Comparative Studies in Jurisprudence, Law, and Politics

Study of Cyber-Related Crimes and Harmful Effects in the Armed Forces and Prevention Policies

1. Mohammad Amirmohammadi: Ph.D. Student, Department of Criminal Law and Criminology, Kish International Branch, Islamic Azad University, Kish Island, Iran
2. Saleh Abdinezhad*: Visiting Assistant Professor, Department of Law, Kish International Branch, Islamic Azad University, Kish Island, Iran. Email: silahlawyer29@gmail.com (Corresponding Author)
3. Alireza Shekarbeigi: Assistant Professor, Department of Law, Payame Noor University, Tehran, Iran.

ABSTRACT

In today's world, alongside the process of globalization and the expansion of media and cyberspace, crimes committed within the framework of this process and space have also increased, giving rise to a new spectrum of crimes. This issue is even more pronounced with regard to the armed forces due to their sensitive position in ensuring security. Therefore, this article aims to explore legal texts, existing laws, and relevant documents while addressing the various crimes committed in cyberspace and proposing appropriate preventive policies in this regard. The article raises the question: What are the most significant crimes related to the armed forces in cyberspace? And what preventive policies, suitable for the harms and crimes in the realm of cyberspace within the armed forces, can be adopted? In response, the hypothesis proposed is that "cyber espionage, disclosure of confidential information and data, negligence, recklessness, failure to comply with governmental regulations, and participation in protest campaigns are the most significant crimes in this domain. Therefore, fostering a culture of cyberspace usage, localizing it, promoting critical thinking, teaching media literacy, criminalizing, and planning deterrent measures in legislation are proposed as the most important preventive policies for cyber-related harms and crimes in the armed forces." The conclusion of the article shows that factors related to cyberspace, the physical environment, and the individual characteristics of armed forces personnel play a significant role in the occurrence of cyber-related harms and crimes in these forces.

Keywords: *Cyber crimes, prevention policy, cyberspace, armed forces.*

How to cite: Amirmohammadi, M., Abdinezhad, S., & Shekarbeigi, A. (2024). Study of Cyber-Related Crimes and Harmful Effects in the Armed Forces and Prevention Policies. *Comparative Studies in Jurisprudence, Law, and Politics*, *6*(4), 285-304.

Submit Date: 30 November 2024
Revise Date: 06 December 2024
Accept Date: 21 December 2024
Publish Date: 31 December 2024

پژوهش‌های تطبیقی فقه،
حقوق و سیاست

مطالعه آسیب‌ها و جرایم مرتبط با فضای مجازی و سیاست‌های پیشگیری از آن‌ها در نیروهای مسلح

۱. محمد امیرمحمدی: دانشجوی دکتری،گروه حقوق جزا و جرم‌شناسی واحدبین المللی کیش، دانشگاه آزاد اسلامی، جزیره کیش، ایران
۲. صالح عبدی نژاد*: استادیار مدعو، گروه حقوق، واحد بین المللی کیش، دانشگاه ازاد اسلامی، جزیره کیش، ایران. پست الکترونیک: silahlawyer29@gmail.com (نویسنده مسئول)
۳. علیرضا شکربیگی: استادیار،گروه حقوق، دانشگاه پیام نور، تهران، ایران.

چکیده

امروزه همزمان با فرآیند جهانی شدن و گسترش رسانه‌ها و فضای مجازی جرائم مرتکب شده در بستر این فرایند و فضا نیز افزایش یافته و طیف جدیدی از جرائم را به وجود آورده است این مسئله در خصوص نیروهای مسلح با توجه به موقعیت حساس آن‌ها در تامین امنیت به مراتب شدیدتر می‌باشد. از این رو مقاله حاضر تلاش دارد تا با واکاوی متون حقوقی، قوانین موجود و اسناد مربوطه ضمن پرداختن به اعم جرائم ارتکابی در بستر فضای مجازی، سیاست‌های پیشگیرانه مناسب در این راستا ارائه دهد. در مقاله این سوال مطرح است که مهمترین جرائم مربوط به نیروهای مسلح در فضای مجازی کدامند؟ و چه سیاست‌های پیشگیرانه مناسبی متناسب با آسیب‌ها و جرایم حوزه‌ی فضای مجازی در نیروهای مسلح می‌توان اتخاذ نمود؟ در پاسخ این فرضیه مطرح است که «جاسوسی سایبری، افشای اطلاعات و داده‌های محرمانه، بی‌احتیاطی یا بی‌مبالاتی یا سهل‌انگاری یا عدم رعایت نظامات دولتی و شرکت در کمپین‌های اعتراضی مهمترین جرائم مربوطه در این حوزه بوده و لذا متناسب با این جرائم نهادینه کردن فرهنگ استفاده از فضای مجازی، بومی‌سازی آن، رشد تفکر انتقادی، آموزش سواد رسانه‌ای، جرم‌انگاری و برنامه‌ریزی بازدارنده در حوزه قانونگذاری به عنوان مهمترین سیاست‌های پیشگیرانه آسیب‌ها و جرایم حوزه‌ی فضای مجازی در نیروهای مسلح پیشنهاد می‌شود.» نتیجه‌گیری مقاله نشان می‌دهد که عوامل مرتبط با فضای مجازی، فضای فیزیکی و ویژگی‌های فردی کارکنان نیروهای مسلح در بروز آسیب‌ها و جرایم سایبری مربوط به این نیروها مؤثر می‌باشند.

واژگان کلیدی: *جرائم سایبری، سیاست پیشگیری، فضای سایبری، نیروهای مسلح.*

نحوه استناددهی: امیرمحمدی، محمد.، عبدی‌نژاد، صالح. و شکربیگی، علیرضا. (۱۴۰۳). مطالعه آسیب‌ها و جرایم مرتبط با فضای مجازی و سیاست‌های پیشگیری از آن‌ها در نیروهای مسلح. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، ۶(٤)، ۳۰٤-۲۸۵.

تاریخ ارسال: ۱۰ آذر ۱٤۰۳
تاریخ بازنگری: ۱٦ آذر ۱٤۰۳
تاریخ پذیرش: ۳۰ آذر ۱٤۰۳
تاریخ چاپ: ۱۰ دی ۱٤۰۳

مقدمه

رشد سریع فناوری و پیشرفت روزافزون در حوزه‌های اطلاعاتی، ارتباطی، ماهواره‌ها و اینترنت موجب شکل‌گیری تحولات پرشتاب در جوامع بشری شده و آثار مثبت و منفی فراوانی را به دنبال داشته است. در این بین آثار اینترنت و فضای مجازی در شکل‌گیری ارتباطات بیش از سایر حوزه‌ها بوده و تغییرات و دگرگونی‌های بسیاری را پدید آورده است. امروزه شبکه‌های اجتماعی به‌عنوان بزرگترین دستاورد اینترنت و فضای مجازی به‌دلایل مختلف از جمله نامحدود بودن ارتباطات، بی‌هویت بودن، آزادی بسیار زیاد، بی‌مکانی و بی‌زمانی کاربران و... با اقبال عموم مواجه شده و فعالیت‌هایشان گسترش یافته است (Amani Kalarijani, 2016)؛ اما با گسترش استفاده آحاد جامعه از فضای مجازی، چالش‌های نوینی در حوزه‌ی آسیب‌شناسی اجتماعی و جرم‌شناسی فضای مجازی پدید آمده است. برخی از این آسیب‌ها و جرایم در فضای حقیقی کم‌وبیش وجود داشته‌اند و فضای مجازی نقشی تسهیل‌کننده، مکمل و یا سرریز را در این رابطه ایفا می‌نماید. همزمان با گسترش عمومی استفاده از فضای مجازی توسط شهروندان، نیروهای مسلح نیز به‌عنوان بخشی از جامعه به‌سمت استفاده از فضای مجازی سوق داده شده‌اند. هرچند به‌دلیل محدودیت‌های ایجاد شده‌ی سازمانی برای کارکنان نیروهای مسلح، امکان فعالیت آن‌ها در فضای مجازی محدودتر از سایر اقشار جامعه بوده ولیکن بررسی اولیه آمار جرایم رسیدگی شده در سازمان قضایی نیروهای مسلح در سال‌های اخیر حاکی از تأثیرپذیری نیروهای مسلح از معضلات و آسیب‌های جرایم فضای مجازی است. از جمله مصادیق این جرایم می‌توان به افشای هویت نظامی و سوابق فعالیت های خود، همکاران و فرماندهان، افشای اطلاعات نظامی، مشارکت در کمپین‌های اعتراضی، انتشار محتوای رسانه‌ای تضعیف کننده اقتدار نیروهای مسلح، ارتباط با عناصر بیگانه و... اشاره کرد. شایان ذکر است که مستند به بند ۵ اصل ۱۵۶ قانون اساسی جمهوری اسلامی ایران و مطابق بند هـ ماده ۲۱۱ از فصل هشتم قانون پنجم توسعه جمهوری اسلامی ایران و تحقق بند ۳ سیاست‌های کلی قضایی پنج ساله ابلاغی از سوی مقام معظم رهبری (مدظله العالی)، قوه قضائیه به‌طور عام متولی پیشگیری از جرم بوده و کلیه دستگاه‌های اجرایی باید در چارچوب وظایف خود همکاری لازم را با قوه قضائیه در اجرای برنامه‌های پیشگیری از جرم معمول دارند؛ سازمان قضایی نیروهای مسلح به‌عنوان بخشی از قوه‌قضائیه متولی پیشگیری از وقوع جرم در نیروهای مسلح می‌باشد. این سازمان از سال‌های نخست پس از پایان دفاع مقدس برنامه‌ریزی برای پیشگیری از جرم را با جلب همکاری نیروهای مسلح در دستور کار خود قرار داده است. مواد مرتبط با مصادیق محتوای مجرمانه در فضای مجازی وفق قانون مجازات اسلامی مصوب ۱۳۹۲ و تعزیرات و مجازات‌های بازدارنده مصوب ۱۳۷۵، ماده ۱۲۶ قانون مجازات اسلامی در خصوص معاونت در جرم، ماده ٤٩٨ قانون مجازات اسلامی در خصوص تشکیل دسته یا گروه در داخل یا خارج از کشور، ماده ۵۰۰ قانون مجازات اسلامی در خصوص تبلیغ بر علیه نظام، ماده ٥٠٤، ماده ۵۱۱، ماده ۵۱۲، ماده ۵۱۳ در خصوص توهین به مقدسات، ماده ٥١٤، ماده ٦٠٩، ماده ٦١٨، ماده ٦٣٩، ماده ٦٩٧، ماده ٦٩٨ در خصوص تشویش اذهان عمومی، ماده ۷۰۰ تعزیرات و مجازات‌های بازدارنده در خصوص هجو، ماده ۷۰۵ تعزیرات در خصوص قمار بازی، ماده ۷۰۸ تعزیرات و در خصوص دایر نمودن قمار خانه، ماده ۷۱۰، ماده ۷۲۹ دسترسی غیر مجاز به داده‌ها سامانه‌های رایانه‌ای، ماده ۷۳۰، ماده ۷۳۱ در خصوص دسترسی به داده‌های سری، ماده ۷۳٤، ماده ۷۳۸، ماده ۷۳۹، ماده ۷٤۱ مبحث جرایم رایانه‌ای را شامل می‌گردد (Hedayati Chenani, 2021).

