌باشد و روش جمع‌آوری اطلاعات نیز به شیوه کتابخانه‌ای و با مراجعه به اسناد، کتب و مقالات، صورت گرفته است.

ملاحظات اخلاقی: در انجام پژوهش حاضر، ضمن رعایت اصالت متون، اصول صداقت و امانتداری رعایت شده است.

یافته‌ها: با واردشدن رایانه در عرصه اطلاعات و پیشرفت قابل تحسین در بخش هوش مصنوعی، به همان اندازه که نگهداری و پردازش اطلاعات آسان شده، سرقت اطلاعات و سوءاستفاده از آن نیز تسهیل شده است. نفوذ یا دسترسی غیر مجاز توسط هکرها که با اهداف گوناگونی صورت می‌پذیرد، حاکی از این واقعیت است که آسیب‌پذیری‌ها و قابلیت بروز آن بسیار زیاد بوده و عنوان کشورهای برنده و بازنده در بُعد علوم بیوسایبری با توجه به میزان توانایی در حفاظت از چنین داده‌هایی در آینده‌ای نه‌چندان دور به واقعیت بدل خواهد شد.

نتیجه‌گیری: تهدیدات و جرائم بیوسایبری می‌تواند نقش بسیار تعیین‌کننده‌ای در زیرساخت‌های حیاتی هر جامعه داشته باشد. جرائم بیوسایبری به مثابه تهدیدهایی جدی در تقابل با نظم اجتماع و یا بالفعل در این بخش، تلقی می‌شوند. لذا امنیت بیوسایبری با حفظ امنیت بین فناوری‌های جدید بیولوژیکی مانند زیست‌شناسی مصنوعی و نیز DNA و فضای سایبری، از اهمیت بالایی برخوردار است.

واژگان کلیدی: امنیت بیوسایبری؛ انقلاب صنعتی چهارم؛ تهدیدات بیوسایبری؛ زیست‌شناسی مصنوعی؛ هوش مصنوعی

۱. مقدمه

با شکستن مرز بین دنیای واقعی و مجازی در اوج انقلاب صنعتی چهارم، تعامل و وابستگی انجام تحقیقات با رایانه و وابستگی روزافزون آن به فضای سایبری و تأثیر فناوری‌های نوظهور و نیازهای جدید در حوزه بیولوژیک و بهره‌وری بیشتر از نیروی کار و ارتقای عملکردها با در اختیارگرفتن جدیدترین فناوری‌های خودکار در فضای مجازی، فعالیت‌های در حال انجام در بخش مربوط به بیوسایبر را وارد مرحله جدیدی از نوآوری و پیشرفت کرده است.

با توجه به این موضوع و اینکه علوم مبتنی بر فضای سایبر و نیز علوم بیولوژیکی به سرعت در حال همبستگی و همگرایی بوده و همچنین دستاوردها و مزایای فراوانی نیز داشته و خواهد داشت، اما علیرغم کاربردهای جدید و سودمندی که دارند، خطرات و تهدیداتی را بر حیات گونه‌های حیوانی و نباتی تحمیل کرده و میزان ارتکاب رفتارهای پرخطر و مجرمانه را نیز افزایش می‌دهند، لذا در این رابطه، فرض بر این است که فضای سایبر در ارتباط با علوم بیولوژیکی در موارد متعدد و متفاوتی می‌تواند بسترساز شرایط تهدید و ارتکاب جرم باشد. به علاوه، فضای سایبر را می‌توان به عنوان یک زمینه مناسب برای ایجاد رفتارهای پرخطر در حوزه علوم زیستی به شمار آورد. این مقاله تلاش دارد تا با تبیین موقعیت علمی که جهان امروز به عنوان انقلاب صنعتی چهارم در آن قرار دارد، به سیاستگذاران و همچنین متولیان بخش سلامت، پیامدهای وابستگی روزافزون زیست‌شناسی و فضای سایبر که در بسیاری موارد به رفتارهای تهدیدآمیز، آسیب‌زا و مجرمانه علیه حوزه سلامت منجر شده است، را با رویکردی تحلیلی ارائه دهد. پژوهش حاضر به دنبال پاسخ به این پرسش است که چگونه فضای سایبر می‌تواند بستری برای ایجاد تهدید و ارتکاب جرائم بیولوژیکی محسوب شود؟

در راستای پاسخ به این پرسش، با اشاره به تحولات علمی شگرف در انقلاب صنعتی چهارم، تهدیدات و جرائم بیوسایبری که قابلیت پیامدهای آسیب‌زا را به ویژه در بخش زیست‌شناسی مصنوعی و یا هک‌کردن DNA دارند، مورد بررسی قرار خواهیم داد و به این مسأله می‌پردازیم که چگونه تهدیدات و جرائم بیوسایبری می‌توانند قدرت نقش‌آفرینی بالایی در جهت اهداف نامشروع داشته باشند و نیز می‌توانند بسیاری از حوزه‌های دیگر را تحت تأثیر قرار دهند، زیرا از یکسو خدمات متقابل سایبری و زیست‌محیطی، بسیار امیدوارکننده و الهام‌بخشِ پدیدآمدن و شکوفایی قابل تحسین را در روزهای پیش رو نوید می‌دهد؛ از سوی دیگر، اهداف بسیار مادی‌گرایانه و خودخواهانه برخی دولت‌ها، سازمان‌ها و نهادهای علمی وابسته، در بخش‌های زیادی موفقیت‌های علمی قابل ستایش را از مسیر حقیقی، اخلاقی و راستین خود منحرف نموده و به تهدیدی علیه بشریت تبدیل کرده است. این امر، باعث کم‌رنگ‌ترشدن فضای اعتماد عمومی در سطح داخلی و بین‌المللی می‌شود. این افزایش بی‌اعتمادی نسبت به فضای سایبر، به عنوان یک رکن اصلی این تحول علمی، بر درک اهمیت انقلاب صنعتی چهارم می‌افزاید.

در خصوص پیشینه این تحقیق برخی آثار، شایان ذکر است؛ مقاله «تهدیدات سایبری و تأثیر آن بر امنیت ملی» نوشته علی خلیلی پوررکن آبادی و یاسر نورعلی‌وند که در سال ۱۳۹۱ به انتشار رسیده، در پی پاسخگویی به این پرسش است که تهدیدهای سایبری چگونه بر امنیت ملی تأثیر می‌گذارند و این اثرگذاری در چه ابعادی خود را نمایان می‌سازد. در پاسخ چنین مطرح شده است که این تهدید به علت برخورداری از ویژگی‌هایی چون قیمت پایین ورود، گمنامی و تأثیرگذاری شگرف، پدیده‌ای به نام انتشار قدرت را به وجود آورده است که نه‌تنها باعث شده دولت‌های کوچک از ظرفیت بیشتری برای اعمال قدرت در این فضا برخوردار شوند، بلکه منجر به ورود بازیگران جدیدی همچون شرکت‌ها، گروه‌های سازمان یافته و افراد به معادلات قدرت جهانی شده است. بنابراین این پدیده امنیت ملی را از ابعاد مفهوم امنیت، دولت‌محوری در امنیت، بعد جغرافیایی تهدید، گستردگی آسیب‌پذیری‌ها، شیوه مقابله با تهدیدها و تعدد بازیگران در این عرصه، تحت تأثیر قرار داده است (۱).

در مقاله «تأثیر تهدیدات امنیتی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن» نوشته سیدمحمدرضا موسوی و همکاران که در سال ۱۳۹۲ به

چاپ رسیده است، نویسندگان بیان می‌دارند: امروزه گسترش فضای سایبر باعث پیدایش مرزهای مجازی شده و از این جهت درک واقع‌بینانه از تهدیدات امنیتی در گرو توجه به عوامل نرم‌افزاری است که در واقع حلقه واسط بین محیط امنیتی کشورها و سخت‌افزارها قرار دارند و بدین جهت برداشت‌ها از مفهوم امنیت ملی در این فضا به چالش کشیده شده است. یکی از محورهای اصلی تهدید امنیتی در عصر ارتباطات و جهانی‌شدن برای کشورها را باید در حوزه سایبری برشمرد که نمونه برجسته آن حمله رایانه‌ای به تأسیسات هسته‌ای و الکترونیکی ایران توسط آمریکا می‌باشد. مقاله مزبور درصدد بررسی تأثیر تروریسم سایبری بر امنیت ملی کشورمان می‌باشد. از نظر نگارندگان، جهانی‌شدن ـ که یکی از ابزارهای آن، فناوری‌های سایبری می‌باشد ـ هم یک فرصت و هم یک تهدید به شمار می‌رود. تروریسم سایبری با هدف نابودسازی ساختارهای اساسی یک کشور از جمله این تهدیدات (علیه امنیت ملی) می‌باشد. این جرم از جمله مهم‌ترین جرائم فراملی در فضای مجازی می‌باشد. نوع پیشگیری، مقابله و مبارزه با این جرم، با نوع اقدامات کنترلی در سایر جرائم به کلی متفاوت می‌باشد. در جرم تروریسم سایبری، جرم فاقد محل وقوع می‌باشد. این جرم عموماً فرامرزی و تهدیدی مستقیم علیه منافع و امنیت ملی کشور است. در این زمینه لازم است تدابیر تقنینی، قضایی و اجرایی ویژه‌ای در سطح ملی و بین‌المللی در نظر گرفته شود (۲).

همانطور که در نمونه‌های فوق قابل مشاهده است، اغلب پژوهش‌های انجام‌شده، در ارتباط با تهدیدات سایبری طراحی شده‌اند، حال آنکه در پژوهش حاضر تهدیدات و جرائم بیوسایبری در چارچوب چالش‌های انقلاب صنعتی چهارم، مورد بحث و بررسی قرار گرفته است.

