Police Criminological researches Journal

Vol. 01 / NO. 01 / winter 2021 Pages 1 - 25

Amin police University

Non-criminal prevention of national security threats in the face of cyber terrorism

Hojjat Sabzevari Nejad[1]
Mohammad Rezazadeh Sultanabad[2]✉

Received: 2020/11/30
Date of acceptance: 2021/03/15
Article Type: Research

Abstract

Field and Aims: Cyber terrorism is a real threat to the rapid advancement of technology today. The rapid rise of Internet users and their reliance on them has alarmingly increased security risks, but despite adequate security measures to help prevent security risks, they have not been sufficient. These threats could potentially damage Iran's national security and critical infrastructure. Therefore, this study examines the impact of cyber terrorism on Iran's national security threats. Also, what are the social prevention strategies and the situation of Iran's national security threats in the direction of cyber terrorism?

Methodology: Due to the nature of the subject, the present study is done in terms of applied purpose and in terms of collecting information by documentary method and by studying domestic laws, international documents and valid sources and the obtained information is analyzed descriptively-analytically. has taken.

Findings: A combination of social and situational prevention strategies can be appropriate in the prevention of cyber terrorism, including the use of experts, crime based on technological advances, public awareness and information, education-oriented measures for the proper use of cyberspace, increase and upgrade Public welfare is the preparation of the ground for social justice.

Conclusion: There is a direct link between cyber terrorism and the threat to Iran's national security. Therefore, the Islamic Republic needs a comprehensive strategy to deal with this issue in order to ensure security and achieve its vital interests.

Keywords: national security, cyber terrorism, social prevention, situational prevention, cyber threats.

[1].Assistant Professor of Law, Islamshahr Branch, Islamic Azad University, Islamshahr, Iran. hojat.sabzavarinejad@yahoo.com
[2].Researcher PhD in Criminal Law and Criminology, Science and Research Branch, Islamic Azad University, Tehran, Iran.
(Corresponding Author): dr.mohamadrezazadeh@gmail.com

فصلنامه علمی پژوهش‌های جرم شناختی پلیس

دوره اول / شماره ۱ / زمستان ۱۳۹۹ **صفحات ۱ تا ۲۵**

پیشگیری غیرکیفری از تهدیدات امنیت ملی در راستای تروریسم سایبری

حجت سبزواری‌نژاد[۱]

محمد رضازاده سلطان آباد[۲]✉

تاریخ دریافت: ۱۳۹۹/۰۹/۱۰

تاریخ پذیرش: ۱۳۹۹/۱۲/۲۵

نوع مقاله: پژوهشی

چکیده:

زمینه و هدف: تروریسم سایبری امروزه تهدیدی واقعی نسبت به پیشرفت سریع تکنولوژی محسوب می‌گردد. افزایش سریع کاربران اینترنت و اتکاء به آن به طرز نگران‌کننده‌ای ریسک‌های امنیتی را افزایش داده است، علیرغم اینکه تدابیر امنیتی مناسبی برای کمک به پیشگیری از ریسک‌های امنیتی وجود داشته، ولی کافی نبوده است. این تهدیدات می‌تواند بطور بالقوه، امنیت ملی ایران و زیرساخت حیاتی آن را مورد آسیب قرار دهد. لذا، در این پژوهش به بررسی این امر پرداخته می‌شود که تروریسم سایبری چه تأثیری بر تهدیدات امنیت ملی ایران می‌گذارد؟ همچنین، راهکارهای پیشگیری اجتماعی و وضعی از تهدیدات امنیت ملی ایران در راستای تروریسم سایبری چیست؟

روش‌شناسی: باتوجّه به ماهیّت موضوع، پژوهش حاضر از نظر هدف کاربردی و به لحاظ گردآوری اطلاعات به روش اسنادی و از طریق مطالعه قوانین داخل، اسناد بین‌المللی و منابع معتبر انجام شده و اطلاعات به دست آمده به صورت توصیفی- تحلیلی مورد تجزیه وتحلیل قرار گرفته است.

یافته‌ها: ترکیبی از راهکارهای پیشگیرانه اجتماعی و موقعیت‌مدار به صورت توأمان می‌تواند در پیشگیری از تروریسم سایبری مناسب باشد که شامل بهره‌گیری از خبرگان، جرم‌انگاری براساس پیشرفت‌های تکنولوژی، آگاه‌سازی و اطلاع‌رسانی همگانی، اقدامات آموزش‌محور در جهت بکارگیری صحیح از فضای سایبری، افزایش و ارتقای درجه رفاه همگانی، مهیاسازی زمینه و بستر عدالت اجتماعی است.

نتیجه‌گیری: ارتباط مستقیمی بین تروریسم سایبری و تهدید امنیت ملی ایران وجود دارد. لذا، جمهوری اسلامی نیازمند استراتژی جامعی برای مقابله با این مسأله در جهت تضمین امنیت و دستیابی به منافع حیاتی خود دارد.

واژگان کلیدی: امنیت ملی، تروریسم سایبری، پیشگیری اجتماعی، پیشگیری وضعی، تهدیدات سایبری.

[۱]. استادیار گروه حقوق، واحد اسلامشهر، دانشگاه آزاد اسلامی، اسلامشهر، ایران. hojat.sabzavarinejad@yahoo.com

[۲]. پژوهشگر دکتری حقوق کیفری و جرم‌شناسی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران.

نویسنده مسئول: dr.mohamadrezazadeh@gmail.com

مقدمه

امروزه فضای سایبری در پرتو جهانی شدن ارتباطات نه تنها فرصت عرضه و تبیین خود را در گستره جهانی پیدا کرده، بلکه دیگر دنیای بدون فضای سایبری برای استفاده‌کنندگان از آن که هر روز بر شمار آن افزوده می‌شود، قابل تصور نیست.

همچنان که جهان امروز در معرض دگرگونی، تغییر و تحولات فزاینده‌ای قرار دارد، شاهد بروز و ظهور چالش‌ها و بحران‌های جدید هستیم که فضای سایبری نیز از آن بی‌نصیب نیست. از جمله این چالش‌ها ظهور گروه‌های تروریستی سازمان‌یافته است که در طول زمان توانسته‌اند خود را با فناوری روز تطبیق داده و فضای مجازی را همانند فضای حقیقی ناامن گردانند (میور و جاینسن[1]، ۲۰۲۰: ۵).

اصطلاح «تروریسم سایبری» پیچیده است و دو مفهوم را با هم ترکیب می‌کند: «سایبر» اشاره به فضای مجازی، و «تروریسم» که معنی و دامنه آنها بعداً تحلیل خواهد شد. بر این اساس، می‌توانیم فرض کنیم تروریسم سایبری نوع خاصی از تروریسم است، جایی که مکان یا واسطه‌ای که در آنجا اقدام تروریستی انجام می‌شود، فضای مجازی است (فلتچر[2]، ۲۰۰۶: ۴).

آنچه که در قالب تروریسم سایبری ظهور نموده، قادر است تا فضای سایبری را در اشکال گوناگون ناامن گرداند. این ناامنی هم می‌تواند در حملات سایبری به زیرساخت‌های یک دولت باشد و هم می‌تواند با استفاده از ویژگی کنترل‌ناپذیری فضای مجازی موجبات ناامنی کودکان و نوجوانان را فراهم کند. اما ویژگی سایبری در کنار تروریسم ماهیت آن را از تروریسم سنتی جدا نمی‌کند و بر این اساس، همچنان چالش اصلی در عدم اجماع پیرامون تعریف و ماهیت تروریسم است.

عامل اصلی در عدم اجماع پیرامون ارائه تعریف مشخص از تروریسم، استفاده از این اصطلاح برای اهداف سیاسی است. اگرچه در محافل آکادمیک تعریف‌هایی در این زمینه ارائه شده، اما در اسناد بین‌المللی شاهد ارائه تعریفی واضح و مشخص از این پدیده نیستیم (جیل و کرنر[3]، ۲۰۱۷: ۳). البته، در قالب دکترین تلاش‌هایی برای تعریف یا ارائه چارچوب تروریسم سایبری شده است. بر این اساس، تروریسم سایبری به معنای تهاجم و تهدید به تهاجم غیرقانونی به رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آنهاست که به منظور ارعاب یا وادار کردن یک دولت یا مردم آن به پیشبرد اهداف سیاسی یا اجتماعی خاص صورت می‌گیرد (هنکوک[4]، ۲۰۰۱: ۵۵۳).

---

1. Muir & Joinson
2. Fletcher
3. Gill & Corner
4. Hancock

از نظر ساختار، تروریسم همیشه جنایتی سازمان‌یافته است، اگرچه عمل تروریستی توسط یک شخص می‌تواند انجام شود. در حقیقت، چیزی به عنوان «تروریست‌های فردی»[1] وجود ندارد، بنابراین، خطر خاص ناشی از تروریسم که تا حدی مجازات شدید آن را در رابطه با سایر جرایم توجیه می‌کند، در وجود یک مجموعه سازمان‌یافته نهفته است که به طور سیستماتیک برای ارتکاب تعداد نامعلوم جرایم فعالیت می‌کند (ویلگس[2]، ۲۰۱۶: ۳).

این امر از آن جهت حائز اهمیت است که ممکن است اقدامی مخرب از طریق فضای مجازی توسط یک هکر انجام گیرد، اما اگر این فرد به یک گروه تروریستی سازمان‌یافته مرتبط نباشد، اقدام او در قالب تروریسم سایبری قابل شناسایی نیست.

موضوع تروریسم سایبری از آن جهت که تاثیر بر نظم و امنیت جامعه دارد، بسیار حائز اهمیت است. لذا، این نگرانی وجود دارد که چگونه خطرات آن را مدیریت کنیم. اگر بخواهیم به یک مدیریت موثر و ایمن اطلاعات برسیم، همه باید مسئولیت مسائل مربوط به امنیت سایبری را به عهده بگیرند (یوهانسن[3]، ۲۰۱۷: ۵).

در این میان و در پیوند با این امر، امنیت انتظامی می‌تواند در ایجاد فضای ایمن موثر باشد. از آنجا که امنیت انتظامی، ایجاد و گسترش حالتی است که در آن منافع و ارزش‌های حیاتی جامعه در برابر تهدیدهای موجود حفظ و تأمین می‌گردند (وفادار و دیگران، ۱۳۸۹: ۲)، لذا توجه به تهدیدات تروریستی در فضای سایبری نیز باید بخشی از سیاست‌های پیش‌بینی‌شده را شامل گردد.