علیرغم وجود مواد قانونی فوق، بروز آسیب‌های نوپدید در این زمینه، جرم‌شناسان و حقوقدانان را بر آن داشته است که مطالعاتی هدفمند با رویکرد علت شناختی و پیشگیری از آسیب‌ها و جرایم انجام دهند. ضرورت و اهمیت این مسئله و برنامه‌ریزی جهت کاهش آسیب‌ها و ارتکاب جرایم مرتبط با فضای مجازی در نیروهای مسلح مستلزم شناخت علمی و تبیین این آسیب‌ها و شیوه‌های اجرایی پیشگیرانه با عنایت

به مزایا و چالش‌های عملی آن‌هاست. لذا در این تحقیق در نظر است تا آسیب‌ها و جرایم مرتبط با فضای مجازی در نیروهای مسلح مورد شناسایی و تبیین قرار گیرد و بررسی گردد که مهمترین جرائم مربوط به نیروهای مسلح در فضای مجازی کدامند؟ و چه سیاست‌های پیشگیرانه مناسبی متناسب با آسیب‌ها و جرایم حوزه‌ی فضای مجازی در نیروهای مسلح می‌توان اتخاذ نمود؟

مبانی نظری تحقیق

در این قسمت تلاش می‌شود تا به مهمترین مبانی مقاله یعنی فضای مجازی و جرائم سایبری پرداخته شود.

فضای مجازی

ظهور اینترنت و همچنین استفاده روزافزون از سیستم‌های اطلاعاتی تغییرات فوق العاده‌ای در زندگی انسان‌ها ایجاد کرده است که بسیاری از کشورها را متحول می‌کند، موانع تجارت را از بین می‌برد، و به مردم در سراسر جهان اجازه می‌دهد بدون توجه به موانع سنتی طبقه اجتماعی، موقعیت جغرافیایی و زمان با یکدیگر ارتباط برقرار، همکاری و تبادل نظر کنند. این ادغام اینترنت، سیستم‌های اطلاعاتی و افراد، که امروزه به عنوان فضای مجازی شناخته می‌شود، یک قلمرو مجازی جهانی برای مزیت رقابتی ایجاد کرده است. در سرتاسر جهان، دولت‌ها، کسب‌وکارها، سازمان‌ها و افراد به‌طور فزاینده‌ای از فناوری‌های فضای مجازی برای بهبود بهره‌وری و سودآوری استفاده می‌کنند. در واقع فعالیت‌های اقتصادی- اجتماعی، وضعیت‌های امنیتی و ایجاد فرصت‌هایی برای نوآوری‌ها و شکوفایی را تغییر می‌دهد. همچنین ابزارهای بهبود حکمرانی عمومی و رفاه مردم را در سطح جهانی گسترش داده است. در واقع، فضای مجازی گزینه‌های بهتری را برای تحقیق، توسعه و نوآوری ارائه کرده است که در نهایت منجر به رشد و شکوفایی استثنایی اقتصادی و همچنین توانمندسازی جوامع آگاه در سراسر جهان با سرعتی شگفت‌انگیز می‌شود (Mbanaso & Dandaura, 2015).

عبارت «فضای مجازی» هنوز تعریفی قابل قبول در سطح جهانی ندارد، اگرچه گاهی اوقات به مفهوم اینترنت یا دیدگاه یک قلمرو مجازی دیجیتال است. تعاریف متعددی توسط سازمان‌های مهمی مانند آژانس اطلاعات مرکزی آمریکا (سیا)، آژانس امنیت ملی آمریکا، اجلاس امنیت سایبری روسیه- آمریکا و غیره (موسسه شرق- غرب و موسسه امنیت اطلاعات دانشگاه دولتی مسکو) به دست آمده است. طبق گفته وزارت دفاع ایالات متحده، فضای مجازی «یک حوزه جهانی در محیط اطلاعاتی است که از شبکه زیرساخت‌های فناوری اطلاعات به هم وابسته، از جمله اینترنت، شبکه‌های مخابراتی، سیستم‌های رایانه‌ای تشکیل شده است.» از سوی دیگر، اجلاس امنیت سایبری روسیه - آمریکا، «فضای مجازی را به عنوان یک رسانه الکترونیکی توصیف می‌کند که از طریق آن اطلاعات ایجاد، انتقال، دریافت، ذخیره، پردازش و حذف می‌شود.» (Mbanaso & Dandaura, 2015)

هر دو تعریف نشان می‌دهند که فضای مجازی ترکیبی از اینترنت و فناوری‌های مخابراتی را در بر می‌گیرد که امکان ضبط، ذخیره‌سازی، بازیابی و انتقال اطلاعات را فراهم می‌کند. این دیدگاه بیشتر توسط کریپندورف[1] (۲۰۱۰) نیز مطرح شده است که استدلال می‌کند، «فضای سایبری مجازی ناشی از توانایی جمعی انسان برای بیان احتمالاتی است که در آن مصنوعات فناورانه طراحی، استفاده و مفهوم‌سازی می‌شوند.» از سوی دیگر، گیبسون[2] (۱۹۸٤) استدلال می‌کند که «فضای مجازی یک بعد انسان‌شناختی دارد، کوه یخی از تغییرات اجتماعی که به فرهنگ

[1] Krippendorff
[2] Gibson

پساصنعتی نزدیک می‌شود.» این موضوع توجه ما را به این واقعیت جلب می‌کند که فضای مجازی رفتار فرهنگی جدیدی را ایجاد کرده است که به نوبه خود تجربه بشر را با دیدگاه‌های جدید در کانون توجه قرار می‌دهد (Mbanaso & Dandaura, 2015).

چوکری[1] (۲۰۱۳) تعریف دیگری از فضای مجازی به عنوان یک دامنه بدون مرز مطرح می‌کند «که از طریق اتصال میلیون‌ها رایانه توسط یک شبکه جهانی مانند اینترنت ایجاد شده است که به عنوان یک ساختار لایه‌ای ساخته شده است، جایی که عناصر فیزیکی چارچوب منطقی اتصال را ایجاد می‌کنند. که امکان پردازش، دستکاری، بهره‌برداری، افزایش اطلاعات و تعامل افراد و اطلاعات را فراهم می‌کند. فضای مجازی با واسطه‌گری و سازماندهی نهادی فعال می‌شود و با تمرکززدایی و تعامل بین این بازیگران، حوزه‌ها و منافع مشخص می‌شود. در مجموع، فضای مجازی را می‌توان به عنوان فضایی خلاصه کرد که توسط افراد، عناصر فرآیند و فناوری مشخص می‌شود، که محدود به قلمروهای منطقی و ساکنان صفر (۰۰۰۰۰) و یک (۱۱۱۱۱) است (Mbanaso & Dandaura, 2015).

جرایم در فضای مجازی

جرایم مجازی یک پدیده رایج در جهان است و به مجموعه‌ای از فعالیت‌ها گفته می‌شود که افراد با ایجاد اختلال در شبکه، سرقت اطلاعات مهم و خصوصی دیگران، اسناد، هک مشخصات و حساب‌های بانکی و انتقال پول به حساب خود انجام می‌دهند. جرایم مجازی، به‌ویژه از طریق اینترنت، با تبدیل شدن رایانه به مرکز تجارت، سرگرمی و دولت اهمیت یافته است. این نوع جرائم که جرایم رایانه‌ای نیز نامیده می‌شود، عبارت است از استفاده از رایانه به عنوان ابزاری برای اهداف غیرقانونی، مانند ارتکاب کلاهبرداری، قاچاق در حوزه مالکیت معنوی، سرقت هویت، یا نقض حریم خصوصی. جرایم مجازی و تاثیرات آن بر جامعه به صورت اخلال اقتصادی، اختلال روانی، تهدید دفاع ملی و غیره می‌باشد. محدود کردن این نوع از جرایم منوط به تحلیل صحیح کارکرد آن‌ها و درک تاثیر آن‌ها بر سطوح مختلف جامعه است. اکنون جرایم مجازی روز به روز در حال افزایش است. مردم به خاطر آن رنج زیادی کشیده‌اند. بنابراین جرایم مجازی یکی از جرایم عمده‌ای است که توسط متخصصان رایانه انجام می‌شود (Gastorn).

در این راستا دباراتی هالدر[2] و دکتر کی. جایشانکار[3] جرایم فضای مجازی را این‌گونه تعریف می‌کنند: «جرایمی که علیه افراد یا گروه‌هایی از افراد به طور مستقیم یا غیرمستقیم با استفاده از شبکه‌های مخابراتی مدرن مانند اینترنت (چت روم، ایمیل) و تلفن همراه با انگیزه مجرمانه برای آسیب رساندن عمدی به قربانی یا ایجاد آسیب جسمی یا روحی یا ضرر به قربانی انجام می‌شود.» فرهنگ لغت آکسفورد اصطلاح جرایم مجازی را به عنوان «فعالیت‌های مجرمانه انجام شده از طریق رایانه یا اینترنت تعریف کرده است.» (همان). جرایم فضای مجازی ممکن است به آن دسته از جرائمی گفته شود که جنس آن همان جرم متعارف است، و در آن رایانه یا شیء یا موضوع رفتار تشکیل دهنده جرم است. «جرایم مجازی به معنای هر جرم دیگری است که با استفاده از ارتباطات الکترونیکی یا سیستم‌های اطلاعاتی است که از طریق هرگونه دستگاه یا اینترنت یا هر یک یا چند مورد از آن‌ها انجام یا تسهیل می‌شود.» جرایم مجازی اصطلاحی است که برای توصیف گسترده فعالیت‌های مجرمانه استفاده می‌شود که در آن رایانه‌ها یا شبکه‌های رایانه‌ای ابزار، هدف یا محل فعالیت مجرمانه هستند. جرائم مجازی می‌تواند هر قطاری را در جایی که هست متوقف کند، ممکن است هواپیماها را در پرواز با سیگنال‌های اشتباه هدایت کند، ممکن است باعث شود اطلاعات مهم نظامی به دست کشورهای خارجی بیفتد، و ممکن است رسانه‌ها و هر سیستمی را متوقف کند (Gastorn).