از حیث تشحیذ ضرورت تحقیق نیز گفتنی است آگاهی از آسیب‌های زیست‌محیطی که جوامع پیشرفته از نظر فناوری بر اکوسیستم‌های طبیعی وارد می‌کنند، به عنوان یکی از دلایل از بین‌رفتن تدریجی اعتماد به شمار می‌رود. در نیمه دوم قرن بیستم، برخی از بینش‌های علمی و نوآوری‌های فناورانه به ویژه در شکل‌گیری مفهوم یک عصر جدید تاریخی نقش داشته‌اند. فناوری هسته‌ای (بمب و نیروگاه)، سفر به ماه و مریخ، تلویزیون، شبکه‌های ارتباطات جهانی، کشف DNA، لقاح آزمایشگاهی، شبیه‌سازی حیوانات، پروژه ژنوم انسانی، فناوری دیجیتال از رایانه شخصی به تارنمای جهانی گسترده و فجایع زیست‌محیطی مانند حوادث سوسو، بوپال و فاجعه چرنوبیل همگی در اهمیت انقلاب صنعتی اخیر ایفای نقش داشته‌اند (۳).

اکنون که بسیاری از کشورها در مواجه با تغییرات فنی و فناوری، در چارچوب چهارمین انقلاب صنعتی در حال انعطاف به سمت دگرگونی‌های علمی هستند، کشورهایی به عنوان کشورهای برنده خواهند بود که بتوانند تعامل بیشتر و مناسب‌تری داشته باشند و کشورهایی بازنده هستند که نتوانند با داشتن و یا احیای زیرساخت‌های مناسب، خود را در شرایط رقابت قرار دهند (۴)، لذا این موضوع به عنوان یک نگرانی و چالش جدی برای جوامع در عصر جدید دارای اهمیتی مضاعف است و با نظرداشتِ سطح نگرانی که در جامعه نسبت به این موضوع با توجه به اتفاقات اخیر از جمله بیماری ناشی از شیوع کووید ۱۹ وجود دارد و در حال افزایش نیز هست، لزوم پرداختن به آن را دوچندان می‌کند.

۲. ملاحظات اخلاقی

در تمامی مراحل تدوین پژوهش حاضر، با در نظر گرفتن اصول حاکم بر اخلاق در پژوهش، ضمن رعایت اصالت متون، صداقت و امانتداری رعایت شده است.

۳. مواد و روش‌ها

این تحقیق از حیث نوع، نظری است و از حیث روش به صورت توصیفی ـ تحلیلی انجام شده است. همچنین، روش جمع‌آوری اطلاعات به شیوه کتابخانه‌ای (اسنادی) است که با مراجعه به اسناد، کتب و مقالات صورت گرفته است.

۴. یافته‌ها

یافته‌های پژوهش حاکی از آن است که با در نظرگرفتن پیشرفت‌های علمی اخیر و تلاقی عمیق ساحت‌های مختلف

فناوری، زیست‌شناسی و حوزه سایبر، لازم است دولت‌ها امنیت سایبری را در اولویت سیاستگذاری داخلی و بین‌المللی قرار دهند. علاوه بر این باید دقت داشت که اصول و هنجارهای اخلاقی و حقوقی تحت تأثیر پیشرفت‌های مزبور قرار گرفته است و نیاز مبرمی برای جرح و تعدیل آن‌ها وجود دارد. باید دقت داشت که پیشرفت‌های علمی نباید بدون حد و مرز و بدون در نظرگرفتن اصول اخلاقی صورت پذیرند.

جرائم زیستی که در فضای سایبری رخ می‌دهند در حال حاضر تبدیل به یکی از مؤلفه‌های اصلی امنیت ملی شده‌اند. نباید از نظر دور داشت که با پیشرفت علم و تکنولوژی، جنبه‌های مختلف مفهوم امنیت با یکدیگر پیوندی وثیق پیدا کرده‌اند. برای مثال گسترش مخاصمات مسلحانه عملاً از یکسو موجب گسترش فروش سلاح و از سوی دیگر موجب گسترش بیماری‌ها و به مخاطره‌افتادن امنیت غذایی و سلامتی می‌شود.

۵. بحث

۵-۱. انقلاب صنعتی: انقلاب صنعتی شامل مجموعه‌ای گسترده و عظیم از تغییرات است و از زمانی آغاز می‌شود که نوآوری‌های بنیادی در فناوری‌ها و اشکال سازمانی به طور گسترده در بخش‌های اصلی تولید ایجاد می‌شوند و در مرحله انقلابی، وقتی این نوآوری‌ها به طور گسترده‌ای انجام می‌شود، پایان می‌یابد (۵). درک وضعیت علمی و صنعتی جهان از این زاویه، می‌تواند به ما کمک کند تا بتوانیم موقعیت خود را از لحاظ زیرساختی، علمی و نحوه تعامل با آن‌ها بیابیم.

۵-۱-۱. پیشینه تاریخی: انقلاب‌های صنعتی همیشه جهان را تحت تأثیر قرار داده و به شکلی بزرگ تغییر داده‌اند. از نظر تاریخی، ظهور فناوری به بهبود بهره‌وری کمک کرده و انسان را به سمت دستیابی به بازده کار با ارزش افزوده بالاتر سوق داده است. در اولین انقلاب صنعتی، دستگاه‌های بافندگی جایگزین کارهایی در تولید منسوجات شدند که با دست انجام می‌گرفت. در طول این انقلاب، زنان بودند که قهرمانان گمنام درآن دوران بودند، زیرا انگشتان زیرک و مهارت آن‌ها در استفاده از ماشین‌آلات بافندگی، باعث شد تا تعداد زیادی از آنان در کارخانه‌های تولیدکننده منسوجات استخدام شوند. با پیشرفت اولین انقلاب صنعتی، استفاده از قدرت جسمی حیوانات و همچنین نیروی انسانی زیادی که برای انجام امور صرف می‌شد، به تدریج با ماشین‌آلات مکانیکی که با انواع انرژی‌های تولیدشده توسط انسان به کار می‌رفتند، جایگزین شدند. در نیمه دوم از اولین انقلاب صنعتی، موتورهای بخار، انرژی خروجی لازم برای کار با ماشین‌های مکانیکی که قبلاً محدود به استفاده از قدرت و توان جسمی حیوانات اهلی بود را ایجاد کردند. این اتفاق به میزان زیادی اثربخشی کار را افزایش داده و در آن زمان، روند جهانی‌سازی را آغاز کرد که باعث شد جهان از طریق مسیر دریایی کوچک‌تر شود. در دهه ۱۹۶۰ و ۱۹۷۰، با ظهور ساخت ترانزیستورهای الکترونیکی، لوازم خانگی الکترونیکی و اولین رایانه و پردازنده مرکزی و سپس رایانه‌های شخصی، جهان، دومین انقلاب صنعتی را تجربه کرد (۶).

سومین انقلاب صنعتی در دهه ۱۹۶۰ شروع شد که معمولاً به آن انقلاب کامپیوتری یا دیجیتالی گفته می‌شود، زیرا به وسیله اجسام نیمه‌هادی، محاسبات (شمارش) پردازده‌های مرکزی (۱۹۶۰ م.) محاسبات شخصی (۸۰-۱۹۷۰) و اینترنت (۱۹۹۰ م.) تسریع شد (۷).

ارتباطات و تعاملات متقابل در این دوره به سرعت انجام شد. سطوح نمایش پیام، ایمیل، اتاق گفتگو و سیستم تابلوی اعلانات برای ارتباط جهانی مردم با یکدیگر به وجود آمد. سومین انقلاب صنعتی، ایجاد یک پایگاه دانش جمعی با اطلاعاتی را که می‌تواند با یکدیگر در سراسر جهان به اشتراک گذاشته شود، ممکن ساخت. این پایگاه دانش جمعی جهانی به اینترنت معروف شد (۶).

۵-۱-۲. انقلاب صنعتی چهارم: بحث «صنعت چهارم» در اوایل سال ۲۰۰۰ از صنعت تولید آلمان ظهور کرد. بسیاری از تغییراتی که رخ داده‌اند، اکنون قابل مشاهده بوده و اکنون اتفاق می‌افتند، زیرا انسان سرانجام ظرفیت محاسباتی را برای ذخیره مقادیر زیادی داده توسعه داده است که به نوبه خود می‌تواند یادگیری ماشین را امکان‌پذیر کند. نتیجه این امر توسعه آنچه سیستم‌های سایبری ـ فیزیکی (CPS) نامیده می‌شوند، است. سیستم‌های سایبری ـ فیزیکی، سیستم‌های

فیزیکی و مهندسی هستند که عملیات و عملکرد آن‌ها توسط مرکز یا هسته محاسبات و نظارت بر ارتباطات، هماهنگ، کنترل و یکپارچه می‌شود. همانطور که اینترنت نحوه تعامل انسان‌ها با یکدیگر را دگرگون کرد، سیستم‌های فیزیکی سایبری نحوه تعامل ما با دنیای فیزیکی اطراف را نیز دگرگون می‌کند. بسیاری از چالش‌های بزرگ در حوزه‌های حیاتی اقتصادی مربوط به حمل و نقل، بهداشت، تولید، کشاورزی، انرژی، دفاع، هوا فضا و ساختمان‌ها در انتظار است. طراحی، ساخت و تأیید سیستم‌های فیزیکی سایبری، بسیاری از چالش‌های فنی را ایجاد می‌کند که باید توسط یک جامعه بین رشته‌ای از محققان و مربیان حل شود (۸).

سرانجام، در قرن بیست و یکم، جهان به اوج انقلاب صنعتی چهارم رسید، جهانی که شامل ظهور هوش مصنوعی (AI)، ربات‌ها، وسایل نقلیه خودمختار، ماشین‌های کنترل‌شده توسط الگوریتم، سیستم‌های تسلیحاتی خودمختار، نرم‌افزار/ برنامه‌های رفتار پیش‌بینی‌کننده مبتنی بر الگوریتم و آغاز تحول در رسانه‌های اجتماعی و شبکه‌های اجتماعی می‌شود (۶).