اهمیت این امر تا بدانجاست که متن در سند چشم‌انداز بیست ساله توسعه به داشتن شرایطی «امن، مستقل و مقتدر با سامان دفاعی مبتنی بر بازدارندگی همه‌جانبه» اشاره شده است. بدیهی است تدوین سیاست‌هایی برای مقابله با تهدیدات تروریسم سایبری و ایمن نگهداشتن فضای سایبری می‌تواند بخشی از اقداماتی باشد که موجب تحقق اهداف سند چشم‌انداز توسعه گردد.

البته، این امر امروزه مورد توجه سایر کشورها نیز می‌باشد، بطوری که اداره اطلاعات آمریکا[4] که وظیفه هماهنگی شانزده سازمان اطلاعاتی آمریکا را بر عهده دارد، از سال ۲۰۱۰ تا به امروز که به بررسی تهدیدات امنیت ملی آمریکا می‌پردازد، تهدیدهای سایبری را از مهمترین تهدیدهای فراروی امنیت ملی آمریکا ذکر کرده است (یزدان‌پناه و کامران، ۱۳۹۴: ۳۶).

بر این مبنا، نظام‌های حقوقی همیشه با توجه به تحولات فناورانه، در تلاش برای مطابقت با این نوآوری‌ها بوده‌اند که ظهور پدیده‌ای با عنوان «تروریسم سایبری» در سال‌های اخیر با مصادیق

1. Individual terrorists
2. Villegas
3. Johansson
4. Director of National Intelligence

متعدد در کشورهای مختلف به عنوان تهدید جدی و بالقوه برای امنیت ملی و بین‌المللی است و قوه قانون‌گذاری کشورها و سازمان‌های بین‌المللی را در راستای مبارزه هدفمند با این پدیده مصمم‌تر نموده است. لذا، در این پژوهش به بررسی این امر پرداخته می‌شود که تروریسم سایبری چه تأثیری بر تهدیدات امنیت ملی ایران می‌گذارد؟ همچنین راهکارهای پیشگیری اجتماعی و وضعی از تهدیدات امنیت ملی ایران در راستای تروریسم سایبری چیست؟

۱. ادبیات تحقیق

اغلب چنین گفته‌اند که تعریف پذیرفته‌شده‌ای از تروریسم وجود ندارد، زیرا تروریسم واژه‌ای مبهم است که هر کشور براساس اهداف و مقاصد سیاسی خود آن را تعریف و تفسیر می‌نماید. (سنبلی، ۱۳۸۰: ۱۱۲۵) بر این اساس در تعریفی از تروریسم می‌توان گفت: «کاربرد غیرقانونی یا تهدید به کاربرد زور یا خشونت بر ضد افراد یا اموال برای مجبور یا مرعوب ساختن حکومت‌ها یا جوامع که اغلب به قصد دستیابی به اهداف سیاسی، مذهبی یا ایدئولوژیک صورت می‌گیرد (فیرحی و ظهیری، ۱۳۸۷: ۱۴۸).

برخی براساس برداشتی که از مفهوم تروریسم قابل درک است به تعریف تروریسم پرداخته‌اند بر این اساس آن را «استفاده غیرمجاز از زور علیه اشخاص و اموال، تا دولت، شهروندان یا هدف دیگری را به منظور پیشبرد هدف خاصی مورد تهدید یا اجبار قرار دهند.» (گوهری مقدم، ۱۳۸۶: ۹۲)

الکس اشمید دست به تحلیل تجربی در مورد تروریسم می‌زند و بیست و دو مولفه مشترک برای آن در نظر می‌گیرد. از جمله اینکه تروریسم نوعی جنگ است، در آن از ابزار خشونت علیه مردم استفاده می‌شود، استفاده از عامل خشونت حد و مرز ندارد و هدف تروریست‌ها نابود ساختن، به منظور اعمال فشار و یا تغییر در نگرش‌های مردم است. (کورنر[1]، ۲۰۰۲: ۴)

نوام چامسکی نیز در تعریف خود از تروریسم آن را «کاربرد خشونت یا تهدید به اعمال خشونت برای دستیابی به اهدافی که طبیعت سیاسی، مذهبی یا عقیدتی دارند. این امر از طریق اعمال زور یا ایجاد ترس و وحشت انجام می‌گیرد و بیشتر غیرنظامیان را هدف قرار می‌دهد» (چامسکی، ۱۳۸۳: ۵).

۲. پیشینه تحقیق

- عبدی (۱۳۹۵)، در مقاله‌ای تحت عنوان «**تروریسم سایبری علیه ایران**» به این موضوع پرداخته است که تروریسم سایبری و رسانه‌ای جزء جدیدترین شکل و مصداق تروریسم است که

1. Connor

در این نوشتار به عنوان یک پدیده مجرمانه مورد تحلیل و بررسی قرار می‌گیرد. یافته‌های این پژوهش نشان می‌دهد که عواملی از قبیل افزایش انواع سلاح‌ها، عدم قانون‌گذار به‌روز، رفتار دوگانه با تروریسم باعث افزایش این پدیده شده است، در کنار این دو اصل باید از توسعه وسائل ارتباط جمعی (همچو فیس‌بوک و...) نام برده که به تروریست‌ها در آشنا کردن با اهداف و انگیزه‌هاشان یاری می‌رسانند؛ و بهترین راه مقابله با اقدامات تروریستی در محیط سایبر، تقویت اقدامات امنیتی در شبکه‌های رایانه‌ای و اینترنتی، قوانین حقوقی به‌روز، و تشکیل شورای مجازی یا سازمانی مقتدر در ایران علیه تروریسم سایبری می‌باشد و این امر مستلزم انجام مطالعات در خصوص تاثیر انقلاب اطلاعاتی بر امنیت ملی است تا باعث کاهش آسیب‌پذیری‌ها و تقویت امنیت ملی در مقابل تروریسم سایبری شود.

- رزمخواه (۱۳۹۵)، در مقاله‌ای با عنوان «**مقابله با تروریسم سایبری در چارچوب نظام حقوقی سازمان‌های بین‌المللی**» به این امر پرداخته که تروریسم سایبری، به عنوان یکی از چالش‌های عصر حاضر در اغلب اسناد حقوقی مرتبط با امنیت سایبری، به عنوان یک تهدید جدی علیه صلح و امنیت بین‌المللی معرفی و بر لزوم مبارزه با آن تاکید شده است. در این زمینه نمی‌توان منکر نقش سازمان‌های بین‌المللی جهانی و منطقه‌ای از جمله سازمان ملل متحد، اتحادیه اروپایی، شورای اروپا و اتحادیه آفریقا در زمینه مبارزه با تروریسم سایبری شد. آنچه مسلم است همکاری و هماهنگی اعضای جامعه بین‌المللی در راستای تدوین یک رهیافت حقوقی جامع و منسجم جهانی در جهت مقابله با تروریسم سایبری امری ضروی و البته اجتناب‌ناپذیر است.

- میربد؛ سلیمی؛ نیاورانی و زمانی (۱۳۹۸)، «**تروریسم سایبری: نقض حقوق بشر و آزادی‌های بنیادین**» تروریسم سایبری به عنوان گونه‌ای جدید از تروریسم، نشانگر آسیب‌پذیربودن تابعان حقوق بین‌الملل در فضای سایبر است. اگر تروریست‌ها زیرساخت‌های حیاتی یک دولت مانند حمل نقل هوایی، سدها، نیروگاه‌های هسته‌ای و تولید برق، سیستم بانکی و مالی را با انواع بدافزارها مورد حمله قرار دهند و از این طریق باعث رعب و وحشت عمومی گردند و با داشتن انگیزه‌های سیاسی یا ایدئولوژیک این اقدامات را در راستای اجبار دولت یا سازمان‌ها انجام دهند، آنگاه تروریسم سایبری محقق می‌گردد. جامعه جهانی بر سر تعریف جامعی از تروریسم، به توفیقی دست نیافته و حتی سند جامع الزام‌آوری نیز در این موضوع وجود ندارد، اما این شکل از تروریسم به همراه دیگر گونه‌های نوینی چون بیوتروریسم، تروریسم هسته‌ای و اکوتروریسم، ممکن است خسارات زیان‌بارتری نسبت به انواع کلاسیک تروریسم ایجاد کند. تروریسم سایبری تهدیدی علیه صلح و امنیت بین‌المللی است و در عین حال ناقض قواعد حقوق بشر در هر چهار نسل شناخته‌شده آن نیز به شمار می‌آید. اهمیت پرداختن به نقض حقوق بشر

توسط تروریست‌ها در فضای سایبر و نیز در سیاق مبارزه با تروریسم سیابری در مقابله همه‌جانبه با این پدیده باید مطمح نظر قرار گیرد.

یافته‌های تحقیق

۱. تأثیر تروریسم سایبری بر امنیت ملی ایران

بسیاری از کارشناسان و تحلیل‌گران حوزه امنیت بر این باورند که پایان یافتن دوران جنگ سرد نه تنها منجر به امن‌تر شدن جهان نشده است، بلکه به وجود آمدن چالش‌های امنیتی غیرنظامی جدیدی هم‌چون تخریب محیط زیست، رفاه اقتصادی، سازمان‌های جنایی بین‌المللی و مهاجرت گسترده افراد، امنیت جهانی را با چالش‌های جدی تری نسبت به گذشته مواجه ساخته است. تحلیل‌گران بر این باورند که اهمیت این مسائل «جدید» نه تنها بازاندیشی در تهدیدهای امنیتی، بلکه تجدیدنظر درباره خود مفهوم امنیت را ضروری می‌سازد (خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱: ۱۷۹).

در عین حال، انتقادی که بر ادبیات موجود امنیت وارد است، این است که اغلب این متون به تهدیدهای سایبری به عنوان یکی از همین چالش‌های امنیتی جدید که در این زمینه هم بسیار پراهمیت به نظر می‌رسد، توجه اندکی داشته‌اند. آنچه در مورد این تهدیدهای جدید قابل توجه است، این است که تهدیدهای سایبری در قالب تروریسم به عنوان یکی از بدترین تهدیدهای منافع ملی تلقی می‌شوند (نجفی علمی و نقیب السادات، ۱۳۹۳: ۶۰).

خطر سایبری طیف گسترده‌ای از خطرات سیستم‌های دیجیتال را شامل می‌شود، مانند نقض داده‌ها یا حملات سایبری کامل به شبکه برق، زیرساخت‌های نظامی، سدها و غیره. همچنین، با توجه به توسعه روزافزون فناوری، روش‌های گروه‌های تروریستی در اقدامات تروریستی از طریق فضای سایبری نیز دائما در حال تحول و پیشرفت می‌باشد (جیکوب و دیگران[1]، ۲۰۲۰: ۷).

