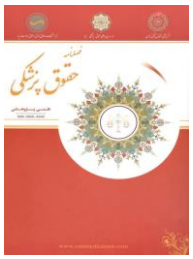
MLJ

مجله حقوق پزشکی

ویژه نامه نوآوری حقوقی، ۱۴۰۰

Journal Homepage: http://ijmedicallaw.ir



مقاله پژوهشی

# واکاوی تهدیدات و جرایم بیوسایبری

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

۱. دانشجوی دکتری حقوق جزا و جرم‌شناسی، گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.

۲. استادیار، گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.

۳. استادیار، گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.

۴. استادیار، گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.

## اطلاعات مقاله

تاریخ دریافت: ۱۴۰۰/۰۲/۱۳

تاریخ پذیرش: ۱۴۰۰/۰۶/۲۰

تاریخ انتشار: ۱۴۰۰/۱۱/۰۷

## واژگان کلیدی:

زیست‌شناسی

سایبر

جرم

امنیت

هوش مصنوعی

* نویسنده مسؤول:

محسن شکرچی‌زاده

آدرس پستی: ایران، نجف آباد، دانشگاه آزاد اسلامی، واحد نجف آباد، گروه حقوق.

کد پستی: ۸۵۱۴۱-۴۳۱۳۱

تلفن: ۳۱-۴۲۲۹۲۹۲۹

پست الکترونیک:

Mohsen.Shekarchi@gmail.com

## چکیده

**زمینه و هدف:** تعامل و وابستگی انجام تحقیقات با رایانه و وابستگی روزافزون آن به فضای سایبر و تأثیر فن‌آوری‌های نوظهور و نیازهای جدید در حوزه تجاری و بهره‌وری بیشتر از نیروی کار و ارتقاء عملکرد تجاری با در اختیار گرفتن جدیدترین فن‌آوری‌های کاملا خودکار در فضای مجاری، فعالیت‌های در حال انجام در بخش مربوط به بیوسایبر را در آغاز مرحله جدیدی از نوآوری و پیشرفت قرار داده است.

**مواد و روش‌ها:** این تحقیق از نوع نظری بوده روش تحقیق به صورت توصیفی تحلیلی می‌باشد و روش جمع‌آوری اطلاعات بصورت کتابخانه‌ای است و با مراجعه به اسناد، کتب و مقالات صورت گرفته است.

**یافته‌ها:** دیر یا زود پیشرفت‌های علمی با هدف افزایش رفاه و تأمین خدمات، خود را بر تمامی جوامع تحمیل خواهند کرد. مسئله 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. نوآوری‌های اخیر در علوم بیولوژیکی می‌توانند در بهره‌مندی از فضای سایبر به عنوان یک بستر گسترده، برای انجام فعالیت‌های غیرقانونی و بر علیه نظم و امنیت اجتماعی مورد استفاده قرار گیرند.

**ملاحظات اخلاقی:** در تمام مراحل نگارش پژوهش حاضر، ضمن رعایت اصالت متون، صداقت و امانت‌داری رعایت شده است.

**نتیجه‌گیری:** رخدادهای اخیر علمی در حوزه ژنتیک بخصوص 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 بخصوص فرصت‌طلبان در جهت منافع مادی و شخصی، که می‌توانند مرتکبان بالقوه‌ای باشند، باز شده است. مرتکبان فوق حرفه‌ای که حتی خود را مجرم نمی‌دانند؛ در نتیجه کنترل بروز و گسترش جرایم بیولوژیکی مبنتی بر فضای سایبر، نه تنها به عنوان یکی از مولفه‌های میزان امنیت ملی در هر کشوری محسوب می‌شود بلکه می‌تواند دارای اهمیتی مضاعف باشد.

## ۱. مقدمه

رسالت اصلی هنجارهای حقوقی، در واقع تنظیم کردن روابط میان تابعان حقوق است. در روند تولد هنجارهای حقوقی، ابتدا نیازهایی برای تابعان حقوق ایجاد می‌شود و تابعان برای رفع نیازهای خود، روابطی را با یکدیگر ایجاد می‌کنند. در هنگامهٔ روابط مزبور، تابعان به دنبال تأمین منافع خود هستند. در اینجاست که تأمین منافع بستگی به میزان قدرت دارد. در نتیجه هرچه میزان قدرت بیشتر باشد، منافع بیشتری نیز تأمین می‌شود. از این رو لازم است که هنجارهایی وجود داشته باشند تا قدرت را مهار کنند. این هنجارها ابتدا در قامت هنجارهای اخلاقی و سپس در قامت هنجارهای حقوقی در فضای روابط میان تابعان حقوق، متولد می‌شوند. در نتیجه نظم و شکل هنجارهای حقوقی و اخلاقی تا حدود زیادی، سایه‌ای از نظم و شکلِ نیازها، منافع و قدرت و در یک کلام «فضای روابط تابعان حقوق» است. در حال حاضر از یکسو با سایه انداختن فضای پست مدرنیزم بر زندگی بشر، فضای روابط نیز با پیچیدگی‌ها و چالش‌هایی مواجه شده است و از سوی دیگر اصول و قواعد عالم حقوق از بدو تولد برای مواجهه با این چالش‌ها طراحی نشده‌اند. نتیجهٔ منطقی این فضا، پیچیده شدن مناسبات مفاهیم، اصول و قواعد حقوقی است.