[1] Choucri
[2] Debarati Halder
[3] K. Jaishankar

انواع مختلفی از جرایم مجازی وجود دارد که عبارتند از: هک، انتشار ویروس، بمب‌های منطقی، حمله انکار سرویس، فیشینگ، بمب ایمیل و ارسال هرزنامه، وب دزدی، مزاحمت سایبری، سرقت هویت و کلاهبرداری از کارت اعتباری، حمله سالامی[1]، دزدی نرم افزاری، هرزه‌نگاری سایبری، فارمینگ[2] گسترش جرایم سایبری فراملی با فقدان هنجارهای مؤثر جهانی و سازوکارهای همکاری برای تعقیب و مجازات مرتکبین تشدید شده است. لذا در این راستا مجمع عمومی سازمان ملل متحد با انعکاس چنین نگرانی‌هایی از جامعه بین‌المللی، مجموعه‌ای از قطعنامه‌ها را به تصویب رسانده است که تاکید می‌کند «انتشار و استفاده از فناوری‌ها و ابزارهای اطلاعاتی، منافع کل جامعه بین‌المللی را تحت تاثیر قرار می‌دهد که سوءاستفاده جنایتکارانه از فناوری اطلاعات ممکن است فاجعه‌ای به همراه داشته باشد. این فناوری‌ها به طور بالقوه می‌توانند برای اهدافی استفاده شوند که با اهداف حفظ ثبات و امنیت بین‌المللی مغایرت دارند. مجمع عمومی سازمان ملل متحد در اجلاس جهانی جامعه اطلاعاتی که در دو مرحله در ژنو در سال ۲۰۰۳ و تونس در سال ۲۰۰۵ برگزار شد، فعالانه از علت مهار جرایم سایبری حمایت کرد. اتحادیه بین‌المللی مخابرات تسهیل‌کننده خط اقدام C5، «اعتمادسازی و امنیت در استفاده از فناوری اطلاعات و ارتباطات» است که در پاسخ به آن، اتحادیه بین‌المللی مخابرات در سال ۲۰۰۷، دستور کار جهانی امنیت سایبری را به عنوان چارچوبی برای همکاری بین‌المللی در این زمینه راه‌اندازی کرد (Gastorn).

جرائم نیروهای مسلح در فضای مجازی

بررسی اولیه آمار جرایم رسیدگی شده در سازمان قضایی نیروهای مسلح در سال‌های اخیر نشان‌دهنده تأثیرپذیری نیروهای مسلح از معضلات و آسیب‌های جرایم فضای مجازی است. لذا ضروری است این آسیب‌ها و جرایم در حوزه فضای مجازی در نیروهای مسلح شناسایی شود از این‌رو در مقاله حاضر به برخی از مهمترین جرائم یعنی جاسوسی سایبری، افشای اطلاعات و داده‌های محرمانه، بی‌احتیاطی یا بی‌مبالاتی یا سهل‌انگاری یا عدم رعایت نظامات دولتی و در نهایت شرکت در کمپین‌های اعتراضی پرداخته و در نهایت سیاست‌های پیشگیرانه و الگوی راهبردی به‌منظور کنترل جرایم و جلوگیری از آسیب‌ها ارائه می‌شود.

الف) جرم جاسوسی

یکی از جرائم بسیار مهم که در فضای مجازی بر آن تاکید فراوان شده است جرم جاسوسی می‌باشد که سابقه دیرینه همزاد با بشر دارد؛ کشورهای مختلف جهان؛ این جرم را در مجموعه قوانین جزایی خود؛ مصوب کرده‌اند و معمولا مجازات‌های سنگینی را برای مرتکبان مقرر داشته‌اند از این رو در تعریف جرم جاسوسی می‌توان بیان داشت که «جاسوس کسی است که محرمانه یا زیر عنوان نادرست به نفع دشمن، در صدد کسب اطلاعات از نقشه و قوای طرف بر می‌آید حداقل باید پای دولتی در میان باشد که مجنی علیه جرم جاسوسی قرار گیرد.» (Hedayati Chenani, 2021). در این راستا ماده ۱۹ قطعنامه بروکسل مصوب ۱۸۷٤بیان می‌دارد: «جاسوس کسی است که بطور مخفیانه و با وسایل و بهانه‌های مخصوص اطلاعات را جمع‌آوری می‌کند. برای تحصیل اطلاعات در نقاط اشغال شده به وسیله نیروی دشمن با قصد اینکه آن‌ها را به طرف مقابل تسلیم نمایند تجسس می‌کند.» در فهرست اختیاری شورای اروپا (توصیه‌نامه شماره ۹(۸۹)) جاسوسی کامپیوتری این‌گونه تعریف شده بود: «کسب اسرار حرفه‌ای یا تجاری از راه‌های نادرست یا افشا، انتقال و یا استفاده از این اسرار بدون داشتن حق یا هرگونه توجیه قانونی با قصد وارد کردن زیان اقتصادی به فردی که محق در نگه داشت اسرار است یا تحصیل یک امتیاز اقتصادی غیر قانونی برای خود یا یک شخص ثالث» و چنانچه ملاحظه می‌شود، جاسوسی کامپیوتری یا به تعبیر دقیق تر جاسوسی تجاری رایانه‌ای، طیف وسیعی

[1] Salami attack
[2] Pharming

از اعمال را شامل می‌شود. ماده ٦٤ قانون تجارت الکترونیک (مصوب ۱۳۸۲) با الگو گرفتن از تعریف شورای اروپا، بدون آنکه نامی از جاسوسی تجاری رایانه‌ای ببرد، در خصوص جرم مزبور مقرر داشته است: «به منظور حمایت از رقابت‌های مشروع و عادلانه در بستر مبادلات الکترونیکی، تحصیل غیرقانونی اسرار تجاری و اقتصادی بنگاه‌ها برای خود و یا افشای آن برای اشخاص ثالث در محیط الکترونیکی جرم محسوب و مرتکب به مجازات مقرر در این قانون خواهد رسید.» با توجه به اهمیت بحث جرم جاسوسی این موضوع در قوانین ایران بازتاب پیدا کرده است در این راستا می‌توان به ماده ۵۰۱ قانون مجازات اسلامی استناد نمود که مقرر می‌دارد: «هرکس نقشه یا اسرار یا اسناد و تصمیمات راجع به سیاست داخلی یا خارجی کشور را عالماً و عامداً در اختیار افرادی که صلاحیت دسترسی به آن‌ها را ندارند، قرار دهد یا از مفاد آن مطلع کند، به نحوی که متضمن نوعی جاسوسی باشد، نظر به کیفیات و مراتب جرم به یک تا ده سال حبس محکوم می‌دارد.» هر چند این قانون عمدتا حالت کلی دارد اما در اصل می‌توان آن را به بحث جرم جاسوسی در میان نیروهای مسلح تسریع داد اما در قوانین اختصاصی مربوط به نیروهای مسلح می‌توان به ماده ٢٤ قانون مجازات جرائم نیروهای مسلح استناد نمود در بند الف ماده ٢٤ به ارائه تعریف از جاسوس پرداخته و اشعار می‌دارد که«هر نظامی که اسناد یا اطلاعات یا اشیای دارای ارزش اطلاعاتی را در اختیار دشمن و یا بیگانه قرار دهد و این امر برای عملیات نظامی یا نسبت به امنیت تاسیسات، استحکامات، پایگاه‌ها، کارخانجات، انبارهای دائمی یا موقتی تسلیحاتی، توقفگاه‌های موقت، ساختمان‌های نظامی، کشتی‌ها، هواپیماها یا وسائل نقلیه زمینی نظامی یا امنیت تاسیسات دفاعی کشور مضر باشد به مجازات محارب محکوم خواهد شد.» بررسی این بند نشان می‌دهد که قانونگذار تلاش نموده است تا ضمن ارائه تعریف جرم جاسوسی حیطه و حدود آن را مشخص نماید در ادامه بحث جرم جاسوسی همچنین می‌توان به ماده ۱۲ «قانون مجازات جرائم نیروهای مسلح جمهوری اسلامی ایران» استناد نمود آنجا که اشعار می‌دارد: «هر نظامی که اسناد یا اطلاعات یا اشیاء دارای ارزش اطلاعاتی را تحصیل کند و در اختیار دشمن قرار دهد و اقدام او برای عملیات نظامی یانسبت به امنیت تأسیسات، استحکامات، پایگاه‌ها، کارخانجات، انبارهای دائمی یا موقتی تسلیحاتی، توقفگاههای موقت، ساختمان‌های نظامی، کشتی‌ها یا هواپیماها یا وسایل نقلیه زمینی نظامی یا امنیت تأسیسات دفاعی کشور مضر باشد به مجازات محارب محکوم خواهد شد.» نکته‌ی بسیار مهم در این قانون و خاصه ماده ۱۲ آن در بند ۵ آن نهفته است آنجه که از افراد نظامی گذر کرده و از کلمه‌ی «بیگانه» استفاده می‌کند[1] این بند از دو جنبه حائز اهمیت است اولا؛ قانون‌گذار به اهمیت تاثیرات مخرب جرم جاسوسی پی برده و ثانیا؛ این قانون فراتر از نیروهای مسلح نگاه عام‌تری به قضیه‌ی جاسوسی مجازی داشته است در همین راستا می‌توان به بند ۲ ماده ٢٤ قانون مجازات جرایم نیروهای مسلح استناد نمود که به بررسی ورود غیرمجاز به مراکز ممنوعه نظامی برای کسب اطلاعات طبقه‌بندی شده پرداخته است که فعل مرتکب عمل به صورت مثبت، مادی و خارجی بوده و شامل جمع‌آوری اطلاعات و اسناد طبقه‌بندی شده و تسلیم آنان به بیگانگان می‌شود. از نظر تحلیل حقوقی و اصول و نظریه‌های جزایی، موضوع بند ۲ ماده ٢٤ یعنی صِرف وارد شدن به محله‌ای گفته شده در قانون را نمی‌توان جرم تام و کامل جاسوسی محسوب کرد و به نظر می‌رسد این بندها یکی از مصادیق روشن و صریح آغاز به جرم جاسوسی است، زیرا ورود به اماکن نگهداری اسناد و اطلاعات، قدمی فراتر از تهیه و ارتکاب اعمال مقدماتی صرف است. در حقیقت ورود به محل نگهداری اسناد و اطلاعات، یکی از اقدامات اجرایی جرم جاسوسی است و عمل، مصداق آغاز به جرم تلقی می‌شود (Fatahi Zafarkandi, 2019). درهرحال قانون‌گذار از نظر اهمیت موضوع و صیانت از حریم امنیتی اماکن و محل نگهداری اسناد

[1] هر بیگانه‌ای که برای کسب اطلاعات به نفع دشمن به پایگاهها، کارخانجات، انبارهای تسلیحاتی، اردوگاه‌های نظامی یگان‌های نیروهای مسلح، توقفگاه‌های موقتی نظامی، ساختمانهای دفاعی نظامی یا وسایط نقلیه زمینی، هوائی، دریائی یا در محل‌های نگهداری اسناد یا اطلاعات داخل شود به‌اعدام و در غیر اینصورت به دو تا ده سال حبس محکوم می‌گردد.