نکته مهم در مقابله با تهدیدات امنیتی سایبری گروه‌های تروریستی این است که باید توان فکری مردم در مقابله با تحرکات تروریستی را تقویت نمود. محققان تروریسم را یک استراتژی دانسته‌اند که مبتنی بر سه اصل و مرحله است (معصومی و ساعی، ۱۳۹۱: ۵۷)، بنابراین، هدف تروریست‌های سایبری ایجاد خشونت صرف و یا انجام یک اقدام نظامی نیست، بلکه در مرحله اول، هدف، ایجاد ترس و وحشت از طریق فضای سایبر در میان شبکه‌های اجتماعی مجازی و کاربران آن است و سپس، در مرحله بعد منتظر پاسخ اشتباه دولت به این اقدام می‌نشیند؛ هدف در این مرحله به قضاوت کشیدن ذهن و فکر توده‌های مردم است. سپس، در مرحله سوم سعی در

[1]. Jacob & others

انتقال مشروعیت از نظام حاکم به تروریست‌ها در دستور کار قرار می‌گیرد. استراتژی تروریسم به شکل جدید به چالش کشیدن مشروعیت نظام حاکم در فضای سایبر و برهم زدن امنیت ملی جمهوری اسلامی از این طریق است.

ساختار اینترنت و فضای سایبر اساساً چالش‌های امنیتی برای دولت‌ها به وجود می‌آورد. اینترنت به عنوان یک سیستم نامتمرکز طراحی شده و کاربران آن غالبا شناخته شده نیستند. همین ناشناختگی باعث می‌شود هیچ اثری از برخی از حملات تروریسمی سایبری باقی نماند. این چالش باعث قدرتمندتر شدن بازیگران قوی و ضعیف می‌شود؛ چرا که ناشناخته بودن یک مزیت برای آن‌ها به حساب می‌آید. بنابراین، در حالی که تداوم این نوآوری فرصت‌های بیشتری برای استفاده مؤثر از اینترنت ارائه می‌کند، برخی نیز از همین مزیت برای حملات سایبری استفاده می‌کنند (عظیمی و خشنودی، ۱۳۹۵: ۱۶۷).

ویژگی مهم فعالیت‌های تروریستی در جمهوری اسلامی ایران آن است که این گروه‌ها از سوی بازیگران منطقه‌ای و فرامنطقه‌ای مخالف ایران، از جمله ایالات متحده آمریکا مورد حمایت مالی، سازمانی و تسلیحاتی قرار می‌گیرند و از این منظر تهدیدی جدی برای امنیت ملی محسوب می‌شوند. تحول چشم‌گیر در فعالیت گروه‌های تروریستی در سال‌های اخیر، بهره‌گیری آن‌ها از قابلیت‌ها و امکانات فضای سایبر مانند پخش تصاویر بریدن سر گروگان‌ها در شبکه‌های اجتماعی همچون توئیتر و... است.

تروریسم سایبری به واسطه کاربست فزاینده فناوری‌های اطلاعاتی و ارتباطاتی از سوی دولت‌ها برای تسریع، افزایش کارایی و کاهش هزینه‌های مرتبط با خدمت‌رسانی به شهروندان، اهمیت فزاینده‌ای پیدا کرده است؛ به گونه‌ای که حتی دولت‌ها نیز از تروریسم سایبری به عنوان ابزاری در الگوهای تنازعی خود استفاده می‌کنند. در این میان، مهم‌ترین مولدهای ناامن‌کننده فضای مجازی در بُعد تروریسم، در دو گروه عمده طبقه‌بندی می‌شوند: گروه اول، کسانی که به یک کشور خارجی وابسته‌اند، از قبیل بخش‌های نظامی، سازمان‌های امنیتی و شرکت‌هایی که وابستگی زیادی به دولت آن کشور دارند و گروه دوم، تروریست‌ها و گروه‌های افراطی. این افراد، ممکن است به دولت خاصی وابستگی نداشته باشند، ولی در جهت اهداف خود اقدام به خرابکاری می‌کنند (نورمحمدی، ۱۳۹۰: ۷۷).

لذا، تروریسم سایبری را می‌توان حمله سایبری دانست که توسط یک گروه تروریستی یا افراد وابسته به آنها صورت می‌پذیرد. موضوع تروریسم سایبری از این جهت که فردی در گوشه‌ای از دنیا تنها با استفاده از رایانه امکان حمله به زیرساخت‌های یک کشور و نقاط حساس و مهم آن را دارد، بسیار حائز اهمیت است؛ زیرا هم به لحاظ مالی، هزینه و لجستیک یک عملیات فیزیکی را

ندارد و هم قابلیت رهگیری افرادی که اقدام به حملات تروریستی از طریق فضای سایبری می‌کنند، بسیار سخت است.

در سال‌های گذشته، کشورهای مختلفی کانون حملات تروریسم سایبری بوده‌اند و از این رو، بسیاری از کشورها استراتژی‌هایی را برای مقابله با این پدیده تدوین نموده‌اند. بطور مثال، استرالیا قانونی را در خصوص تروریست‌ها به منظور جلوگیری از پست الکترونیک (با تفویض اختیار به سازمان اصلی امنیت اطلاعات استرالیا) و حمله مستقیم علیه آماده‌سازی برنامه‌ریزی فعالیت‌های تروریستی وضع کرد. این قانون اجازه می‌دهد که اموال تروریستی ضبط شده یا کنار گذاشته شود. نیوزیلند نیز به منظور اجرای توافق دوجانبه در زمینه هماهنگی قانونی بین این دو کشور قانون مشابه‌ای را وضع کرد (بوگانسکی و پترسکی، ۱۳۹۴: ۲۶۰).

در حقیقت، فناوری ابزار جدیدی را در اختیار تروریست‌ها قرار داده است که با استفاده از آن و بدون آن که خطرهای سایر اقسام تروریسم را برای آنها در بر داشته باشد، می‌توانند اهداف وحشت‌بار خود را عملی سازند. گسترش استفاده از این فضای مجازی که از دهه ۱۹۹۰ شدت گرفته است، امکان رسیدن تروریست‌ها به اهدافشان را بیشتر کرده است. حضور میلیون‌ها کاربر در دنیای مجازی، همراه با شرکت‌ها، کارخانجات و صنایع عمده بسیار که در اغلب موارد از قابلیت آسیب‌پذیری بالایی برخوردارند، خطر استفاده سوء از فضای مجازی را بیشتر کرده و جذابیت آن را نیز افزایش داده است (کارگری، ۱۳۹۰: ۷۳ – ۷۲).

در این میان، ایران در چند سال گذشته با حملات سایبری متعددی مواجه بوده که معروف‌ترین آنها استفاده از ویروس استاکس نت[1] برای حمله به تاسیسات اتمی ایران بوده است. اما بدافزارهای دیگری چون مینی فیلم، گاوس، مادیا[2] و داکو فضای سایبری ایران را تهدید کرده است. البته، خلأ قانونی در مبارزه علیه تروریسم به خصوص تروریسم سایبری در دولت‌های مختلف دنیا وجود دارد. در قوانین ایران قبل و بعد از انقلاب نیز این خلأ دیده می‌شود، زیرا توجه جدی به آن نشده است. با توجه به اینکه امروزه این نوع تروریسم تهدید جدی برای امنیت و صلح بین‌المللی به ویژه ایران است و با وجود حمایت گسترده از گروه‌های تروریستی، لزوم اتخاذ تدابیر حفاظتی ایران دوچندان شود، به ویژه در زمینه پرکردن خلاء قانونی با حضور متخصصین و نخبگان این امر و با ایجاد قوانین به‌روز تقویت شود (عبدی، ۱۳۹۵: ۶).

بر این اساس، اتخاذ قوانین و سیاست‌هایی به منظور امنیت انسانی می‌تواند در برابر حملات احتمالی موثر باشد. امنیت انسانی دو جنبه عمده دارد: نخست، ایمنی در برابر تهدیدهای همیشگی

[1]. Staks net
[2]. Madia

دوره اول / شماره ۱ / زمستان ۱۳۹۹ - نویسندگان: حجت سبزواری نژاد، محمد رضازاده سلطان آباد

نظیر گرسنگی، بیماری و افسردگی و دوم، معنای مراقبت در برابر اختلال‌های آسیب‌رسان و ناگهانی چه در منازل، محل کار یا در اجتماع. امنیت انسانی در مراتب متفاوت خود، می‌تواند در شکل‌گیری مفهوم امنیت انتظامی نقشی ویژه داشته باشد (وفادار و دیگران، ۱۳۸۹: ۶).

۲. پیشگیری اجتماعی از تهدیدات امنیت ملی ایران در راستای تروریسم سایبری

پیشگیری اجتماعی مجموعه اقدام‌های پیشگیرانه است که برکلیه محیط‌های پیرامون فرد که در فرایند جامعه پذیری نقش داشته و دارای کارکرد اجتماعی هستند، تأثیر می‌گذارد. این روش پیشگیری از جرم با تمرکز بر برنامه‌های تکمیلی، سعی در بهبود بهداشت زندگی خانوادگی، آموزش، مسکن، فرصت‌های شغلی و اوقات فراغت دارد تا محیطی سالم و امن ایجاد نماید». در حقیقت، پیشگیری اجتماعی «به طور مستقیم یا غیرمستقیم باهدف تأثیرگذاری بر شخصیت افراد است تا از سازماندهی فعالیت خود، حول محور انگیزه‌های بزهکارانه پرهیز کنند (کی‌نیا، ۹۷:۱۳۷۶).

شورای اقتصادی و اجتماعی سازمان ملل متحد در بند (۲۵) قطعنامهٔ خود در خصوص پیشگیری اجتماعی عنوان نموده است که پیشگیری از جرم از طریق توسعه اجتماعی را با روش‌هایی مانند استفاده از راهبردهای آموزش و آگاه‌سازی عمومی برای رواج فرهنگ قانون‌مداری و انعطاف در عین احترام به هویت‌های فرهنگی و ترویج عوامل حمایتی از طریق برنامه‌های جامع و موافق توسعهٔ اجتماعی و اقتصادی و غیره امکان‌پذیر است (صفاری، ۱۳۸۱: ۴۸).