در فضای روابط میان تابعان حقوق، متغیرهای مختلفی وجود دارد. یکی از این متغیرها، پیشرفت صنعت و فضای سایبری است. تعامل و وابستگی انجام تحقیقات با رایانه و وابستگی روزافزون آن به فضای سایبر و تأثیر فن‌آوری‌های نوظهور و نیازهای جدید در حوزه تجاری و بهره‌وری بیشتر از نیروی کار و ارتقاء عملکرد تجاری با در اختیار گرفتن جدیدترین فن‌آوری‌های کاملا خودکار در فضای مجاری، فعالیت‌های در حال انجام در بخش مربوط به بیوسایبر را در آغاز مرحله جدیدی از نوآوری و پیشرفت قرار داده است.

با توجه به این موضوع و اینکه علوم مبتنی بر فضای سایبر و نیز علوم بیولوژیکی (زیست‌محیطی) به سرعت در حال همبستگی و همگرایی بوده و قطعا 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. همچنین در این مقاله تلاش می‌شود تا به سیاست‌گذاران و همچنین متولیان بخش سلامت، پیامدهای وابستگی روزافزون زیست‌شناسی و فضای سایبر که در بسیاری موارد به تهدیدات رفتارهای تهدیدآمیز، آسیب‌زا و مجرمانه علیه حوزه سلامت منجر شده است، را با رویکردی تحلیلی ارائه دهد. همچنین به این سؤال پاسخ داده می‌شود که چگونه فضای سایبر می‌تواند بستری برای ایجاد تهدید و ارتکاب جرایم بیولوژیکی باشد؟

در پاسخ به این پرسش، این فرضیه مورد بحث قرار خواهد گرفت که، رخدادهای اخیر علمی در حوزه ژنتیک بخصوص در بخش مطالعات مربوط به (DNA) نیز کارگزاری انواع ریزتراشه‌ها در بدن انسان‌ها و سایر جانداران، گویای این واقعیت است که پنجره جدیدی به روی کاربران سایبری و بخصوص فرصت‌طلبان در جهت منافع مادی و شخصی، که می‌توانند مرتکبان بالقوه‌ای باشند، باز شده است. برای این منظور، برخی تهدیدات و جرایم بیوسایبری را که قابلیت پیامدهای آسیب‌زا دارند بویژه در بخش زیست‌شناسی مصنوعی و یا هک کردن DNA متذکر می‌شویم و درمی‌یابیم که چگونه تهدیدات و جرایم بیوسایبری می‌توانند قدرت نقش‌آفرینی بالایی در جهت اهداف نامشروع داشته باشند و نیز می‌توانند بسیاری از حوزه‌های دیگر را نیز تحت تأثیر قرار دهند.

## ۲. ملاحظات اخلاقی

در تمام مراحل نگارش پژوهش حاضر، ضمن رعایت اصالت متون، صداقت و امانت‌داری رعایت شده است.

## ۳. مواد و روش‌ها

این تحقیق از نوع نظری بوده روش تحقیق به صورت توصیفی تحلیلی می‌باشد و روش جمع‌آوری اطلاعات بصورت کتابخانه‌ای است و با مراجعه به اسناد، کتب و مقالات صورت گرفته است.

## ۴. یافته‌ها

یافته‌های پژوهش حاضر نشان می‌دهد که، دیر یا زود پیشرفت‌های علمی با هدف افزایش رفاه و تأمین خدمات، خود را بر تمامی جوامع تحمیل خواهند کرد. مسئله 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 (۱). نوآوری‌های اخیر در علوم بیولوژیکی می‌توانند در بهره‌مندی از فضای سایبر به عنوان یک بستر گسترده، برای انجام فعالیت‌های غیرقانونی و بر علیه نظم و امنیت اجتماعی مورد استفاده قرار گیرند. تهدیدات و جرایم بیوسایبری به عنوان یک رشته ترکیبی در حال ظهور و مرتبط با حوزه‌های بیولوژیکی (زیستی) مختلف بر پایه فضای مجازی و اینترنت شناخته می‌شود (۲) و در پی آن، امنیت سایبری و امنیت بیوسایبری اهمیت ویژه‌ای پیدا می‌کند. اصطلاح اخیر -با توجه به نام و کاربرد اصطلاح- 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، محافظت در برابر تهدیدات مرتبط و کاهش آنها است.

## ۵. بحث

### ۵-۱. پیشینه تحقیق

مقالهٔ «تهدیدات سایبری و تأثیر آن بر امنیت ملی» نوشتهٔ علی خلیلی پورکن آبادی و یاسر نورعلی وند که در سال ۱۳۹۱ به چاپ رسیده است. مقاله حاضر 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 می‌توان گفت 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 نه تنها باعث شده دولت‌های کوچک از ظرفیت بیشتری برای اعمال قدرت در این فضا برخوردار شوند، بلکه منجر به ورود بازیگران جدیدی همچون شرکت‌ها، گروه‌های سازمان‌یافته 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 (۳).

مقالهٔ «تأثیر تهدیدات امنیتی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن» نوشتهٔ سید محمدرضا موسوی و همکاران که در سال ۱۳۹۲ به چاپ رسیده است. از نظر نویسندگان، امروزه گسترش فضای سایبر باعث پیدایش مرزهای مجازی شده و از این جهت درک واقع بینانه 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 جهانی شدن برای کشورها را باید در حوزه سایبری دانست که نمونه بارز آن حمله رایانه‌ای به تأسیسات هسته‌ای و الکترونیکی ایران توسط آمریکا می‌باشد. مقاله حاضر درصدد بررسی تأثیر تروریسم سایبری بر امنیت ملی کشورمان است. جهانی شدن -که یکی از ابزارهای آن، فن‌آوری‌های سایبری می‌باشد- 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 جرایم فراملی در فضای مجازی می‌باشد. نوع پیشگیری، مقابله و مبارزه با این جرم، با نوع اقدامات کنترلی در سایر جرایم به کلی متفاوت می‌باشد. در جرم تروریسم سایبری، جرم فاقد محل وقوع می‌باشد. این جرم عموما فرامرزی بوده 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 (۴).

