Quarterly Journal of Hamedan Police Science

Journal homepage: http://hamedan.jrl.police.ir/

45 Vol.7, No.26, Autumn 2020

Effectiveness of Cyber Police Measures in Hamedan against Cyberbullying in a Period of 5 Years with a Technical and Social Approach (Case Study of Hamadan Province)

Mohammad Baqer Zarei
*Master of Combating Criminal Crimes - Amin University of Law Enforcement Sciences, Tehran, Iran.
(Corresponding Author)
zareihamedan@gmail.com

Mehdi Naghavi
Master of Software Computer- Malayer Azad University, Iran.
mehdin418@gmail.com

Received: 2020/10/11
Accepted: 2020/12/05

DOI: *******************

ABSTRACT

Today, cyberspace and its crimes have become an important problem of human societies, and unfortunately, this trend is increasing day by day. To reduce the risk of their criminal acts, cybercriminals prefer cyberspace platforms to real and traditional space. The purpose of this study is to investigate the effectiveness of Cyber Police actions against cyberbullying over a period of 5 years with a technical and social approach. This research is in the group of descriptive cross-sectional survey research and is typically an applied research. The sampling method is the whole number and sample size of the whole statistical population. The statistical population in this study is equal to the statistics received from the Cyber Police (FATA) and the field research conducted by the statistics researcher in charge of cybercrime and the information and public security police. FATA and PAVA specialized police are active in the internal departments. After extracting the data, statistical data were summarized and classified and analyzed using SPSS software. From the obtained results, it can be said that the use of cyber defense tools as well as the existing cyber platforms of Cyber Police in the country for carrying out and carrying out operations in cyberspace is not appropriate and is evaluated as weak.

Keywords: Cyberbullying, Cyberspace, Psychology, Multimedia, Cyber Police

►**Citation (Vancouver):** Bager Zarei M, Naghavi M. Effectiveness of Cyber Police Measures in Hamedan against Cyberbullying in a Period of 5 Years with a Technical and Social Approach (Case Study of Hamadan Province). Quarterly J Hamedan Police Sci. Autumn 2020; 7(3):45-57.

►**Citation (APA):** Bager Zarei, M., Naghavi, M. (Autumn 2020). Effectiveness of Cyber Police Measures in Hamedan against Cyberbullying in a Period of 5 Years with a Technical and Social Approach (Case Study of Hamadan Province). *Quarterly Journal of Hamedan Police Science*, *7*(3), 45-57.

اثربخشی اقدامات پلیس فتا در مقابله با مزاحمت‌های سایبری در بازهٔ زمانی ۵ ساله با رویکرد فنی و اجتماعی (مورد مطالعه: استان همدان)

محمدباقر زارعی
* کارشناس ارشد مبارزه با جرایم جنایی، دانشگاه علوم انتظامی امین، تهران، ایران.
(نویسندهٔ مسؤول)
Zareihamedan@gmail.com

مهدی نقوی
کارشناس ارشد نرم افزار، دانشگاه آزاد اسلامی ملایر، ایران.
mehdin418@gmail.com

نوع مقاله: پژوهشی
صص: ۴۵-۵۷
تاریخ دریافت: ۱۳۹۹/۰۷/۲۰
تاریخ پذیرش: ۱۳۹۹/۰۹/۱۵
شناسه دیجیتال (DOI): ********

چکیده

امروز، فضای مجازی و جرائم ناشی از آن به معضل مهم جوامع بشری تبدیل‌شده و متأسفانه این روند روزبه‌روز در حال افزایش است. مزاحمان سایبری برای کاهش ریسک اعمال مجرمانهٔ خود، بسترهای فضای مجازی را به فضای حقیقی و سنتی ترجیح می‌دهند. هدف این پژوهش بررسی اثربخشی اقدامات پلیس فتا در مقابله با مزاحمت‌های سایبری در بازهٔ زمانی ۵ ساله با رویکرد فنی و اجتماعی است. این تحقیق در گروه تحقیقات توصیفی پیمایشی مقطعی قرار می‌گیرد و از نظر نوع، کاربردی است. روش نمونه‌گیری به‌صورت تمام شمار و حجم نمونه کل جامعهٔ آماری است. جامعهٔ آماری در این تحقیق برابر آمار واصله از پلیس فتا ناجا و تحقیقات میدانی صورت گرفته از سوی محقق آمار متولیان مقابله با جرائم سایبری و پلیس اطلاعات و امنیت عمومی است، پس از بررسی‌های به‌عمل‌آمده و مستندات ارائه‌شده ۴۰ نفر برآورد می‌گردد که این افراد در ادارات داخلی پلیس‌های تخصصی فتا و پاوا فعال می‌باشند. پس از استخراج اطلاعات، داده‌های آماری خلاصه و طبقه‌بندی گردید و با استفاده از نرم‌افزار SPSS سه مورد تجزیه‌وتحلیل قرار گرفت. از نتایج به‌دست‌آمده می‌توان استدلال کرد که استفاده از ابزارهای دفاع سایبری و همچنین بسترهای سایبریک موجود پلیس فتا در سطح کشور جهت اجرا و انجام عملیات در فضای سایبری مناسب نبوده و ضعیف ارزیابی می‌گردد.

کلیدواژه‌ها: مزاحمت سایبری، فضای مجازی، روان‌شناسی، چندرسانه‌ای، پلیس فتا

◄**استناد (ونکوور):** زارعی م، نقوی م. اثربخشی اقدامات پلیس فتا در مقابله با مزاحمت‌های سایبری در بازهٔ زمانی ۵ ساله با رویکرد فنی و اجتماعی (مورد مطالعه استان همدان). فصلنامه علمی دانش انتظامی همدان. پاییز ۱۳۹۹؛ ۷(۳):۴۵-۵۷.

◄**استناد (APA):** زارعی، محمدباقر؛ نقوی، مهدی. (پاییز ۱۳۹۹). اثربخشی اقدامات پلیس فتا در مقابله با مزاحمت‌های سایبری در بازهٔ زمانی ۵ ساله با رویکرد فنی و اجتماعی (مورد مطالعه استان همدان). *فصلنامه علمی دانش انتظامی همدان*، ۷(۳)، ۴۵-۵۷.