طبقه‌بندی شده، مرتکبان را جاسوس شناخته است. مطابق قوانین و مواد مصرّح در قانون مجازات اسلامی و قانون مجازات جرایم نیروهای مسلح، افشای اسناد و اطلاعات به صورت عمد و غیرعمد، و تسلیم عمدی اسناد، اطلاعات و اسرار نظامی به دشمن و کسانی که صلاحیت دسترسی به آن را ندارند، از مصادیق جاسوسی و خیانت به کشور است و قانونگذار مجازات سنگین محاربه را ـ در صورت قصد براندازی نظام ـ برای فرد یا افراد خاطی در نظر گرفته است.

ب) افشای اطلاعات و داده‌های محرمانه

یکی دیگر از جرائمی که ممکن است در فضای مجازی از سوی نیروهای مسلح رخ دهد افشای اطلاعات و داده‌های محرمانه است بنابراین می‌توان تحلیل نمود که حق دسترسی به اطلاعات و اسناد نظامی مانند سایر حقوق و آزادی های فردی با محدودیت امنیت ملی همراه است. به همین منظور بیشتر دولت‌ها سیستم طبقه‌بندی اطلاعات را پذیرفته‌اند، تا به این وسیله میان نیاز دولت به حفظ محرمانگی و حق مردم به دریافت اطلاعات دولتی، تعادل ایجاد کنند بنابراین، در صورت افشای اطلاعات طبقه‌بندی شده نظامی این رفتار برای امنیت ملی زیانبار بوده و به دلیل آثار و پیامدهای خطیر آن، جرم علیه امنیت محسوب می‌گردد. از این رو قانونگذار نیز متناسب با این حساسیت مبادرت به جرم‌انگاری نموده است در همین راستا می‌توان به ماده ۵۰۱ قانون مجازات اسلامی استناد نمود که اشعار می‌دارد: «هرکس نقشه یا اسرار یا اسناد و تصمیمات راجع به سیاست داخلی یا خارجی کشور را عالماً و عامداً در اختیار افرادی که صلاحیت دسترسی به آن‌ها را ندارند، قرار دهد یا از مفاد آن مطلع کند، به نحوی که متضمن نوعی جاسوسی باشد، نظر به کیفیات و مراتب جرم به یک تا ده سال حبس محکوم می‌دارد.» و همچنین ماده ٤٨ آیین‌نامه انضباطی نیروهای مسلح جمهوری اسلامی ایران اشعار می‌دارد که: «هر یک از کارکنان نیروهای مسلح بایستی همواره با هوشیاری و رعایت اصول و مقررات حفاظتی در حفظ اسراری که در اختیار اوست کوشا باشد و حتی در شرایط بحرانی با نهایت فداکاری از افشای آن جلوگیری نماید و در برخورد با موارد مشکوک از قبیل (براندازی، جاسوسی، خرابکاری، موارد ایجاد نارضایتی) مراتب را بلافاصله به مقام مافوق مسئول گزارش نماید.» بررسی مفاد این ماده به خوبی نقش و وظیفه‌ی کارکنان نیروهای مسلح را به خوبی نشان داده و حفاظت از اسرار و داده‌های نظامی را در واقع نوعی فداکاری و از خودگذشتگی تعریف نموده است این مسئله به خوبی اهمیت حفاظت از اسرار نظامی را نشان می‌دهد اما در صورت بی‌مبالاتی و بی‌احتیاطی نیروهای مسلح در صورت افشاء اطلاعات و داده‌های سری قانونگذار به جرم‌انگاری روی آورده و در این راستا به ترتیب بند «الف، ب، ج» این ماده حبس از شش ماه تا دو سال در نظر گرفته است اما در ادامه همین ماده علاوه بر مجازات حبس طی یک تبصره بیان داشته است که: «هرگاه اسناد و مدارک، مذاکرات، اطلاعات یا تصمیمات، عنوان محرمانه داشته باشد از طرف فرمانده یا رئیس مربوط تنبیه انضباطی خواهد شد.» همچنین در ماده ٢٦ قانون مجازات جرائم نیروهای مسلح در خصوص افشای اطلاعات طبقه‌بندی شده به ترتیب در بندهای «الف، ب و ج» به ترتیب از سه تا ۱۵ سال در صورتی که اطلاعات به کلی سری باشند، از دو تا ده سال درصوتی که عنوان سری داشته باشند و حبس از سه ماه تا یک سال در صورتی که عنوان خیلی محرمانه داشته باشند این مطلب به خوبی نشان‌دهنده‌ی جرم انگاری جرائم است که هم حبس برای آن در نظر گرفته و هم این اجازه را به فرمانده یا رئیس مربوط داده است تا تنبیه انضباطی برای آن در نظر بگیرد.

همان‌گونه که ملاحظه می‌شود ماده ٢٦ ق.م ن. ج.ا.ا از جهاتی نسبت به ماده ۵۰۱ قانون مجازات اسلامی کامل‌تر است زیرا اولا؛ تفاوت در مصادیق ارتکاب عمل جرم در دو قانون واضح و روشن است مبنی بر اینکه در قانون مجازات جرایم نیروهای مسلح جمع‌آوری اطلاعات جرم است اما در قانون مجازات اسلامی برای جمع‌آوری اطلاعات مجازات پیش‌بینی نشده است ثانیا؛ در ماده ٢٦ به اطلاعات طبقه‌بندی شده

اشاره شده است و بر حسب طبقه‌بندی آن مجازات‌های متناسب در نظر گرفته شده است ولی در ماده ۵۰۱ قانون گذار به این جهت توجه نکرده است با این حال ماده ۲۶ نیز مانند ماده ۵۰۱ دارای ابهام و اشکال است. یکی از اشکالات با مقایسه تبصره ۱ ماده ۵۰۱ قانون مجازات اسلامی این است که بر اساس قانون مجازات اسلامی در اختیار گذاشتن اسناد محرمانه جرم و قابل مجازات است ولی تبصره ۱ ماده ۲۶ برای آن تنبیه انضباطی در نظر گرفته که با توجه به جدا ساختن آن از متن ماده و گنجاندن آن تحت تبصره به نظر می‌رسد که عمل جرم تلقی نشده است. ولی در صورتی که جرم باشد بر اساس تبصره ۲ باید به قانون مجازات اسلامی مراجعه کرد زیرا مجازات آن اشد است و در صورت جرم نبودن آن چگونه توجیه‌پذیر است که عمل نظامی در افشاء اسناد محرمانه جرم نباشد ولی عمل یک انسان عادی در افشاء آن جرم و قابل مجازات است (Sarikhani, 2014).

ج) مشارکت در کمپین‌های اعتراضی

یکی دیگر از جرائمی که می‌تواند حائز اهمیت و همچنین توام با خطرات برای امنیت ملی در میان نیروهای مسلح باشد بحث مشارکت در کمپین‌های اعتراضی از نوع مخالف نظام جمهوری اسلامی است البته در اینجا منظور از کمپین‌های اعتراضی آن نوع از کمپین‌هایی است که هیچ مجوز قانونی نداشته و به قصد بر اندازی شکل گیرد متناسب با پیامدها و مخاطراتی که این نوع از کمپین‌ها دارند ماده ٤٩٨ قانون مجازات اسلامی مقرر می‌دارد: «هر کس با هر مرامی، دسته، جمعیت یا شعبه جمعیتی بیش از دو نفر در داخل یا خارج از کشور تحت هر عنوانی تشکیل دهد یا اداره نماید که هدف آن برهم زدن امنیت کشور باشد و محارب شناخته نشود[1]، به حبس از دو سال تا ده سال محکوم می‌شود.» مهمترین نکته‌ی مطرح شده در این ماده لحاظ نمودن قید محارب است یعنی اینکه چنانچه شخصی در دایره تعریف قانون از محارب گنجانده نشود صرفا دو سال تا ده سال حبس بسته به نوع مخاطراتی که متوجه امنیت می‌کند در نظر گرفته شده است اما این قانون به معنای اعم آن است مطابق با اهمیت این مسئله ماده ۸ قانون مجازات جرائم نیروهای مسلح جمهوری اسلامی ایران اشعار می‌دارد که: «هر نظامی که به منظور براندازی نظام جمهوری اسلامی جمعیتی تشکیل دهد یا اداره نماید یا در چنین جمعیتی شرکت یا معاونت مؤثر داشته باشد، محارب محسوب می‌شود.» نکات مهم در این ماده این است در تبصره ۱ و ۲ آن است که اولا؛ رسیدگی به جرائم در محاکم نظامی منوط به اکثریت اعضا از پرسنل نیروهای مسلح دانسته است و ثانیا؛ و منظور از جمعیت همکاری حداقل سه نفر یا حداکثر بیشتر از سه نفر باشد. همچنین در ماده ۱ قانون فعالیت احزاب ۱۳٦۰ بیان شده است که: «چنانچه یک نفر نظامی اقدام به تشکیل سازمان یا حزب و یا جمعیت سیاسی نماید و یا در آن عضویت یابد و تشکیل مربوط برنامه براندازی نظام جمهوری اسلامی ایران را طراحی یا بدان اقدام نماید. تحت عناوین مجرمانه متعدد موضوع مواد ۱۷ و ٤۰ همین قانون، قابل تعقیب و مجازات است در همین راستا ماده ۱۹ نیز اشعار می‌دارد که هر نظامی که به منظور بر هم زدن امنیت کشور (ایجاد رعب، آشوب و قتل)، جمعیتی با بیش از دو نفر تشکیل دهد یا اداره کند، چنانچه محارب شناخته نشود به حبس ازسه تا پانزده سال محکوم می‌گردد. اعضای جمعیت که نسبت به اهداف آن آگاهی دارند. در صورتی که محارب شناخته نشوند به دو تا پنج سال محکوم می‌گردند.» قانونگذار در این ماده، بر هم زدن امنیت کشور را منحصر به سه مورد ایجاد رعب، آشوب و قتل دانسته است بدون تردید بر هم زدن امنیت کشور مفهومی عام و کلی و فرا تر از مواد مذکور در ماده می‌باشد؛ اما نظر به این که مقنن از کلماتی مانند: از قبیل، مانند و... استفاده نکرده است، پس موارد مذکور در پرانتز، حصری بوده و نمی‌توان از آن برداشت تمثیلی نمود؛ زیرا تفسیر

---

۱ روشن نیست که چگونه مقنن مبنا و تعریفی که خود از محاربه- به تبعیت از قول مشهور فقها- ارائه نموده است به صرف تشکیل جمعیت به قصد بر هم زدن امنیت را که در آن نه عنصر اخافه وجود دارد و نه به کارگیری اسلحه، فرض محارب بودن مرتکبین را تصور نموده است، بلکه چنین می‌توان گفت که محاربه رانسبت به موضوع ماده فرض کرد.