در شبکه‌های اجتماعی در حال تحول، اخبار جعلی، حسادت و احساساتی‌بودن افراد نسبت به پست‌های یکدیگر و پست‌های نژادپرستانه یا علیه زنان به صورت فراوان دیده می‌شود. اکنون با دوستی‌های آنلاین، تفاهم بیشتر بین فرهنگی یا بین دینی در بین جوامع و دنیای کوچک‌تر و به هم وابسته‌تر، هم‌زیستی می‌کنند. در دنیاهای دیگر، رسانه‌های اجتماعی دیجیتال یک شمشیر دولبه است که می‌تواند به نفع جوامع باشد و یا شکاف‌های بیشتری را در ساختار اجتماعی آن‌ها وارد کند. اکنون اخبار جعلی در رسانه‌های بین‌المللی مورد توجه قرار گرفته است. اخبار جعلی برای تأثیرگذاری بر دولت‌ها و انتخابات عنوان شده است، این امر با این واقعیت امکان‌پذیر شده است که اکنون تعداد زیادی از مردم اخبار خود را از شبکه‌های اجتماعی دریافت می‌کنند (۶). این شرایط می‌تواند منجر به مهندسی اجتماعی شود که می‌تواند با اهداف نامشروعی صورت گیرد. همچنین فعالیت‌های بسیار زیاد و افزایشی در فضای اینترنت باعث جهانی‌ترشدن سیتیزن سایبری می‌شود.

با نگاهی به آینده اما، برخی اندیشمندان حوزه علم و محیط زیست، عصر پساصنعتی تمدن غربی را نوید داده‌اند، مانند Venter در کتاب زندگی با سرعت نور که به این مسأله اشاره می‌کند که در دهه‌های آینده سهم عمده‌ای که علم می‌تواند به انسان ببخشد، ازدواج زیست‌شناسی با فناوری‌های دیجیتال است. ما با ظهور و رشد قوی طراحی مبتنی بر زیست‌شناسی وارد عصر پساصنعتی تمدن غربی خواهیم شد: با داشتن پایگاه عظیم داده‌های رایانه‌ای و مقادیر بسیار زیاد DNA، اطلاعات دیجیتالی باید ما را قادر به بازآفرینی مواد، سلول‌های زنده و موجودات زنده کند (۹). با این وجود، همانطور که انقلاب‌های صنعتی متوالی اتفاق افتاده‌اند، انقلاب صنعتی دیگری نیز وجود خواهد داشت. روشن است که انقلاب صنعتی چهارم در زمان حال است، اما قرار نیست به اندازه انقلاب‌های صنعتی دیگر دوام بیاورد.

۵-۲. فضای سایبر و جرائم سایبری: محیط سایبر محیطی حقیقی و واقعی است و نه مجازی و یا غیر واقعی. جهان سایبر، هرچند به شکل مادی و ملموس احساس شدنی نیست، اما همچنانکه به اطلاعات ناشی از امری نمی‌توان عنوان مجازی داد به فضای سایبر هم نمی‌توان فضای مجازی گفت.

از محیط سایبر به محیط فناوری و اطلاعات (IT) یا محیط اطلاعات و ارتباطات نیز یاد شده است. از این رو مشاهده می‌شود که برای نمونه به جرم‌های محیط سایبر، جرم‌های علیه فناوری و اطلاعات نیز اطلاق می‌شود (۱۰). فضای سایبری، همه شبکه‌های رایانه‌ای موجود در دنیا و هر چیزی است که به این شبکه‌ها متصل است یا آن‌ها را کنترل می‌کند. فضای سایبر فقط اینترنت نیست. فضای سایبر را نباید با اینترنت یکی دانست، چراکه فضای سایبر شامل ارتباطات صورت‌گرفته مبتنی بر سیستم‌های مخابراتی نیز می‌شود. اینترنت شبکه ارتباط عمومی در مقیاس جهانی است که امکان ارتباط هر فرد را از طریق شبکه‌های محلی یا ارائه کنندگان خدمات اینترنتی فراهم می‌کند (۱۱).

در مورد اصطلاحات جرائم رایانه‌ای و جرائم سایبری، این نکته مورد توجه است که در غالب موارد، شباهت کاربردی و ترجمه‌ای، منتج به این ابهام شده است که این دو به صورت یکسان دیده شوند. با این حال، از اصطلاح جرائم سایبری، می‌توان به صورت عام استفاده کرد. جرائم رایانه‌ای عمدتاً به مجموعه جرائمی محدود مانند جرائمی چون سرقت خدمات رایانه‌ای و دسترسی غیر مجاز به رایانه‌های محافظت شده اشاره دارد. برای تطبیق‌دادن با این شرایط ابهامی، معنای عمومی‌تر مربوط به رایانه، برای هر جرمی که شامل رایانه‌ها و شبکه‌های اینترنتی باشد، به کار می‌رود؛ از جمله جرائمی که وابستگی زیادی به رایانه ندارند. از آنجا که هر جرمی می‌تواند شامل رایانه‌ها نیز باشد، مشخص نیست که کجا مرز بین جرائم ارتکابی با استفاده از رایانه و جرائمی که صرفاً مربوط به رایانه است، تعیین شود. اگرچه در مورد تعریف جرم رایانه‌ای توافق نشده است، اما با گذشت زمان معنای این اصطلاح مشخصتر می‌شود (۱۲).

نکته قابل اهمیت در مورد ارتباط انقلاب صنعتی چهارم و امنیت یا تهدیدات سایبری و بیوسایبری این است که به طور اساسی بسیاری از تحقیقات، توسعه‌ها و فناوری‌های اخیر، از ویژگی‌های اینترنت و فضای سایبر استفاده کرده و گسترش یافته‌اند. دستیابی به اطلاعات برخط، ایجاد انواع اینترانت‌ها و دیتاسنترهای اختصاصی و ایجاد امنیت و حفاظت از اطلاعات با طراحی جدیدترین ابداعات سیستمی و رایانه‌ای و دستگاه‌های هوشمندی که با دقت و ظرافت، توانمندی لازم برای اهداف برنامه‌ریزی‌شده را مهیا می‌کنند. در این خصوص، سئوالی که همواره مطرح است این است که اگر نفوذ غیر مجاز (هک) رخ دهد و انحراف یا دستکاری صورت گیرد، با وجود غیر قابل برگشت‌بودن تحولات شیمیایی و بیولوژیکی در زیست‌محیط، آیا می‌توان یک امنیت کامل و صددرصدی برای حفاظت از داده‌ها در این موارد ایجاد کرد؟

۵-۳. زیست‌شناسی مصنوعی: از موضوعات بسیار بااهمیت و زمینه‌ای در آغاز انقلاب صنعتی چهارم می‌توان به زیست‌شناسی مصنوعی اشاره کرد که به سرعت در حال رشد، توسعه و تحول است. علیرغم عدم توافق در مورد تعریف یکسانی از زیست‌شناسی مصنوعی، یک جنبه متمایز از این رشته نیز به نام کاربرد اصول مهندسی در زیست‌شناسی ظهور کرده است.

چهارمین انقلاب صنعتی، فقط در مورد سیستم‌ها و ماشین‌های هوشمند و متصل به اینترنت نیست و حیطه آن بسیار وسیع‌تر است. امواج این تحول در مواضعی که از محدوده توالی ژن گرفته تا نانوفناوری، از منابع تجدیدشدنی گرفته تا محاسبه کوانتومی به طور هم‌زمان مشاهده می‌شوند. ادغام این فناوری‌ها و اثرات متقابل آن‌ها در حوزه‌های فیزیکی، دیجیتالی و زیستی است که انقلاب صنعتی چهارم را با انقلاب‌های قبلی متفاوت می‌سازد (۷).

«کافی است: مهندسی ژنتیک و پایان ماهیت آدمی» عنوان کتابی است که نویسنده آن Bill McKibben است و نتایج حاصل‌شده نسبت به زیست‌محیط را با نگاهی نقادانه مورد ارزیابی قرار داده است. مخالفت جدی با این پدیده علمی همچنان ادامه دارد و در حالی که می‌تواند از فضای سایبر در تحولات عمیق خود استفاده کند از آن به عنوان تهدیدی در آینده نام برده و همچنان از بعد اخلاقی و اعتقادی بیشترین منتقدان را دارد.

بسیاری از ابزارهای مهندسی زیستی اکنون به راحتی توسط بیوهکرها قابل دسترسی هستند و خودتان به عنوان علاقمندان به زیست‌شناسی می‌توانید برخی کارهای مربوط را انجام دهید. تعامل آنلاین بین مهندسین بیولوژی و شرکت‌های هم‌نهاد و خدماتی DNA به عنوان یک حامل نوعی حمله اضافه شده است که از طریق آن حملات اضافی بارگزاری‌شده، می‌توان اطلاعات ژنتیکی مخرب را به سیستم بیولوژیکی تزریق کرد (۱۳).

محصولات سیستم‌های بیولوژیکی ممکن است مواد بسیار خطرناکی مانند سموم یا ویروس‌های مصنوعی باشند. یکی از تعریف‌های معمول استفاده‌شده از زیست‌شناسی مصنوعی این است که استخراج قطعات زنده برای ارگانیسم‌هایی است که پس از اینکه به درون موجودات دیگر وارد می‌شوند، باعث می‌شوند تا یک سازماندهی جدید با قطعاتی از اهداکننده و گیرنده ایجاد شود. زیست‌شناسی مصنوعی همچنین به عنوان

استفاده از مهندسی بیولوژیکی به کمک رایانه برای طراحی و ساخت قسمت جدید بیولوژیکی مصنوعی توصیف شده است. برخی دیگر مانند بنیاد ملی علوم و شورای تحقیقات مهندسی و علوم فیزیکی متذکر شده‌اند که زیست‌شناسی مصنوعی در شناسایی و کاربرد زیست‌شناسی به منظور طراحی قطعات و سیستم‌های بیولوژیکی برای استفاده در ایجاد یا طراحی مجدد سیستم‌های بیولوژیکی طبیعی مفید است (۱۴).