پیشگیری اجتماعی از تروریسم سایبری رشد و توسعه‌یافتگی اجتماعی، اقتصادی و فرهنگی در هر جامعه‌ای منجر به کم‌رنگ شدن انواع و اقسام جرائم و بزهکاری‌های واقعی و مجازی می‌گردد و به طور یقین بر میزان و مقدار ظهور و بروز تروریسم سایبری نیز اثرگذار است.

آموزش و اطلاع‌رسانی دو راهکار عمده‌ی پیشگیری اجتماعی هستند. تا زمانی که پیش‌زمینه‌ی فکری و فرهنگی در یک جامعه فراهم نگردد، نمی‌توان به اتخاذ تدابیر و تأثیر آن‌ها امیدوار بود. بار اصلی پیشگیری اجتماعی بر دوش دولت است و باید هم در راستای اصلاح ساختار خویش و هم آگاهانیدن شهروندان از جرائم سایبری و عوارض و عواقب آن دست به برنامه‌ریزی بزند. برخی افراد به دنبال محدودیت‌ها و محرومیت‌های اجتماعی به خرابکاری و تخریب در محیط سایبری روی می‌آورند و از سویی دیگر، پاره‌ای از آنارشیست‌ها به دنبال مهار یا حذف قدرت به عنوان علت و عامل معضلات و مشکلات اجتماعی هستند که این خود یکی از مولفه‌های اصلی و اساسی برای برانگیختن تروریسم سایبری است.

عنصر دوم مسئولیت حفظ مردم و تعهد به حقوق مدنی آن‌هاست، که شامل صفت‌هایی چون

خبررسانی، مذاکرات آزاد و مستقل و توان مشارکت در تصمیم‌گیری ها است. عنصر سوم اعتقاد و الزام به حاکمیت قانون اساسی است، انقیاد دولت به اصول اعم از قانونی یا غیر قانونی، نیاز مبرم و احتیاج بارز به اختیاراتی خاص و ویژه شامل ارائه عمومی راهکارها در حمایت و پشتیبانی از اقدامات انجام شده برای رفاه عمومی و حل‌وفصل بحران‌ها از طریق مکانیزم‌های مفید و موثر مبنا و شالوده‌ی حاکمیت دولت است، ولی از طرفی، الزام و اعتقاد به لزوم حاکمیت قانون اساسی مستلزم مقابله با افراط‌کاری‌ها و زیاده‌روی‌ها از طریق دادگاه و مراجع قضایی است (پاکزاد، ۱۳۸۸: ۲۹۵).

رهنمود ۱۹۸۷ شورای اروپا، در زمینه‌ی مبارزه فرهنگی با تروریسم با تاکید بر این که فرهنگ در تمامی جنبه‌های آن مانند علم، هنر، مذهب، تعلیم و تربیت، رسانه و ورزش قادر است در پیشگیری از بسط و گسترش تفکر تروریستی نقش مهمی را ایفا کند، اما اهمیت آن اغلب نادیده گرفته می‌شود. اینکه اساس و مبنای اقدامی فرهنگی علیه تروریسم در شناخت رابطه پیچیده و حساس بین تروریسم و زمینه‌ی فرهنگی آن نهفته است، بیان می‌دارد جامعه‌ی اطلاعاتی می‌تواند باعث بسط و گسترش بالقوه تروریسم و ایدئولوژی شود که به چندین طریق آن را تعریف می‌کنند (پاکزاد، ۱۳۸۸: ۳۳۹).

اکنون با طراحی بدافزارهای رایانه‌ای و انتشار آن در سامانه‌های زیرساختی و حیاتی یک کشور در قالب تروریسم سایبری و همچنین، ایجاد انواع شرکت‌های هرمی به منظور اخلال در اقتصاد یک کشور، انتشار سلاح‌های میکروبیولوژیکی و انتشار عمدی میکروارگانیسم‌های مختلف در قالب بیوتروریسم و انجام اقداماتی از این دست، وجه تروریسم نوین را مطرح می‌نماید. بدیهی است «زیرساخت‌های حیاتی» از بهترین اهداف محسوب می‌شوند که با توجه به الکترونیکی شدن آن‌ها، نه تنها ارتکاب اقدامات تروریستی آسان‌تر شده، بلکه لطمات واردشده بسیار غیرقابل جبران هستند. البته، ماهیت «چندرسانه‌ای» فضای سایبر، به تروریست‌ها امکان بهره‌برداری‌های سوء دیگری را هم داده است (شهبازی و براری، ۱۳۹۶: ۲۱۳).

پیشگیری اجتماعی را در دو دسته طبقه‌بندی نموده‌اند: پیشگیری اجتماعی جامعه‌مدار، پیشگیری اجتماعی رشدمدار که به تحلیل و تفسیر آن‌ها می‌پردازیم.

۲-۱. پیشگیری اجتماعی جامعه‌مدار از تهدیدات امنیت ملی ایران در راستای تروریسم سایبری

درباره‌ی فضای سایبر، علل و عوامل اجتماعی می‌توانند زمینه‌ساز جرائم و بزهکاری‌های سایبری از قبیل تروریسم سایبری نیز گردند. در تطبیق و تعمیم این رویکرد با پدیده‌های سایبری، باید به طور اصولی و اساسی بر کیفیت زندگی و انتظارات و توقعات کاربران رایانه و اینترنت از فضای مجازی

توجه و تأکید ویژه داشت. شخص به دلایل گوناگونی وارد دنیای مجازی می‌شود که مطالعه و بررسی آن‌ها می‌تواند به تبیین و تفسیر بهتر و بیشتر چرایی و چگونگی این گونه انحرافات کمک کند.

مباحث و موضوعات درباره‌ی پیشگیری جامعه‌مدار با محدودیت کدهای رفتاری مطرح می‌گردد، به طور کلی با کدهای رفتاری می‌توان گروه‌های ویژه و خاصی را که تعهد و وظیفه‌ای به آن‌ها سپرده شده است، در مقابل کارها و اعمال خود، مسئول و پاسخگو نگه داشت. از جمله آن‌ها گروه‌های شغلی و حرفه‌ای هستند که در حوزه‌های مختلف به کار و فعالیت می‌پردازند و چون که به متصدیان شبکه‌ای خود اطلاعات و داده‌های واجد ارزش و اعتبار را واگذار کرده‌اند تا با رعایت سه اصل محرمانه بودن، تمامیت و دسترس‌پذیری در فضای سایبر منتشر و توزیع کنند، ضروری است مناسب و متناسب با حرفه و شغل، نوع و میزان اطلاعات آن‌ها و دیگر شرایط کد رفتاری مربوط و مرتبط را برای آنها تدوین کنند (منفرد و جلالی فراهانی، ۱۳۹۱: ۱۴۳- ۱۴۲).

در زمینه اقدامات پیشگیرانه در حوزه پیشگیری اجتماعی از تروریسم سایبری، مسئله آموزش کاربران اینترنت، اعم از کاربران خانگی و کارکنان ادارات و فرهنگ‌سازی در جامعه، مؤثرترین عامل در انصراف بزهکاران بالقوه از ارتکاب جرم در محیط سایبر است. کاربران خانگی و کارکنان ادارات که با تأسیسات رایانه‌ای و مخابراتی مخصوصا در مراکز حساس سرو کار دارند، باید در زمینه امنیت سایبری با هدف تربیت نیروی انسانی ممتاز و متعهد، مباحث مربوط به امنیت، شامل امنیت شبکه، امنیت در سرویس‌های وب، امنیت سامانه عامل، رمزنگاری، تحلیل بدافزار، مهندسی اجتماعی معکوس، ردگیری در فضای سایبر و امنیت سامانه‌های تلفن همراه، آموزش و آگاهی کافی داشته باشند (قدیر و کاظمی فروشانی، ۱۳۹۸: ۲۴۴-۲۴۵).

در قطعنامه مجمع عمومی سازمان ملل متحد، طی ششمین نشست بررسی استراتژی جهانی ضد تروریسم، کشورهای عضو از افزایش استفاده تروریست‌ها از فناوری‌های اطلاعاتی و ارتباطی، به ویژه اینترنت و سایر رسانه‌ها و استفاده از چنین فناوری‌هایی برای ارتکاب، تحریک، استخدام، تامین اعتبار یا برنامه‌ریزی اقدامات تروریستی تاکید کردند. بر این اساس، دفتر مبارزه با تروریسم سازمان ملل متحد[1] ابتکارات متعددی در قالب برنامه امنیت سایبری در زمینه فناوری‌های جدید دارد. برنامه امنیت سایبری و فناوری‌های نوین به منظور ارتقاء ظرفیت‌های کشورهای عضو و سازمان‌های خصوصی در جلوگیری و کاهش سوءاستفاده از پیشرفت‌های فناوری توسط تروریست‌ها می‌باشد. این برنامه شامل مقابله با تهدید حملات سایبری توسط گروه‌های تروریستی علیه زیرساخت‌های حیاتی و همچنین، توسعه استفاده از رسانه‌های اجتماعی برای جمع‌آوری

[1]. The UN Office of Counter-Terrorism

اطلاعات و شواهد دیجیتالی برای مقابله با تروریسم آنلاین ضمن رعایت حقوق بشر می‌باشد. این پروژه همچنین به دنبال کاهش تأثیرات و امکان بازیابی سیستم‌های مورد هدف در صورت وقوع چنین حملاتی است.[1]

شورای امنیت که مطابق منشور ملل متحد وظیفه اصلی و اولیه حفظ صلح و امنیت بین‌المللی را بر عهده دارد، در قطعنامه خود در سال ۲۰۱۷ ضمن اشاره به اینکه تروریسم سایبری تهدیدکننده نظم و امنیت بین‌المللی می‌باشد، از دولت‌های عضو می‌خواهد «که مشارکت‌های ملی، منطقه‌ای و بین‌المللی را با ذی‌نفعان، اعم از دولتی و خصوصی، در صورت لزوم ایجاد یا تقویت کنند تا اطلاعات و تجربیات را به منظور جلوگیری، محافظت، تحقیق، پاسخگویی و بازیابی خسارات ناشی از حملات تروریستی به تأسیسات مهم و زیرساختی بتواند در زمان بروز حمله بکار گرفته شود. از جمله این اقدامات آموزش مشترک و استفاده یا ایجاد شبکه‌های ارتباطی یا هشدار اضطراری مربوطه می‌باشد.»[2]

این‌ها نیز پاره‌ای از تمهیدات و تکنیک‌های پیشگیری اجتماعی در حوزه‌ی رایانه‌ای و سایبری هستند که می‌توانند با حفظ و نگهداری آیتم‌ها و فاکتورهایی که برای حفظ و حفاظت فضای مجازی لازم هستند، از بروز و ظهور جرائم رایانه‌ای و به طور موردی تروریسم سایبری که امنیت ملی را به طور مستقیم تحت تأثیر قرار می‌دهد، ممانعت به عمل آورند.