قضایی با برداشت تمثیلی از سه مورد موصوف با تفسیر اصولی قوانین کیفری و نتایج اصل برائت لزوم تفسیر مضیق قوانین جزایی و تفسیر قانون جزا به نفع متهم مغایرت دارد. پس، به نظر می‌رسد منظور از بر هم زدن امنیت کشور در این ماده، ایجاد رعب، آشوب و قتل باشد.

بررسی مواد قانونی فوق و ارتباط آن با جرائم فضای مجازی نشان می‌دهد که، امکان تحقق موضوع ماده ٤٩٨ از طریق امکانات رایانه‌ای، امری ممکن است. البته ممکن است در تحقق عنصر مادی جرم تشکیل یا اداره جمعیت، حضور فیزیکی افراد را در یک زمان و مکان شرط دانسته شود. لیکن دلیلی بر صرف نظر کردن از اطلاق ماده ٤٩٨ از این جهت وجود ندارد، زیرا اطلاق ماده تشکیل جمعیت اینترنتی نیز شامل می‌شود؛ به خصوص آنکه تشکیل جمعیت به هدف بر هم زدن امنیت کشور مطابق ماده ٤٩٨ جرم شناخته شده است. به عبارت دیگر مقنن با جرم‌انگاری تشکیل جمعیت، قبل از هر گونه اقدامی خواسته است تا از به وجود آمدن زمینه آن جلوگیری کند و چنین مصلحتی در جرم انگاشتن تشکیلات به وجود آمده از طریق رایانه نیز وجود دارد. تشکیل گروه علیه امنیت کشور به این دلیل جرم تلقی می‌گردد که: اولاً ممکن است جرم خیانت به کشور توسط همین گروه‌ها انجام شود، زیرا اقدام گروهی و دسته جمعی با اقتدار و جرأت بیشتری همراه است. بنابراین، وقتی این گروه‌ها خواسته‌های نامشروع خود را عملی ندیدند، در مقابل کشور، دولت و ملت قیام کرده و جنایات علیه امنیت و تمامیت کشور را مرتکب خواهند شد. ثانیاً، تاریخ سیاسی کشورها نشان می‌دهد در صورتی که اینگونه گروه‌ها از آغاز تشکیل مبارزه و مقابله نشود، رفته‌رفته به قدرتی مبدل می‌شوند و معمولاً وسیله‌ای برای سوءاستفاده قدرت‌های بیگانه به عنوان اهرم فشار بر کشور قرار می‌گیرند. در نتیجه، کسانی که خیانت را به طور گروهی و دسته جمعی مرتکب می‌شوند یا در آینده، مرتکب خواهند شد، بالقوه، امنیت کشور را تهدید می‌کنند. بنابراین، اساساً تشکیل و اداره اینگونه دستجات بر خلاف مصالح و امنیت کشور بوده و جرم و قابل تعقیب و مجازات است.

د) بی احتیاطی و بی مبالاتی

امروزه با توجه به گستردگی شبکه‌های اجتماعی در قالب فضای مجازی هر نوع سهل‌انگاری یا کوتاهی در امور نظامی به سرعت تمام می‌تواند آسیب‌ها و پیامدهای مخربی بر امنیت ملی و بدنه‌ی نیروهای مسلح داشته باشد متناسب با این اهمیت قانونگذار همواره تلاش داشته است تا به این موضوع رسیدگی جدی داشته باشد از این رو در تعریف بی‌احتیاطی و بی‌مبالاتی می‌توان بیان داشت که «بی‌احتیاطی، انجام یا ارتکاب عمل یا فعلی است که فرد نباید انجام دهد، ولی بی‌مبالاتی، انجام ندادن کاری است که انجام آن لازم و ضروری بوده است. مبنا و معیار سنجش بی‌احتیاطی یا بی‌مبالاتی می‌تواند قضاوت عرف و یا مقررات مدون باشد.» (یزدانیان، ۱۳۸۵: ۳-۸) تعریف بی‌احتیاطی و بی‌مبالاتی نشان می‌دهد که این مسئله چه در سطح عمومی و چه در سطح خاصه یعنی نیروهای مسلح می‌تواند توام با خسارات باشد از این رو مطابق ماده ٥٠٦ قانون تعزیرات مصوب ۱۳۷۵ بیان شده است که: «چنانچه مأمورین دولتی که مسئول امور حفاظتی و اطلاعاتی طبقه‌بندی شده می‌باشند و به آن‌ها آموزش لازم داده شده است در اثر بی‌مبالاتی و عدم رعایت اصول حفاظتی توسط دشمنان تخلیه اطلاعاتی شوند به یک تا شش ماه حبس محکوم می‌شوند.» شبیه این ماده در قسمت اخیر ماده ۲ «قانون مجازات افشای اسناد محرمانه و سرّی» مصوب سال ۱۳۵۳ پیش‌بینی شده بود که مطابق آن، «در صورتی که افشای اسناد مذکور در اثر عدم رعایت نظامیات یا در اثر غفلت و مسامحه‌ی مأمور حفاظت آن‌ها صورت گرفته باشد، مجازات او سه ماه تا شش ماه حبس جنحه‌ای خواهد بود.» بررسی ماده ٥٠٦ در خصوص بی‌مبالاتی نشان‌دهنده‌ی دو نکته کلیدی است اولا نکته‌ی قابل ذکر دیگر در مورد عنصر «بی‌مبالاتی» آن است که بی‌مبالاتی مأمور دولتی مذکور در ماده هم می‌تواند نسبت به اصل ارائه اطلاعات باشد (مثل این که وی بدون دقّت و توجه کافی در مورد تحت کنترل بودن خط تلفن خود یا

وجود وسایل استراق سمع در اتاق هتل محل اقامتش اطلاعات محرمانه را برای همکاش بیان نماید) و هم نسبت به شناسایی هویتِ گیرنده‌ی اطلاعات که مـثلاً بـدون تحقیـق کـافی و بـه صِرف ادعای وی او را مأمور ذی صلاح دولت ایران تلقی کرده و اطلاعات خود را در اختیار وی بگذارد ثانیا؛ برای تحقق جرم موضوع ماده ٥٠٦، مأمور دولتی باید توسط «دشمنان» تخلیـه اطلاعـاتی شـود علاوه بر قوانین فوق همچنین می‌توان به ماده ماده ٥٤ قانون مجازات نیروهای مسلح اشعار می‌دارد که: «هرگاه بی‌احتیاطی یا بی‌مبالاتی یا عدم رعایت نظامات دولتی در ارتباط با امور خدمتی توسط فرماندهان و مسؤولان رده‌های مختلف نیروهای مسلح موجب تلفات جانی و یا صدمات بدنی گردد چنانچه به موجب مواد دیگر این قانون و یا سایر قوانین مستلزم مجازات شدیدتر نباشد مرتکب به حبس از یک تا سه سال محکوم می‌شود. همچنین می‌توان به ماده ١٤ قانون مجازات جرائم نیروهای مسلح جمهوری اسلامی ایران استناد نمود که اشعار می‌دارد: «هر نظامی که بر اثر بی‌احتیاطی یا بی‌مبالاتی یا عدم رعایت نظامات دولتی موجب افشاء یا فقدان اسناد مذکور در ماده (١٣) بشود با توجه به طبقه‌بندی اسناد افشاء شده، به ترتیب ذیل محکوم می‌شود» از سه ماه تا یک سال به حبس محکوم می‌شود.

سیاست‌های پیشگیرانه مناسب با جرایم حوزه‌ی فضای مجازی در نیروهای مسلح

در این قسمت تلاش می‌شود تا مهمترین سیاست‌هایی که جنبه پیشگیری داشته و می‌توانند سبب کاهش جرائم نیروهای مسلح در فضای مجازی شوند مورد بررسی و مطالعه قرار گیرد.

جرم انگاری جرائم سایبری

امروزه جرم‌انگاری جرم همواره یکی از راهکارهای مقابله با جرائم می‌باشد که می‌تواند حالت پیشگیرانه به خود گرفته و مانع از ارتکاب جرائم شود این مسئله زمانی حائز اهمیت است که توجه شود در حقوق اسلامی براساس قاعده "قبح عقاب بلبیان" نمی‌توان کسی را به علت عملی که جرم شناخته نشده مجازات کرد. بر اساس "اصاله الاباحه" هر کس در مورد اشیاء و امور حق هرگونه دخل و تصرف دارد، مگر در مواردی که قانون منع کرده باشد. بنابر این قاعده، اگر در جواز یا عدم جواز امری شک کنیم، عمل به آن مباح بوده و مرتکب، مجازات نمی‌شود.» (Naimi, 2022) در قانون اساسی ایران بر اساس اصل ٣٦، حکم به مجازات و اجرای آن فقط ازطریق دادگاه صالح و به موجب قانون است. با استنباط از اصل ١٦٩ قانون اساسی، فعل یا ترک فعلی جرم شناخته می‌شود که آن فعل یا ترک فعل در قوانین مدون جرم بوده باشد اعم مطالب فوق نشان می‌دهد تا زمانی که جرائم سایبری مربوط به نیروهای مسلح به تفکیک جرم‌انگاری نشوند نمی‌توان انتظار سیاست پشگیرانه در این راستا داشت زیرا یکی از راهکارهای مبارزه با جرائم سایبری جرم انگاری آن‌ها می‌باشد که می‌تواند نقش مهمی در پیشگیری از ارتکاب جرم ایفا نماید اهمیت این موضوع تا بدانجا است که بنتام می‌گوید: «مجازات را معلق یا تعطیل کنید، آنگاه دنیا صحنه جرم و جنایت شده و جامعه از بین می‌رود.» (Wilson, 1983). جیمز کیو ویلسون یکی از نظریه‌پردازان معاصر آمریکایی و طرفدار همین تفکر، مبانی آن را در یک جمله کوتاه چنین خلاصه می‌کند: «به همان اندازه که احتمال اعمال ضمانت اجراهای کیفری بیشتر شود، جرم شیوع کمتری خواهد داشت.» (Wilson, 1983). همان‌طور که ملاحظه می‌شود یک رابطه مستقیم بین افزایش ارعاب و کاهش از جرم به‌وجود می‌آید. و در این نوع پیشگیری نقطه ثقل پیشگیری در آن کیفر و برخورد با مرتکب است و نقش مرتکب اعم از بزه‌دیده و اجتماع در آن نادیده گرفته شده است (Safari, 2001). در این نوع پیشگیری تعدد تابعان حقوق کیفری از یک‌سو و به اجرا گذاشتن این تهدید از طریق مجازات کسانی که ممنوعیت‌های کیفری را نقض کرده‌اند از سوی دیگر، در مقام پیشگیری عام و پیشگیری خاص از جرم است (Najafi

Abrandabadi, 2009). بنابراین در نتیجه‌گیری از بحث می‌توان بیان داشت که جرم‌انگاری جرائم سایبری مربوط به نیروهای مسلح، با در نظر گرفتن شناسایی ماهیت و خصوصیت فضای مجازی و کاربران آن است که می‌تواند با استفاده از ابزار قانون و راهکارهای جامعه‌شـــناختی، قبل از وقوع جرم از بروز آن ممانعت به عمل آورد در واقع جرم‌انگاری جرائم سایبری نیروهای مسلح در واقع همان پیشگیری قبل از وقوع جادثه است.