زیست‌شناسی مصنوعی یک حوزه علمی در حال تکامل است که به طور فزاینده‌ای در بحث عمومی و رسانه‌ها مطرح می‌شود. این مواجهه رو به رشد ناشی از مزایای بزرگی است که این حوزه در بخش سلامت، انرژی و بخش‌های غذایی نوید می‌دهد. همچنین نگرانی‌هایی که از نظر علمی، اخلاقی، ایمنی و نظارتی ایجاد می‌کند (۱۵). زیست‌شناسی مصنوعی ایجاد سیستم‌های جدید بیولوژیکی را مفروض می‌داند که می‌توانند برای انجام وظایف تعیین‌شده توسط انسان استفاده شوند، اگرچه این وظایف معمولاً با اهداف خوش‌خیم همراه است، اما سوءاستفاده و امکان آن خود نشان‌دهنده ایجاد شرایط خطر و عدم ایمنی مناسب است، هرچند منشأ انتشار این خطرات می‌توانند عمدی یا سهوی باشد (۱۵). با توجه به پتانسیل زیست‌شناسی مصنوعی، این خطرات می‌توانند بخش‌های زیادی از زندگی مردم و محیط را تحت تأثیر قرار دهند. از این رو دانشمندان، سازمان‌ها، دولت‌ها و شرکت‌ها، استراتژی‌های مختلفی را برای ارزیابی و رفع این تهدیدها ایجاد کرده‌اند، با توجه به اینکه حذف مطلق خطر به طور کلی غیر قابل دستیابی است.

زیست‌شناسی مصنوعی با تأکید زیاد بر زیست‌شناسی مدل محور، همچنین شامل سیستم‌های سایبری ـ فیزیکی است (۱۶). زیست‌شناسی مصنوعی مهندسی سیستم‌های بیولوژیکی را دربر می‌گیرد، از ژن گرفته تا کل ژنوم‌ها. حوزه نوظهور ژنومیک مصنوعی ابزارهای جدیدی را برای پرداختن به سؤالات و مقابله با چالش‌های زیست‌شناسی و بیوتکنولوژی فراهم می‌کند که با روش‌های فعلی پرداختن به آن‌ها غیر ممکن است (۱۷).

استفاده دوگانه از زیست‌شناسی مصنوعی به عنوان یک فناوری قدرتمند به نفع بشریت و به عنوان یک سلاح بالقوه، مسأله‌ای دیرینه است. خطرات زیست‌شناسی مصنوعی بسیار زیاد است و آن‌ها به کنترل‌های دقیق امنیتی احتیاج دارند. یکی از این کنترل‌ها، راهنمای چارچوب غربالگری وزارت بهداشت و خدمات انسانی (HSS) برای ارائه‌دهندگان زیست‌شناسی مصنوعی است (۱۳).

انسان برای هزاران سال توسط پرورش افراد انتخابی با ویژگی‌های مطلوب در حال تغییر کد ژنتیکی گیاهان و حیوانات بوده است، مانند بیوتکنولوژیست‌ها که در طول زمان دریافته‌اند چگونه کدهای ژنتیک را خوانده و دستکاری کنند، آن‌ها شروع به یافتن اطلاعات ژنتیکی مرتبط با ویژگی‌های مفید در یک موجود و اضافه‌کردن این اطلاعات ژنتیکی به موجود دیگر کرده‌اند که این پروسه، اساس مهندسی ژنتیک است و به دانشمندان امکان می‌دهد که به روند ایجاد نژادهای جدید گیاهان و حیوانات سرعت ببخشند. این رویکرد مبتنی بر این ایده است که سیستم‌های زنده ذاتاً پیچیده هستند، زیرا از طرق خاص تکاملی و تحت فشار توسعه می‌یابند. به طور خاص، در مورد بیولوژی مصنوعی، کاهش پیچیدگی سیستم‌های بیولوژیکی قرار است به کنترل آن‌ها کمک کند، رفتار آن‌ها قابل پیش‌بینی‌تر است و آن‌ها را به روشی منطقی و سیستماتیک طراحی می‌کند. ابزار دستیابی به این اهداف در اصول اصلی مهندسی قرار گرفته است که می‌تواند در تمام سطوح بیولوژیکی (به عنوان مثال مولکول‌ها، سلول‌ها، ارگانیسم‌ها) استفاده شود (۱۵).

۵-۴. تهدیدات و جرائم بیولوژیکی: امکان دستکاری و شبیه‌سازی ژنتیکی انسان با وجود ابراز امیدواری طرفداران برای درمان‌های بسیار مؤثرتر بیماری‌های انسانی و نیز مخالفانی که در این مورد به سناریوی دیستوپیایی، نقطه مقابل شهر آرمانی «انسان‌های طراح» اشاره می‌کنند، اما این عنوان همچنان خشن‌ترین بحث‌ها را برانگیخته است. این اتفاق می‌تواند تعصبات فرهنگی جامعه را به واقعیت‌های زیستی تبدیل کند و زندگی انسان را به کالایی دیگر که می‌تواند بنا به میل خود تولید شود، تنزل دهد. از بعضی

جهات، این بحث‌ها، ترس و جذابیت پیرامون سایبورگ را تکرار می‌کند (۳).

وقتی بیشتر ما به فناوری‌های ژنتیکی فکر می‌کنیم، دلایل بسیار خوبی برای وجود مراقبت‌های بهداشتی به ذهن خطور می‌کند. درک روزافزون ما از چگونگی تأثیر ژن‌ها بر عملکرد بدن ما، نوآوری‌های باورنکردنی پزشکی را برای بهبودی و حتی درمان برخی از بیماری‌های ژنتیکی واقعاً وحشتناک، ممکن کرده است، اما ژنوم‌های ما تنها مربوط به سلامتی ما نیستند که فقط سلامتی ما را تأیید کنند، بلکه آن‌ها طرح اصلی بخش زیادی از زندگی ما هستند. از آنجا که زندگی ما موضوعی بیش از مراقبت‌های بهداشتی است، تأثیر انقلاب ژنتیک نیز بسیار فراتر از حوزه سلامت خواهد بود. با این رویکرد در نهایت نحوه ارزیابی خطرات و فرصت‌هایمان، نحوه تولد نوزادان، طول عمر، ماهیت نوزادانی که می‌سازیم و در نهایت سیر تکاملی ما به عنوان یک گونه جانوری تغییر خواهد کرد. این موضوع پیامدهای گسترده‌ای بر مفهوم امنیت ملی خواهد داشت (۱۸).

با انجام این تحول، کاربردهای فناوری‌های ژنتیکی برای تغییر وراثت ژنتیکی انسان‌ها به طور فزاینده‌ای بحث‌برانگیز می‌شود. باید به این فکر کرد که چگونه افراد نسبت به تبدیل ساختار جدید محصولات اصلاح‌شده ژنتیکی (GMO) واکنش نشان می‌دهند، حتی اگر هیچ شواهدی وجود نداشته باشد که نشان دهد مصرف محصولات GMO برای مردم خطرناک‌تر از محصولات غیر GMO یا تراریخته است. باید به همه جنجال‌ها و خشونت‌هایی که بحث سقط جنین را همراهی کرده‌اند، اندیشید. اگر مردم راغب باشند به دلیل اختلاف نظر در مورد محصولات تراریخته و سقط جنین، به خشونت متوسل شوند، باید تصور نمود که وقتی مسأله راجع به تغییر انسان‌های ژنتیکی است، چه کاری ممکن است انجام دهند. اولین انسان ویرایش شده ژن در جهان سال گذشته در چین متولد شد که نتیجه یکسری اقدامات مخفیانه و از نظر نگارنده غیر اخلاقی توسط یک بیوفیزیکدان چینی بود. این اولین قدم بسیار تأسف‌آور بود، اما حتی اگر این اتفاق نیفتاده باشد، بدون شک چند سال بعد، اولین کاربرد اخلاقی، شفاف و مؤثرتر ویرایش ژن انسانی وراثتی انجام می‌شود (۱۸).

نکته اساسی این است که ویرایش ژن انسان در حال وقوع است. این موضوع، همراه با افزایش توانایی انتخاب آگاهانه در بین جنین از قبل کاشته شده و همچنین ایجاد تعداد نامحدود تخمک‌های انسانی از سلول‌های بنیادی ناشی از سلول‌های بالغ مادر است که به طور اساسی روش تولید مثل گونه‌ها و توانایی ما در دستکاری ژنتیکی خودمان و نسل‌های آینده را دگرگون خواهد کرد، اما با فرض اینکه این فناوری به مرور زمان مزایای کودکان سالم و با عمر طولانی‌تر، ضریب هوشی بالاتر و سایر توانایی‌ها را به همراه داشته باشد، کسانی که ترجیح داده‌اند به این رویه عمل نکنند، چه کاری انجام خواهند داد؟ آیا آن‌ها منتظر می‌مانند تا ببینند چه اتفاقی می‌افتد؟ آیا آن‌ها از اکنون می‌دانند که از این پس یک نسل، در معرض آسیب واقعی خواهد بود؟ آیا آن‌ها سعی خواهند کرد جوامع دیگر را با تشویق یا اقناع تصمیم به ماندن در شرایط قبل کنند، یا با قوانین بین‌المللی و زور مجبور به همراهی می‌شوند؟یا اینکه آن‌ها تصمیم می‌گیرند که جهان در حال تغییر است و در صورت تمایل به ادامه راه، چاره‌ای جز انتخاب ندارند؟ به راحتی می‌توان فهمید که چگونه این مسأله می‌تواند به یک مسأله کاملاً دشوار، پیچیده، بحث‌برانگیز و حتی بی‌ثبات‌کننده در درون جامعه و بین جوامع تبدیل شود. اکنون دولت‌های سراسر جهان باید به صورت پیشگیرانه به این موضوعات بپردازند و سعی کنند فناوری‌های ژنتیکی (و سایر فناوری‌ها) را به گونه‌ای توسعه دهند که هدف اصلی آن بهینه سازی برای مصلحت عمومی و به حداقل‌رساندن هرگونه آسیب احتمالی و خطر ایجاد تعارض در این مسیر باشد؛ اما کارهای خیلی کمی انجام شده است (۱۸). واقعیت غیر قابل انکار امکان استفاده از این فناوری در بخش نظامی و به عنوان سلاح‌های بیولوژیکی است، اما نکته مورد بحث این است که این سلاح‌ها به بخش سایبری با حفظ اهداف ضد حیات انسانی خود نیز ورود کرده‌اند.