۲-۲. پیشگیری اجتماعی رشدمدار از تهدیدات امنیت ملی ایران در راستای تروریسم سایبری

پیشگیری رشدمدار یکی از زیرشاخه‌های پیشگیری اجتماعی است که متمرکز بر کودکان و نوجوانان در معرض خطر بوده و هدف از آن مداخله در دوره‌های مختلف رشد اطفال و نوجوانان بزهکار، منحرف یا در معرض بزهکاری به منظور پیشگیری از مزمن شدن و تکراری شدن بزهکاری آنها در آینده (دوران بزرگسالی) است (یاراحمدی و میلانی، ۱۳۸۹: ۲).

از این رو، اتخاذ تدابیر و سیاست‌هایی در زمینه پیشگیری اجتماعی رشدمدار می‌تواند زمینه‌های شکل‌گیری تروریسم سایبری را کم‌رنگ نماید. این امر که امنیت همواره در کنار آموزش امکانپذیر است، امروزه به یک مهم در پیشگیری از جرم بدل شده و در سیاست‌های دولت‌ها نقش پررنگی ایفاء می‌کند.

1. A / RES / 72/284
2. SC/RES/ 2341(2017)

۱-۲-۲. اقدامات و تدابیر آموزشی و تربیتی در جهت امنیت و سلامت فضای سایبر از تهدیدات امنیت ملی

بحث تعلیم دادن سلامت کودکان در اینترنت و فضای سایبر، اهدافی را در جهت چگونگی برخورد با شرایط گوناگون در فضای مجازی دنبال می‌کند. این فرآیند به کودکان یاد می‌دهد برای عدم مواجهه با موقعیت‌های ناامن و وضعیت‌های ریسک‌مدار چه کارهایی انجام دهند و چه کارهایی انجام ندهند.

با این اوصاف، ضروری است که مهارت‌های لازم برای حضور در شبکه‌های اجتماعی سایبری به کودکان و نوجوانان و والدین آن‌ها آموخته شود تا از آسیب‌های احتمالی جلوگیری شود؛ یکی از مهم‌ترین نقش‌ها برای حضور سالم کودکان در شبکه‌های اجتماعی را والدین و متولیان امور آموزش به ویژه مشاوران و روان‌شناسان مدرسه بر عهده دارند؛ آشنا نمودن و آموزش دادن در زمینه‌ی افزارها و ابزارهای حفاظتی و امنیتی، نوع و نحوه‌ی کارآیی و بهکارگیری آن‌ها، جدی گرفتن آلارم‌ها و هشدارها و... از این قبیل هستند (طارمی، ۱۳۸۷: ۳۵- ۳۲).

از جمله اسناد بین‌المللی که در زمینه ارائه راهکارهای پیشگیرانه غیرکیفری در زمینه تروریسم سایبری وجود دارد، می‌توان به کمیته تخصصی دستورالعمل و توصیه‌نامه‌های سازمان همکاری و توسعه اقتصادی در سال ۱۹۸۹ اشاره کرد که اقداماتی را به منظور اتخاذ سیاستی مشترک برای مقابله با جرایم اینترنتی و هماهنگی قوانین کیفری، همچنین حمایت از حقوق فردی و جریان فراملی داده‌های شخصی شروع کرد. در ژوئیه سال ۲۰۰۲ این سازمان، سند جامع «خط‌مشی‌هایی برای امنیت سامانه‌های اطلاعاتی و شبکه‌ای: به سوی فرهنگ امنیتی» را منتشر کرد (قدیر و کاظمی فروشانی، ۱۳۹۸: ۲۶۰).

شورای اقتصادی- اجتماعی سازمان ملل متحد نیز در این خصوص لزوم آموزش را در اولویت برنامه‌های دولت‌ها برشمرده و در قطعنامه خود به نقش مهم خانواده‌ها و مراکز آموزشی چون مدرسه و دانشگاه اشاره کرده و آموزش را امری مهم در ارائه شناخت بیشتر به کودکان و نوجوانان و جوانان در خصوص ناامنی فضای سایبری می‌داند. لذا، نه تنها از دولت‌های عضو می‌خواهد تا شرایط آموزش در این خصوص را در کنار مقابله کیفری فراهم آورند، بلکه از سایر دولت‌ها می‌خواهد تا در صورت توان به ایجاد شرایط آموزش در این کشورها در صورت عدم توانایی دولت و رضایت او اقدام نماید. این امر کمک می‌نماید تا اهداف مورد نظر در مقابله و کنترل تروریسم سایبری به نحو موثری محقق گردد.[1]

در این میان لازم است تا ضمن درج مطالبی در این خصوص در کتب درسی، با برگزاری

[1]. E/RES/2019/18

همایش‌های مختلف با استفاده از ظرفیت‌های معلمان و اساتید دانشگاه ابعاد تروریسم سایبری و راه‌های انجام آن به روشنی تبیین گردد. به علاوه، در این خصوص از سازمان‌های مردم‌نهاد که در زمینه مسائل اجتماعی فعال هستند نیز در جهت امنیت انسانی و اجتماعی می‌توان کمک گرفت. با توجه به اینکه امنیت انتظامی در برقراری امنیت انسانی نقش مهمی دارد، لذا نیروی انتظامی می‌تواند در برگزاری این همایش‌ها نقش مهمی داشته باشد. همچنین، نیروی انتظامی و پلیس سایبری از فضای رسانه برای آگاهی‌بخشی به مردم نیز می‌توانند بهره ببرند.

۲-۲-۲. راهکارها و تدابیر رسانه‌ای در جهت امنیت و سلامت فضای سایبر از تهدیدات امنیت ملی

نقش و تاثیر تعلیمی و تبلیغی رسانه و مولتی مدیا بر کسی پوشیده و پنهان نیست و چه بسا با خصلت و ویژگی همه‌گیری و فراگیری خود، حتی در شرایطی که به دلایل گوناگون، امکان و احتمال آموزش‌های مستقیم و مهارت‌های عینی و عملی نیست، می‌تواند به عنوان وسیله و شیوه‌ای مهم و موثر عمل کرده و مورد استفاده قرار گیرد. آنچه در خصوص مفهوم و ماهیت اخلاقیات سایبری در میان متون معتبر و مهم علمی ملاحظه می‌گردد، چیزی جز کد سلامت یا رفتار و کردار مسئولانه در اجتماع سایبری نیست.

یکی از نکات بسیار مهمی که باید در خصوص تدابیر و راهکارهای پیشگیرانه اجتماعی مورد توجه قرار داد، نمی‌توان انتظار داشت در کوتاه‌مدت، آثار و نتایج محسوس و قابل‌مشاهده‌ای به دست آید. البته، این مساله یک نقطه ضعف محسوب نمی‌شود، زیرا این رویکرد، زیربنای فکری – شخصیتی بزه‌کاران و بزه‌دیدگان بالقوه را هدف قرار می‌دهد که در صورت تحقق اهداف پیش‌بینی‌شده، جامعه‌ای سالم، پایبند و متعهد به رعایت هنجارها و ارزش‌های پذیرفته شده به وجود خواهد آمد (جلالی فراهانی و باقری اصل، ۱۳۸۷: ۱۸).

بدیهی است اقداماتی که در این راستا انجام می‌شود، شامل آگاه ساختن از خطرات رفتار زیان‌بار و غیرقانونی آنلاین و یادگیری نحوه محافظت از خود و دیگر کاربران اینترنت در برابر آن‌هاست. از این رو، بهتر است در کنار حرکت پرشتاب و تا حدودی لگام گسیخته‌ی سایبری کردن امور خرد و کلان جامعه، به ویژه دسترس‌پذیر کردن هرچه بیشتر و گسترده‌تر این فضا برای قشر جوان و نوجوان در محیط‌های مختلف که نمونه بارز آن را در عزم دولت برای متصل کردن تمامی واحدهای آموزشی عالی به شبکه جهانی اینترنت شاهد هستیم، قدری به فکر ساماندهی آن براساس الگوهای خردگرایانه و واقع‌گرایانه باشیم تا بیش از این نسل جدید با چالش‌ها و مشکلات سایبری مواجه نباشند.

دوره اول / شماره ۱ / زمستان ۱۳۹۹ - نویسندگان: حجت سبزواری نژاد، محمد رضازاده سلطان آباد

۳. پیشگیری وضعی از تهدیدات امنیت ملی ایران در راستای تروریسم سایبری

به علت حجم گسترده‌ی ارتباطات موجود در فضای سایبر، هرگونه ضعف و یا خلل امنیتی، امکان آسیب‌دیدگی شمار فراوانی از کاربران را به وجود می‌آورد. همچنین، علی‌رغم اقداماتی که در راستای مبارزه با تروریسم در سال‌های اخیر در کشورمان انجام گرفته است و علی‌القاعده باید منجر به کاهش این پدیده گردد، اما عواملی از قبیل رشد فناوری‌ها و سهولت دسترسی به آنها عدم سیاست کلان و قانونگذاری تخصصی و به‌روز و نیز عدم ساماندهی صحیح در زمینه فضاهای مجازی باعث افزایش این پدیده در کشور شده است. در کنار این عوامل باید از توسعه وسائل ارتباط جمعی شبکه‌های اجتماعی بدافزارها و نرم‌افزارهای سایبری نام برد که به تروریست‌ها در آشنایی با اهداف و انگیزه‌هایشان یاری می‌رساند (عبدی، ۱۳۹۵: ۷).

از این رو، به منظور پیشگیری از خسارات کلان احتمالی ناشی از بزه‌دیدگی تروریسم سایبری، پیشگیری وضعی یا موقعیت مدار یکی از بهترین و مؤثرترین گزینه های تأمین امنیت به شمار می‌آید. بسیاری از تکنیک‌های پیشنهادی تدابیر موقعیت‌مدار قابلیت کاربست در فضای سایبر را دارا هستند و با استفاده از ابزارهای فناوری اطلاعات و ارتباطات می‌توان آنها را در این فضا بکار بست.