آموزش سواد رسانه‌ای

سواد رسانه‌ای به دنبال آن است تا در فرد توانایی لازم برای استفاده از رسانه‌ها را آموزش دهد به‌طوری که فرد بتواند ضمن درک و تحلیل و ارزیابی پیام‌های رسانه‌های مختلف، پیام‌ها و برنامه‌های مثبت، مفید و سازنده را از پیام‌های منفی و بی‌محتوا تشخیص دهد. یعنی فرد آگاهانه در برابر رسانه‌ها قرار گیرد و توانایی دسترسی به پیام‌های مورد نظر خود از میان انبوه پیام، تجزیه و تحلیل انتقادی، ارزیابی و ارسال پیام‌ها در انواع مختلف را پیدا کند (Shams, 2014). تعریف سواد رسانه‌ای نشان می‌دهد که کاربرد آن در فضای سایبری تا چه حد حائز ضرورت و اهمیت می‌باشد زیرا نوظهور بودن جرایم سایبری، کثرت بزه‌دیدگان در فضای سایبر و عدم درک دقیق آثار تهدیدات سایبری و نیز غیرقابل سنجش و غیرفیزیکی بودن آن‌ها، ضرورت تکیه بر تدابیر آموزشی- آگاهی یا سواد رسانه‌ای را در این دسته جرایم بیش از هر جرم و انحراف دیگری موجه می‌سازد. در این راستا می‌توان به پژوهش «آناپانگ» استناد نمود که در مطالعه‌ای با روش پیمایشی روی ۲۹۲ جوان معتقد است افرادی که در دوره‌های آموزش سواد رسانه‌ای شرکت کرده بودند، آگاهی بیشتر و تفکر انتقادی بالاتری نسبت به افرادی که در دوره‌های مزبور شرکت نکرده بودند، داشتند متناسب با این اهمیت و ضرورت قانونگذار در ایران نیز تلاش نموده تا سبب افزایش سطح سواد رسانه‌ای شود مصادق بارز این تلاش در بند «ب» ماده ۱۰ قانون برنامه پنج ساله نمود پیدا می‌کند آنجا که دولت موظف است سازوکارهای اجرای لازم جهت «ارتقاء آگاهی، دانش و مهارت همگانی، تقویت رسانه‌های ماهواره‌ای و اینترنتی همسو و مقابله با رسانه‌های معارض خارجی» به منظور سازماندهی فضای رسانه‌ای، مقابله با تهاجم فرهنگ بیگانه و جرائم و ناهنجاری‌های رسانه‌ای فراهم سازد بنابراین در جمع‌بندی از بحث می‌توان بیان داشت که در راستای پیشگیری کنشی از جرایم سایبری در میان نیروهای مسلح، هیچ ابزاری به اندازه «آموزش» نمی‌تواند مؤثر واقع شود (Najafi Abrandabadi, 2009)؛ زیرا نیروهای مسلحی که افراد آن سواد رسانه‌ای دارند، از توسعه انسانی و اجتماعی بیشتری در مقابله با جرائم سایبری برخوردار بوده و افراد آن مخاطب صرف، منفعل و تحت کنترل فضای سایبری نبوده بلکه به طور فعال با پیام‌ها برخورد کرده و به مخاطب انتخابگر و گزینشگر مبدل خواهند شد.

گسترش تفکر انتقادی

آموزش تفکر انتقادی به افراد کمک می‌کند تا نگرشی عاقلانه و مستدل نسبت به مسائل پیرامون خود پیدا کنند در این راستا نعمتی فر و کاظمی (۲۰۱۹) در پژوهشی مداخله‌ای، ارتقای سواد رسانه‌ای را در زمینه کاهش آسیب‌های اجتماعی در فضای مجازی موثر می‌دانند مددی‌زاده و همکاران (۲۰۲۱) در پژوهش خود به این نتیجه رسیده‌اند که آموزش سواد رسانه‌ای در کاهش اثرات مخرب فضای مجازی موثر است از آنجا که دانش‌آموزان برای بسیاری از اطلاعات و پاسخ و پرسش‌های خود از فضای مجازی استفاده می‌کنند و از طرفی معیار درستی در مورد سنجش صحت مطالب و نقد و ارزیابی آن‌ها ندارند ممکن است بسیاری از مطالب سبب گمراهی آن‌ها شود (Rouhparvar, 2022). حال

این موضوع را می‌توان به نیروهای مسلح نیز تعمیم داد و استدلال نمود که افزایش قدرت نقد در نیروهای مسلح در زمینه کاهش آسیب‌زا از شبکه‌های اجتماعی، مهم و ضروری است این نوع تفکر ابزاری مفید و سودمند برای پیدا کردن بهترین مسیر در لابه‌لای فوران اطلاعات روزانه به حساب می‌آید چرا که این حجم انبوه از اطلاعات که روزانه به ذهن می‌رسد تنها اندکی از آن‌ها نیازمند توجه است بنابراین در نتیجه‌گیری از بحث می‌توان بیان داشت تفکر انتقادی از دو منظر باعث کاهش جرائم سایبری در نیروهای مسلح می‌شود اولا؛ اگر تفکر انتقادی به مجموعه‌ای از نگرش‌ها و مهارت‌های فکری اطلاق شود که برای ارزیابی و محک زد ادعاها و استدلال‌ها به کار می‌آیند آن وقت می‌توان استدلال نمود که در تفکر نقادانه سعی بر آن خواهد داشت که هر ادعا یا استدلالی پیش از پذیرفته شدن با استفاده از معیارهای معینی محک زده شود تا بتوان درباره‌ی عقلانی بودن یا نبودنش داوری کرد بنابراین می‌توان بیان داشت که نیروهای مسلحی که به سطح شناختی بالاتری دست یافته باشند مسائل و اطلاعات حاکم در شبکه‌های اجتماعی را راحتر و بهتر مورد نقد قرار می‌دهند از این‌رو تغییر در نگرش آن‌ها به راحتی ممکن نخواهد بود این موضوع در راستای توانبخشی‌شناختی نیروهای مسلح در پیشگیری از حملات سایبری شناختی و ایدئولوژیکی در بستر فضای مجازی از اهمیت بالایی برخوردار است ثانیا؛ تفکر انتقادی سبب ایجاد شک و تردید نسبت به صحت یا عدم صحت هر نوع اطلاعات یا خبر می‌شود زیرا شک بی‌غرض و راهبردی از لوازم درست اندیشیدن است؛ چنان‌که می‌توان آن را به منزله سرآغاز فعالیت ذهن هدفمند و خلاق شناخت. پیر شارون می‌گوید: «اساس همه معرفت و جوهر خردمندی، شک است.» (Avi, 2014). شک آن توان را دارد که با برملا کردن پایه‌های دروغ و ویران کردن بنیاد امور بی‌ارزش و آسیب‌زا، راه را بر آغازی دیگر و مسیری بهتر بگشاید. به گفته رابرت بریجز، «شک به آن گیاهان طبی می‌ماند که اگر شیره‌شان به مصرف تنقیه برسد، تندرستی را به بدن بازمی‌گرداند.». از این رو تفکر انتقادی به نیروهای مسلح قدرت سنجیدن و ارزیابی اطلاعات و ایجاد شک و تردید نسبت به صحت یا عدم صحت آن‌ها می‌دهد که نه تنها بر افزایش خلاقیت تأثیر می‌گذارد، بلکه بر کنجکاوی و پویایی ذهن و قدرت تصمیم‌گیری و حل مساله می‌افزاید. تفکر انتقادی فرایند قضاوت هدفمندی است که در نتیجه تفسیر، تحلیل، ارزیابی و استنباط شکل می‌گیرد. در نتیجه تفکر انتقادی نیروهای مسلح را با انواع شگردهای رسانه‌ای و پیام‌های دروغین و فریبنده آشنا می‌کند تا از گزند انواع و اقسام آسیب‌ها مصون بمانند.

نهادینه کردن فرهنگ استفاده از فضای مجازی و بومی‌سازی آن

در دنیای پیچیده امروز با تغییر ماهیت دانش، نیازهای آموزشی، نیاز به یادگیری، گسترش علم و فناوری و بازآموزی مادام‌العمر به دلیل افزایش انتظارات، محدودیت منابع در مقایسه با رشد روزافزون جمعیت و تقاضای فزاینده جهت برخورداری از فرصت‌های آموزشی انعطاف پذیر به علت عدم امکان حضور منظم و مداوم در کلاس‌های فیزیکی و حضوری (سنتی)، گسترش فرصت‌های آموزشی را به یکی از دغدغه‌های اصلی کشورها و دولت‌ها تبدیل نموده است (Asgharzadeh et al., 2023). بنابراین متناسب با این ضرورت کشورها مبادرت به استفاده از فضای مجازی و توسعه و گسترش آن نموده‌اند اما استفاده از فضای مجازی بدون نهادینه کردن و بومی‌سازی آن نمی‌تواند چندان موثر واقع گردد از این رو بومی‌سازی فناوری‌ها در واقع در معنایی کلی به اهمیت دادن به سرمایه‌ها و استفاده از روش‌های فناوری است که توان ملی را از جنبه‌های مختلف ارتقا می‌دهد شیوه و برنامه‌هایی که هم مسیر درستی به استفاده از امکانات جامعه می‌بخشد تا سرمایه‌ها هدر داده نشوند و از طرفی هم در راستای شکوفایی و توسعه سرمایه‌های فکری و مادی عمل می‌کند لذا رسانه‌ها نیز با توجه به رسالت و تاثیر مهمی که در جامعه دارند باید از الگوهای بومی‌سازی پیروی نمایند به این معنا که شیوه فعالیت آن‌ها متناسب با شرایط جامعه باشد (Saberi, 2017).

