

معیارهای مشروعیت در منازعات سایبری و هوشمند (تحلیل احکام مربوط به حملات سایبری، حفاظت غیرنظامیان و موازین پاسخ دفاعی)

□ حسین حجتی *

چکیده

ظهور فناوری‌های نوین در عرصه نظامی، به‌ویژه جنگ سایبری و سامانه‌های هوشمند مسلح، چالش‌های بنیادینی را در برابر فقه دفاعی اسلامی قرار داده است. این پژوهش با هدف تبیین معیارهای مشروعیت در منازعات سایبری و هوشمند، از منظر فقه اسلامی و حقوق بین‌الملل بشردوستانه، به روش توصیفی-تحلیلی و با رویکرد تطبیقی انجام شده است. داده‌ها از طریق مطالعه کتابخانه‌ای و بررسی اسناد فقهی، حقوقی و نظامی گردآوری شده‌اند. یافته‌های پژوهش نشان می‌دهد که اصول بنیادین فقه دفاعی اسلامی، از جمله اصل تمیز (تفکیک نظامیان از غیرنظامیان)، اصل تناسب، اصل ضرورت و نهی از فساد فی‌الارض، قابلیت انطباق با فضای سایبری را دارند، اما این انطباق نیازمند اجتهاد نوین و بازتعریف مفاهیم کلاسیک است. همچنین، مسئله حفاظت از غیرنظامیان در برابر حملات سایبری که زیرساخت‌های حیاتی را هدف می‌گیرند، از پیچیده‌ترین مسائل فقهی معاصر است. این پژوهش با ارائه چارچوب فقهی-حقوقی یکپارچه، به تبیین موازین پاسخ دفاعی مشروع در برابر تهدیدات سایبری و هوشمند می‌پردازد و پیشنهاد می‌کند که فقیهان و حقوقدانان اسلامی با تشکیل کمیته‌های تخصصی مشترک، به تدوین فقه دفاعی نوین بپردازند.

واژگان کلیدی: فقه دفاعی، جنگ سایبری، سامانه‌های هوشمند مسلح، اصل تمیز، حفاظت غیرنظامیان، مشروعیت دفاع، حقوق بین‌الملل بشردوستانه، اجتهاد نوین.

۱. مقدمه

۱-۱. بیان مسئله

در دهه‌های اخیر، ماهیت جنگ و منازعه مسلحانه دستخوش تحولاتی شگرف شده است. ظهور فضای سایبری به عنوان پنجمین حوزه عملیاتی جنگ، در کنار زمین، دریا، هوا و فضا، و توسعه سامانه‌های تسلیحاتی هوشمند از جمله پهپادهای مسلح، ربات‌های جنگنده و سامانه‌های تسلیحاتی خودمختار، پارادایم‌های کلاسیک جنگ را به چالش کشیده است (Schmitt, 2013, p. 3). این تحولات، فقه دفاعی اسلامی را با پرسش‌هایی مواجه ساخته که پاسخ به آن‌ها نیازمند اجتهاد عمیق و روش‌مند است.

مسئله اصلی این پژوهش آن است که آیا اصول و قواعد فقه دفاعی اسلامی، که در بستر جنگ‌های کلاسیک شکل گرفته‌اند، توانایی پاسخگویی به چالش‌های منازعات سایبری و هوشمند را دارند؟ و اگر دارند، این انطباق چگونه و بر اساس چه مبانی و معیارهایی صورت می‌گیرد؟ این پرسش از آن جهت اهمیت دارد که جمهوری اسلامی ایران و سایر کشورهای اسلامی، در معرض تهدیدات سایبری جدی قرار دارند و نیاز به چارچوب فقهی-حقوقی روشن برای پاسخ دفاعی مشروع احساس می‌شود. حمله سایبری استاکس‌نت به تأسیسات هسته‌ای ایران در سال 2010 (Langner, 2011, p. 49)، نمونه‌ای بارز از این تهدیدات است که نشان می‌دهد جنگ سایبری دیگر یک سناریوی فرضی نیست، بلکه واقعیتی است که کشورهای اسلامی با آن دست‌وپنجه نرم می‌کنند.