۳-۱. دیوارهای آتشین

یکی از مهم‌ترین تدابیر صیانت از آماج بزه از طریق دشوارسازی دسترسی دیوارهای آتشین[۱] هستند. به عبارت بهتر، دیوارهای آتشین، یکی از مهم‌ترین راهکارهای امنیت شبکه و سامانه‌های رایانه‌ای در مقابل حملات تروریسم سایبری است. این دیوارها که در دو نوع سخت‌افزاری و نرم‌افزاری موجود هستند، به مثابه محافظی عمل می‌کنند که از دسترسی غیرمجاز به شبکه‌های داخلی و خروج اطلاعات پیشگیری می‌کنند. نظارت و مسدودسازی دسترسی به شبکه بر اساس تطبیق ورودی‌ها با الگوهای غیرمجاز تعیین شده صورت می‌گیرد. بدین صورت که در یک فرآیند کلی، درخواست‌های دسترسی به شبکه داخلی را در پوشه‌ای ذخیره کرده، آن را با الگوها مقایسه می‌کند و در صورتی که موارد غیرمجازی را مشاهده نماید، کاربر را مطلع خواهد نمود. برای دیواره‌های آتش پیکربندی‌ها و کاربردهای مختلفی وجود دارد: صافی‌ها، تقویت‌کننده‌های برنامه‌های کاربردی، رمزگذاری، ایجاد منطقه غیرنظامی و سایر موارد مشابه که سبب افزایش

[۱]. دیوار آتشین در اصطلاح علوم رایانه‌ای عبارت است از: یک سامانه ایمنی برای محافظت از شبکه یک سازمان در مقابل تهدیدهای خارجی همچون نفوذگران که از شبکه‌های خارجی همچون اینترنت وارد می‌شوند. دیوار آتش که به طور معمول، ترکیبی از سخت‌افزار و نرم‌افزار است، از ارتباط مستقیم کامپیوترهای عضو شبکه داخلی با شبکه‌های خارجی و برعکس جلوگیری می‌کند (ماه پیشانیان، ۱۳۹۰: ۹۷).

ضریب امنیتی آن‌ها می‌شود (فرهادی آلاشتی، ۱۳۹۵: ۴۴).

با نگاهی به سند چشم‌انداز بیست ساله مشاهده می‌گردد که عبارت «سامانه دفاعی برای بازدارندگی همه‌جانبه» با نگاه امنیت ایجابی به دنبال تحقق هدف بازدارندگی است. تروریسم سایبری به عنوان امری که امنیت فردی و اجتماعی را به خطر می‌اندازد نیز در دسته این سیاست‌ها قرار می‌گیرد و لذا، باید تمهیداتی به منظور مقابله با آن اندیشید. از این رو، در برنامه ششم توسعه شاهد برخی تمهیدات می‌باشیم، اما بطور جدی موضوع تروریسم سایبری در سند سیاست‌های برنامه ششم توسعه تبیین نشده و بیشتر به سایر تهدیدات امنیتی توجه شده که لازم است در برنامه هفتم این خلاء جبران شود. ضمناً با توجه به رویکرد نظم انتظامی، استفاده بهتر از ظرفیت‌های نیروی انتظامی در این زمینه می‌تواند مفید باشد. در این خصوص لازم است تا نقاط ضعف اقدامات امنیت سایبری بررسی و در سیاست‌های جدید اصلاح گردد.

۲-۳. پالایشگرها[1]

یکی دیگر از روش‌های دشوارسازی دسترسی به آماج جرم، استفاده از پالایشگرها[2] می‌باشد. همان‌گونه که از نام این تدابیر پیداست، اجازه‌ی دسترسی به برخی و یا تمام محتویات موجود در شبکه را نخواهند داد و با توجه به الگوهای تعیین شده محتویات خاصی را غربال خواهند کرد. پالایشگرها بر اساس فهرست سفید[3] یا فهرست سیاهی[4] که برای آنها تعیین می‌شود، فعالیت می‌کنند. «فهرست سفید، اجازه دسترسی به مشخصات تعیین شده را می‌دهد، در حالی که فهرست سیاه اجازه‌ی دسترسی به مشخصات تعیین شده را نخواهد داد.» (شوابک[5]، ۲۰۰۶: ۱۷۳).

مواردی همچون نام دامنه[6]، نشانی پروتکل اینترنت[7]، مکان یاب یکنواخت منبع وب[8]، کلید واژگان و یا تصاویر مورد نظر در این فهرست‌ها گنجانیده می‌شوند و منجر به دسترسی و یا عدم دسترسی کاربران به محتویات مورد نظر خواهند شد. به عنوان نمونه، چنانچه واژه‌ی پورنو در

---

1. Filtering.

2. پالایش یا فیلترینگ را در دو معنای عام و خاص به کار برده‌اند. در معنای عام پالایش عبارت است از فناوری‌هایی که از دستیابی به انواع خاص محتوا یا بسته ویژه‌ای از محتوای اینترنتی در دسترسی، جلوگیری به عمل می‌آورد، اما در تعریف خاص، فیلترینگ عبارت است از جلوگیری از دسترسی به اطلاعات بر مبنای محتوای اطلاعات و نه آدرس سایت. در حقیقت، معنای خاص پالایش، در مقابل مسدود کردن به کار می‌رود. طبق این تفکیک هنگامی که دسترسی به کل یک سایت بر اساس آدرس آن سایت ممنوع می‌شود، آن سایت مسدود (یا بلاک) شده و در صورتی که بخشی از محتوای آن ممنوع شده باشد، پالایش گشته است (کرامتی معز و میرخلیلی، ۱۳۹۹: ۷۸).

3. Whitelist.
4. Blacklist
5. Schwabac
6. Domain Name System.
7. Internet Protocol Address.
8. Uniform Resource Locator.

فهرست سیاه پالایشگری قرار گیرد، از دسترسی کاربران به محتویات مرتبط با آن واژه (اعم از فیلم، عکس، نوشتار و ...) جلوگیری خواهد کرد. لازم به ذکر است، زمانی دقت پالایشگرها بالا می‌رود که از چندین مؤلفه برای سلب و یا محدودیت دسترسی به شبکه استفاده شود. به عنوان نمونه، چنانچه پالایشگری صرفا بر اساس مکان یاب یکنواخت منبع وب تنظیم شده باشد، تنها می‌تواند درخواست‌هایی که در رابطه با این نشانی است را مسدود نماید و چنانچه کاربر شماره‌ی پروتکل اینترنت آن نشانی را وارد کند، اجازه دسترسی به وی داده خواهد شد. از همین رو، امروزه سعی بر این است که برای تأمین امنیت حداکثری، پالایشگرهای چندمؤلفه‌ای جایگزین پالایشگرهای تک‌مؤلفه‌ای شوند.

پالایشگرها نیز همچون دیواره‌های آتشین می‌توانند در سطوح خرد همچون صیانت از کاربران خانگی و مراکز آموزشی و یا در سطوح کلان همچون صیانت از سازمان‌ها و افراد یک کشور مورد استفاده قرار گیرند. همچنین، پالایشگرها می‌توانند از سوی کاربران نهایی، ارائه‌دهندگان خدمات دسترسی حضوری (کافی‌نت‌ها) یا ارائه‌دهنده خدمات اینترنتی، از سوی ایجادکننده نقطه‌ی تماس بین‌المللی و بر روی موتور جستجو اعمال شوند (خانعلی‌پور واجارگاه، ۱۳۹۰: ۱۲۷).

بر مبنای نظام حقوقی کشورمان، بالاترین سطح کاربست این تدابیر در بعد داخلی لازم‌الاجرا می‌باشد. بر اساس ماده ۷۴۹ قانون مجازات اسلامی بخش تعزیرات (ماده ۲۱ قانون جرایم رایانه‌ای مصوب ۱۳۸۸)، ارائه‌دهندگان خدمات دسترسی یا همان میزبان‌های داخلی، موظف به کاربست پالایشگرها می‌باشند. طبق این ماده: ارائه‌دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی کارگروه (کمیته) تعیین مصادیق موضوع ماده ذیل محتوای مجرمانه که در چارچوب قانون تنظیم شده است، اعم از محتوای ناشی از جرایم رایانه‌ای و محتوایی که برای ارتکاب جرایم رایانه‌ای به کار می‌رود را پالایش (فیلتر) کنند. در صورتی که عمدا از پالایش (فیلتر) محتوای مجرمانه خودداری کنند، منحل خواهند شد و چنانچه از روی بی‌احتیاطی و بی‌مبالاتی زمینه دسترسی به محتوای غیرقانونی را فراهم آورند، در مرتبه نخست به جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال و در مرتبه دوم، به جزای نقدی از یکصد میلیون ریال تا یک میلیارد ریال و در مرتبه سوم، به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

در برخی از موارد ماهیت مجرمانه و یا غیرمجرمانه‌ی برخی از اطلاعات برای نرم‌افزارهای پالایشگر قابل تشخیص نبوده و چنانچه مشتقات محتویات مورد نظر، در لیست سیاه قرار داشته باشند، نرم‌افزار دسترسی به این محتویات را نیز غیرممکن خواهد ساخت، که اصطلاحاً به این گونه محتویات، «موضوعات خاکستری» و به این حالت «پالایش بیش از اندازه[1]» گفته می‌شود (فرهادی

[1]. Over blocking filtering.

آلاشتی، ۱۳۹۵: ۱۴۸). به عبارت بهتر، مشکل از آن جایی آغاز می‌شود که در بسیاری از موارد با ترکیبی از داده‌های قانونی و غیرقانونی روبرو می‌باشیم. عدم توانایی نرم‌افزارهای پالایشگر در تشخیص داده‌های قانونی از غیرقانونی و زمان‌بر بودن رفع کاستی‌ها توسط عامل انسانی، نتیجه‌ای جز عدم دسترسی به تعداد بی‌شماری از محتویات قانونی برای مدت زمانی خاص را در پی ندارد. به همین دلیل، در بسیاری از موارد داده‌های قانونی نیز به همراه داده‌های غیرقانونی، در زمره‌ی اطلاعات غیرمجاز قرار می‌گیرد و تا تشخیص اشتباه و رفع آن، کاربران قادر به دسترسی به اطلاعات مورد نظر خود نیستند.

۳-۳. لزوم توجه به همکاری بین‌المللی

قطعنامه‌های مجمع عمومی سازمان ملل متحد، شورای امنیت و شورای اقتصادی- اجتماعی بر دو موضوع مهم تاکید دارند: نخست اینکه لازم است تا زیرساخت های سایبری در هر کشور مطابق با استانداردهای بین‌المللی باشد تا امکان دفاع در برابر عملیات‌های تروریستی در فضای سایبری ممکن گردد و دیگر اینکه اجرای سیاست‌های مد نظر جز با همکاری بین‌المللی میسر نمی‌گردد. لذا، لازم است دولت‌ها در تدوین سیاست‌های خود در زمینه مقابله با تروریسم سایبری ضمن لحاظ نمودن استانداردهای بین‌المللی در این خصوص، زمینه‌های همکاری‌های منطقه‌ای و بین‌المللی را مهیا نمایند. لذا، در قوانین و سیاست‌های خود باید شرایط انجام چنین همکاری را فراهم نمایند. همچنین، برای شناسایی فناوری‌های نوین که گروه‌های تروریستی ممکن است از آنها در اقدامات خود استفاده نمایند، لازم است تا از بخش خصوصی بالاخص شرکت‌های دانش‌بنیان کمک گرفت تا امکان اقدام بازدارنده و پیشگیرانه در زمان مناسب وجود داشته باشد.