جرائم زیستی یا بیولوژیکی در اینجا به عنوان بهره‌برداری از آسیب‌پذیری در ابزارهای بیولوژیکی، داده‌ها و پایگاه داده‌ها،

دستگاه‌ها یا تکنیک‌ها برای مقاصد مجرمانه که می‌توانند کاملاً جدید باشند یا ترکیبی از انواع جرائم فعلی باشند، هم با افزایش در میزان داده‌های بیولوژیکی و هم با کاهش هزینه‌های فناوری استفاده‌شده امکان‌پذیرند، تعریف شده است. علاوه بر این، در حالی که مقادیر بیشتری از داده‌های بیولوژیکی در حال ارائه است، اقدامات فعلی با هدف مقابله با جرائم بیولوژیکی ناقص است، زیرا آن‌ها محدود به استفاده از عوامل بیولوژیک هستند و آسیب‌پذیری در زنجیره تأمین گسترده امروز را در نظر نمی‌گیرند. امروزه، بیوتکنولوژی شامل گردش کار یکپارچه‌ای است که به طور فزاینده‌ای به سیستم‌های خودکار کنترل‌شده توسط کامپیوتر بستگی دارد. این کارایی همچنین فرصت‌های جدیدی را برای وقوع جرائم بیولوژیکی ایجاد می‌کند، در نتیجه همانطور که در بالا ذکر شد، جرائم بیولوژیکی در اینجا مفهوم‌سازی شده است و شامل جرائمی است که شامل سیستم‌های بیولوژیکی و سایبری برای ارتکاب جرائم کاملاً جدید، جرائم سنتی یا ترکیبی از این دو است. شکل‌های جرائم بیولوژیکی از طریق پروتکل‌ها ـ موافقت مقدماتی ـ جرم و آمادگی ما برای اقدام، در نظر گرفته شده است (۱۹).

۵-۵. تهدیدات و جرائم بیوسایبری: ورود به عصر فناوری اطلاعات، بزه‌کاران را هم دربر گرفته است. عده‌ای از رایانه برای ارتکاب جرم بهره می‌گیرند، برخی دیگر خود رایانه را موضوع جرم قرار می‌دهند و گاه، داده‌ها و آنچه که محتوای اطلاعات رایانه‌ای را تشکیل می‌دهد، موضوع بزه واقع می‌شود (۲۰). به نظر می‌رسد در بخش مربوط به زیست‌شناسی، بخش سوم بیشتر مورد استفاده قرار می‌گیرد.

پیرامون فعالیت‌ها و تهدیدهایی که در فضای اینترنت و غالباً به صورت آنلاین با آن‌ها مواجه هستیم، هیچ‌گاه نمی‌توان با قطعیت در مورد اینکه این تهدیدها واقعاً جدی (دارای سوءنیت) هستند یا خیر اظهار نظر کرد. بنابراین همه این تهدیدهایی که وجود دارند از هر دسته‌ای که باشند، بایستی جدی گرفته شوند. از این رو می‌توان چنین فعالیت‌هایی را که در آن فرد یا گروهی از جامعه قربانی هرگونه توجه خواسته یا ناخواسته، رفتار پرخاشگرانه، برخورد نفرت‌انگیز می‌شوند، در چارچوبی قرار بگیرند که آن را «رفتار ضد اجتماعی آنلاین» می‌نامیم (۲۱). بنابراین نظر و همچنین بر طبق تعریف ارائه‌شده از سوی گروهی از کارشناسان که به دعوت سازمان همیاری اقتصادی و توسعه (OECD) در پاریس در سال ۱۹۸۳ گرد آمده بودند، جرم رایانه‌ای عبارت است از: «هر عمل غیر قانونی، غیر اخلاقی یا غیر مجاز نسبت به پردازش خودکار و یا انتقال داده‌ها» (۲۲). می‌توان فعالیت‌های غیر مجاز و تهدیدهایی که در این زمینه مورد مطالعه قرار می‌گیرند را نیز موضوع جرائم سایبری قرار داد. بنابراین صرف شامل‌شدن این رفتارها به عنوان برهم‌زننده نظم اجتماع و در تقابل با آن، از آن‌ها به عنوان جرم سایبری نام برده شده است. رفتارهای ضد اجتماعی که هنوز ناشناخته مانده‌اند و در بسیاری موارد نامفهوم هستند و شاید جرم‌انگاری این رفتارها ـ در حوزه‌های اختصاصی ـ مدتی به طول بیانجامد.

در تعریف جرائم بیوسایبری می‌توان گفت علاوه بر پایگاه داده، زیست‌شناسی مصنوعی شامل یک فرآیند تولید زیستی است جایی که یک اثر فیزیکی مطلوب مانند تولید داروی مصنوعی یا بیولوژیک ایجاد می‌شود. این ادغام و وابستگی روزافزون به فضای دیجیتال (به عنوان مثال، ابزارهای تحت کنترل رایانه در فرآیندهای تولید داروی مصنوعی یا بیولوژیک) دسته جدیدی از خطرات را بین سیستم‌های سایبری و بیولوژیکی ایجاد می‌کند. جرائم بیوسایبری همچنین فعالیت‌های مجرمانه‌ای را که به وسیله ترکیبی از رایانه متصل به اینترنت و مواد بیولوژیکی و بیوشیمیایی انجام می‌شود را توصیف می‌کند (۱۹).

نویسندگان تحقیق «یک مرور سیستماتیک از پتانسیل جرم شناسی زیست‌شناسی مصنوعی و مسیرهای پیشگیری از جرم در آینده» اظهار می‌دارند که شایع‌ترین فرصت‌های جرم، از طریق داده‌های زیستی (بیولوژیک) ناامن، فناوری‌های زیست‌شناسی مصنوعی و مجموعه‌ای از پردازش داده‌های تولیدشده، فراهم آمده است. فناوری‌های زیست‌شناسی مصنوعی با ۴۶ درصد از انواع جرائم شناسایی‌شده مرتبط بوده‌اند. همچنین ۴۰ درصد از رایج‌ترین تهدیدات خارجی برای جرم زیست‌شناسی مصنوعی شناسایی‌شده، هکرهای

زیستی و هکرها بوده‌اند (۱۹). این نویسندگان همچنین عنوان می‌کنند: سه مقاله که در این رابطه شناسایی شده‌اند، استفاده در جهت نادرست و بد از ویروس‌های مهندسی‌شده را به عنوان خطر جرم در آینده توضیح می‌دهد. تغییر در فناوری، دولت، رویه‌های صنعتی و نگرش‌های فرهنگی متداول‌ترین فاکتورهای استنادی برای جرم مؤثر در زیست‌شناسی مصنوعی بودند. برای اتخاذ یک رویکرد پیشگیرانه مؤثر در برابر این قسم خطرات جرائم نوظهور، توجه فوری و یک رویکرد پیشگیرانه خلاقانه لازم است (۱۹).

همچنانکه طبیعت سایبری فیزیکی بیوتکنولوژی منجر به پیشرفت‌های جذاب در سراسر رشته علوم زیست‌شناسی شده است، اخیراً نگرانی‌هایی در مورد خطرات جدید که ممکن است منجر به عواقب ناخواسته یا پتانسیل‌های شناخته‌نشده‌ای برای سوءاستفاده در این بخش شود، نیز مطرح شده است. همانطور که ظهور اینترنت در چند دهه پیش منجر به یک انقلاب بزرگ و ضروری شد که با حوزه امنیت سایبری تکمیل شد، اکنون ما با دوره امنیت زیستی سایبری رو به رو هستیم که آسیب‌پذیری‌های امنیتی خاص خود را دارد. از آنجا که این نگرانی‌ها باعث ظهور امنیت سایبری به عنوان یک رشته جدید شده است، ضروری است که درک کنیم تمرکز آن فقط در حملات سایبری سنتی نیست. ماهیت فیزیکی و سایبری بیوتکنولوژی نگرانی‌های امنیتی بی‌سابقه‌ای را ایجاد می‌کند. رایانه‌ها می‌توانند با رمزگذاری بدافزار در توالی DNA به خطر بیفتند و تهدیدهای بیولوژیکی را می‌توان با استفاده از داده‌های عمومی موجود در دسترس، همگانی ساخت. اعتماد به جامعه بیوتکنولوژی آسیب‌پذیری‌هایی را در فضای مجازی و زیست‌شناسی ایجاد می‌کند. آگاهی پیش‌شرط مدیریت این خطرات است (۱۶).

۵-۶. امنیت بیوسایبری: امنیت بیوسایبری درک خطرات جدیدی است که در مرز بین فضای مجازی و زیست‌شناسی به منظور تدوین سیاست‌هایی برای مدیریت آن‌ها به وجود آمده است. سیاست‌های ایمنی بیولوژیکی و امنیت بیولوژیکی برای کنترل تعداد محدودی از تهدیدهای بیولوژیکی از جمله عوامل بیماری‌زای تنظیم‌شده طراحی شده‌اند، اما از تهدیدات ناشی از روابط پیچیده بین گردش کار محاسباتی (روشی که یک پروژه خاص توسط یک شرکت سازماندهی می‌شود، از جمله اینکه کدام قسمت از پروژه و چه زمانی شخصی قصد انجام آن را دارد) و تجربی یا آزمایشگاهی، محافظت نمی‌کنند (۱۶).