مقدمه

امروز، به خاطر پیشرفت در فنّاوری ارتباطات و الکترونیک، خدمات و سرویس‌های سامانه‌های اطلاعاتی به سمت الکترونیکی شدن پیش می‌رود؛ یعنی خدمات و سامانه‌های کاربردی از حالت سنّتی کم‌کم خارج می‌شود و بیشتر تجهیزات الکترونیکی است که می‌تواند هدایت خدمات، سرویس‌ها و سامانه‌های کاربردی را از راه دور بر عهده بگیرد. مزاحمت‌های سایبری امروزی با پیشرفت فنّاوری و تجهیز دستگاه‌ها بخصوص دستگاه‌ها، و تجهیزات انتظامی، و وابستگی زندگی شهری به فناوری رایانه‌ای و شبکه‌ای ازجمله اینترنت شکل جدیدی به خود گرفته و نیاز به دفاع در مقابل این‌گونه تهدیدات بشدت حس می‌گردد. به جرأت می‌توان گفت فناوری اطلاعات و ارتباطات، به‌عنوان یک فناوری برتر و عام‌منظوره (مادر) را، زمینه‌ساز و پیشران توسعهٔ علوم، فناوری و صنعت در هر کشور دانست. رایانه‌ها، تجهیزات جانبی، شبکه‌های ارتباطی ثابت و همراه، شبکه‌های سازمانی (اینترانت و اکسترانت)، شبکه‌های ملی و فراملی (همچون اینترنت)، نرم‌افزارهای پایه، دستگاه‌های اطلاعاتی و خدمات الکترونیکی را می‌توان در مجموع زیرساخت فناوری اطلاعات یک کشور دانست. بخشی از این زیرساخت در بخش مزاحمت‌های سایبری قرار دارد.

پدیدهٔ سوءرفتار و بدرفتاری در فضای مجازی را اصطلاحاً مزاحمت سایبری[1] نامیده‌اند. مزاحمت سایبری یعنی زمانی که شخصی به‌وسیله ابزارهای رایج فناوری شخص دیگری را ناراحت می‌کند و مزاحم او می‌شود که این ابزار الکترونیکی می‌تواند ایمیل، پیام، تماس تلفنی یا هر چیز دیگری از این قبیل باشد. مزاحمت سایبری می‌تواند شامل ارسال ویروس کامپیوتری، هک کردن یک اکانت، ایجاد مزاحمت برای یک بازی باز در حین انجام یک بازی اینترنتی در فضای اجتماعی توسط بازی‌های دیگر، توهین کردن به یک کاربر در شبکه‌های اجتماعی و دیگر اقدامات مشابه این‌ها باشد. مزاحمت‌های سایبری انواع مختلفی دارند، اما هرکدام از آن‌ها می‌توانند بر روی زندگی واقعی فردی که مورد مزاحمت قرارگرفته نیز تأثیرگذار باشد و مشکلاتی از قبیل تهدید انسجام شخصیت، افسردگی و انزوا را در پی داشته باشد. گروهی از محققین که روی مسأله مزاحمت‌های سایبری تحقیق کرده‌اند معتقدند که فضای اینترنت بدرفتاری را آسان‌تر می‌کند. در واقع، آن گمنامی و پوششی که اینترنت در اختیار کاربران قرار می‌دهد باعث می‌شود مزاحمان احساس کنند که در ایمنی کامل هستند و درنتیجه رفتارهای بد خود را با خیال راحت بروز می‌دهند. همچنین، این پوشش باعث می‌شود که فرد احساس کند کاربران درواقع آدم‌های واقعی نیستند و فقط مجازی هستند که این مسأله هم منجر به این می‌شود که مزاحمان با آسودگی خاطر به مزاحمت خود بپردازند.

در زمینهٔ مزاحمت‌های سایبری، برابر بررسی‌های انجام‌شده و مستند به اعلام مرکز اسناد وزارت علوم، تحقیقات و فناوری و منابع موجود در معاونت پژوهش دانشگاه علوم انتظامی امین، تحقیقی با این عنوان صورت نگرفته است و در کشور ما به دلیل این‌که بخش‌های خصوصی به حوزهٔ مطالعاتی و مأموریتی پلیس چندان ورود نمی‌کنند، تحقیقات زیادی که توسط دانشگاه‌ها و مجامع علمی غیر پلیس صورت گرفته باشد، وجود ندارد. ولی به چند پژوهش که تا حدودی مرتبط با این موضوع است، به‌طور مختصر اشاره می‌شود.

-اشراقی سامانی، عادله و کارگر، محمدجواد: ۱۳۹۶ «ارزیابی مزاحمت سایبری در شبکه اجتماعی اینستاگرام».

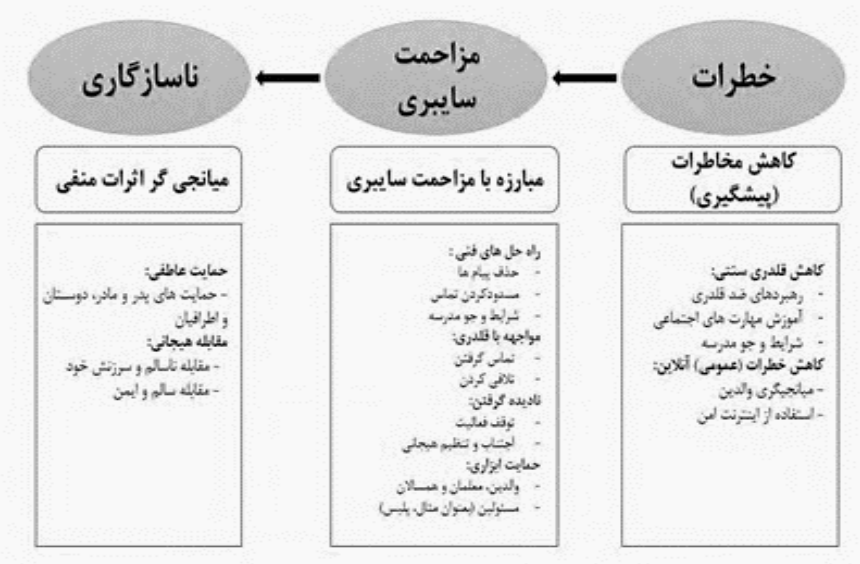
1. CyberBullying

آن‌چنان‌که شبکه اینستاگرام محبوبیت زیادی در کاربران ایرانی پیداکرده است، این تحقیق بر روی این شبکه اجتماعی صورت گرفته است. در این مقاله، پس از استخراج پارامترهای مزاحمت سایبری، پرسشنامه‌ای آنلاین تهیه‌شده است و تجزیه‌وتحلیل‌های مختلفی بر روی داده‌ها صورت گرفته است. نتایج حاصل از تحقیق نشان می‌دهد که تفاوت معناداری بین مزاحمت سایبری با جنسیت، سنین و ساعات استفاده از اینستاگرام وجود دارد.