### ۵-۲. نوآوری تحقیق با عنایت به تحقیقات مشابه

همانطور که در قسمت پیشین مشاهده شد، جرائم فضای سایبری مورد توجه نویسندگان و پژوهشگران به صورت پراکنده قرار گرفته است اما تا جایی که نگارندگان جست و جو نموده‌اند، در ارتباط با تهدیدات و جرائم بیوسایبری ادبیات نویسندگان حقوقی و روابط بین‌المللی سابقه‌ای وجود ندارد.

### ۵-۳. اهمیت و ضرورت پژوهش

از یک سو خدمات متقابل سایبری و زیست‌محیطی (بیولوژیکی)، بسیار امیدوارکننده و الهام‌بخش، پدید آمدن و شکوفایی قابل تحسین را در روزهای پیش رو نوید می‌دهد، از سوی دیگر، اهداف بسیار مادی‌گرایانه و خودخواهانه برخی دولت‌ها و سازمان‌ها و نهادهای علمی وابسته، در بخش‌های زیادی موفقیت‌های علمی قابل ستایش را از مسیر حقیقی و راستین خود منحرف نموده و به تهدیدی علیه بشریت تبدیل و باعث کم رنگ‌تر شدن فضای اعتماد عمومی در سطح داخلی و بین‌المللی می‌شود (۵).

آگاهی از آسیب‌های زیست‌محیطی که جوامع پیشرفته از نظر فناوری بر اکوسیستم‌های طبیعی وارد می‌کنند به عنوان یکی از دلایل از بین رفتن تدریجی اعتماد است. اکنون که بسیاری از کشورها در مواجه با تغییرات فنی و فن‌آوری، 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 احیاء زیرساخت‌های مناسب، خود را در شرایط رقابت قرار دهند (۶). لذا این موضوع به عنوان یک نگرانی و چالش جدی برای جوامع در عصر جدید دارای اهمیتی مضاعف بوده و با توجه به سطح نگرانی که در جامعه نسبت به این موضوع با توجه به اتفاقات اخیر از جمله بیماری ناشی از بیماری کوئید ۱۹ وجود دارد و در حال افزایش نیز هست، لزوم پرداختن به این موضوع را دوچندان می‌کند.

### ۵-۴. محدودیت‌های پژوهش

با در نظر گرفتن متغیرهای پژوهش حاضر، در ارتباط با محدودیت‌های این پژوهش باید عنایت داشت که، تهدیدات و جرائم حوزهٔ سایبری بسیار گسترده می‌باشند اما در پژوهش حاضر صرفاً تهدیدات و جرائم بیوسایبری مدنظر نویسندگان قرار دارد؛ در نتیجه سایر حوزه‌های تهدیدات سایبری در قلمرو موضوعات پژوهش حاضر قرار نمی‌گیرد.

### ۵-۵. فضای سایبر

هرچند در فارسی واژه سایبر را به مجاز و مجازی و فضای سایبر را نیز فضای مجازی به کار می‌برند لکن این ترجمه دقیق نبوده و گویای این واژه نیست. زیرا محیط سایبر محیطی حقیقی و واقعی است و نه مجازی و یا غیرواقعی. جهان سایبر هرچند به شکل مادی و ملموس احساس‌شدنی نیست اما همچنان که به اطلاعات ناشی از امری نمی‌توان عنوان مجازی داد به فضای سایبر هم نمی‌توان فضای مجازی گفت.

از محیط سایبر به محیط فن‌آوری 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 فن‌آوری و اطلاعات نیز گفته می‌شود (۷). 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. چرا که فضای سایبر شامل ارتباطات صورت گرفته 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 ارائه‌کنندگان خدمات اینترنتی فراهم می‌کند (۸).

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 بین‌رشته‌ای از محققان و مربیان حل شود (۹). در شبکه‌های اجتماعی در حال تحول، اخبار جعلی، حسادت و احساساتی بودن افراد نسبت به پست‌های یکدیگر و پست‌های نژادپرستانه یا زن‌ستیز 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 دو لبه 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 (۱۰). 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 جهانی‌تر شدن سیتیزن سایبری می‌شود.

### ۵-۵-۱. جرایم رایانه‌ای و سایبری

در مورد جرایم رایانه‌ای و جرایم سایبری، این نکته مورد توجه است که در غالب موارد، شباهت کاربردی و ترجمه‌ای، منتج به این ابهام شده است که این دو بصورت یکسان دیده شوند. در واقع این دو اصطلاح با وجودی که مرز مشخصی ندارند، صرفا از جرایم سایبری، می‌توان بصورت عام استفاده کرد.

جرایم رایانه‌ای عمدتاً به مجموعه جرایمی محدود مانند جرایمی شامل سرقت خدمات رایانه‌ای و دسترسی غیرمجاز به رایانه‌های محافظت شده اشاره دارد. برای تطبیق دادن با این شرایط ابهامی، اصطلاح عمومی‌تر مربوط به رایانه، برای هر جرمی که شامل رایانه‌ها و شبکه‌های اینترنتی باشد، به کار می‌رود، از جمله جرایمی که وابستگی زیادی به رایانه ندارند. از آنجا که هر جرمی می‌تواند شامل رایانه‌ها نیز باشد، مشخص نیست که کجا مرز بین جرایم ارتکابی با استفاده از رایانه و جرایمی 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 (۱۱).