یک اتصال و ارتباط سایبری ـ بیولوژیکی هنگامی رخ می‌دهد که اطلاعات بیولوژیکی اندازه‌گیری، نظارت یا تغییر کرده است و به اطلاعات دیجیتال (سایبری) تبدیل می‌شوند یا برعکس، وقتی اطلاعات دیجیتالی (سایبری) برای دستکاری سیستم بیولوژیکی استفاده می‌شود. به طور مشابه، رابط فیزیکی سایبری هنگامی رخ می‌دهد که یک مکانیزم فیزیکی با استفاده از دیجیتال (سایبر) کنترل یا نظارت می‌شود، مانند کامپیوتر که سرعت مخلوط‌کردن یک راکتور بیولوژیکی را کنترل می‌کند (۲۳).

در فرآیند تولید داروهای پروتئینی، آسیب‌پذیری‌های امنیت سایبری در هر نقطه‌ای که اطلاعات ژنتیکی از طریق سیستم‌های سایبری یا سایبری ـ فیزیکی (مکانیزم کنترل یا نظارت توسط الگوریتم‌های مبتنی بر کامپیوتر) ذخیره، بیان، تکثیر یا نظارت می‌شود، وجود دارد. یک مثال ساده، ذخیره بانک‌های سلول اصلی در یخچال فریزر با سیستم‌های زنگدار و شبکه‌ای‌شده‌ای است که کار نظارت بر درجه حرارت را انجام می‌دهد، جایی که خرابی در شبکه می‌تواند عدم اطمینان از ماندگاری بانک سلول اصلی را ایجاد کند. یک نوع مخرب‌تر از این سناریوی ساده، نفوذ سایبری است که رکورد دیجیتال مستند شرایط ذخیره‌سازی برای بانک اصلی سلول را خراب می‌کند. در هر دو مورد، عدم اطمینان از زنده‌ماندن سلول‌ها آسیب‌پذیری ایجاد می‌کند، حتی اگر تأثیر واقعی بر روی سلول‌های ذخیره‌شده ناچیز باشد. یک نوع مخرب‌تر از این سناریوی ساده، نفوذ سایبری است که سیستم بایگانی دیجیتالی را که شرایط ذخیره‌سازی برای بانک سلول اصلی را ثبت و مستند می‌کند، ناکارآمد کرده و یا از بین می‌برد. در این مورد نیز، عدم اطمینان از زنده‌ماندن سلول‌ها آسیب‌پذیری ایجاد می‌کند، حتی اگر تأثیر واقعی بر روی سلول‌های ذخیره‌شده ناچیز باشد (۲۳).

در این مثال‌ها، آسیب‌زدن، از کارانداختن، منحرف‌کردن، غیر قابل رؤیت و مخفی‌کردن و... هدفی است که از وابستگی روزافزون جامعه علوم زیستی، مانند بسیاری علوم دیگر، ناشی می‌شود. این شرایط می‌تواند برای اهداف خصمانه‌تری نیز انجام شود و یا حتی به صورت سازمان‌یافته انجام گیرد. تلاش‌های طولانی‌مدت در جامعه زیست‌شناسی مصنوعی برای آگاهی از کاربردهای بالقوه امنیتی از این فناوری‌ها هزینه‌های بالایی را پرداخت کرده است که این روند باید گسترش یابد. جامعه باید اطمینان حاصل کند که شرکت‌های با کاربری ترکیبی DNA به عنوان تنها نقطه استفاده نادرست تلقی نمی‌شوند. شرکت‌هایی که مدارهای ژنتیکی و موجودات جدیدی را طراحی می‌کنند، غالباً شرکت‌کننده فعال در ارزیابی تهدیدات مربوط به امنیت و تخمین سوءاستفاده بالقوه از فناوری‌های اختراع، پیشرفت و فروش آن‌ها هستند (۲۴).

۵-۷. بیوهکرها و داده‌های ژنتیکی: جرائم بیوسایبری خود حوزه گسترده‌ای را شامل می‌شوند، لکن مواردی مانند هک DNA بیشتر مورد توجه قرار گرفته و به نوعی یک تهدید باقوه و یا بالفعل هستند. هدف در روزهای اولیه از نفوذ غیر مجاز هکرهای بزه‌کار، این بود که توان خود را برای شکستن حفاظت سیستم‌ها نشان دهند و این کار را برای سرگرمی خود، رقابت و چالش با دیگر هکرها انجام می‌دادند. پس از آن به دلیل ایجادشدن و غالب‌شدن تفکر انگیزه منفعت، سود و درآمد صرف در جهان، عناصر و عوامل بزه‌کار در فضای مجازی که در کارشان جدی و صرفاً قصد مجرمانه داشتند، جذب نهادهای جهانی و سازمان‌یافته شدند. ایالت متحده نیز در ادامه این روند، اکنون فضای سایبر را به عنوان دامنه قابل توجهی از جنگ می‌شناسد که با طبقه‌بندی‌کردن آن به هوا، خشکی و دریا، سازمان‌های مربوطه جدیدی را برای تأمین امنیت در آن ایجاد نموده است (۲۵).

در ادامه فعالیت‌ها و نفوذهای غیر مجاز در فضای سایبر، عرصه جدیدی پیش روی هکرها قرار گرفت. این رخداد در حوزه جدید سایبری، احتمالاً پیچیده‌ترین اتفاق خواهد بود: هک کردن آن آسان است و دفاع از آن سخت است، زیرا بدون آن راهی برای زندگی وجود ندارد. این حوزه زیست‌شناسی است. طی ۲۰ سال گذشته، ده‌ها میلیارد پوند به صنایع زیست‌شناسی مولکولی و ژنتیک سرازیر شده است. این امر منجر به ایجاد فناوری‌های جدید برای خواندن DNA شده است. هر روز ژنوم‌های جدید در پایگاه داده‌های علوم بهداشتی بارگذاری می‌شوند و سرعت آن‌ها با شتاب در حال افزایش است. همه این داده‌ها ارتشی از دانشمندان بیوانفورماتیک را به وجود آورده است که وظیفه آن‌ها سازماندهی همه این کدها و کشف کارکرد آن‌ها است. اما خواندن DNA تنها آغاز کار است: علم تا جایی پیشرفت کرده است که بشر می‌تواند کد DNA را نیز بنویسد، در نتیجه هزاران دانشمند، که به عنوان مهندس ژنتیک شناخته می‌شوند، مستقیماً موجودات زنده را برنامه‌ریزی می‌کنند (۲۵).

بیشترین موارد نقض‌های امنیتی در ارتباط با DNA که تا به امروز آزمایش شده است، مربوط به شرکت‌هایی بوده است که انواع سرقت با روش و اهداف مخصوص، با استفاده از نامه‌های الکترونیکی و رمزهای عبور را تجربه می‌کنند. وقتی داده‌های مربوط به DNA به صورت محوری مورد بررسی و توجه قرار می‌گیرند خطرات در این رابطه نیز روند افزایشی پیدا می‌کنند. سیستم‌های بهداشتی می‌توانند نقض داده‌های ژنتیکی از باج افزار را تجربه کنند و مجبور به خرید مجدد داده‌های بیمار شوند. هکرها همچنین ممکن است از داده‌های ژنتیکی به سرقت‌رفته برای باج‌خواهی از افرادی که اطلاعات مخرب در DNA خود دارند، استفاده کنند (۲۶). این قابلیت با ورود حداکثری جوامع به عصر دیجیتال و استفاده حداکثری از اینترنت و همچنین کاربرد پزشکی و یا نظارتی ریز تراشه‌ها، بسیار پراهمیت خواهد بود. داده‌های بیماران که به صورت بر خط در اختیار پزشکان قرار می‌گیرد، می‌تواند برای هکرها قابل توجه باشد. بیشتر این داده‌های شخصی، از فناوری‌های پوشیدنی که شامل سنسورهای الکترونیکی هستند، حاصل می‌شوند. حسگرهای الکترونیکی که می‌پوشیم، حمل می‌کنیم یا می‌بلعیم می‌تواند داده‌ها را با یک شبکه دیجیتال ضبط و تبادل کنند. به عنوان مثال می‌توان به ساعت، لباس، عینک، تلفن همراه و قرص‌های دیجیتال اشاره کرد که حاوی سنسورهایی هستند که هنگام بلعیدن، اطلاعات را به یک

پزشک متخصص متقاضی می‌فرستند (۲۷). این حسگرهای الکترونیکی که به همراه لباس و قابل پوشیدن هستند، طیف گسترده‌ای از رفتارها و صفات بیولوژیکی را ردیابی و نظارت می‌کنند، از جمله ضربان قلب، فشار خون، سطح گلوکز خون، وضعیت قلب، ضربه مغزی، عفونت گوش، سرطان پوست، بیماری پارکینسون، بیماری آلزایمر، دمای بدن، الگوهای خواب، سطح استرس، وزن، سطح فعالیت، حالت‌ها (۲۸).