۲-۱. ضرورت و اهمیت پژوهش

ضرورت این پژوهش از چند جهت قابل تبیین است: نخست، خلأ فقهی موجود در حوزه منازعات سایبری و هوشمند که می‌تواند به بی‌ضابطگی در اقدامات دفاعی منجر شود؛ دوم، افزایش روزافزون تهدیدات سایبری علیه کشورهای اسلامی که نیاز به پاسخ فقهی-حقوقی مشخص دارد؛ سوم، ضرورت مشارکت فعال فقه اسلامی در شکل‌دهی به هنجارهای بین‌المللی حاکم بر جنگ سایبری؛ و چهارم، حفاظت از جان و مال غیرنظامیان که در فضای

سایبری به شدت آسیب پذیر هستند. چنان که شهید مطهری (۱۳۶۸، ص. ۱۱۲) تأکید می کند، فقه اسلامی باید پویا و پاسخگوی نیازهای زمان باشد و این پویایی در حوزه فقه دفاعی از اهمیت ویژه ای برخوردار است.

۳-۱. پیشینه پژوهش

مطالعات انجام شده در این حوزه را می توان به دو دسته تقسیم کرد: مطالعات فقهی-اسلامی و مطالعات حقوق بین الملل. در حوزه فقهی، آثار محدودی به این موضوع پرداخته اند. محقق داماد (۱۳۹۳) در کتاب «حقوق بین الملل اسلامی» به برخی جنبه های فقه دفاعی پرداخته، اما به منازعات سایبری توجه نکرده است. ضیاءالدین سردار (Sardar، 2010) در مقاله ای به چالش های فناوری نوین برای اخلاق اسلامی پرداخته، اما رویکرد فقهی-تحلیلی ندارد. در حوزه حقوق بین الملل، راهنمای تالین (Tallinn Manual) که توسط گروهی از متخصصان حقوق بین الملل تدوین شده (Schmitt، 2013)، مهم ترین سند در این زمینه است، اما رویکرد اسلامی ندارد. هنکرتز و دوسوالد-بک (Henckaerts & Doswald-Beck، 2005) در مطالعه جامع حقوق بین الملل بشردوستانه عرفی، اصولی را مطرح کرده اند که قابل تطبیق با فقه اسلامی هستند. در ایران، پژوهش های نسبتاً محدودی در این زمینه انجام شده است؛ از جمله مقاله رضایی و همکاران (۱۳۹۹) در مجله فقه و حقوق اسلامی که به برخی جنبه های حقوقی جنگ سایبری پرداخته، اما عمق فقهی کافی ندارد. بنابراین، خلأ پژوهشی جدی در این حوزه وجود دارد که این مقاله در صدد پر کردن آن است.

۲. مبانی فقهی دفاع مشروع در اسلام

۲-۱. مفهوم جهاد دفاعی و مشروعیت آن

فقه اسلامی، دفاع در برابر تجاوز را نه تنها مجاز، بلکه در شرایطی واجب می داند. قرآن کریم در این باره می فرماید:

«وَقَاتِلُوا فِي سَبِيلِ اللَّهِ الَّذِينَ يُقَاتِلُونَكُمْ وَلَا تَعْتَدُوا إِنَّ اللَّهَ لَا يُحِبُّ الْمُعْتَدِينَ» (البقره: ۱۹۰).

این آیه شریفه، دو اصل بنیادین را در فقه دفاعی اسلامی مستقر می‌کند: نخست، مشروعیت دفاع در برابر کسانی که به مسلمانان حمله می‌کنند؛ و دوم، نهی از تجاوز و تعدی. طباطبایی (۱۳۷۴، ج. ۲، ص. ۵۶) در تفسیر المیزان، این آیه را دلیل روشنی بر مشروعیت جهاد دفاعی می‌داند و تأکید می‌کند که قید «الَّذِينَ يُقَاتِلُونَكُمْ» نشان‌دهنده آن است که اسلام جنگ تهاجمی بی دلیل را مجاز نمی‌شمارد.

همچنین آیه شریفه دیگری می‌فرماید:

«أُذِنَ لِلَّذِينَ يُقَاتِلُونَ بِأَنَّهُمْ ظَلِمُوا وَإِنَّ اللَّهَ عَلَىٰ نَصْرِهِمْ لَقَدِيرٌ» (الحج: ۳۹).

این آیه، اولین آیه‌ای است که اذن صریح به جنگ دفاعی می‌دهد و مبنای آن را ظلم‌ستیزی قرار می‌دهد (مکارم شیرازی، ۱۳۷۴، ج. ۱۴، ص. ۹۸). از منظر فقهی، این آیه نشان می‌دهد که مشروعیت دفاع، مبتنی بر وجود ظلم و تجاوز است، نه صرف اختلاف عقیده یا منافع. در روایات نیز بر این اصل تأکید شده است. امام علی علیه السلام در نهج البلاغه می‌فرماید: «لَا تَبْدَأَنَّ بِقِتَالٍ إِلَّا أَنْ يُبْدَأَ بِكَ» (نهج البلاغه، نامه ۱۴، ص. ۳۶۹).