### ۵-۶. زیست‌شناسی مصنوعی

با نگاهی به آینده اما، برخی اندیشمندان حوزه علم و محیط زیست، عصر پساصنعتی تمدن غربی را نوید داده‌اند. با اعتقاد راسخ وینتر که در کتاب زندگی با سرعت نور به آن اشاره می‌کند، در دهه‌های آینده سهم عمده‌ای که علم می‌تواند به انسان ببخشد ازدواج زیست‌شناسی با فناوری‌های دیجیتال (سایبری) 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 (۱۲).

«کافی است: مهندسی ژنتیک و پایان ماهیت آدمی» عنوان کتابی است که نویسنده آن بیل مک کیبن است و نتایج حاصل شده نسبت به زیست‌محیط را با نگاهی نقّادانه 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 به اصطلاح، خودتان به عنوان علاقه‌مندان به زیست‌شناسی می‌توانید برخی کارهای مربوط را انجام دهید. تعامل آنلاین بین مهندسین بیولوژی و شرکت‌های هم نهاد و خدماتی DNA به عنوان یک حامل نوعی حمله اضافه شده است که از طریق آن حملات اضافی

بارگزاری شده 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 استفاده شده 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 و همچنین نگرانی‌هایی است که از نظر علمی، اخلاقی، ایمنی و نظارتی ایجاد می‌کند. زیست‌شناسی مصنوعی ایجاد سیستم‌های جدید بیولوژیکی را مفروض می‌داند که می‌توانند برای انجام وظایف تعیین شده 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 منشا این انتشار برای بروز خطرات می‌تواند 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 غیرقابل دستیابی است.

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

استفاده دوگانه از زیست‌شناسی مصنوعی به عنوان یک فناوری قدرتمند به نفع بشریت و به عنوان یک سلاح بالقوه، مسئله‌ای 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 اضافه کردن 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).

تلاش‌های طولانی مدت در جامعه زیست‌شناسی مصنوعی برای آگاهی از کاربردهای بالقوه امنیتی از این فن‌آوری‌ها هزینه‌های بالایی را پرداخت کرده و 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 فن‌آوری‌های اختراع، پیشرفت و فروش آنها هستند (۱۸).

### ۵-۷. تهدیدات و جرایم بیولوژیکی

امکان دستکاری و شبیه‌سازی ژنتیکی انسان با وجود ابراز امیدواری طرفداران برای درمان‌های بسیار موثرتر 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 برخی جهات، این بحث‌ها، ترس و جذابیت پیرامون سایبورگ را تکرار می‌کند (۵).

وقتی بیشتر ما به فن‌آوری‌های 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 فرصت‌های ما، 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 (۱۹).

با انجام این تحول، کاربردهای فن‌آوری‌های ژنتیکی برای تغییر وراثت ژنتیکی انسان‌ها به طور فزاینده‌ای بحث برانگیز می‌شود. به این فکر کنید که چگونه افراد نسبت به تبدیل ساختار جدید محصولات اصلاح شده ژنتیکی (GMO) یا تراریخته واکنش نشان می‌دهند، حتی اگر هیچ شواهدی وجود نداشته باشد که نشان دهد مصرف محصولات (GMO) برای مردم خطرناک‌تر از محصولات غیر (GMO) است. به همه جنجال‌ها و خشونت‌هایی که بحث سقط جنین را همراهی کرده‌اند فکر کنید. اگر مردم راغبند به دلیل اختلاف‌نظر در مورد محصولات تراریخته و سقط جنین، به خشونت متوسل شوند، تصور کنید که وقتی مسئله 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 یک سری اقدامات مخفیانه و از نظر نگارنده غیراخلاقی 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 موثرتر ویرایش ژن انسانی وراثتی انجام می‌شود (۱۹).

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 بطور اساسی روش تولیدمثل 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 که با تشویق یا اقناع تصمیم به ماندن در

شرایط قبل کنند، با قوانین بین‌المللی یا زور مجبوربه همراهی کنند؟ یا اینکه آنها تصمیم می‌گیرند که جهان در حال تغییر است و در صورت تمایل به ادامه راه، چاره‌ای جز انتخاب ندارند؟ بـه راحتی می‌تـوان فهمید کـه چگونه ایـن مسئله می‌تواند به یک مسئله کاملاً دشوار، پیچیده، بحث برانگیز 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 فن‌آوری‌های ژنتیکی (و سایر فناوری‌ها) را به گونه‌ای توسعه دهند که هدف اصلی آن بهینه‌سازی برای مصلحت عمومی و به حداقل رساندن هرگونه آسیب احتمالی و خطر ایجاد تعارض در این مسیر باشد. اما کارهای خیلی کمی انجام شده است (۱۹). واقعیت غیر قابل انکار استفاده از این فناوری در بخش نظامی است که به عنوان سلاح‌های بیولوژیکی مورد استفاده قرار گرفته است. اما نکته مورد بحث این است که این سلاح‌ها به بخش سایبری با حفظ اهداف ضد حیات انسانی خود نیز ورود کرده‌اند.