- سیدهاشمی، سید قاسم و حقیقتی، فروغ: ۱۳۹۶ «شبکه‌های اجتماعی و مشکلات سلامت روانی در نوجوانان: با تأکید بر نقش محوری مزاحمت سایبری» هدف این مقاله بررسی ابعاد مختلف مزاحمت سایبری در سایت‌های شبکه‌های اجتماعی و اثرات آن بر سلامت روان نوجوانان بوده است. روش پژوهش: برای انجام این مطالعه از طریق استنادی به بررسی مبانی نظری و ادبیات پژوهشی موجود پیرامون موضوع تحقیق پرداخته شد. یافته‌ها: در این مقاله به مزاحمت سایبری در کودکان و نوجوانان، پاسخ‌ها و واکنش‌های قربانیان، مشکلات سلامت روانی مرتبط با آن و راهبردهای مقابله‌ای مورداستفاده برای مواجهه با آن پرداخته‌شده است و با توجه به پیشینهٔ مطالعاتی موجود، نقش و مسؤولیت والدین، مدارس، متخصصان و سایت‌های شبکه‌های اجتماعی در قبال مزاحمت سایبری و قربانی شدن نوجوانان تبیین و توصیف شد.

فضای مجازی یا سایبر: محیط واقعی و غیرملموس، موجودیت یافته در شبکه‌های الکترونیکی که در آن تمام اطلاعات، روابط، تبادلات و... که در کره خاکی به‌صورت ملموس و فیزیکی وجود دارد، در یک فضای جدید به شکل دیجیتالی نیز موجود بوده و قابل‌استفاده و در دسترس استفاده‌کنندگان و کاربران است و از راه رایانه اجزای آن به هم مرتبط هستند. فضای سایبر درواقع دنیایی است که در آن، خود واقعیت (وجود مادی-نمادین)، کاملاً در جهانی واقعی نما غرق‌شده است. در این فضا، زمان و مکان به‌طور کامل مبنای قبلی خود را از دست‌داده و به پدیده‌ای تبدیل‌شده‌اند که «دیویدها روی» آن را فشردگی فضا- زمان می‌نامد (کینان،۲۰۰۵: ۱۰۹).

مزاحمت‌های سایبری: مزاحمت گونه‌ای از رفتار مقدماتی بر ضد امنیت جان، آبرو و دارایی دیگری است ولی به‌طور واقعی نسبت به آن‌ها آسیبی نمی‌رسد اما چون مزاحمت برای تهدید و به دردسر انداختن دیگری است، می‌تواند زمینه بیشتر بزه‌ها شود... به همین دلیل، از یک‌سو نمی‌توان گسترهٔ آن را به‌طور دقیق روشن کرد و از سوی دیگر گوناگونی مزاحمت در فضای سایبر به جهت امکاناتی که دارد، می‌تواند بسیار بیشتر از فضای سنتی باشد. در فضای سنتی رفتارهایی مانند مزاحمت از حق بهره‌مندی از دارایی غیرمنقول، مزاحمت اطفال و زنان در خیابان و مکان‌های همگانی، مزاحمت تلفنی و مزاحمت با چاقو و یا با سلاح دیگر از رفتارهای مجرمانه شایع به شمار می‌روند که در قانون دارای کیفرند. ولی در فضای سایبری رفتارهای مزاحم بسیار گسترده‌اند.



شکل ۱- مفهوم‌سازی پاسخ به مزاحمت سایبری اقتباس از پرن و همکاران، (۲۰۱۲).

روان‌شناختی: آزار و اذیت اینترنتی نشان می‌دهد که تأثیرات بلندمدت منفی برای کودکان و افراد جوان دارند. درواقع، پیامدهای روان‌شناختی و هیجانی مزاحمت سایبری یکی از بزرگ‌ترین مسائلی هست که افراد قربانی با آن مواجه هستند. تحقیقات مختلف نشان داده‌اند که قرار گرفتن در معرض مزاحمت سایبری با علائم افسردگی، انزوا و ناامیدی، خودکشی، عزت‌نفس پایین، اضطراب و تنهایی ارتباط دارد. نوع و ماهیت مواد آزار و اذیت سایبری تأثیرات روان‌شناختی متفاوتی بر افراد قربانی دارد. برخی محققان دریافته‌اند که بروز مزاحمت سایبری با تصاویر یا کلیپ‌های ویدئویی برای قربانی‌ها بدترین حالت در نظر گرفته‌شده است.

به‌طور خاص، Menesini[1] و همکاران (۲۰۱۱) نشان دادند که ارسال تصاویر شرم‌آور بدترین شکل مزاحمت سایبری برای نوجوانان ایتالیایی بود. **جرم‌شناسی سایبری**[2] با الهام از تعاریف ارائه‌شده از جرم‌شناسی سایبری و تطبیق آن با تعاریفی که تاکنون از جرم‌شناسی ارائه‌شده است، مطالعهٔ عوامل ایجاد جرم در فضای مجازی و تأثیرات آن بر دنیای حقیقی و راهکارهای پیشگیری از حدوث این‌گونه جرائم است.

مطالعات عینی پرونده‌های جرائم سایبری نشان می‌دهد که ایجاد شخصیت مجازی با ذهنیت عدم شناسایی و البته سهولت و گستردگی ارتکاب برخی بزه‌ها در فضای مجازی بستر مناسبی را برای بروز خلأهای شخصیتی و روانی فراهم می‌سازد؛ لذا ما بر این باور هستیم که شخصیت واقعی بزهکار سایبری را باید در همان شخصیت مجازی وی جستجو کرد به دیگر سخن شخصیت مجازی که بزهکار سایبری از خودساخته است. درواقع، همان خود واقعی اوست که به دلایل مختلف امکان بروز آن در دنیای حقیقی را نداشته است پس بنا به قول پروفسور گاستون استفانی اندیشمند فرانسوی، شناخت شخصیت بزهکار امر مهمی در مطالعات جرم‌شناسی سایبری است (پایگاه نشر مقالات حقوقی، حق‌گستر).

آسیب‌شناسی مدل سه‌شاخگی

این مدل در طبقه‌بندی مدل‌ها از نوع مدل‌های منطقی است که بسیاری از مفاهیم، رویدادها و پدیده‌ها را می‌توان در قالب نظری سه‌شاخگی (ساختار- رفتار- زمینه) موردبررسی، مطالعه و تجزیه‌وتحلیل قرارداد.