این موضوع در خصوص نیروهای مسلح از اهمیت دوچندانی برخوردار می‌باشد زیرا نیروهای نظامی جمهوری اسلامی ایران در زمره مهمترین و پیچیده‌ترین سازمانهای موجود در ایران بوده و سرمایه انسانی در سازمانهای نظامی مهمترین منبع به شمار می‌روند، به صورتی که آموزش و توسعه آن‌ها از جمله برنامه‌های راهبردی نیروهای مسلح است و فناوریهای نوین تمام جنبه‌های سرمایه اجتماعی ازجمله سازمانها را متحول کرده و آموزش و توسعه سرمایه انسانی نیروهای مسلح نیز از این فناوری‌ها تأثیر پذیرفته است (ایزدی طامه، ۱۳۹۰). ارتش و سازمانهای نظامی به عنوان حیاتی‌ترین سازمان‌های کشوری به تربیت و آموزش نیروهای انسانی در زمینه‌های مختلف می‌پردازند و دارای بخش و سیستم آموزشی خاص خود هستند باید هرروز و لحظه به دنبال استفاده و به کارگیری روش‌های آموزش نوین و در صورت لزوم نهادینه کردن این نوع آموزش‌ها در سازمان خود باشند (Izadi Tameh, 2018). در مطالعه‌ای با عنوان "تأثیر فناوری‌های نوین بر آموزش و توسعه سرمایه انسانی در سازمان‌های نظامی" به این نتیجه رسیده است که استفاده بهینه از فناوری‌های نوین در آموزش و توسعه نیروهای مسلح، بیش از هر چیز نیازمند تغییر در باورها، نگرشها، دیدگاه‌ها و رفتارهای تمام فرماندهان به ویژه برنامه‌ریزان آموزشی و درسی، مدیران آموزشی و بالاخره مربیان نسبت به این فناوری‌هاست (Izadi Tameh, 2018). این نتیجه‌گیری در واقع نشان‌دهنده‌ی فرهنگ استفاده از فضای مجازی و بومی‌سازی آن می‌باشد که در صورت تحقق آن می‌توان شاهد کاهش حجم جرائم سایبری نیروهای مسلح در فضای مجازی بود.

نتیجه‌گیری

تحولات ساختاری ناشی از به‌کارگیری فناوری‌های اطلاعات و ارتباطات، جوامع بشری را در همه‌ی عرصه‌های اجتماعی با چالش‌های نوینی مواجه کرده است و این چالش در میان نیروهای مسلح نیز صدق می‌کند که منجر به اتخاذ دو پیامد متفاوت شده است اولاً، جرائم سایبری در میان نیروهای مسلح یکی از پدیده‌های نوظهور جرائم در عصر جهانی شدن و مدرن بوده که ساختار جرم را از دو منظر ماهیت و نوع آن تغییر داده است ثانیاً، ظهور اینترنت و گسترش پهنا و باند آن سبب شده است تا علاوه بر اینکه جرائم سایبری در تمام ابعاد کمی و کیفی آن متحول شود نوعی جابجایی جرائم از فضای حقیقی به فضای مجازی صورت گیرد از این رو بررسی چهار جرم جاسوسی، افشای اطلاعات و داده‌های سری، بی‌احتیاطی و بی‌مبالاتی و شرکت در کمپین‌های اعتراضی در میان نیروهای مسلح نشان می‌دهد که اولا؛ در زمینه موضوع جرم، برخی از کشورها من‌جمله کشور فرانسه علاوه بر اطلاعات، بحث جاسوسی را گسترش داده و بحث جاسوسی در خصوص اشیاء هم مطرح نموده به عبارت بهتر در قوانین فرانسه اشیاء هم می‌توانند به نوبه خود موضوع جاسوسی واقع شوند، این در حالی است که در عمده قوانین ایران و خاصه قوانین نیروهای مسلح فقط اطلاعات می‌تواند موضوع جرم جاسوسی باشند ثانیا؛ در خصوص افشای اسرار و داده‌های سری و همچنین جاسوسی مجازی به نظر می‌رسد برخلاف قوانین کشورهای پیشرو در این زمینه که معاونت در جرم جاسوسی را به عنوان نوعی جرم مستقل جرم‌انگاری کرده‌اند قوانین ایران این موضوع را مستقلا جرم‌انگاری نکرده بلکه بیشتر صورت استعاره‌ای به خود گرفته است ثالثا، در خصوص شرکت نیروهای مسلح در کمپین‌های اعتراضی می‌توان بیان داشت که اگر این نوع از جرائم از طریق اینترنت انجام شود چون دارای حجم وسیع و گسترده مخاطبین است و همچنین آثار زیانبار گسترده‌ای می‌تواند داشته باشد لازم است تا به عنوان کیفیت مشدده در میزان مجازات‌ها در نظر گرفته شده و مجازات‌های شدیدتری برای آن وضع شود رابعا؛ در خصوص موضوع جرم بی‌مبالاتی و بی‌احتیاطی نیروهای مسلح قانونگذار ارتکاب این جرم را منوط به دو عامل آموزش دیدن مامور حفاظتی اطلاعات طبقه‌بندی شده و برخورداری از مسئولیت دانسته است

چند چالش در اینجا ایجاد می‌شود اینکه قانونگذار شرط داشتن مسئولیت امور حفاظتی و اطلاعاتی را پیش‌بینی نکرده است علاوه بر دشمنان تخلیه‌ی نظامیان توسط بیگانگان را مجرم شناخته است این مسائل نشان می‌دهد که تعریف مشخصی از جرم بی‌مبالاتی و بی‌احتیاطی ارائه نشده، نوع، میزان و کیفیت آموزش مشخص نشده است، تفکیکی بین طبقات مختلف اسناد شکل نگرفته است و در نهایت سایر کارمندان آموزش دیده در حوزه‌ی اطلاعات طبقه‌بندی شده را مجرم نداسته است این مسئله نوعی اختلاف دیدگاه و تفاوت در برداشت جرم از این ماده را در پی داشته است.

پیشنهادات

الف) پیشنهاد می‌شود ضمن ایجاد بستر قانونی، اجرایی و قضایی برای رسیدگی امر جرایم رایانه‌ای لازم است تا ستاد حفاظت نیروهای مسلح به ایجاد اطمینان از گردش اطلاعات میان نهادهای نیروهای مسلح، مبادرت ورزد.

ب) جلوگیری از پیامدهای جرائم سایبری در میان نیروهای مسلح در گروه ضرورت آموزش است زیرا برای اجرای یک سیاست کیفری مؤثر جهت پیشگیری از جرایم رایانه‌ای به خصوص جاسوسی رایانه‌ای و اینترنتی، گسترش آموزش و سواد رسانه‌ای می‌بایستی در مقاطع مختلف زمانی در میان نیروهای مسلح تکرار و روزآمد شود.

ج) پیشنهاد می‌شود تا نهادی تحت عنوان (سازمان پیشگیری از وقوع جرائم سایبری در میان نیروهای مسلح) مرکب از جرم‌شناسان، حقوقدانان، روان‌شناسان و جامعه‌شناسان تاسیس گردد.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

حامی مالی

این پژوهش حامی مالی نداشته است.

EXTENDED SUMMARY

The rapid advancement of technology and continuous progress in information, communication, satellite, and internet domains have catalyzed profound transformations within human societies, yielding a multitude of both positive and negative consequences. Among these, the impact of the internet and cyberspace on communication has been particularly significant, engendering numerous changes and disruptions across various sectors. Social networks, recognized as the most substantial achievement of the internet and cyberspace, have gained widespread popularity due to their limitless connectivity, anonymity, extensive freedom, and the ability of users to interact without geographical and temporal constraints (Amani Kalarijani, 2016). However, the widespread adoption of cyberspace has introduced novel challenges in the realms of social pathology and cybercriminology. Certain harms and crimes, which were previously less prevalent in the physical world, have been exacerbated by the facilitative, complementary, or overflow roles of cyberspace. Concurrently, as the general population increasingly engages with cyberspace, armed forces have also been drawn into its usage.

Despite organizational restrictions that limit the online activities of military personnel compared to other societal groups, preliminary analyses of crime statistics handled by military judicial organizations in recent years indicate that armed forces are susceptible to the dilemmas and harms associated with cybercrimes. Examples of such crimes include the disclosure of military identities and operational histories, leaking of classified military information, participation in protest campaigns, dissemination of media content undermining military authority, and interactions with foreign entities. This study aims to identify and analyze cyber-related harms and crimes within the armed forces and propose appropriate preventive policies based on legal texts and existing regulations.

Cyberspace, a term that lacks a universally accepted definition, is often interchangeably used with the internet or a digital virtual realm. Definitions from prominent organizations such as the U.S. Central Intelligence Agency (CIA), the U.S. National Security Agency (NSA), and the Russia-U.S. Cybersecurity Summit describe cyberspace as a global domain within the information environment, comprised of interconnected information technology infrastructures, including the internet, telecommunications networks, and computer systems (Mbanaso & Dandaura, 2015). Additionally, Cripendorff (2010) posits that cyberspace emerges from humanity's collective ability to design, utilize, and conceptualize technological artifacts, while Gibson (1984) emphasizes its anthropological dimension as a significant cultural shift towards a post-industrial society.

Cyber crimes, or computer crimes, represent a prevalent global phenomenon involving activities that disrupt networks, steal sensitive and private information, hack into identities and bank accounts, and transfer funds illicitly. These crimes have gained prominence alongside the centralization of computers in commerce, entertainment, and government operations. Defined by Hedayati Chenani (2021), cyber crimes are offenses committed against individuals or groups, directly or indirectly, using modern telecommunication networks such as chat rooms, emails, and mobile phones, with criminal intent to cause deliberate harm or physical and psychological damage to victims. The Oxford Dictionary characterizes cyber crimes as criminal activities conducted via computers or the internet (Oxford Dictionary). These crimes encompass a wide range of illicit activities, including hacking, virus dissemination, logic bombs, denial-of-service attacks, phishing, email bombing, web theft, cyber harassment, identity theft, credit card fraud, salami attacks, software piracy, cyber pornography, and pharming (Hedayati Chenani, 2021). The proliferation of transnational cyber crimes is exacerbated by the absence of effective global norms and cooperative mechanisms for prosecuting and punishing offenders. In response, the United Nations General Assembly has adopted resolutions emphasizing the detrimental impact of malicious use of information technologies on global stability and security. The International Telecommunication Union (ITU) has facilitated initiatives like the C5 Action Line—fostering trust and security in information and communication technologies—and launched a global cybersecurity agenda in 2007 to promote international cooperation in this domain (Gastorn).