جرایم 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 جرایم فعلی باشند، هم با افـزایش در میـزان داده‌های بیولوژیـکی و هم با کاهش هزینه‌های فناوری استفاده شده امکان‌پذیرند، تعریف شده است. علاوه بر این، در حالی که مقادیر بیشتری از داده‌های بیولوژیکی در حال انجام 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 بـه سیستم‌های خودکار کنترل‌شده توسط کامپیوتر بستگی دارد. این کارایی همچنین فرصت‌های جدیدی را برای وقوع جرایم بیولوژیکی ایجاد می‌کند. در نتیجه، همانطور که در بالا ذکر شد، جرایم بیولوژیکی در اینجا مفهوم‌سازی شده است و شامل جرائمی است که شامل سیستم‌های بیولوژیکی و سایبری برای ارتکاب جرایم کاملاً جدید، جرایم سنتی یا ترکیبی از این دو است. شکل‌های جرایم بیولوژیکی از طریق پروتکل‌ها -موافقت مقدماتی- جرم و آمادگی ما برای اقدام در نظر گرفته شده است (۲۰).

### ۵-۸. تهدیدات و جرایم بیوسایبری

ورود به عصر فناوری اطلاعات، بزهکاران را هم در بر 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 (۲۱). بنظر می‌رسد در بخش مربوط به زیست‌شناسی، بخش سوم بیشتر مورد استفاده قرار می‌گیرد. فعالیت‌ها و تهدیدهایی که در فضای اینترنت و غالبا بصورت آنلاین با آنها مواجه هستیم، هیچگاه نمی‌توان با قطعیت در مورد اینکه این تهدیدها واقعا جدی (دارای سوءنیت) هستند یا خیر اظهارنظر 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 ضداجتماعی آنلاین» می‌نامیم (۲۲). بنابراین نظر و همچنین بر طبق تعریف ارایه شده 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 غیرقانونی، غیراخلاقی یا غیرمجاز نسبت به پردازش خودکار و یا انتقال داده‌ها" تعریف کردند (۲۳). می‌توان فعالیت‌های غیرمجاز و تهدیدهایی که در این زمینه مورد مطالعه قرار می‌گیرند نیز موضوع جرایم سایبری قرار داد. بنابراین، صرف شامل شدن این رفتارها به عنوان بر هم زننده نظم اجتماع و در تقابل با آن، از آنها به عنوان جرم سایبری نام برده شده است. رفتارهای ضداجتماعی که هنوز ناشناخته مانده و در بسیاری موارد نامفهوم هستند و شاید برای جرم‌انگاری -در حوزه‌های اختصاصی- این رفتارها مدتی به طول بیانجامد.

در تعریف جرایم 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. جرایم بیوسایبری همچنین فعالیت‌های مجرمانه‌ای را که به وسیله ترکیبی از رایانه متصل به اینترنت و مواد بیولوژیکی و بیوشیمیایی انجام می‌شود را توصیف می‌کند (۲۰).

نویسندگان تحقیق "یک مرور سیستماتیک از پتانسیل جرم‌شناسی زیست‌شناسی مصنوعی و مسیرهای پیشگیری از جرم در آینده" اظهار می‌دارند که شایع‌ترین فرصت‌های جرم از طریق داده‌های بیولوژیک ناامن، فن‌آوری‌های زیست‌شناسی مصنوعی و مجموعه‌ای از پردازش داده‌های تولید شده آمده است. فن‌آوری‌های زیست‌شناسی مصنوعی با چهل و شش درصد از انواع جرایم شناسایی شده مرتبط بوده‌اند. همچنین چهل درصد از رایج‌ترین تهدیدات خارجی برای جرم زیست‌شناسی مصنوعی شناسایی شده، هکرهای زیستی و هکرها بوده‌اند (۲۰). 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 فن‌آوری، دولت، رویه‌های صنعتی و نگرش‌های فرهنگی متداول‌ترین فاکتورهای استنادی برای جرم موثر در زیست‌شناسی مصنوعی بودند. برای یک رویکرد پیشگیرانه موثر در برابر این خطرات جرایم نوظهور، توجه فوری و یک رویکرد پیشگیرانه خلاقانه لازم است (۲۰).

همچنان که 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 شناخته نشده‌ای 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 روبرو 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).

### ۵-۸-۱. امنیت بیوسایبری

امنیت بیوسایبری درک خطرات جدیدی است که در مرز بین فضای مجازی و زیست‌شناسی به منظور تدوین سیاست‌هایی برای مدیریت آنها بوجود آمده است. سیاست‌های ایمنی بیولوژیکی و امنیت بیولوژیکی برای کنترل تعداد محدودی از تهدیدهای بیولوژیکی از جمله عوامل بیماری‌زا تنظیم شده 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- بیولوژیکی هنگامی رخ می‌دهد که اطلاعات بیولوژیکی اندازه‌گیری، نظارت یا تغییر کرده 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 مخلوط کردن یک راکتور بیولوژیکی را کنترل می‌کند (۲۴).

در فرآیند تولید داروهای پروتئینی، آسیب‌پذیری‌های امنیت سایبری در هر نقطه‌ای که اطلاعات ژنتیکی از طریق سیستم‌های سایبری یا سایبری- 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 شبکه‌ای شده‌ای 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 زنده ماندن سلول‌ها آسیب‌پذیری ایجاد می‌کند، حتی اگر تأثیر واقعی بر روی سلول‌های ذخیره شده 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 (۲۴).