این روایت، اصل «عدم ابتدا به جنگ» را به عنوان یک قاعده فقهی مستقر می‌کند که در فضای سایبری نیز قابل اعمال است.

۲-۲. اصول بنیادین فقه دفاعی

فقه دفاعی اسلامی بر چند اصل بنیادین استوار است که در ادامه به تفصیل بررسی می‌شوند:

الف) اصل تمیز (تفکیک): این اصل که در فقه اسلامی به «تمیز بین مقاتل و غیرمقاتل» معروف است، یکی از محکم‌ترین اصول فقه دفاعی است. قرآن کریم می‌فرماید:

«وَلَا تَقْتُلُوا النَّفْسَ الَّتِي حَرَّمَ اللَّهُ إِلَّا بِالْحَقِّ» (الأنعام: ۱۵۱).

فقه‌های اسلامی، از جمله ابن‌قدامه (۱۳۸۸: ۱۰، ص. ۵۰۳) در المغنی، به صراحت از حرمت کشتن زنان، کودکان، سالمندان، کشاورزان و سایر غیرنظامیان در جنگ سخن گفته‌اند. این اصل، معادل اصل «تمایز» در حقوق بین‌الملل بشردوستانه است (Henckaerts & Doswald-Beck, 2005, p. 3).

ب) اصل تناسب: فقه اسلامی، پاسخ دفاعی را باید متناسب با تهدید بداند. قرآن می‌فرماید:

«فَمَنْ اعْتَدَى عَلَيْكُمْ فَاعْتَدُوا عَلَيْهِ بِمِثْلِ مَا اعْتَدَى عَلَيْكُمْ» (البقره: ۱۹۴).

این آیه، اصل تناسب را در پاسخ دفاعی مستقر می‌کند. البته فقها تأکید می‌کنند که «مثل» در این آیه به معنای تناسب کلی است، نه تقلید دقیق از روش دشمن (طباطبایی، ۱۳۷۴، ج. ۲، ص. ۶۸).
ج) اصل ضرورت: فقه اسلامی، استفاده از زور را تنها در حد ضرورت مجاز می‌داند. قاعده فقهی «الصَّرُورَاتُ تُبَيِّحُ الْمَحْظُورَاتِ» (ضرورت‌ها محرمات را مباح می‌کند) در این زمینه کاربرد دارد، اما با قید «الصَّرُورَةُ تُقَدَّرُ بِقَدَرِهَا» (ضرورت به اندازه خودش سنجیده می‌شود) محدود می‌شود (سیوطی، ۱۴۱۱ق.، ص. ۸۴).

د) نهی از فساد فی الارض: قرآن کریم به صراحت از ایجاد فساد در زمین نهی می‌کند:
«وَلَا تُفْسِدُوا فِي الْأَرْضِ بَعْدَ إِصْلَاحِهَا» (الأعراف: ۵۶).

این اصل، در فضای سایبری اهمیت ویژه‌ای دارد، زیرا حملات سایبری می‌تواند زیرساخت‌های حیاتی را که میلیون‌ها غیرنظامی به آن‌ها وابسته‌اند، مختل کنند.

۳-۲. نظریه جنگ عادلانه در فقه اسلامی

نظریه جنگ عادلانه (Just War Theory) در اسلام، ریشه‌های عمیقی در فقه و کلام اسلامی دارد. غزالی (۱۴۰۹ق.، ج. ۲، ص. ۳۰۷) در احیاء علوم الدین، شرایط جنگ مشروع را تبیین کرده است. ماوردی (۱۳۸۶ق.، ص. ۴۵) در الأحکام السلطانیة نیز به تفصیل از شرایط جهاد دفاعی سخن گفته است. در دوران معاصر، شهید صدر (۱۳۹۹ق.، ص. ۱۷۸) در اقتصادنا، رویکرد جامعی به مسئله دفاع مشروع ارائه داده است.