1. Menesini
2. cyber criminology

منظور از «شاخهٔ سازمان»، همهٔ عناصر، عوامل و شرایط فیزیکی و غیرانسانی سازمانی است که با نظم، قاعده، قالب، پوسته و بدنه و یا هیکل فیزیکی و مادری سازمان را می‌سازند؛ و منظور از«شاخه محتوا» انسان در روابط انسانی در سازمان که با برگه‌های رفتاری، ارتباطات (غیررسمی) و الگوهای خاصی به‌هم‌پیوسته و محتوای اصلی سازمان را شکل می‌دهند و منظور از شاخهٔ زمینه، تمام شرایط و عوامل محیطی و برون‌سازمانی می‌باشند که بر سازمانی محیط بوده و سامانه‌های اصلی یا ابر سامانه‌های سازمان را تشکیل می‌دهند؛ مثل مخاطبین یا ارباب‌رجوع، دولت، ذینفع‌ها و ... (میرزایی اهرنجانی، ۱۳۷۶: ۳۰۵).

علت نام‌گذاری این مدل به سه‌شاخگی آن است که ارتباط بین عوامل ساختاری، رفتاری و زمینه‌ای به نحوی است که هیچ پدیده‌ای نمی‌تواند خارج از تعامل این سه‌شاخه انجام گیرد. بدین معنی که نوع روابط موجود بین این سه‌شاخه از نوع لازم و ملزومی بوده و به‌مثابه سه‌شاخه روییده از تنه واحد حیات سازمان می‌باشند. در چنان رابطه‌ای، الزاماً عوامل ساختاری- رفتاری- زمینه‌ای به‌طور وقفه‌ناپذیر و به شکل روابط سامانه‌ای دائماً باهم در تعامل بوده و درواقع سه‌شاخهٔ «ساختار- رفتار- زمینه» سه گونه از یک نوع (عمدتاً از نوع غالب زمینه) بوده و بین آن‌ها به‌هیچ‌وجه سه‌گانگی حاکم نیست. بنابراین، تمایز و تشخیص این سه جنبه از حیات سازمانی صرفاً نظری بوده و فقط به‌منظور تجزیه‌وتحلیل و شناخت مفاهیم و پدیده‌های سازمانی است (میرزایی اهرنجانی، ۱۳۷۶، ۵۵-۴۹).

مزاحمین سایبر

مزاحمین سایبری عبارت است از مجموعه افراد، سازمان و یا تشکل‌هایی که انجام یا آماده شدن برای انجام عملیات سایبری مطابق با اصول مربوط به اطلاعات. برای دانستن این‌که او کیست؟ کجاست؟ چه‌کاری را در چه زمانی می‌تواند انجام دهد؟ چه تهدیداتی در اولویت قرار دارند؟ و غیره. در مزاحمت سایبری تلاش می‌شود تا همه‌چیز را دربارهٔ افراد و سلایق آن‌ها بدانیم و درعین‌حال، نگذاریم او هیچ‌چیزی دربارهٔ ما بداند. به‌بیان‌دیگر، هدف اصلی در مزاحمت سایبر، بر هم زدن «موازنه اطلاعات و دانش» به نفع خود است، به‌ویژه اگر «موازنه توان مدیریت اجتماعی» وجود ندارد. بنابراین، در مزاحمت سایبری می‌توان با بهره‌گیری از انواع فناوری‌های پیشرفته بهره جست.

سؤال‌های پژوهش

۱-آموزش افسران پرونده در مقابله با مزاحمت‌های اینترنتی نقش دارد؟

۲-تجهیزات و سخت‌افزارها در مقابله با مزاحمت‌های اینترنتی نقش دارد؟

۳-به‌کارگیری نرم‌افزارهای تخصصی در مقابله با مزاحمت‌های اینترنتی نقش دارد؟

۴-بانک‌های اطلاعاتی در مقابله با مزاحمت‌های اینترنتی نقش دارد؟

روش تحقیق

ازآنجایی‌که این تحقیق درصدد بررسی اقدامات پلیس فتا ف.ا.همدان در مقابله با مزاحمت‌های اینترنتی است و بایستی افراد متخصص باتجربه و خبره در این باره نظر دهند و این افراد در استان همدان محدود بودند. نمونه‌گیری از نوع تمام شمار انتخاب‌شده و حجم نمونه کل جامعه آماری است که شامل ۴۰ نفر از کارکنان پلیس فتا فا.ا.همدان و مرکز فضای مجازی پاوا می‌باشند که دارای سوابق کاری و تحصیلاتی در این زمینه دارند.

این تحقیق از نوع کاربردی است؛ و در گروه تحقیقات توصیفی-پیمایشی-مقطعی قرار می‌گیرد با توجه به ساختاریافته بودن الگوی تحقیق از روش پیمایش استفاده‌شده است. بدین منظور، برای گردآوری نظر خبرگان از پرسشنامه به‌عنوان ابزار اصلی جمع‌آوری اطلاعات

استفاده‌شده است و به‌منظور کمی‌سازی نظر خبرگان در این پرسشنامه از طیف لیکرت ۵ تایی (بسیار کم – بسیار زیاد) استفاده‌شده است.

برای این‌که پرسشنامه بتواند متغیرهای تحقیق را به‌درستی اندازه‌گیری کند، دو معیار عمده برای آزمون صحت و خوب بودن آن، روایی و پایایی است. روایی نشان می‌دهد که ابزار تا چه حد مفهومی را که باید اندازه‌گیری شود، می‌سنجد و پایایی به ثبات و پیوستگی سؤالات مربوط به یک شاخص بستگی دارد. روایی و پایایی دقت علمی پژوهش را تصدیق و تأیید می‌کند (دانایی‌فرد و همکاران، ۱۳۸۳: ۲۴۳).

- ✓ **روایی:** سؤال‌های تشکیل‌دهنده معرف قسمت‌های محتوای انتخاب‌شده است. بنابراین روایی محتوا است که هم‌زمان با تدوین آزمون در آن تنیده شده است.
- ✓ **پایایی:** پایایی پرسشنامه از طریق بازآزمایی بین گروه نمونه در زمان متفاوت انجام‌شده است و اختلافی بین نتایج به دست نیامد.