در این مثال‌ها، آسیب زدن، از کار انداختن، منحرف کردن، غیرقابل رویت و مخفی کردن و... اهدافی هستند که از وابستگی روزافزون جامعه علوم بیولوژیکی، مانند بسیاری علوم دیگر، ناشی می‌شود. این شرایط می‌تواند برای اهداف خصمانه‌تری نیز انجام شود و یا حتی بصورت سازمان‌یافته انجام گیرد. نکته قابل اهمیت در مورد 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 برنامه‌ریزی شده را مهیا می‌کنند. فلذا سئوالی که همواره مطرح است این است که اگر نفوذ غیرمجاز (هک) رخ دهد و انحراف یا دستکاری صورت گیرد، با وجود غیر قابل برگشت بودن تحولات شیمیایی و بیولوژیکی در زیست‌محیط، آیا می‌توان یک امنیت کامل و صد درصدی برای حفاظت از داده‌ها در این موارد ایجاد کرد؟

### ۵-۹. بیوهکرها و داده‌های ژنتیکی

جرایم 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 غیرمجاز 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 ایجاد شدن و غالب شدن تفکر انگیزه منفعت، سود و درآمد صرف در جهان، عناصر و عوامل بزه‌کار در فضای مجازی که در کارشان جدی و صرفا 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 طبقه‌بندی کردن آن به هوا، خشکی و دریا، سازمان‌های مربوطه جدیدی را برای تأمین امنیت در آن ایجاد نموده است (۱۴).

در ادامه فعالیت‌ها و نفوذهای غیرمجار 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 به سرعت 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 (۱۴).

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 سرقت رفته برای باج‌خواهی از افرادی که اطلاعات مخرب در DNA خود دارند، استفاده کنند (۲۵). این قابلیت با ورود حداکثری جوامع به عصر دیجیتال و استفاده حداکثری از اینترنت اشیاء و همچنین کاربرد پزشکی و یا نظارتی از ریزتراشه‌ها، بسیار پر اهمیت خواهد بود. داده‌های بیماران که بصورت 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. 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 (۲۶).

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، بدست آورد. همانطور که تجزیه و تحلیل DNA به برنامه‌های عملی روزمره راه پیدا می‌کند، خطر هک بیولوژیکی افزایش می‌یابد. آزمایش‌های مربوط نشان می‌دهد که DNA مخرب می‌تواند ترکیب شده و در ای.کولی، 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. ما شرح دادیم که با استفاده از تکنیک‌های کنترل ورودی اختصاصی مشابه روش‌های استفاده شده برای مقابله با حملات تزریق معمولی که می‌توان خطر هک بیولوژیکی را کاهش داد (۲۶).

در تحقیقی با عنوان "امنیت سایبری: تزریق DNA از راه دور، تهدیدی در زیست‌شناسی مصنوعی" نمونه‌هایی از حملات سایبری را اثبات می‌کند که در آن یک مرتکب یا مهاجم از راه دور یک قربانی را فریب می‌دهد تا یک ماده خطرناک را در آزمایشگاه قربانی تولید کند، 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 جرایم تروریستی علیه فضای بیوسایبر نیز استفاده کرد.

تروریست‌ها کارزار خود را از دنیای فیزیکی به فضای سایبر انتقال داده‌اند که بدیهی است، به دلیل قرار گرفتن در یک دنیای دیگر با شرایط و امکانات خاص و منحصر بفرد، سلاح‌ها و اهداف نیز ماهیت و کارکرد متمایزی از دنیای فیزیکی پیدا می‌کنند (۲۷).

واقعیت این است که برنامه‌های امنیت بیولوژیکی و ایمنی بیولوژیکی بسیار پرهزینه هستند و توسعه آنها کند است.

برعکس، تهدید سلاح‌های بیولوژیکی و خطرات توسط پتانسیل نامحدود برای صدمه زدن دارند، مضاعف می‌شود. استفاده از سلاح‌های بیولوژیکی توسط متجاوز می‌تواند باعث کشته شدن میلیون‌ها نفر، اخلال در جوامع، تضعیف اقتصاد و تغییر زندگی به همان شکلی که ما می‌شناسیم شود. بطور مشخص فضای سایبر خود قابلیت تبدیل شدن به بستری مناسب برای اینگونه اقدامات باشد.

### ۵-۱۰. آینده رابطهای سایبری-بیولوژیکی فعال شده توسط هوش مصنوعی

جان مک کارتی تعریف زیر را برای اصطلاح هوش مصنوعی که در سال ۱۹۵۵ ابداع کرده ارائه می‌دهد: هوش مصنوعی یک علمی است که مطالعه روند حل مسئله 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 (۲۸). هوش مصنوعی مدرن به دلیل قابلیت یادگیری بی‌سابقه در پردازش داده‌های پیچیده، بر علم داده‌های بیولوژیکی تسلط خواهد داشت (۲۹).

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 نظر گرفتن اجرای افزایشی و گسترده الگوریتم‌های یادگیری ماشین و قابلیت‌های گسترش‌دهنده هوش مصنوعی شوند. با نگاه به جلو، رایانه‌ها و زیست‌شناسی در همان حلقه مشابه کنترل یک منطقه در حال ظهور هستند که می‌توانند آسیب‌پذیری‌های جدید امنیت سایبری را به عنوان هوش مصنوعی و یادگیری ماشینی در مسیر اصلی هوش مصنوعی معرفی کند. در حالی که قابلیت‌های هوش مصنوعی فعلی بیشتر با یادگیری غیرفعال همراه است، سیستم‌هایی که قادر به یادگیری فعال هستند و شبکه‌های عصبی، در حال حاضر برای کاربردهای مختلف در حال توسعه هستند. با هر پیشرفت، امنیت سایبری و امنیت بیوسایبری ممکن است به طور کامل‌تری به یک رشته واحد و یکپارچه نزدیک شوند. از آنجایی که هوش مصنوعی کاربرد روزافزونی را در ساخت بیولوژیکی و انتقال از حالت کاملاً وابسته به حالت نیمه خودکار، به حالت کاملاً مستقل تغییر پیدا می‌کند، ارزیابی کاملی از آسیب‌پذیری‌ها و تهدیدها باید شامل راهکارهایی برای کاهش این موارد مخاطره‌آمیز باشد (۲۴).