دوره اول / شماره ۱ / زمستان ۱۳۹۹ - نویسندگان: حجت سبزواری نژاد، محمد رضازاده سلطان آباد

نتیجه‌گیری

سایبر تروریسم شیوه‌ای نوین از تروریسم می‌باشد که با توجه به گسترش رو به رشد فضای سایبری و استفاده دولت‌ها و عموم مردم در تمامی ابعاد و قلمروها اعم از داخلی و بین‌المللی، حاکمیتی و غیرحاکمیتی، شخصی و دولتی، پولی و بانکی از ظرفیت نامحدود آن و همچنین، عدم تخصص و اشراف کامل فنی کاربران به طور عام بر این فضا، آن را به مکانی مناسب و عاملی تحریک‌کننده، برای افزایش فرصت‌های جنایی و مخرب مبدل نموده است. در این میان، اشخاص و گروه‌های تروریستی نیز از تمام خصوصیات پیدا و پنهان این فضا استفاده کرده و اقدامات و حملات تروریستی سایبری را در دستور کار خود قرار داده و منجر به تهدید امنیت ملی شده‌اند؛ سایبر تروریسم به عنوان یکی از چهره‌های جدید از اقدامات تروریستی، محل تلاقی تروریسم و فضای سایبر می‌باشد؛ گستردگی این فضا، عدم وجود محدودیت و موانع جغرافیایی، دامنه تخریب بسیار بالا، وسیع و غیرقابل‌کنترل، پنهان ماندن هویت عاملان آن، امکان ردیابی سخت، هزینه‌های پایین ارتکاب عمل و نقص‌ها و خلأهای حقوقی و قانونی باعث شده است که این گونه از تروریسم در مقایسه با تروریسم سنتی، سهل‌تر و فراگیرتر انجام پذیرفته و گسترش رو به رشد فزاینده و مستمر داشته باشد.

یکی از محدودیت‌هایی که طی دستیابی به اقدامات سایبری اتفاق می‌افتد، این است که تعادل بین اقدامات امنیتی و آزادی‌های مدنی برقرار باشد. همچنین، تعادل باید بین مقررات منافع ویژه یک سازمان خاص یا دولت و الزامات عمومی‌تر در جهت منافع کلیه کاربران قانونی تا ارتباطات بین‌المللی و محیط تکنولوژیک را شکل دهند، حاکم باشد؛ که این امر در راستای خواسته‌های تروریست‌های سایبری و افراطی‌ها، مجرمین سایبری و هکرها خوشایند نمی‌باشد. با این اوصاف، جمهوری اسلامی نیازمند استراتژی جامعی برای مقابله با این مسأله در جهت تضمین امنیت و دستیابی به منافع حیاتی خود دارد و لذا، برنامه‌ریزی مقابله با این مسأله به عنوان یکی از مهم‌ترین تهدیدها و آسیب‌ها باید در اولویت سیاست جنایی قرار بگیرد.

تدابیر پیشگیرانه موقعیت‌مدار با شناسایی فرصت‌های پیش جنایی و صیانت از آماج احتمالی بزه، دامنه‌ی آسیب‌های احتمالی را کاهش داده و امنیت نسبی را تأمین می نمایند. امروزه، ابزارهای فناوری اطلاعات و ارتباطات پیشگیری از بزه را آسان‌تر نموده و به آن سرعت بخشیده است. لیکن، علی‌رغم اهمیت پیشگیری از تروریسم سایبری، کاربست برخی از تدابیر پیشگیرانه موقعیت‌مدار با محدودیت‌ها و مشکلاتی مواجه می‌شود. چالش‌هایی که می‌توانند مانع از اتخاذ همه‌جانبه این تدابیر شوند و یا در صورت اجرا، کارآیی آن‌ها را با کاستی‌هایی مواجه نماید. در صدر این چالش‌ها، پایبندی به موازین حقوق بشری قرار دارد که عموماً در قالب پایبندی به

صیانت از حقوق حریم خصوصی، آزادی بیان و آزادی جریان اطلاعات در تمام مراحل پیشگیری از جرم نمود می‌یابد؛ از این رو، ترکیبی از راهکارهای پیشگیرانه اجتماعی و موقعیت‌مدار به صورت توأمان می‌تواند مناسب باشد.

پیشنهادها

- استفاده و استخدام خبرگان و متخصصان علوم و فنون رایانه‌ای- اینترنتی جهت به‌روز کردن دانش‌ها و معلومات و نیز تشخیص و شناسایی موارد مرموز و مشکوک و ارائه راه‌حل‌ها و راهکارهای عملی در حوزه‌ی تقنین و اجرا.
- جرم‌انگاری دقیق‌تر و کامل‌تر و مشخص نمودن تفاوت‌ها و تشابهات این جرائم؛ تدوین و تنظیم قوانین و قواعد منسجم و متمرکز بدون ابهام و شبهه که در تطبیق و تصدیق موردی و موضوعی کاملاً گویا و رسا باشند.
- آگاه‌سازی و اطلاع‌رسانی همگانی و عمومی در خصوص روش و شیوه اخلاق و رفتار سایبری و چگونگی واکنش و عکس‌العمل در مقابله و مواجهه با موضوعات و موارد ناآشنا و غیرمعمولی.
- آموزش و یادگیری امنیت و حفاظت سایبری و اینترنتی در سطوح خرد و کلان جامعه، هم برای رایانه‌های شخصی و هم سیستم‌های عمومی.
- توجه و تاکید به فرهنگ‌سازی و جامعه‌پذیری مناسب و متناسب مردم جامعه برای تربیت و پرورش شهروندان قانون‌مدار و قانونمند.
- افزایش و ارتقای درجه‌ی رفاه همگانی، کیفیت و مرغوبیت زندگی و نیز سطح آرامش و آسایش اجتماعی برای امنیت بیشتر و بهتر و داشتن جامعه‌ای با تنش‌ها و تشویش‌های کمتر و پایین‌تر.
- مهیاسازی زمینه و بستر عدالت اجتماعی و فراهم‌آوری فرصت‌ها، امکانات، شرایط و موقعیت‌های یکسان و برابر در جهت تحرک اجتماعی برای تمامی افراد و اشخاص، خرده‌فرهنگ‌ها و اجتماعات و همچنین، تشویق و ترغیب روحیه‌ی جمعی و افکار عمومی و همگانی در راستای تقویت احساس تعلق و مالکیت اجتماعی، میهن‌دوستی و...
- بکارگیری و جهت‌دهی، هدایت و کنترل قابلیت و توانایی نخبگان کامپیوتری و اینترنتی در جهت ارتقا و بالا بردن کمیت سرویس‌دهی و بهره‌برداری و کیفیت امنیت و حفاظت در محیط مجازی از حیث جذب و جلب کار کرد و بازخورد سازنده و سازگار.
- تهیه و تدارک برنامه‌های آموزشی، مشاوره‌های خانوادگی، کارگاه‌های علمی و عملی و از طریق سیستم‌ها و سازمان‌های مردنهاد و جامعه‌محور و نیز رسانه‌های جمعی در راستای بالا بردن

فرهنگ عمومی و الگوسازی درست و صحیح برای کودکان و نوجوان.
- تأسیس مؤسسات پژوهشی تخصصی در زمینه امنیت فضای سایبر و گسترش مبادلات علمی با مراکز تخصصی و بهره‌گیری از فناوری های نوین در جهت هوشمندسازی زیرساخت‌ها و تأسیسات نظامی.

تشکر و قدردانی

پژوهشگران، از عزیزانی که در فرآیند ویراستاری ادبی و صفحه‌آرایی این مقاله همکاری و راهنمایی داشتند، کمال تشکر و امتنان را دارند.

منابع

- افتخاری، اصغر (۱۳۹۲). **امنیت اجتماعی‌شده**. تهران: پژوهشگاه علوم انسانی و مطالعات فرهنگی.
- افتخاری، اصغر (۱۳۹۰). **راهبرد جمهوری اسلامی ایران در مقابله با تروریسم**. آفاق امنیت. ۴(۱۲): ۳۵-۵. قابل بازیابی از:
https://ps.ihu.ac.ir/article_200385.html
- بختیاری، حسین و صالح نیا، علی (۱۳۹۷). **اولویت بندی تهدیدات امنیت ملی جمهوری اسلامی ایران با روش تحلیلی سلسله مراتبی (AHP)**. مطالعات راهبردی سیاست گذاری عمومی. ۸ (۲۷): ۲۷۷-۲۵۵. قابل بازیابی از:
http://sspp.iranjournals.ir/article_31401.html
- بخشی، عبدالله (۱۳۹۵). **اطلاعات و امنیت در کتاب و سنت**. تهران: مؤسسهٔ چاپ و انتشارات دانشکدهٔ اطلاعات.
- بوگانسکی، میتکو و پترسکی، دریژ (۱۳۹۴). **تروریسم سایبری، تهدید علیه امنیت جهانی**. ترجمه ندا نیازمند. در مجموعه مقاله‌ها تروریسم شناسی. چاپ اول. تهران: انتشارات نگاه بینه.
- جلالی فراهانی، امیرحسین و باقری اصل، رضا (۱۳۸۷). **پیشگیری اجتماعی از جرایم سایبری: راهکاری اصلی برای نهادینه سازی اخلاق سایبری**. ره آورد نور. ۷(۲۴). قابل بازیابی از:
magiran.com/p612320
- چامسکی، نوام (۱۳۸۳) .**تروریست های جهانی چه کسانی هستند؟** ترجمه: مجتبی طاهری، گزارش راهبردی. پژوهشکده مطالعات راهبردی.
- خانعلی پور واجارگاه، سکینه (۱۳۹۰). **پیشگیری فنی از جرم**. چاپ اول. تهران: بنیاد حقوقی میزان.
- خلیلی پور رکن آبادی، علی و نورعلی‌وند، یاسر (۱۳۹۱). **تهدیدات سایبری و تأثیر آن بر امنیت ملی**. مطالعات راهبردی. ۱۵(۵۶): ۱۹۶-۱۶۷. قابل بازیابی از:
http://quarterly.risstudies.org/article_2414.html
- سنبلی، نبی (۱۳۸۰). **عملکرد سازمان ملل در زمینه مقابله با تروریسم**، سیاست خارجی. ۱۵(۴).
https://www.sid.ir/fa/journal/ViewPaper.aspx?ID=167994
- شهبازی، امید و براری، مجید (۱۳۹۶). **پیشگیری از تأمین مالی تروریسم، الگوها و راهکارها**. چکیده مقالات همایش بین‌المللی ابعاد حقوقی – جرم‌شناسی. تهران: انتشارات دانشگاه علامه طباطبایی. دانشکده حقوق و علوم سیاسی.
- فیرحی، داوود، ظهیری، صمد (۱۳۸۷). **تروریسم؛ تعریف، تاریخچه و رهیافت های موجود در تحلیل پدیده تروریسم**. ۳۸(۳): ۱۶۵-۱۴۵. قابل بازیابی از:
https://jpq.ut.ac.ir/article_27332.html
- طارمی، محمدحسین (۱۳۸۷). **فضای سایبر: آسیب‌ها و مخاطرات**. ره آور نور. (۲۲). قابل بازیابی از:
http://noo.rs/mHzve
- عظیمی، فاطمه و خشنودی، هادی (۱۳۹۵). **نقش تروریسم سایبری در تهدید علیه امنیت ایران و راه‌های پیشگیری از آن. مطالعات سیاسی**. ۹(۳۴): ۲۱۲-۱۹۹. قابل بازیابی از:

http://jourm.iauaz.ac.ir/article_532644.html
– عبدی، مهدی (۱۳۹۰). **تروریسم سایبری علیه ایران**. همایش بین المللی شرق شناسی، فردوسی و فرهنگ و ادب پارسی.
– کارگری، نوروز (۱۳۹۰). **مفهوم‌یابی و گونه‌شناسی تروریسم، در: تروریسم و مقابله با آن (به اهتمام عباسعلی کدخدایی و نادر ساعد)**. تهران: انتشارات مجمع جهانی صلح اسلامی.
– فرهادی آلاشتی، زهرا (۱۳۹۵). **پیشگیری وضعی از جرایم سایبری راهکارها و چالش‌ها**. چاپ اول. تهران: بنیاد حقوقی میزان.
– قدیر، محسن و کاظمی فروشانی، حسین (۱۳۹۸). **بررسی تطبیقی حقوق کیفری ایران با اسناد بین‌المللی در زمینه مقابله و پیشگیری از وقوع تروریسم سایبری**. حقوق بین المللی. ۳۶(۶۰): ۲۶۷-۲۳۷. قابل بازیابی از:
cilamag.2019.35084/10.22066:doi
– قدیم‌زاده، سمیه (۱۳۹۵). **مطالعه جرم شناسی وندالیسم سایبری و تروریسم سایبری و راهکارهای پیشگیری از آن**. پایان نامه کارشناسی ارشد، رشته حقوق جزا و جرم شناسی. دانشگاه گیلان. پردیس دانشگاهی.
– کرامتی معز، هادی و میرخلیلی، سید محمود (۱۳۹۹). **نقد سیاست‌های پالایش(فیلترینگ) در پیشگیری از بزه‌دیدگی نوجوانان در شبکه‌های اجتماعی مجازی به عنوان محیطی نوین از جغرافیای انسانی**. نگرش‌های نو در جغرافیای انسانی. ۱۲(۴۶): ۹۶-۷۵. قابل بازیابی از:
http://geography.journals.iau-garmsar.ac.ir/article_672279.html
– ماه پیشانیان، مهسا (۱۳۹۰). **فضای سایبر و شیوه های نوین درگیری ایالات متحده آمریکا با جمهوری اسلامی ایران**. مطالعات فرهنگ و ارتباطات. ۱۲(۱۳): ۱۲۱-۹۵. قابل بازیابی از:
http://www.jccs.ir/article_3413.html
– معصومی، مجید و ساعی، احمد (۱۳۹۱). **تأثیر تروریسم بر امنیت ملی جمهوری اسلامی ایران.** سیاست. ۴۱(۲): ۱۷۷-۱۶۱. قابل بازیابی از:
https://jpq.ut.ac.ir/article_29748.html
– معین، محمد (۱۳۶۳). **فرهنگ معین**. چاپ ششم. تهران: انتشارات امیرکبیر.
– منفرد، محبوبه و جلالی فرهانی، امیرحسین (۱۳۹۱). **کدهای رفتاری و پیشگیری از بزهکاری،** پژوهش نامه حقوق کیفری. ۳(۲): ۱۳۴-۱۰۵. قابل بازیابی از:
https://jol.guilan.ac.ir/article_614.html
– موسوی، سید محمدرضا؛ حیدری، خدیجه و قنبری، علی (۱۳۹۲). **تأثیر تهدیدات امنیتی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن**. فصلنامه علمی ترویجی مطالعات پلیس بین‌الملل. ۴(۱۴): ۱۴۵-۱۲۳. قابل بازیابی از:
http://journals.police.ir/article_12759.html
– میر محمد صادقی؛ حسین (۱۳۹۲). **حقوق کیفری اختصاصی (جرایم علیه امنیت و آسایش عمومی)**. چاپ بیست و یکم. تهران: نشر میزان.

دوره اول / شماره ۱ / زمستان ۱۳۹۹ - نویسندگان: حجت سبزواری نژاد، محمد رضازاده سلطان آباد

– نجفی علمی، مرتضی و نقیب السادات، رضا (۱۳۹۳). **روند تحولات فضای سایبر و نقش آن در تهدیدات ناشی از جرم در محیط سایر ج.ا.ا**. پژوهش‌نامه نظم و امنیت انتظامی. ۷(۲۵): ۷۸-۵۳. قابل بازیابی از:

http://journals.police.ir/article_9807.html

– نمامیان، پیمان (۱۳۹۲). **مواجهه با تروریسم سایبری در حقوق بین‌الملل کیفری**. فصلنامه پژوهش‌های ارتباطی. ۲۰(۷۳): ۴۲-۹. قابل بازیابی از:

10.22082/CR .2013.23464

– نورمحمدی، مرتضی (۱۳۹۰). **سایبر تروریسم، تروریسم در عصر اطلاعات، در: تروریسم و مقابله با آن**. تهران: انتشارات مجمع جهانی صلح اسلامی.

– وفادار، حسین (۱۳۸۹). **امنیت انتظامی و سند چشم انداز ۱۴۰۴**. پژوهشنامه نظم و امنیت انتظامی. ۳(۱۲): ۲۱-۱. قابل بازیابی از:

http://osra.jrl.police.ir/article_9783.html

– یزدان پناه درو، کیومرث و کامران، حسن (۱۳۹۴). **تروریسم در فضای مجازی و اثرات آن بر حوزه جغرافیای سیاسی**. انجمن جغرافیای ایران. ۱۳(۴۴). قابل بازیابی از:

magiran.com/p1422275

– بیرانوند، رضا؛ یاراحمدی، حسین و میلانی، علیرضا (۱۳۹۹). **تحلیل پیشگیری رشدمدار از جرم در نظام حقوقی ایران**. پژوهش های دانش انتظامی. ۲۲(۲): ۱۲۳-۱۰۰. قابل بازیابی از:

http://pok.jrl.police.ir/article_93759.html

-Anwar, Muhammad Azfar, Rongting, Zhou, Dong, Wang, Asmi, Fahad, Meissner, Richard (2018). **Mapping the knowledge of national security in 21st century a bibliometric study**. Journal Cogent Social Sciences.

- Carroll, Paul, Windle James (2018). **Cyber as an enabler of terrorism financing**. now and in the future. 13(3): 285-300. Retrieved from: https://doi.org/10.1080/18335330.2018.1506149

-Connor, Nancy (2002). **The rationality if Terrorism by secure and religious group**. University of Alabama.

-Fletcher, G. (2006). **The Indefinable Concept of Terrorism**. Journal of International Criminal Justice. 4(5): 1-21. Retrieved from: DOI:10.1093/jicj/mql060

- Gill, Paul, Corner, Emily (2017). **There and back again: The study of mental disorder and terrorist involvement**. American Psychologist. 72(3): 231–241. Retrieved from: https://doi.org/10.1037/amp0000090.

-Gross, Michael L., Canetti, Daphna, and Vashdi ,Dana R. (2017). **The psychological effects of cyber terrorism.** US National Library of Medicine National Institutes of Health.

-Hancock, B. (2001). **Cyber-Tracking, Cyber-terrorism**. Computers and Security. Vol.20, No7.

- Jore, S.H. (2017). **The Conceptual and Scientific Demarcation of Security in Contrast to Safety**. European Journal for Security Research. 7.157–174. Retrieved from:

دوره اول / شماره ۱ / زمستان ۱۳۹۹ – نویسندگان: حجت سبزواری نژاد، محمد رضازاده سلطان آباد

https://link.springer.com/article/10.1007/s41125-017-0021-9.
-Johansson, Morgan (2017). **A national cyber security strategy**. The Government office of Sweden.
-Jacob, Johanna, Peters, Michelle L., Yang, T. Andrew (2020). **Interdisciplinary Cybersecurity: Rethinking the Approach and the Process**. National Cyber Summit. 6(2).
-Muir, Kate, Joinson, Adam (2020). **An Exploratory Study Into the Negotiation of Cyber-Security Within the Family Home**. Front Psychol, v.11.
-Sussex ,Matthew, Clarke, Michael, Medcalf, Rory (2017). **National security: between theory and practice**. Journal of Strategic Studies.
-Schwabach, Aaron. (2006). **Internet and the Law: Technology, Society and Compromises**. United States of America: ABC-CLIO.
-Smith, P (2012). **Crime prevention in USA**. first edition. New York: mcmillan.
-Stevens, Daniel, Williams, Nick Vaughan (2016). **Citizens and Security Threats: Issues, Perceptions and Consequences Beyond the National Frame**. -Villegas, Díaz, M. (2016). **Contribuciones para un concepto de terrorismo en el derecho penal chileno**. Política Criminal. 11(21): 7-18. Retrieved from: http://dx.doi.org/10.4067/S0718-33992016000100006.

دوره اول / شماره ۱ / زمستان ۱۳۹۹ - نویسندگان: حجت سبزواری نژاد، محمد رضازاده سلطان آباد