در این تحقیق، ابتدا نظرات ارائه‌شده توسط صاحب‌نظران دسته‌بندی و پس از بررسی مشترکات و موارد اختلاف آن‌ها مورد تحلیل قرارگرفته و سپس با تقسیم‌بندی منابع مورد مطالعه و اسناد و مدارک جمع‌آوری‌شده شرایط موجود تشریح و تبیین شده است. و پرسشنامه‌ای در اختیار کارکنان منتخب پلیس فتا ناجا گذاشته که نرم‌افزار spss اقدام به تحلیل داده‌های به‌دست‌آمده به روش آزمون t تک نمونه‌ای نموده و رد یا تأیید فرضیه‌های پرسشنامه مشخص شد. در پایان، به‌منظور پایان تحلیل محقق در راستای ارائه الگوی ساختار امنیت سایبری پلیس فتا از تعدادی کارشناس و افسران ارشد متخصص مصاحبه به‌عمل‌آمده و کلیه سؤالات مصاحبه به‌صورت تحلیل کیفی موردبررسی و تحلیل قرارگرفته است.

یافته‌های پژوهش

یکی از قسمت‌های مهم هر روش تحقیق، تجزیه‌وتحلیل یافته‌هاست. این قسمت مشتمل بر توضیحات، جداول و همچنین تجزیه‌وتحلیل اطلاعات است.

برای تحلیل یافته‌های پژوهش از روش‌های خاص آماری استفاده می‌شود و در این رابطه اطلاعات آماری جمع‌آوری‌شده برای مقایسه و تجزیه‌وتحلیل فرضیه‌های پژوهش آماده می‌گردند. در تجزیه‌وتحلیل داده‌ها، پژوهشگر به دنبال به دست آوردن نتایج مطلوب دربارهٔ جامعه‌ی موردبررسی به‌وسیلهٔ مشاهداتی است، که از جامعه (نمونه) استخراج گردیده است. بدین منظور، با استفاده از روش‌های آماری ابتدا به توصیف داده‌ها پرداخته‌شده، آنگاه نتایج به‌دست‌آمده مورد بررسی و تفسیر قرار می‌گیرند. در این پژوهش، استخراج نتایج مربوطه با استفاده از نرم‌افزار SPSS انجام‌گرفته است. بنابراین، با توجه به مطالب فوق ابتدا به بیان جداول و سپس به تجزیه‌وتحلیل داده‌ها پرداخته خواهد شد. یافته‌ها به دو بخش تفکیک می‌شوند:

۱-یافته‌های توصیفی: در قسمت یافته‌های توصیفی، توزیع فراوانی و نمودارهای مربوط به هر یک از متغیرهای پژوهش آورده می‌شود. در قسمت دوم، با استفاده از آزمون‌های آماری، مشخص می‌شود کدام‌یک از فرضیات تحقیق، رد نمی‌گردد. آمار استنباطی مشخص می‌کند که آیا الگوها و فرایندهای کشف‌شده در نمونه، در جامعهٔ آماری کاربرد دارد یا خیر.

۲-یافته‌های استنباطی: به‌منظور بررسی نرمال بودن توزیع داده‌های هر یک از متغیرهای پژوهش، از بررسی مقادیر کشیدگی و چولگی مربوط به این متغیرها استفاده می‌نماییم. این نتایج در جدول زیر ارائه‌شده است.

جدول ۱- بررسی نرمال بودن متغیرهای پژوهش

	تعداد	کشیدگی	خطای کشیدگی	چولگی	خطای چولگی
امنیت شبکه‌های اجتماعی	۱۰۰	۱/۰۵۰	۰/۲۴۱	-۰/۲۹۵	۰/۴۷۸
تجهیزات تاکتیکی	۱۰۰	۰/۱۴۲	۰/۲۴۱	-۰/۹۴۸	۰/۴۷۸
تجهیزات استقراری	۱۰۰	-۰/۹۴۰	۰/۲۴۱	-۰/۰۸۶	۰/۴۷۸
آموزش و فرهنگ‌سازی	۱۰۰	۰/۹۵۳	۰/۲۴۱	-۰/۵۳۸	۰/۴۷۸

ازآنجاکه نتایج مربوط به بررسی مقادیر کشیدگی و چولگی همه متغیرهای این پژوهش در دامنهٔ ۲- تا ۲+ قرا دارند، می‌توان نتیجه گرفت که توزیع داده‌ها در این متغیرها نرمال است. بر این اساس، می‌توانیم از آزمون‌های پارامتری، به عنوان آزمون‌های مناسب برای بررسی فرضیات این پژوهش استفاده کنیم.

سؤال ۱-آموزش افسران پرونده در مقابله با مزاحمت‌های اینترنتی مؤثر است؟

جدول ۲- نتایج آزمون t تک نمونه‌ای در مقایسه میانگین متغیر آموزش افسران پرونده

متغیر	میانگین	مقدار آزمون				
		t	درجه آزادی	سطح معناداری	اختلاف میانگین	محدوده اطمینان ۹۵ درصد
						حد پایین / حد بالا
آموزش افسران پرونده	۱/۴۵۰	-۲۹/۸۵۰	۹۹	۰/۰۰۱	-۰/۰۵۰۰۰	-۱/۱۱۹۸ / -۰/۹۸۰۲

نتایج آزمون t تک نمونه‌ای نشان می‌دهد که تفاوت معناداری بین میانگین متغیر آشنایی (۱/۴۵۰) و وضعیت متوسط (۲/۵) وجود دارد. به‌عبارت‌دیگر، بر اساس مقدار t محاسبه‌شده (۲۹/۸۵۰-) و مقدار t مرجع برای درجه آزادی ۹۹ (۱/۶۶۰) و بزرگ‌تر بودن قدر مطلق مقدار t محاسبه‌شده، همچنین بر اساس سطح معناداری محاسبه‌شده (۰/۰۰۱) و کوچک‌تر بودن آن از مقدار عددی ۰/۰۵ می‌توان نتیجه گرفت که در سطح اطمینان ۹۵ درصد، اختلاف معناداری بین میانگین متغیر آشنایی و مقدار متوسط (۲/۵) وجود دارد. لذا فرض صفر مبنی بر عدم معناداری اختلاف میانگین متغیر آموزش افسران پرونده و وضعیت متوسط (۲/۵) رد می‌شود. همچنین، بر اساس کوچک‌تر بودن میانگین متغیر آشنایی از مقدار متوسط می‌توان نتیجه گرفت آموزش افسران پرونده در مقابله با مزاحمت‌های اینترنتی مؤثر است.

در زمینهٔ مؤثر ترین شاخص در افزایش آگاهی امنیتی کاربران، همه پاسخ‌دهندگان (۱۰۰ درصد) همه موارد شرکت در سمینار، آگاه‌سازی حفاظتی و فرهنگ‌سازی را به‌عنوان موثرترین شاخص‌ها دانسته‌اند. ۵ درصد از پاسخ‌دهندگان، آموزش حین خدمت (عرضی)، ۱۵ درصد آموزش‌های طولی و ۸۰ درصد هر دو نوع آموزش عرضی و طولی را به‌عنوان موثرترین مؤلفه در افزایش آگاهی امنیتی کاربران معرفی نموده‌اند.