اگرچه اینترنت برای هماهنگی تلاش برای تعیین توالی و به اشتراک‌گذاری ثمرات آن بسیار مهم بوده، اما بزرگترین پیشرفت تکنولوژیکی که توالی مقیاس بزرگ انسان را امکان‌پذیر می‌کند، توسعه ربات‌های توالی یابی فلورسانس لیزری با مهندسی عالی است (۳۰) 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 موردنظر 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 -یک زمینه در حال رشد به نام بیوانفورماتیک- که به آنها امکان می‌دهد کل ژنوم‌ها را بازنویسی و دوباره برنامه‌ریزی کنند (۳۱).

### ۶. نتیجه‌گیری

دیر یا زود پیشرفت‌های علمی با هدف افزایش رفاه و تأمین خدمات، خود را بر تمامی جوامع تحمیل خواهند کرد. مسئله 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. همچنان که 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 غیرقانونی و بر علیه نظم و امنیت اجتماعی مورد استفاده قرار گیرند. تهدیدات و جرایم بیوسایبری به عنوان یک رشته ترکیبی در حال ظهور و مرتبط با حوزه‌های بیولوژیکی (زیستی) مختلف بر پایه فضای مجازی و اینترنت شناخته

می‌شود و در پی آن، امنیت سایبری و امنیت بیوسایبری اهمیت ویژه‌ای پیدا می‌کند. اصطلاح اخیر -با توجه به نام و کاربرد اصطلاح- 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، محافظت در برابر تهدیدات مرتبط و کاهش آنها است.

در ادامه پژوهش، فرضیه بدین گونه به اثبات می‌رسد که، رخدادهای اخیر علمی در حوزه ژنتیک بخصوص در بخش مطالعات مربوط به (DNA) نیز کارگزاری انواع ریزتراشه‌ها در بدن انسان‌ها و سایر جانداران، گویای این واقعیت است که پنجره جدیدی به روی کاربران سایبری و بخصوص فرصت‌طلبان در جهت منافع مادی و شخصی، که می‌توانند مرتکبان بالقوه‌ای باشند، 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، توجیح این موضوع است که مراحل پیشگیری زودتر از آنچه که تصور میشد، بخصوص برای محافظت از حوزه زیستی بایستی هر جامعه‌ای در نظر گرفته شود.

جامعه علوم بیولوژیکی به طور سنتی تحت یک سیستم ناامن فعالیت می‌کند که انتظار دارد تمام کسانی که عضو، مرتبط یا شرکت‌کنندگان در این جامعه هستند، خود هنجارمند و با قواعد تنظیم و سازگار شوند و اغلب تهدیدهای امنیتی را بخوبی کنترل نمی‌کنند. اکنون که توالی، سنتز (ساخت یا ترکیب)، دستکاری و ذخیره‌سازی (DNA) به طور فزاینده‌ای دیجیتالی می‌شود، بیش از هر زمان دیگری عوامل خطرناک در داخل و خارج از جامعه برای به خطر 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- 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 کنند.

با دیدگاهی آینده‌نگرانه و مبتنی بر سناریوهای مختلف و انتخاب سیاست‌گذاری‌های متناسب و لحاظ آن در مدیریت کلان در نگاه به دستاوردهای علمی با محوریت جرایم بیوسایبری و امنیت بیوسایبری، آنچه می‌تواند قابل تأمل باشد ضروری بودن و الزامی بودن 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 و مدیریت شود. تعبیر جنون دانش برای فن‌آوری‌ها و ایده‌های در دست تحقیق شاید اصطلاح بجایی باشد زیرا برخی هیچگونه محدودیتی را نمی‌پذیرند و همچنان در جهت منافع مادی در مسیر خود می‌تازند. دارک نت یا بخش تاریک فضای سایبری چنان مملو از رفتارها، ایده‌ها و ابداعات غیراخلاقی و غیرانسانی مربوط به انحرافات بیوسایبری است که به یک چالش جدی و دغدغه بزرگ جامعه جهانی تبدیل خواهد شد. و نهایتا اینکه کنترل بروز و گسترش جرایم بیولوژیکی مبتنی بر فضای سایبر، نه تنها به عنوان یکی از مولفه‌های میزان امنیت ملی در هر کشوری محسوب می‌شود بلکه می‌تواند دارای اهمیتی مضاعف باشد.

## ۷. تقدیر و تشکر

از تمام عزیزانی که در تهیه و تدوین این پژوهش مساعدت و همکاری نمودند تقدیر و تشکر می‌کنم.

## 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. Partington M. Introduction to the English Legal System 2019-2020. Oxford: Oxford University Press, USA; 2019.

2. Siliquini-Cinelli L. Legal Positivism in a Global and Transnational Age. Dundee: Springer; 2019.

3. Khalili A, Nooralivand Y. Cyber threats and their impact on national security. *Strategic Studies.* 2012;15(2):167-96. (Persian).

4. Musavi M, Heydari K, 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):123-45. (Persian).

5. Connor S. The Cambridge companion to postmodernism. Cambridge: Cambridge University Press; 2004.

6. Czarniawska B, Joerges B. Robotization of work?: Answers from popular culture, media and social sciences. London: Edward Elgar Publishing; 2020.