Preliminary statistics from military judicial organizations reveal that armed forces personnel are increasingly vulnerable to cyber-related harms and crimes. This necessitates the identification and elucidation of cybercrimes within the military context, focusing on significant offenses such as cyber espionage, disclosure of classified information and data, negligence or carelessness, non-compliance with governmental regulations, and participation in unauthorized protest campaigns. Cyber espionage, a critical concern, has long been recognized across various national legal frameworks, typically warranting severe penalties. Espionage involves the clandestine acquisition of information in favor of an adversary, necessitating stringent legal repercussions. According to Article 19 of the

Brussels Resolution No. 1874, espionage is defined as the covert collection of information using special means and pretexts, with the intent to surrender it to the opposing side. The European Council's optional list (Recommendation No. 9(89)) defines computer espionage as the acquisition, disclosure, transfer, or use of professional or commercial secrets without authorization, intending economic harm or illicit economic advantage (Hedayati Chenani, 2021). Iran's Electronic Commerce Law of 2003 similarly criminalizes the illegal acquisition and dissemination of commercial and economic secrets within the electronic environment, prescribing penalties for such actions. Specifically, Article 501 of the Islamic Penal Code imposes imprisonment from one to ten years for individuals who deliberately disclose national policy secrets to unauthorized persons, reflecting the severe implications of espionage within the military. Additionally, Article 24 of the Islamic Republic of Iran's Penal Code for Armed Forces defines espionage with a focus on the military context, mandating harsh penalties for military personnel who provide classified information to enemies or unauthorized foreign entities (Fatahi Zafarkandi, 2019).

Another significant cybercrime within the military is the unauthorized disclosure of confidential information and data. Access to military information is restricted due to national security considerations, and most governments implement classification systems to balance the state's need for confidentiality with the public's right to information. Disclosure of classified military data jeopardizes national security and is therefore treated as a severe offense. Article 501 of the Islamic Penal Code stipulates imprisonment for individuals who knowingly or intentionally disclose national policies to unauthorized persons, equating such actions with espionage. Furthermore, military-specific regulations, such as Article 48 of the Disciplinary Regulations of the Armed Forces of the Islamic Republic of Iran, mandate strict adherence to information protection protocols, imposing imprisonment from six months to two years for unauthorized disclosures. Article 26 of the Penal Code for Armed Forces outlines more severe penalties based on the classification level of the disclosed information, ranging from three to fifteen years of imprisonment, highlighting the differentiated treatment based on the sensitivity of the information involved (Sarikhani, 2014).

Participation in unauthorized protest campaigns also constitutes a significant cybercrime within the military, posing substantial risks to national security. Article 498 of the Islamic Penal Code criminalizes the formation or management of groups aimed at undermining national security, prescribing imprisonment from two to ten years for non-military personnel and defining similar offenses within the Armed Forces Penal Code. The formation of such groups, especially when conducted via the internet, leverages the expansive reach and potential harm of cyber platforms, necessitating stringent legal measures to prevent the destabilization of national security through collective actions. Negligence or carelessness in handling classified information represents another critical cybercrime within the military context. Given the extensive use of social networks and the ease of information dissemination, even inadvertent lapses in information security can lead to significant national security breaches. Article 506 of the Disciplinary Regulations imposes imprisonment from one to three years for military personnel whose negligence results in the unauthorized disclosure of classified information. Similarly, Article 14 of the Penal Code for Armed Forces mandates imprisonment for three months to one year for military personnel who, through carelessness, disclose classified information. These regulations underscore the imperative for stringent information security protocols and the severe consequences of failing to adhere to them within the military.

Criminalization of cybercrimes remains a fundamental strategy in combating cyber offenses within the military. Establishing clear legal definitions and stringent penalties serves as a deterrent against

the perpetration of such crimes. According to Naimi (2022), criminalization can adopt a preventive role by deterring potential offenders through the threat of punishment, thereby reducing the incidence of cybercrimes (Naimi, 2022). This approach aligns with the principle that increasing the likelihood of punishment diminishes the prevalence of criminal behavior (Wilson, 1983). In the context of the military, criminalizing cyber offenses involves codifying specific acts as crimes, defining their scope, and implementing corresponding penalties. For instance, the differentiation between various levels of classified information and the corresponding legal repercussions ensures that the severity of the punishment matches the gravity of the offense. Additionally, legislative measures must account for the unique operational environments of military personnel, ensuring that the laws are both comprehensive and adaptable to evolving cyber threats.

Effective criminalization requires not only robust legal frameworks but also the integration of sociological strategies to address the root causes of cybercrimes. Najafi Abrandabadi (2009) emphasizes that criminalization should be complemented by societal measures, such as enhancing awareness and education about cyber threats, thereby fostering a culture of compliance and vigilance within the military (Najafi Abrandabadi, 2009). By incorporating both legal and sociological dimensions, prevention policies can more effectively mitigate the risks associated with cybercrimes, ensuring that military personnel are both aware of the legal consequences and equipped with the knowledge to prevent such offenses.

Enhancing media literacy and fostering critical thinking among military personnel are pivotal strategies in preventing cybercrimes. Media literacy equips individuals with the skills to critically evaluate and analyze media messages, discern credible information from misinformation, and effectively navigate the complexities of cyberspace (Shams, 2014). In the military context, media literacy training can empower personnel to recognize and mitigate the risks associated with cyber threats, such as phishing, social engineering, and the dissemination of malicious content. Studies, such as those by Anapang, have demonstrated that individuals who undergo media literacy training exhibit higher levels of awareness and critical thinking, making them less susceptible to cyber manipulations (Najafi Abrandabadi, 2009).

Critical thinking, as defined by Rouhparvar (2022), involves the ability to adopt a rational and reasoned approach to problem-solving, enabling individuals to assess the validity of information and make informed decisions. In the military, fostering critical thinking is essential for evaluating the reliability of cyber information, identifying potential threats, and developing effective countermeasures. Encouraging a culture of skepticism and analytical reasoning within the armed forces can significantly reduce the likelihood of personnel falling victim to cyberattacks or inadvertently contributing to security breaches. Moreover, critical thinking enhances the ability of military personnel to respond adaptively to dynamic cyber environments, ensuring that they can effectively counter emerging threats and maintain operational security (Rouhparvar, 2022).

Institutionalizing a culture of cyberspace usage and localizing technological practices are essential components of effective cybercrime prevention within the military. Cultural localization involves adapting technological tools and practices to align with the specific cultural, operational, and security needs of the military organization (Saberi, 2017). This process ensures that cyberspace is utilized in a manner that enhances national security, leverages existing technological assets, and mitigates the risks associated with cyber vulnerabilities. By fostering a culture that prioritizes cybersecurity and adheres to localized protocols, the military can create a resilient and secure cyber environment.

Moreover, organizational integration of cybersecurity measures involves embedding security practices into the everyday operations of military institutions. This includes the implementation of

standardized protocols for information handling, regular cybersecurity training, and the establishment of dedicated cybersecurity units within the military structure (Izadi Tameh, 2018). Effective integration ensures that cybersecurity is not an isolated function but a core aspect of military operations, thereby enhancing the overall security posture of the armed forces.

The strategic localization of technology also involves the development and deployment of indigenous cybersecurity solutions tailored to the unique needs of the military. This approach reduces dependency on foreign technologies, mitigates the risks of supply chain vulnerabilities, and enhances the ability to respond swiftly to emerging cyber threats. Additionally, localized technological practices facilitate the creation of robust defense mechanisms that are congruent with national security objectives and operational requirements (Izadi Tameh, 2018).

Institutionalizing a culture of cybersecurity within the military encompasses not only technological measures but also the cultivation of ethical standards and professional responsibilities related to cyber conduct. This holistic approach ensures that military personnel are not only technically proficient but also ethically committed to maintaining the integrity and security of cyberspace. By fostering a pervasive culture of cybersecurity, the military can effectively deter cybercrimes and enhance its defensive capabilities against cyber threats.

Structural transformations driven by the adoption of information and communication technologies have presented new challenges to human societies, including the armed forces. Cybercrimes within the military are an emergent phenomenon in the era of globalization and modernization, altering the nature and scope of criminal activities. The proliferation of the internet and the expansion of its bandwidth have not only transformed the quantitative and qualitative aspects of cybercrimes but have also facilitated the migration of criminal activities from the physical realm to cyberspace. This study examined four primary cybercrimes within the armed forces: espionage, disclosure of classified information, negligence or carelessness, and participation in unauthorized protest campaigns. Comparative analysis reveals that while some countries, such as France, extend the definition of espionage to include objects, Iranian military laws predominantly focus on information as the subject of espionage. Additionally, unlike progressive nations that classify aiding espionage as a distinct offense, Iranian laws metaphorically incorporate such acts within broader legal provisions. The regulation of participation in protest campaigns via the internet underscores the necessity for stringent legal penalties due to the extensive reach and potential harm of such actions. Furthermore, the criminalization of negligence and carelessness in handling classified information highlights the need for clear legal definitions and robust training programs to prevent security breaches. These findings underscore the imperative for comprehensive legal frameworks and preventive measures tailored to the unique cybercrime challenges faced by the military.

References

Amani Kalarijani, A. (2016). Virtual space and the analysis of preventive policies in the control of emerging social harms. *Crime Prevention Approach*.

Asgharzadeh, A., Mohammadzadeh, M., & Mirjamehri, A. (2023). Investigating the institutionalization of virtual education culture (a psychological study). 2nd Researcher scientific Congress, Bandar Abbas.

Avi, A. (2014). *The course of philosophy in Europe*. Zovar.

Fatahi Zafarkandi, S. (2019). Prevention of the cyber espionage crime of the armed forces and its role in ensuring the right to security. *Islamic human rights studies*, *9*(1).

Gastorn, K. Relevance of International Law in Combating Cybercrimes: Current Issues and AALCO's Approach.

Hedayati Chenani, R. (2021). Examining the crime of espionage in international law and the criminal law of the armed forces. *Research and studies of Islamic sciences*, *3*(24).

Izadi Tameh, A. (2018). The effect of new technologies on training and development of human capital in military organizations. *Naja Human Resources Scientific Quarterly*, *2*(25).

Mbanaso, U., & Dandaura, E. (2015). The Cyberspace: Redefining A New World. *IOSR Journal of Computer Engineering (IOSR-JCE)*, *17*(3).

Naimi, R. (2022). The principles, standards and obligations governing criminalization in Iran's legal system. *Quarterly journal of interdisciplinary jurisprudence studies*, *2*(4).

Najafi Abrandabadi, A. H. (2009). *Just Prevention of Crime, a collection of criminal science articles in honor of Dr. Ashuri*. Samit Publications.

Rouhparvar, E. (2022). Investigate the Effectiveness of Critical Thinking Training Package in Adolescents' Attitudes and Harmful Use of Virtual Social Networks Among High School Students. *Military Psychology*, *13*(50).

Saberi, A. (2017). Scientific and cultural engineering in order to institutionalize media literacy. The second international conference on media and information literacy on the topic of family,

Safari, A. (2001). Theoretical foundations of crime prevention. *Legal Research*.

Sarikhani, A. (2014). *Crimes against public security and comfort*. University of Qom.

Shams, A. (2014). Media literacy, virtual space management technique. The second international research conference in science and technology,

Wilson, J. Q. (1983). *Thinking about Crime*. Basic Books Inc.