سؤال۲-امنیت تجهیزات (تاکتیکی و استقراری) و سخت‌افزارها در مقابله با مزاحمت‌های اینترنتی نقش دارد؟

جدول ۳- نتایج آزمون t تک نمونه‌ای در مقایسه میانگین متغیر امنیت و سطح متوسط

متغیر	میانگین	مقدار آزمون				
		t	درجه آزادی	سطح معناداری	اختلاف میانگین	محدوده اطمینان ۹۵ درصد
						حد پایین / حد بالا
امنیت	۲/۳۲۵	-۲/۹۵۳	۹۹	۰/۰۰۴	-۰/۱۷۵۰۰	-۰/۲۹۲۵ / -۰/۰۵۷۵

نتایج آزمون t تک نمونه‌ای نشان می‌دهد که تفاوت معناداری بین میانگین متغیر امنیت (۲/۳۲۵) و وضعیت متوسط (۲/۵) وجود دارد. به‌عبارت‌دیگر، بر اساس مقدار t محاسبه‌شده (۲/۹۵۶-) و مقدار t مرجع برای درجه آزادی ۹۹ (۱/۶۶۰) و بزرگ‌تر بودن قدر مطلق مقدار t محاسبه‌شده، همچنین بر اساس سطح معناداری محاسبه‌شده (۰/۰۰۴) و کوچک‌تر بودن آن از مقدار عددی ۰/۰۵ می‌توان نتیجه گرفت که در سطح اطمینان ۹۵ درصد، اختلاف معناداری بین میانگین متغیر امنیت و مقدار متوسط (۲/۵) وجود دارد. لذا فرض صفر مبنی بر عدم معناداری اختلاف میانگین متغیر امنیت و وضعیت متوسط (۲/۵) رد می‌شود. همچنین بر اساس کوچک‌تر بودن میانگین متغیر امنیت از مقدار متوسط می‌توان نتیجه گرفت که شبکه‌های اجتماعی از طریق انواع رمز کننده‌های نرم‌افزاری و سخت‌افزاری امن نمی‌باشد۱۵ درصد پاسخ‌دهندگان، مؤلفهٔ اصلی امنیت شبکه‌های اطلاعاتی را امنیت داده، ۵ درصد امنیت دستورالعمل و آیین‌نامه و ۸۰ درصد، امنیت شبکه و زیرساخت رسانه‌ها انتخاب نموده‌اند. ۸۵ درصد از پاسخ‌دهندگان، مؤثرترین زیرساخت شبکه و ارتباط را فیبر نوری و ۱۵ درصد، خطوط اختصاصی دانسته‌اند. در زمینهٔ مؤلفهٔ امنیتی – اجرایی در افزایش ضریب امنیت شبکه‌های اطلاعاتی، ۸۰ درصد پاسخ‌دهندگان گزینه رمزنگاری و ۲۰ درصد ایشان گزینه دیوارهٔ آتش را به‌عنوان مؤلفهٔ اصلی انتخاب نموده‌اند.

سؤال۳-به‌کارگیری نرم‌افزارهای تخصصی اینترنتی نقش داشته است؟

جدول ۴- نتایج آزمون t تک نمونه‌ای در مقایسه میانگین اطلاعات و سطح متوسط

متغیر	میانگین	مقدار آزمون				
		t	درجه آزادی	سطح معناداری	اختلاف میانگین	محدوده اطمینان ۹۵ درصد
						حد پایین / حد بالا
بکارگیری نرم افزارهای تخصصی	۲/۲۷۵	-۷/۵۹۵	۹۹	۰/۰۰۱	-۰/۲۲۵۰۰	-۰/۲۸۳۸ / -۰/۱۶۶۲

نتایج آزمون t تک نمونه‌ای نشـــان می‌دهد که تفاوت معناداری بین میانگین به‌کارگیری نرم‌افزارهای تخصـــصـــی (۲/۲۷۵) و وضـــعیـــت متوســـط (۲/۵) وجود دارد. به‌عبارت‌دیگر، بر اساس مقدار t محاسبه شده (۷/۵۹۵-) و مقدار t مرجع برای درجه آزادی ۹۹ (۱/۶۶۰) و بزرگ‌تر بودن قدر مطلق مقدار t محا سبه شده، همچنین، بر ا ساس سطح معناداری محاسبه‌شده (۰/۰۰۱) و کوچک‌تر بودن آن از مقدار عددی ۰/۰۵ می‌توان نتیجه گرفت که در سطح اطمینان ۹۵ درصد، اختلاف معناداری بین میانگین متغیر به‌کارگیری نرم‌افزارهای تخصصی و مقدار متوسط (۲/۵) وجود دارد. لذا فرض صفر مبنی بر عدم معناداری اختلاف میانگین متغیر به‌کارگیری نرم‌افزارهای تخصصی و وضعیت متوسط (۲/۵) رد می‌شود. همچنین بر اساس کوچک‌تر

بودن میانگین متغیر اطلاعات از مقدار متوسط می‌توان نتیجه گرفت که به‌کارگیری نرم‌افزارهای تخصصی درزمینهٔ مقابله با مزاحمت‌های سایبری مؤثر است. در زمینه شاخص اصلی در ساخت امنیت پلیس فتا، ۹۰درصد پاسخ‌دهندگان، رصد (پایش تهدیدات) و ۱۰ درصد، تجزیه‌وتحلیل داده‌ها را به‌عنوان شاخص اصلی معرفی نموده‌اند.

سؤال۴-بانک‌های اطلاعاتی در مقابله با مزاحمت‌های اینترنتی نقش دارد.