7. Zandi M. Preliminary Research in Cybercrime. Tehran: Jangal Publications; 2015. (Persian).

8. Sadri M. Electronic Transactions, Principles-Nature-Legitimacy. Tehran: Legal Thoughts; 2012. (Persian).

9. Gleason NW. Higher education in the era of the fourth industrial revolution. Singapore: Palgrave Macmillanp; 2018.

10. Lim TW. Industrial revolution 4.0, tech giants, and digitized societies. Singapore: University of Social Sciences; 2019.

11. Casey E. Digital evidence and computer crime: Forensic science, computers, and the internet. Maryland: Elsevier; 2011.

12. Venter JC. Life at the speed of light: from the double helix to the dawn of digital life. New York: penguin Books; 2016.

13. Murch R, DiEuliis D. Mapping the cyberbiosecurity enterprise. London: Frontiers Media SA; 2019.

14. Trump BD, Cummings CL, Kuzma J, Linkov I. Synthetic Biology 2020: Frontiers in Risk Analysis and Governance. London: Springer; 2019.

15. De Lisa I. The Patentability of Synthetic Biology Inventions. Hannover: the registered company Springer Nature Switzerland AG; 2020.

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

17. Marchisio A. Computational Methods in Synthetic Biology. Washington: Humana Springer; 2021.

18. Carlson RH. Biology is technology. Washington: Harvard University Press; 2010.

19. Watson JD, Berry A, Davies K. DNA: The Story of the Genetic Revolution. London: Alfred A. Knopf; 2017.

20. Bruinsma GJ, Bruinsma G, Johnson SD. The Oxford handbook of environmental criminology. Oxford: Oxford University Press; 2018.

21. Elsan M. Cyberspace Law. Tehran: Shahrdanesh; 2018. (Persian).

22. Owen T, Noble W, Speed F. New Perspectives on Cybercrime. New York: Palgrave Macmillanp; 2017.

23. Ziber U. Computer Crimes. Tehran: Ganj-e-Danesh; 2011. (Persian).

24. Arai K. Advances in Information and Communication. Proceedings of the 2021 Future of Information and Communication Conference, London: Springer; 2021.

25. Zimmerman C. The strategies of a world-class cybersecurity operations center. London: MITRE Corporation; 2014.

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

27. Jalali Farahani A. An Introduction to the Criminal Procedure Code of Cybercrime. Tehran: Khorsandi Publications; 2010. (Persian).

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

29. Ashenden SK. The Era of Artificial Intelligence, Machine Learning, and Data Science in the Pharmaceutical Industry. London: Elsevier Science; 2021.

30. Metzl J. Hacking Darwin: Genetic engineering and the future of humanity. London: Sourcebooks, Inc.; 2019.

31. Wong K. Big Data Analytics in Genomics. London: Springer International Publishing; 2016.

The Iranian Association of Medical Law

MLJ

Medical Law Journal

2021; Legal Innovation

Journal Homepage: http://ijmedicallaw.ir

ORIGINAL ARTICLE

# Analysis of Bio-cyber Threats and Crimes

**Abbas Amiri[1], Mohsen Shekarchizadeh[2*], Ahmadreza Shekarchizadeh Esfahani[3], Gholamhossein Masoud[4]**

1. PhD Student Criminal Law and Criminology, Department of Law, Najafabad Branch, Islamic Azad University, Najafabad, Iran.
2. Assistant Professor, Department of Law, Najafabad Branch, Islamic Azad University, Najafabad, Iran.
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.

## ARTICLE INFORMATION

**Received:** 3 May 2021

**Accepted:** 11 September 2021

**Published online:** 27 January 2022

**Keywords:**

Biology

CybeR

Crime

Security

Artificial Intelligence Judgment

*** Corresponding Author:**

Mohsen Shekarchizadeh

**Address:** Department of Law, Najafabad Branch, Islamic Azad University, Najafabad, Iran.

**Postal Code:** 85141-43131

**Telephone:** 31-42292929

**Email:** Mohsen.Shekarchi@gmail.com

## ABSTRACT

**Background and Aim:** Interaction and dependence of research with computer and its increasing dependence on cyberspace and the impact of emerging technologies and new needs in the field of business and greater productivity of the workforce and promotion of business performance by acquiring the latest fully automated technologies in cyberspace, Puts ongoing activities in the biosyber sector at the beginning of a new phase of innovation and progress.

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

**Results:** Sooner or later, scientific advances will impose themselves on all societies with the aim of increasing welfare and providing services. The point to consider is that this situation, like other human achievements, will be accompanied by very worrying threats that special measures must be taken to deal with them. Recent innovations in the biological sciences can be used to take advantage of cyberspace as a broad platform for illegal activities against social order and security.

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

**Conclusion**: Recent scientific developments in the field of genetics, especially in the field of DNA studies, as well as the implantation of microchips in the bodies of humans and other living things, indicate the fact that a new window on cyber users, especially opportunists, for material and personal gain, which Can be potential perpetrators, is open. Super-professional perpetrators who do not even plead guilty; As a result, controlling the occurrence and spread of biological crimes based on cyberspace is not only considered as a component of national security in any country, but can be doubly important.



**Cite this article as:** Amiri A, Shekarchizadeh M, Shekarchizadeh Esfahani A, Masoud Gh. Analysis of Bio-cyber Threats and Crimes. *Medical Law Journal* 2021; Legal Innovation.