نظریه جنگ عادلانه اسلامی دارای دو بُعد است: «jus ad bellum» (حق توسل به جنگ) و «jus in bello» (حقوق در جنگ). در بُعد اول، شرایطی چون وجود تجاوز، نیت صادقانه، اعلام رسمی و اتمام حجت مطرح است. در بُعد دوم، اصول تمییز، تناسب و ضرورت حاکم هستند (Kelsay, 2007, p. 89).

۳. جنگ سایبری: ماهیت، ابعاد و چالش‌های فقهی

۳-۱. تعریف و ماهیت جنگ سایبری

جنگ سایبری را می‌توان به‌عنوان «استفاده از فناوری اطلاعات و ارتباطات برای انجام عملیات تهاجمی یا دفاعی در فضای سایبری با هدف ایجاد اختلال، تخریب یا کنترل سیستم‌های اطلاعاتی دشمن» تعریف کرد (Clarke & Knake, 2010, p. 6). این تعریف، سه عنصر اساسی دارد: ابزار (فناوری اطلاعات)، هدف (سیستم‌های اطلاعاتی) و غایت (اختلال، تخریب یا کنترل).

از منظر فقهی، جنگ سایبری با جنگ کلاسیک تفاوت‌های بنیادینی دارد که تحلیل فقهی آن را پیچیده می‌کند:

۱. فقدان مرز جغرافیایی: جنگ سایبری مرزهای جغرافیایی را نمی‌شناسد و یک حمله می‌تواند از هر نقطه‌ای از جهان انجام شود (Libicki, 2009, p. 23).

۲. ابهام در انتساب: شناسایی عامل حمله سایبری بسیار دشوار است و این ابهام، اعمال اصل تناسب را با چالش مواجه می‌کند (Rid & Buchanan, 2015, p. 7).

۳. آثار غیرمستقیم بر غیرنظامیان: حملات سایبری به زیرساخت‌های حیاتی می‌تواند آثار مخربی بر غیرنظامیان داشته باشند، حتی اگر هدف اولیه نظامی باشد (Schmitt, 2013, p. 157).

۴. ماهیت دوگانه فناوری: بسیاری از فناوری‌های سایبری هم کاربرد نظامی و هم غیرنظامی دارند (dual-use) که تمیز بین اهداف نظامی و غیرنظامی را دشوار می‌کند.

۳-۲. انواع حملات سایبری و تحلیل فقهی آنها

حملات سایبری را می‌توان به چند دسته تقسیم کرد که هر کدام از منظر فقهی حکم متفاوتی دارند:

الف) حملات به زیرساخت‌های نظامی: این نوع حملات که سیستم‌های فرماندهی و کنترل، شبکه‌های ارتباطی نظامی و سامانه‌های تسلیحاتی دشمن را هدف می‌گیرند، از منظر فقهی در چارچوب جهاد دفاعی قابل توجیه هستند، مشروط بر اینکه اصول تمیز و تناسب رعایت شوند. شیخ طوسی (۱۳۸۷ق، ج. ۲، ص. ۱۱) در المبسوط، تخریب ابزار جنگی دشمن را در چارچوب دفاع مشروع جایز می‌داند.

ب) حملات به زیرساخت‌های دوگانه: این حملات که سیستم‌هایی مانند شبکه برق، آب و ارتباطات را هدف می‌گیرند، از منظر فقهی پیچیده‌تر هستند. این زیرساخت‌ها هم کاربرد نظامی و هم غیرنظامی دارند. فقهای معاصر، از جمله آیت‌الله جوادی آملی (۱۳۹۲، ص. ۲۳۴)، تأکید می‌کنند که در چنین مواردی باید میزان آسیب به غیرنظامیان در مقابل مزیت نظامی سنجیده شود و اگر آسیب به غیرنظامیان بیش از حد متعارف باشد، حمله مشروع نیست.

ج) حملات به زیرساخت‌های صرفاً غیرنظامی: حملات سایبری به بیمارستان‌ها، مدارس، بانک‌های اطلاعاتی غیرنظامی و سایر تأسیسات صرفاً غیرنظامی، از منظر فقهی حرام و از مصادیق «فساد فی الارض» است. قرآن کریم می‌فرماید:

«مِنْ أَجْلِ ذَلِكَ كَتَبْنَا عَلَىٰ بَنِي إِسْرَآئِيلَ أَنَّهُ مَن قَتَلَ نَفْسًا بِغَيْرِ نَفْسٍ أَوْ فَسَادٍ فِي الْأَرْضِ فَكَأَنَّمَا قَتَلَ النَّاسَ جَمِيعًا» (المائدة: ۳۲).