جدول ۵- نتایج آزمون tتک نمونه‌ای در مقایسه میانگین متغیر بانک‌های اطلاعاتی و سطح متوسط

متغیر	میانگین	مقدار آزمون				
		t	درجه آزادی	سطح معناداری	اختلاف میانگین	محدوده اطمینان ۹۵ درصد
						حد پایین / حد بالا
بانک‌های اطلاعاتی	۱/۷۷۵	-۱۹/۴۹۸	۹۹	۰/۰۰۱	-۰/۷۲۵۰۰	-۰/۷۹۸۸ / -۰/۶۵۱۲

نتایج آزمون t تک نمونه‌ای نشان می‌دهد که تفاوت معناداری بین میانگین متغیر بانک‌های اطلاعاتی (۱/۷۷۵) و وضعیت متوسط (۲/۵) وجود دارد. به‌عبارت‌دیگر، بر اساس مقدار t محاسبه‌شده (۱۹/۴۹۸-) و مقدار t مرجع برای درجه آزادی ۹۹ (۱/۶۶۰) و بزرگ‌تر بودن قدر مطلق مقدار t محاسبه‌شده، همچنین بر اساس سطح معناداری محاسبه‌شده (۰/۰۰۱) و کوچک‌تر بودن آن از مقدار عددی ۰/۰۵ می‌توان نتیجه گرفت که در سطح اطمینان۹۵ درصد، اختلاف معناداری بین میانگین متغیر ساختار یکپارچه و مقدار متوسط (۲/۵) وجود دارد. لذا فرض صفر مبنی بر عدم معناداری اختلاف میانگین متغیر بانک‌های اطلاعاتی و وضعیت متوسط (۲/۵) رد می‌شود. همچنین، بر اساس کوچک‌تر بودن میانگین متغیر ساختار یکپارچه از مقدار متوسط می‌توان نتیجه گرفت که بانک‌های اطلاعاتی در مقابله با مزاحمت‌های اینترنتی نقش دارد. از نظر ۱۰ درصد پاسخ‌دهندگان، موثرترین راهکار جهت ایجاد بانک‌های اطلاعاتی در مقابله با مزاحمت‌های سایبری، ایجاد مرکز فوریت‌های سایبری و از نظر ۹۰ درصد ایشان، ایجاد مرکز اطلاعات و همچنین ایجاد مرکز فوریت‌های سایبری انتخاب‌شده است.

جدول ۶- تجزیه و تحلیل کلی

شماره سوال	موضوع سوال	ارزش
۶	به نظر شما موثرترین شاخص مقابله با مزاحمت‌های سایبری کدام گزینه می‌باشد؟	تجهیزات – افراد متخصص- آموزش و فرهنگ‌سازی
۱۱	به نظر شما کدام مولفه امنیتی در افزایش ضریب امنیتی شبکه‌های اجتماعی پلیس فتا جهت مقابله با مزاحمت‌های سایبری اجرایی‌تر می‌باشد؟	رمزنگاری
۵	به نظر شما به چه میزان تجهیزات (اعم از تاکتیکی و استقراری) در مدیریت فضای مزاحمت سایبری وابسته خواهد بود؟	۸۰>
۱۶	به نظر شما شبکه‌های اجتماعی به چه میزان بر مبنای امنیت نرم‌افزار طراحی شده است؟	متوسط
۱۸	به نظر شما کدام مولفه به عنوان شاخص اصلی در ساخت امنیت پلیس فتا همدان جهت مقابله یا مزاحمت‌های سایبری در راستای مأموریت‌های محوله اجرایی‌تر است؟	رصد و پایش
۱۹	ساختار فعلی بانک‌های اطلاعاتی جهت مدیریت فضای مزاحمت‌های سایبری به چه میزان آسیب‌پذیر می‌دانید؟	متوسط
۲۰	به نظر شما ساختار فعلی پلیس فتا همدان به چه میزان دارای ساختار یکپارچه مقابله با مزاحمت‌های سایبری است؟	ضعیف
۲۱	به نظر شما کدام ساختار به عنوان موثرترین راهکار جهت ایجاد بانک اطلاعاتی یکپارچه سایبری پلیس فتا پیشنهاد می‌شود؟	Soc-Cert

بحث و نتیجه‌گیری

با توجه به منابع موردمطالعه، اطلاعات جمع‌آوری‌شده از طریق مصاحبه با خبرگان و همچنین پرسشنامه از جامعهٔ نمونه، تجزیه‌وتحلیل آن‌ها می‌توان گفت: در کل بسترها و زیرساخت‌های فضای مجازی در کشور به‌طور مطلوب ایجاد نگردیده است. قابل‌ذکر است که این مطلب به‌خودی‌خود باعث ایمنی در برابر حملات و خطرات فضای سایبری می‌گردد. چنانکه بیان گردید، بسترها، ساختارها و ابزارهای عملیات مقابله با مزاحمت‌های سایبری موجود در سطح استان ضعیف بوده لیکن توان علمی و فنی نسبتاً مناسبی با توجه به سطوح تحصیلات و آموزش‌های نوین علوم فناوری اطلاعات در پلیس فتا وجود دارد. درنهایت، نتایج تحقیقی زیر حاصل گردیده است: در حال حاضر ساختار مورد نیاز (یگان سایبری) برای اجرای مقابله با مزاحمت‌های سایبری در سطح استان وجود ندارد هم‌اکنون پرونده‌های تشکیل‌شده در پلیس فتا فرماندهی انتظامی استان همدان با عنوان مزاحمت‌های سایبری در دو حوزهٔ کاربری (استفادهٔ کاربران از خدمات، موجود در فضای مجازی و مواجه‌شدن با مزاحمان سایبری) و در حوزهٔ زیرساخت (ایجاد مزاحمت برای سازمان‌های، شرکت‌ها نهادها و ... با انجام حملات سایبری) انجام می‌شود، لیکن در حوزهٔ کاربری با توجه به این‌که بیشترین پرونده‌های مزاحمت سایبری در حوزه شبکه‌های اجتماعی اینستاگرام و تلگرام رخداده و بستر هر دو خارج از کشور است و از طرفی، بانک‌های اطلاعاتی تجمیع نشده و در اختیار این پلیس نیست فرایند شناسایی و پیگیری دشوار بوده است. در حوزهٔ زیرساخت نیز ساختار مناسبی جهت مقابله با مزاحمت‌های سایبری نسبت به سایر سامانه‌های مبتنی بر فناوری اطلاعات در سطح استان وجود نداشته و

در راستای استحکام دیوار دفاعی و پدافند اطلاعاتی و سایبری موجود شبکه‌های اجتماعی مورداستفاده (شبکه‌های اطلاعاتی، فرماندهی و کنترل و شبکه اختصاصی ISP) در پلیس فتا، با ایجاد یگان مقابله با مزاحمت‌های سایبری تکیه‌بر دانش علمی موجود و ابزارهای روزآمد و مناسبی همچون دیوارهٔ آتش، رمزنگاری و پایش مستمر سیستم در برابر حملات سایبری می‌توان به‌صورت پیش‌دستانه (قبل از اقدامات دشمن) اقدام نمود.