تحقیقات اخیر نشان داده است که چگونه یک مرتکب می‌تواند با استفاده از ابزارهای معمول مواد بیولوژیکی را ترکیب کند که این ترکیب به محض تجزیه و تحلیل DNA، درب مخفی سایبری را برای مرتکب باز می‌کند تا کنترل یک منبع محاسباتی را از طریق خط لوله توالی DNA، به دست آورد. همانطور که تجزیه و تحلیل DNA به برنامه‌های عملی روزمره راه پیدا می‌کند، خطر هک‌زیستی افزایش می‌یابد. آزمایش‌های مربوطه نشان می‌دهد که DNA مخرب می‌تواند ترکیب‌شده و در E-Coil یک آلاینده شایع قرار گیرد. بر این اساس، ما حمله جدیدی را مطرح می‌کنیم؛ در موقعیتی که یک هکر برای رسیدن به هدف، DNA را که با کد مخرب ساخته است، بر روی سطوح مشترک (به عنوان مثال، کت آزمایشگاه، نیمکت، دستکش لاستیکی) پنهان می‌کند. این مسأله قابل تبیین است که با استفاده از تکنیک‌های کنترل ورودی اختصاصی مشابه روش‌های استفاده‌شده برای مقابله با حملات تزریق معمولی می‌توان خطر هک‌زیستی را کاهش داد. همانطور که گفته شد، بیشترین موارد نقض‌های امنیتی در ارتباط با DNA که تا به امروز آزمایش شده است، مربوط به شرکت‌هایی است که انواع سرقت با روش و اهداف مخصوص، با استفاده از نامه‌های الکترونیکی و رمزهای عبور را تجربه می‌کنند. وقتی داده‌های مربوط به DNA به صورت محوری مورد بررسی قرار می‌گیرند، خطرات نیز روند افزایشی پیدا می‌کنند. سیستم‌های بهداشتی ممکن است با نقض داده‌های ژنتیکی از طریق باج افزار مواجه شوند و مجبور به خرید مجدد داده‌های بیمار گردند. هکرها ممکن است از داده‌های ژنتیکی به سرقت‌رفته برای باج‌خواهی از افرادی که اطلاعات مخرب در DNA خود دارند، استفاده کنند (۲۶).

در تحقیقی با عنوان «امنیت سایبری: تزریق DNA از راه دور، تهدیدی در زیست‌شناسی مصنوعی» نمونه‌هایی از حملات سایبری اثبات می‌شود که در آن یک مرتکب یا مهاجم از راه دور یک قربانی را فریب می‌دهد تا یک ماده خطرناک در آزمایشگاه قربانی تولید شود، بدون اینکه قربانی از آن مطلع شود یا تعامل بدنی بین مهاجم و اجزای آزمایشگاه داشته باشد... . حملات ساده‌تر در مواردی وجود دارد که مهاجمی با جای پای الکترونیکی در رایانه قربانی ممکن است آزمایش‌های بیولوژیکی را دستکاری کند (۱۳). از بسیاری از این قابلیت‌های دوگانه می‌توان در جرائم تروریستی علیه فضای بیوسایبر نیز استفاده کرد.

تروریست‌ها کارزار خود را از دنیای فیزیکی به فضای سایبر انتقال داده‌اند که بدیهی است، به دلیل قرارگرفتن در یک دنیای دیگر با شرایط و امکانات خاص و منحصر به فرد، سلاح‌ها و اهداف نیز ماهیت و کارکرد متمایزی از دنیای فیزیکی پیدا می‌کنند (۲۸).

واقعیت این است که برنامه‌های امنیت بیولوژیکی و ایمنی بیولوژیکی بسیار پرهزینه هستند و توسعه آن‌ها کند است، برعکس تهدید ناشی از سلاح‌های بیولوژیکی و خطرات آن‌ها، پتانسیل نامحدودی برای صدمه‌زدن دارند. استفاده از سلاح‌های بیولوژیکی توسط متجاوز می‌تواند باعث کشته‌شدن میلیون‌ها نفر، اخلال در جوامع، تضعیف اقتصاد و تغییر زندگی به همان شکلی که ما می‌شناسیم شود. به طور مشخص فضای سایبر خود قابلیت تبدیل‌شدن به بستری مناسب برای این‌گونه اقدامات را دارا است.

۵-۸. آینده رابطه‌ای سایبری ـ بیولوژیکی فعال‌شده توسط هوش مصنوعی:

John McCarthy تعریف زیر را برای اصطلاح هوش مصنوعی که در سال ۱۹۵۵ مطرح کرده، ارائه می‌دهد: هوش مصنوعی یک علمی است که مطالعه روند حل مسأله و دستیابی به هدف در شرایط پیچیده را انجام می‌دهد. یک علم اساسی مانند ریاضیات یا فیزیک که دارای مشکلات متمایز از کاربردها و متمایز از مطالعه نحوه کار مغز انسان و حیوان است (۲۹). هوش مصنوعی مدرن به دلیل

قابلیت یادگیری بی‌سابقه در پردازش داده‌های پیچیده، بر علم داده‌های بیولوژیکی تسلط خواهد داشت (۳۰).

داده‌های دیجیتالی ممکن است به طور فزاینده‌ای شبیه به داده‌های بیولوژیکی شوند، به این دلیل که داده‌های دیجیتالی ممکن است پویاتر و وابسته‌تر به محتوای آن، به ویژه با در نظرگرفتن اجرای افزایشی و گسترده الگوریتم‌های یادگیری ماشین و قابلیت‌های گسترش‌دهنده هوش مصنوعی باشند. با نگاه به جلو، رایانه‌ها و زیست‌شناسی در همان حلقه مشابه کنترل یک منطقه در حال ظهور هستند که می‌توانند آسیب پذیری‌های جدید امنیت سایبری را به عنوان هوش مصنوعی و یادگیری ماشینی در مسیر اصلی هوش مصنوعی معرفی کنند. در حالی که قابلیت‌های هوش مصنوعی فعلی بیشتر با یادگیری غیر فعال همراه است، سیستم‌هایی که قادر به یادگیری فعال هستند و شبکه‌های عصبی در حال حاضر برای کاربردهای مختلف در حال توسعه هستند. از آنجایی که هوش مصنوعی کاربرد روزافزونی را در ساخت زیستی و انتقال کاملاً وابسته به نیمه خودکار به کاملاً مستقل پیدا می‌کند، ارزیابی کاملی از آسیب‌پذیری‌ها و تهدیدات باید شامل راهکارهایی برای کاهش آن باشد. با هر پیشرفت، امنیت سایبری و امنیت بیوسایبری ممکن است به طور کامل‌تری به یک رشته واحد و یکپارچه نزدیک شوند (۲۳).

اگرچه اینترنت برای هماهنگی تلاش برای تعیین توالی و به اشتراک‌گذاری ثمرات آن بسیار مهم بوده است، اما بزرگ‌ترین پیشرفت تکنولوژیکی که توالی مقیاس بزرگ انسان را امکان‌پذیر می‌کند، توسعه ربات‌های توالی‌یابی فلورسانس لیزری با مهندسی عالی است (۳۱)، هوش مصنوعی این قابلیت برای جستجوهای بسیار دقیق حتی در بین داده‌های کلان را دارد و به عنوان یکی از رابط‌های سایبر و بیولوژی می‌توان به آن اشاره کرده و به اهمیت آن پی برد. می‌توان با هوش مصنوعی هرگونه‌ای از DNA و در بین هر تعداد از کاربران یا هر قشری که مورد نظر است را به راحتی یافت، نوشت یا ساخت. به عنوان مثال دانشمندان و مهندسان در حال کار با ابزارهای پیشرفته طراحی و مدل‌سازی با کمک رایانه هستند ـ یک زمینه درحال رشد به نام بیوانفورماتیک ـ که به آن‌ها امکان می‌دهد کل ژنوم‌ها را بازنویسی و دوباره برنامه‌ریزی کنند (۳۲).

۶. نتیجه‌گیری

اگر بخواهیم در شرایط پیشرفت قرار بگیریم، باید به چالش‌ها بپردازیم. دیر یا زود پیشرفت‌های علمی با هدف افزایش رفاه و تأمین خدمات، خود را بر تمامی جوامع تحمیل خواهند کرد. مسأله قابل تأمل این است که این شرایط به مانند سایر دستاوردهای بشری، همراه با تهدیدات بسیار نگران‌کننده‌ای خواهد بود که برای رویارویی با آن‌ها بایستی تدابیر ویژه‌ای اندیشیده شود. همچنانکه در این پژوهش مورد مطالعه قرار گرفت، نوآوری‌های اخیر در علوم بیولوژیکی می‌توانند در بهره‌مندی از فضای سایبر به عنوان یک بستر گسترده، برای انجام فعالیت‌های غیر قانونی و بر علیه نظم و امنیت اجتماعی مورد استفاده قرار گیرند. تهدیدات و جرائم بیوسایبری به عنوان یک رشته ترکیبی در حال ظهور و مرتبط با حوزه‌های زیستی مختلف بر پایه فضای مجازی و اینترنت شناخته می‌شود و در پی آن، امنیت سایبری و امنیت زیستی سایبری اهمیت ویژه‌ای پیدا می‌کنند. اصطلاح اخیر ـ با توجه به نام و کاربرد اصطلاح ـ در رابطه با حفظ امنیت در سبک زندگی آینده در حوزه‌های علوم پزشکی سایبری و فیزیکی سایبری، زنجیره تأمین امنیت و ایجاد سیستم‌های زیرساختی و تدوین و وضع اقدامات پیشگیری و محافظت در برابر تهدیدات مرتبط و کاهش آن‌ها است.

این نکته قابل تأمل می‌نماید که رخدادهای اخیر علمی در حوزه ژنتیک به خصوص در بخش مطالعات مربوط به (DNA) و نیز کارگزاری انواع ریزتراشه‌ها در بدن انسان‌ها و سایر جانداران، گویای این واقعیت است که پنجره جدیدی به روی کاربران سایبری و به خصوص فرصت‌طلبان -که می‌توانند مرتکبان بالقوه‌ای باشند- در جهت منافع مادی و شخصی باز شده است. مرتکبان فوق حرفه‌ای که حتی خود را مجرم نمی‌دانند (مجرمین بی‌گناه)، زیرا روش‌هایی را اتخاذ می‌کنند که یا جرم‌انگاری نشده‌اند یا به سختی می‌توان عنوان مجرمانه برای این رفتارها انتخاب کرد. بنابراین پیش‌بینی تهدیدها و

فرصت‌های جرم ناشی از هر یک از موارد فوق در آینده که ممکن است توسط فناوری در حال ظهور، مانند بیولوژی مصنوعی تسهیل شود، توجیه این موضوع است که مراحل پیشگیری زودتر از آنچه که تصور می‌شد، به خصوص برای محافظت از حوزه زیستی بایستی در هر جامعه‌ای در نظر گرفته شود.