این آیه شریفه، حرمت کشتن نفس محترم را به قتل تمام انسان‌ها تشبیه می‌کند و نشان می‌دهد که اسلام چه اهمیت عظیمی به حفظ جان انسان‌ها می‌دهد (طباطبایی، ۱۳۷۴، ج. ۵، ص. ۲۸۹).

د) جاسوسی سایبری: جمع‌آوری اطلاعات از طریق نفوذ به شبکه‌های رایانه‌ای دشمن، از منظر فقهی در چارچوب «تجسس» قرار می‌گیرد. قرآن کریم می‌فرماید:

«وَلَا تَجَسَّسُوا» (الحجرات: ۱۲).

اما فقها بین تجسس در امور خصوصی افراد (که حرام است) و جمع‌آوری اطلاعات نظامی دشمن در شرایط جنگ (که جایز است) تفکیک قائل شده‌اند. شهید اول (۱۴۱۰ق.، ج. ۲، ص. ۲۴۵) در اللمعه الدمشقیه، جاسوسی نظامی در شرایط جنگ را جایز می‌داند، مشروط بر اینکه به حریم خصوصی افراد تجاوز نشود.

۳-۳. چالش انتساب در جنگ سایبری و پیامدهای فقهی آن

یکی از بزرگ‌ترین چالش‌های جنگ سایبری، مسئله انتساب (attribution) است. شناسایی قطعی عامل یک حمله سایبری بسیار دشوار است، زیرا مهاجمان می‌توانند از تکنیک‌های

پیچیده‌ای برای پنهان کردن هویت خود استفاده کنند (Rid & Buchanan, 2015, p. 15). این مسئله، از منظر فقهی اهمیت حیاتی دارد، زیرا پاسخ دفاعی مشروع مستلزم یقین یا اطمینان قوی به هویت متجاوز است.

فقه اسلامی در این زمینه بر اصل «البینه علی المدعی» (دلیل بر عهده مدعی است) تأکید دارد (نجفی، ۱۴۰۴ق.، ج. ۴۰، ص. ۲۳۴). بنابراین، کشوری که قصد پاسخ دفاعی به یک حمله سایبری را دارد، باید دلایل کافی برای انتساب حمله به یک کشور یا گروه خاص داشته باشد. سطح اثبات مورد نیاز در فقه، «اطمینان قلبی» یا «ظن قوی» است که در حقوق بین‌الملل معادل «clear and convincing evidence» است (Schmitt, 2013, p. 89).

آیت‌الله خامنه‌ای (۱۳۹۵، ص. ۱۵۶) در بیانات خود تأکید کرده‌اند که در مسائل دفاعی، تصمیم‌گیری باید بر اساس اطلاعات دقیق و قابل اعتماد باشد و عجله در پاسخ دفاعی بدون اطمینان کافی، می‌تواند به ظلم به بی‌گناهان منجر شود.

۳-۴. مفهوم «حمله مسلحانه» در فضای سایبری

یکی از مباحث کلیدی در حقوق بین‌الملل و فقه دفاعی، این است که آیا یک حمله سایبری می‌تواند به عنوان «حمله مسلحانه» تلقی شود که توجیه‌کننده دفاع مشروع باشد. راهنمای تالین (Schmitt, 2013, p. 106) معیار «scale and effects» را مطرح می‌کند: اگر آثار یک حمله سایبری معادل یک حمله مسلحانه کلاسیک باشد، می‌تواند حق دفاع مشروع را فعال کند.

از منظر فقهی، معیار مشابهی قابل استخراج است. فقها در تعریف «محارب» (کسی که با مسلمانان می‌جنگد) به آثار و نتایج اقدامات او توجه می‌کنند، نه صرفاً ابزار مورد استفاده (ابن‌قدامة، ۱۳۸۸ق.، ج. ۱۰، ص. ۲۷۸). بنابراین، اگر یک حمله سایبری منجر به کشته شدن افراد، تخریب گسترده اموال یا اختلال جدی در زندگی مردم شود، از منظر فقهی می‌تواند معادل حمله مسلحانه تلقی شود و پاسخ دفاعی متناسب را توجیه کند.

مثال حمله استاکس‌نت به تأسیسات هسته‌ای ایران در این زمینه آموزنده است. این حمله که منجر به تخریب فیزیکی سانتریفیوژها شد (Langner, 2011, p. 58)، از منظر فقهی قابل

تلقی به عنوان حمله مسلحانه است، زیرا آثار فیزیکی قابل توجهی داشت و می توانست به خطرات جدی تری منجر شود.