هم‌اکنون، در شبکه‌های موجود تحت کنترل پلیس فتا، با ایجاد یگان دفاع سایبری استانی، با تکیه‌بر دانش علمی موجود و ابزارهای روزآمد و مناسبی همچون دیواره آتش، رمزنگاری و پایش سیستم می‌توان به پدافند سایبری پیش‌دستانه (قبل از اقدامات دشمن) اقدام و یا در صورت حملهٔ سایبری، تهاجمات را منحرف نمود.

پیشنهادها

۱-پیشنهاد می‌گردد معاونت طرح و برنامه، مرکز مطالعات و تحقیقات و معاونت عملیات با هماهنگی یکدیگر به تدوین دکترین، استراتژی‌های جنگ و دفاع سایبر و همچنین توسعه فناوری‌های این عرصه اقدام نمایند.

۲-پیشنهاد می‌گردد معاونت آموزش با تدوین برنامه آموزش حین خدمت به‌منظور ارتقای سطح دانش فناوری اطلاعات کارکنان، خصوصا مدیران و فرماندهان (در ابعاد جنگ‌های نوین، سایبری، اطلاعات و ارتباطات) اقدام نماید.

۳-پیشنهاد می‌گردد دانشگاه امین نیروی انتظامی با هماهنگی معاونت آموزش با تدوین برنامه آموزش بلندمدت طولی در دانشگاه به‌منظور ارتقای سطح دانش سایبری کارکنان، خصوصاً مدیران و فرماندهان با ایجاد رشته‌های دانشگاهی با عناوین ذیر اقدام نماید:

-مهندسی فناوری اطلاعات با گرایش پدافند سایبری

-مهندسی فناوری اطلاعات با گرایش مدیریت فضای سایبری

-مهندسی فناوری اطلاعات با گرایش سخت‌افزار و شبکه سایبر

-مهندسی فناوری اطلاعات با گرایش مدیریت مزاحمت‌های اینترنتی

۴-پیشنهاد می‌گردد معاونت طرح و برنامه به ایجاد رشته‌های فناوری اطلاعات و علوم وابسته و همچنین ایجاد و سازماندهی واحدها و یگان‌های ویژه‌ای برای مقابله با مزاحمت‌های سایبری اقدام نماید.

۵-پیشنهاد می‌گردد معاونت نیروی انسانی برای تأمین نیروی موردنیاز یگان‌های برخورد و یا اصلاح مزاحمین سایبری به جذب و گزینش نیروهای متخصص در زمینهٔ علوم سایبر و فناوری اطلاعات از طریق دانشگاه‌های ناجا اقدام نماید.

۶-طراحی و پیاده‌سازی یک بانک اطلاعاتی یکپارچه از کلیه اقدامات اساسی، تعداد و تنوع مزاحمت‌های سایبری و...با استانداردهای مقابله با مزاحمت‌های سایبری جهت جمع‌آوری و تجزیه‌وتحلیل اطلاعات.

۷-ایجاد مرکز پردازش اطلاعات مزاحمین سایبری و عوامل مزاحمت سایبر در مجموعه فتا از نیازمندی‌های روز بشمار می‌رود.

۸-معاونت عملیات پلیس فتا ناجا نسبت به بکارگیری انواع تجهیزات تاکتیکی و سیار در راستای ایجاد ساختار سازمانی مقابله با مزاحمت‌های سایبری اقدام نماید.

منابع

براری نیا، زهرا و محمودی، مهدی. (۱۳۹۷). فضای مجازی فرصت یا تهدید برای هویت دینی جوانان ایرانی. ششمین همایش علمی پژوهشی علوم تربیتی و روانشناسی، آسیب‌های اجتماعی و فرهنگی ایران، *انجمن توسعه و ترویج و فنون بنیادین*.
https://www.civilca.com/paper-PSCON06-PSCONF06-034.html

باستانی، برومند. (۱۳۸۳). *جرائم کامپیوتری و اینترنتی*. تهران، انتشارات بهنامی.

۱- پورونچی صلوات، میلاد. (۱۳۹۷). بررسی تأثیر دنیای مجازی بر سبک زندگی سالم. ششمین همایش علمی پژوهشی علوم تربیتی و روانشناسی، آسیب‌های اجتماعی و فرهنگی ایران، *انجمن توسعه و ترویج و فنون بنیادین*. https://www.civilca.com/papern PSCON06-PSCONF06-135.html

۲- دانایی‌فرد، حسن؛ الوانی، سید مهدی و عادل، آذر. (۱۳۸۳). *روش‌شناسی پژوهش کیفی در مدیریت: رویکردی جامع*. تهران، انتشارات صفار اشراقی.

۳- دیوسالار، عبدالرسول. (۱۳۸۵). *راهبردها و معماری کلان فرماندهی و کنترل جنگ اطلاعات (جلد ۲)*. تهران، موسسه آموزشی و تحقیقاتی صنایع دفاعی.

۴- ضیایی پور، حمید (۱۳۹۱). جنگ نرم۱(ویژه جنگ رایانه‌ای). تهران: انتشارات مرکز مطالعات و تحقیقات بین‌المللی ابرار معاصر.

۵- عقلمند، احمد. (۱۳۸۵). *مروری بر تاریخ تحولات فناوری سلاح‌های نظامی*. تهران، انتشارات امیرکبیر.

۶- معین، محمد. (۱۳۸۵). *فرهنگ فارسی معین*. تهران، انتشارات اشجع.

۷- اسکیلز، رابرت. (۱۳۸۴). جنگ *آینده، ترجمه عبدالمجید حیدری*. تهران، سپاه پاسداران انقلاب اسلامی، دانشکده فرماندهی و ستاد، دوره عالی جنگ.

۸- مکنزی، کنت. (۱۳۸۲). جنگ *ناهمتراز، ترجمه عبدالمجید حیدری و محمد تمنائی*. تهران، سپاه پاسداران انقلاب اسلامی، دانشکده فرماندهی و ستاد دوره عالی جنگ.

۹- مؤسسه آموزشی و تحقیقاتی صنایع دفاعی (۱۳۸۴). طرح فرا سازمانی فرماندهی و کنترل، چشم‌انداز مشترک ارتش آمریکا در افق ۲۰۲۰، تهران.

۱۰- مونکلر، هرفرید. (۱۳۸۴). *جنگ‌های نوین، ترجمه حسین درگاهی*. تهران، سپاه پاسداران انقلاب اسلامی، دانشکده فرماندهی و ستاد، دوره عالی جنگ.

11- Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security*, *31*(4), 418-436.

12- Tirenin, W., & Faatz, D. (1999, October). A concept for strategic cyber defense. In *MILCOM 1999. IEEE Military Communications. Conference Proceedings (Cat. No. 99CH36341)* (Vol. 1, pp. 458-463). IEEE.