جامعه علوم زیستی به طور سنتی تحت یک سیستم ناامن فعالیت می‌کنند که انتظار دارد شرکت‌کنندگان خودتنظیم شوند و اغلب تهدیدهای امنیتی را کنترل نمی‌کند. اکنون که توالی، سنتز، دستکاری و ذخیره‌سازی DNA به طور فزاینده‌ای دیجیتالی می‌شود، بیش از هر زمان دیگری عوامل خطرناک در داخل و خارج از جامعه برای به مخاطره انداختن امنیت وجود دارد. برای کاهش این خطرات، فرهنگ جامعه علوم زیستی باید از یک اعتماد بدون اندیشه به یک آگاهی روشنگرانه و گسترده تغییر یابد. کسانی که بر روی فرآیندهای بیولوژیکی و تولید متمرکز هستند، باید دیدگاه گسترده‌تری را ایجاد کنند که شامل درک دقیق تهدیدات سایبری ـ فیزیکی است. هنگامی که افراد جامعه از خطرات امنیت سایبری آگاه شدند، می‌توانند اقدامات حفاظتی را در محیط کار خود شروع کرده و با نهادهای نظارتی همکاری کنند تا سیاست‌های جلوگیری از نقض امنیت سایبری را تدوین و اجرا کنند.

با دیدگاهی آینده‌نگرانه و مبتنی بر سناریوهای مختلف و انتخاب سیاستگذاری‌های متناسب و لحاظ آن در مدیریت کلان در نگاه به دستاوردهای علمی در انقلاب صنعتی چهارم با محوریت جرائم بیوسایبری و امنیت بیوسایبری آنچه می‌تواند قابل تأمل باشد، ضروری‌بودن و الزامی‌بودن مدیریت دولت‌ها بر امنیت سایبری در عرصه‌های بین‌المللی و داخلی خواهد بود، زیرا در مسیر پیشرفت علمی محدودیتی وجود ندارد، ولی در ابعاد اخلاقی و قانونی است که برای این سیر تحولات و نوآوری‌ها خطوط قرمزی تعیین شده است. تعبیر جنون دانش برای فناوری‌ها و ایده‌های در دست تحقیق شاید اصطلاح به جایی باشد، زیرا برخی هیچ‌گونه محدودیتی را نمی‌پذیرند و همچنان در جهت منافع مادی در مسیر خود می‌تازند. Dark-Net یا بخش تاریک فضای سایبری چنان مملو از رفتارها، ایده‌ها و ابداعات غیر اخلاقی و غیرانسانی است که به یک چالش و دغدغه بزرگ جامعه جهانی تبدیل خواهد شد.

نهایتاً اینکه کنترل بروز و گسترش جرائم زیستی مبتنی بر فضای سایبر، نه‌تنها به عنوان یکی از مؤلفه‌های میزان امنیت ملی در هر کشوری محسوب می‌شود، بلکه به لحاظ عملی، می‌تواند دارای اهمیتی مضاعف باشد. چنانکه وقتی با ایجاد بحران در منطقه‌ای و احتمال جنگ بین کشورها، فروش اسلحه به یکی از منابع مادی و درآمدهای کلان برخی کشورهای پیشرفته جهان تبدیل می‌شود، احتمال انتشار و گسترش بیماری‌های مختلف، باعث فروش داروها و معالجات مربوط به آن‌ها می‌شود و ساخت و صادرات واکسن بیماری‌های ناشی از گسترش ویروس‌های هوشمند نیز در آینده به عنوان یکی از منابع درامد این کشورها، قابل پیش-بینی است. این مسأله در وهله اول ایجاب می‌کند بخش‌های دولتی و خصوصی که باید مسؤول امنیت بیوسایبری باشند، باید به اندازه کافی قدرتمند و سازماندهی شده و از نظر مالی نیز پشتیبانی شوند. همچنین با اولویت‌بندی برنامه‌های پیشگیرانه با مشارکت افراد صاحب اندیشه و متخصص، بایسته است که در بازه‌های زمانی مختلف ایمنی در فضای سایبر در این بخش را مضاعف کرد و نهایتاً اینکه متولیان سیاستگذاری‌های کلان با هماهنگی بخش‌های مربوطه، با طراحی انواع سناریوها خود را آماده تقابل با هرگونه پیشامد ممکن کنند.

۷. تقدیر و تشکر

بدینوسیله از تمام عزیزانی که در تهیه و تدوین این پژوهش مساعدت و همکاری نموده‌اند، تقدیر و تشکر می‌شود.

۸. سهم نویسندگان

کلیه نویسندگان به صورت برابر در تهیه و تدوین پژوهش حاضر مشارکت داشته‌اند.

۹. تضاد منافع

در این پژوهش هیچ‌گونه تضاد منافعی وجود ندارد.

References

1. Khalili A, Nooralivand Y. Cyber threats and their impact on national security. *Strategic Studies.* 2012; 15(2): 167-196. [Persian]

2. Musavi M, Heydari KH, Ghanbari A. The Impact of Cyber Terrorism Security Threats on the National Security of the Islamic Republic of Iran and Strategies to Counteract It. *Quarterly Journal of International Police Studies.* 2013; 14(1): 123-145. [Persian]

3. Conner E. The Cambridge Companion to Postmodernism. New York: Cambridge University Press; 2004. p.136-137.

4. Czarniawska-Joerges B, Joerges B. Robotization of Work? Answers from Popular Culture, Media and Social Sciences. London: Edward Elgar Publishing; 2020. p.1-6.

5. Stearns P. The Industrial Revolution in World History. London: Routledge; 2021. p.13-14.

6. Lim W. Industrial Revolution 4.0, Tech Giants and Digitized Societies. Singapore: University of Social Sciences; 2019. p.11-15.

7. Schwab K. The Fourth Industrial Revolution. Switzerland: Crown Business; 2017. p.11, 16.

8. Gleason N. Higher Education in the Era of the Fourth Industrial Revolution. Singapore: Palgrave Macmillanp; 2018. p.2-4.

9. Venter C. Life at the Speed of Light: From the Double Helix to the Dawn of Digital Life. New York: Penguin Books; 2016. p.25-63.

10. Zandi M. Preliminary Research in Cybercrime. Tehran: Jangal Publications; 2015. p.19-20. [Persian]

11. Sadri M. Electronic Transactions, Principles-Nature-Legitimacy. Tehran: Legal Thoughts; 2012. p.32-33. [Persian]

12. Casey E. Digital Evidence and Computer Crime. Maryland: Elsevier; 2011. p.37-38.

13. DiEuliis D, Murch R. Mapping the Cyber Biosecurity Enterprise. London: Frontiers Media SA; 2019. p.56-57.

14. Goodman M. Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It. New York: Knopf Doubleday Publishing Group; 2015. p.41-51.

15. Lisa I. The Patentability of Synthetic Biology Inventions New Technology, Same Patentability Issues. Hannover: the registered company Springer Nature Switzerland AG; 2020. p.7, 65.

16. Payne B, Payne K, Wu H. ICCWS 2020 15th International Conference on Cyber Warfare and Security. Hague: Academic Conferences and Publishing Limited; 2020. p.370-376.

17. Marchisio A. Computational Methods in Synthetic Biology. Washington: Humana Springer; 2021. p.169-170.

18. Watson J, Berry A, Davies K. DNA: The Story of the Genetic Revolution. London: Alfred A. Knopf; 2017. p.3-6, 8-10.

19. Bruinsma G, Johnson S. The Oxford Handbook of Environmental Criminology. Oxford: Oxford University Press; 2018. p.1-35.

20. Elsan M. Cyberspace Law. Tehran: Shahredanesh; 2018. p.165-166. [Persian]

21. Owen T, Noble W, Speed F. New Perspectives on Cybercrime. New York: Palgrave Macmillanp; 2017. p.119-120.

22. Ziber U. Computer Crimes. Translated by Noori MA, Rahimi A. Tehran: Ganj-e Danesh; 2011. p.18-19.

23. Arai K. Advances in Information and Communication: Proceedings of the 2021 Future of Information and Communication Conference. London: Springer; 2021. p.665-669.

24. Carlson R. Biology Is Technology: The Promise, Peril, and New Business of Engineering Life. Washington: Harvard University Press; 2010. p.129-130.

25. Trump B, Cummings C, Linkov I, Kuzma J. Synthetic Biology 2020: Frontiers in Risk Analysis and Governance. London: Springer International Publishing; 2019. p.380-384.

26. Zimmerman C. Ten Strategies of a World-Class Cybersecurity Operations Center. London: MITRE Corporation; 2014. p.11-22.

27. Reagan J, Singh M. Block chain Technologies Management 4.0: Cases and Methods for the 4th Industrial Revolution. Singapore: Springer Singapore; 2020. p.80.

28. Jalali Farahani A. An Introduction to the Criminal Procedure Code of Cybercrime. Tehran: Khorsandi Publications; 2010. p.177-178. [Persian]

29. Skilton M, Hovsepian F. The 4th Industrial Revolution Responding to the Impact of Artificial Intelligence on Business. Gewerbestrasse: Palgrave Macmillanp; 2018. p.83-84.

30. Ashenden S. The Era of Artificial Intelligence, Machine Learning, and Data Science in the Pharmaceutical Industry. London: Elsevier Science; 2021. p.11-17.

31. Metzl J. Hacking Darwin: Genetic Engineering and the Future of Humanity. London: Sourcebooks; 2019. p.21-24.

32. Wong K. Big Data Analytics in Genomics. London: Springer International Publishing; 2016.p.1-3.