۴. سامانه های هوشمند مسلح و چالش های فقهی

۴-۱. تعریف و انواع سامانه های هوشمند مسلح

سامانه های تسلیحاتی خودمختار (Autonomous Weapon Systems) یا سامانه های هوشمند مسلح، سیستم هایی هستند که می توانند بدون دخالت انسان، اهداف را شناسایی، انتخاب و مورد حمله قرار دهند (Arkin, 2009, p. 29). این سامانه ها طیف وسیعی از پهپادهای مسلح تا ربات های جنگنده زمینی و دریایی را شامل می شوند.

از منظر سطح خودمختاری، این سامانه ها به سه دسته تقسیم می شوند:

۱. سامانه های نیمه خودمختار: که انسان در حلقه تصمیم گیری حضور دارد (human-in-the-loop)

۲. سامانه های خودمختار با نظارت انسانی: که انسان می تواند مداخله کند (human-on-the-loop)

۳. سامانه های کاملاً خودمختار: که بدون دخالت انسان عمل می کنند (human-out-of-the-loop)

از منظر فقهی، این تقسیم بندی اهمیت حیاتی دارد، زیرا مسئله «مسئولیت اخلاقی و شرعی» در هر کدام متفاوت است.

۴-۲. چالش مسئولیت اخلاقی و شرعی در سامانه های خودمختار

یکی از بنیادین ترین چالش های فقهی در مورد سامانه های هوشمند مسلح، مسئله «تکلیف» و «مسئولیت» است. در فقه اسلامی، تکلیف مستلزم «عقل» و «اختیار» است (علامه حلی، ۱۴۱۳ق، ج. ۱، ص. ۸۹). ماشین ها فاقد عقل و اراده آزاد هستند، بنابراین نمی توانند مکلف باشند. این مسئله، پرسش های جدی را در مورد مسئولیت شرعی و حقوقی استفاده از این سامانه ها مطرح می کند.

فقها در این زمینه دو رویکرد دارند:

رویکرد اول: مسئولیت بر عهده طراح، برنامه‌نویس و فرمانده‌ای است که سامانه را به کار می‌گیرد. این رویکرد مبتنی بر قاعده «التسبیب» (سبب‌سازی) است که در فقه اسلامی، کسی که سبب ضرر می‌شود، ضامن است (نجفی، ۱۴۰۴ق، ج. ۳۷، ص. ۱۵۶).

رویکرد دوم: استفاده از سامانه‌های کاملاً خودمختار در جنگ، به دلیل عدم امکان کنترل کامل بر تصمیمات آن‌ها و خطر نقض اصل تمیز، اساساً نامشروع است. این رویکرد مبتنی بر قاعده «لاضرر» و اصل احتیاط در حفظ نفوس محترمه است (مکارم شیرازی، ۱۳۹۲، ص. ۲۶۷).

آیت الله سیستانی (۱۳۹۴، ص. ۱۸۹) در استفتائات خود تأکید کرده‌اند که استفاده از هر سلاحی که کنترل دقیق بر آن ممکن نباشد و احتمال آسیب به غیرنظامیان را افزایش دهد، مشکل شرعی دارد.

۳-۴. اصل تمیز و سامانه‌های هوشمند

یکی از مهم‌ترین چالش‌های فقهی سامانه‌های هوشمند، توانایی آن‌ها در رعایت اصل تمیز است. آیا یک سامانه هوشمند می‌تواند به‌طور قابل اعتماد بین نظامیان و غیرنظامیان تمایز قائل شود؟ تحقیقات نشان می‌دهند که حتی پیشرفته‌ترین سامانه‌های هوش مصنوعی نیز در شرایط پیچیده جنگی، خطای قابل توجهی دارند (Sharkey, 2012, p. 787).

از منظر فقهی، اصل تمیز یک الزام قطعی است که نمی‌توان از آن چشم‌پوشی کرد. امام خمینی (۱۴۲۱ق، ج. ۱، ص. ۴۵۶) در تحریرالوسیله تأکید می‌کند که در جنگ، کشتن کسانی که در جنگ شرکت ندارند، حرام است و این حکم استثنایی ندارد. بنابراین، استفاده از سامانه‌ای که نمی‌تواند به‌طور قابل اعتماد این تمایز را رعایت کند، از منظر فقهی مشکل‌ساز است.

البته برخی فقها استدلال می‌کنند که اگر سامانه هوشمند در رعایت اصل تمیز دقیق‌تر از انسان عمل کند، استفاده از آن نه تنها جایز، بلکه ممکن است واجب باشد، زیرا منجر به کاهش تلفات غیرنظامی می‌شود (Arkin, 2009, p. 67). این استدلال مبتنی بر قاعده «اهم و مهم» در فقه است که در تراحم دو واجب، واجب مهم‌تر مقدم است.

۴-۴. مسئله قصد و نیت در استفاده از سامانه‌های خودمختار

در فقه اسلامی، «نیت» و «قصد» نقش محوری در احکام دارد. پیامبر اکرم صلی الله علیه و آله فرموده‌اند:

«إِنَّمَا الْأَعْمَالُ بِالنِّيَّاتِ» (صحیح بخاری، ج. ۱، ص. ۳).

در مورد سامانه‌های خودمختار، این پرسش مطرح می‌شود که آیا می‌توان نیت را به ماشین نسبت داد؟ فقها پاسخ می‌دهند که نیت به کسی نسبت داده می‌شود که سامانه را برنامه‌ریزی و به کار می‌گیرد، نه خود سامانه (محقق داماد، ۱۳۹۳، ص. ۳۴۵). بنابراین، اگر فرمانده‌ای سامانه خودمختار را با نیت کشتن غیرنظامیان به کار گیرد، مسئولیت شرعی و حقوقی بر عهده اوست. اما مسئله پیچیده‌تر زمانی است که سامانه خودمختار بر خلاف برنامه‌ریزی اولیه، غیرنظامیان را هدف قرار دهد. در این صورت، آیا طراح، برنامه‌نویس یا فرمانده مسئول هستند؟ فقها بر اساس قاعده «الغرور» (فریب‌دهی) و «التسبیب» (استدلال می‌کنند که اگر خطا ناشی از نقص طراحی یا برنامه‌نویسی باشد، طراح و برنامه‌نویس ضامن هستند؛ و اگر ناشی از تصمیم فرمانده برای استفاده از سامانه در شرایط نامناسب باشد، فرمانده مسئول است (نجفی، ۱۴۰۴: ۴۳/۲۳۴).

۵. معیارهای مشروعیت حملات سایبری دفاعی

۱-۵. شرایط توسل به دفاع سایبری

از منظر فقهی، توسل به دفاع سایبری مستلزم تحقق شرایطی است که در ادامه به تفصیل بررسی می‌شوند:

الف) وجود تجاوز واقعی یا قریب‌الوقوع: فقه اسلامی، دفاع پیشگیرانه را تنها در صورت وجود تهدید قریب‌الوقوع و قطعی مجاز می‌داند. قرآن کریم می‌فرماید:

«وَقَاتِلُوا فِي سَبِيلِ اللَّهِ الَّذِينَ يُقَاتِلُونَكُمْ» (البقره: ۱۹۰).

فعل مضارع «يُقَاتِلُونَكُمْ» نشان می‌دهد که تجاوز باید واقعی یا در حال وقوع باشد (طباطبایی، ۱۳۷۴، ج. ۲، ص. ۵۸). در فضای سایبری، این معیار به معنای آن است که باید شواهد قوی از یک حمله سایبری قریب‌الوقوع یا در حال انجام وجود داشته باشد. صرف توانایی فنی یک کشور برای انجام حمله سایبری، توجیه‌کننده حمله پیشگیرانه نیست.

ب) انتساب قابل اعتماد: همان طور که پیش تر ذکر شد، انتساب حمله سایبری به یک عامل مشخص، شرط ضروری برای پاسخ دفاعی است. سطح اثبات مورد نیاز، «ظن قوی» یا «اطمینان قلبی» است که در اصطلاح حقوقی معادل «clear and convincing evidence» است (Schmitt, 2013, p. 92).

ج) عدم وجود راه حل مسالمت آمیز: قرآن کریم تأکید می کند:

«وَإِنْ جَنَحُوا لِلسَّلْمِ فَاجْنَحْ لَهَا» (الأنفال: ۶۱).

این آیه نشان می دهد که اسلام صلح را بر جنگ ترجیح می دهد. بنابراین، قبل از توسل به پاسخ سایبری، باید راه حل های دیپلماتیک و مسالمت آمیز جست و جو شود (مکارم شیرازی، ۱۳۷۴، ج. ۹، ص. ۱۷۸).

د) نیت صادقانه: هدف از پاسخ دفاعی باید دفع تجاوز باشد، نه انتقام جویی یا تحمیل اراده. امام علی (علیه السلام) می فرماید:

«لَا تَقَاتِلُوا الْقَوْمَ حَتَّى يَبْدَءُوكُمْ فَإِنْ كُمْ بِحَمْدِ اللَّهِ عَلَى حُجَّةٍ وَ تَرْكُكُمْ إِيَّاهُمْ حَتَّى يَبْدَءُوكُمْ حُجَّةٌ أُخْرَى لَكُمْ عَلَيْهِمْ» (نهج البلاغه، خطبه ۱۴، ص. ۷۸).

۵-۲. اصل تناسب در پاسخ سایبری

اصل تناسب یکی از محوری ترین اصول در فقه دفاعی است. قرآن کریم می فرماید:

«فَمَنْ اعْتَدَى عَلَيْكُمْ فَاعْتَدُوا عَلَيْهِ بِمِثْلِ مَا اعْتَدَى عَلَيْكُمْ» (البقرة: ۱۹۴).

در فضای سایبری، اعمال این اصل چالش برانگیز است، زیرا سنجش «مثل» در حملات سایبری دشوار است. آیا تناسب بر اساس ابزار مورد استفاده، آثار حمله، یا هدف حمله سنجیده می شود؟

فقها بر این نظر هستند که معیار اصلی، «آثار و نتایج» حمله است، نه ابزار (ابن قدامه، ۱۳۸۸ق، ج. ۱۰، ص. ۲۸۹). بنابراین، اگر یک حمله سایبری منجر به تخریب زیرساخت نظامی شود، پاسخ متناسب می تواند شامل حمله سایبری به زیرساخت نظامی مشابه یا حتی حمله کلاسیک متناسب باشد. اما پاسخ نباید از حد دفع تجاوز فراتر رود.

آیت الله مکارم شیرازی (۱۳۹۲، ص. ۲۷۸) تأکید می‌کند که در تعیین تناسب، باید به «مصلحت عمومی» و «حفظ نفوس محترمه» توجه ویژه داشت و از پاسخ‌هایی که منجر به تشدید درگیری و آسیب گسترده به غیرنظامیان می‌شود، پرهیز کرد.

۳-۵. اصل ضرورت و حداقل زور لازم

قاعده فقهی «الضَّرُورَةُ تُقَدَّرُ بِقَدَرِهَا» (ضرورت به اندازه خودش سنجیده می‌شود) در پاسخ سایبری دفاعی نیز حاکم است (سیوطی، ۱۴۱۱ق.، ص. ۸۷). این اصل ایجاب می‌کند که پاسخ دفاعی باید به حداقل زور لازم برای دفع تجاوز محدود شود.

در فضای سایبری، این اصل به معنای آن است که:

۱. اگر یک حمله سایبری را می‌توان با اقدامات دفاعی غیرتخریبی (مانند فایروال‌ها و سیستم‌های دفاعی) خنثی کرد، توسل به حمله متقابل تخریبی مجاز نیست.
۲. اگر حمله متقابل ضروری است، باید به اهداف نظامی محدود شود و از آسیب به زیرساخت‌های غیرنظامی پرهیز شود.
۳. شدت و دامنه پاسخ باید متناسب با تهدید باشد و از اقدامات افراطی که منجر به تشدید بی‌رویه درگیری می‌شود، اجتناب شود.

۴-۵. اصل تمییز در عملیات سایبری

اصل تمییز در فضای سایبری با چالش‌های خاصی مواجه است. در جنگ کلاسیک، تمایز بین اهداف نظامی و غیرنظامی نسبتاً روشن است، اما در فضای سایبری، بسیاری از زیرساخت‌ها کاربرد دوگانه دارند. برای مثال، شبکه اینترنت هم برای مقاصد نظامی و هم غیرنظامی استفاده می‌شود.

فقه اسلامی در این زمینه معیارهای روشنی ارائه می‌دهد:

- (الف) اولویت با اهداف صرفاً نظامی: اگر امکان هدف‌گیری اهداف صرفاً نظامی وجود دارد، حمله به اهداف دوگانه مجاز نیست (شهید ثانی، ۱۴۱۳ق.، ج. ۲، ص. ۲۳۴).
- (ب) سنجش آسیب جانبی: اگر حمله به یک هدف دوگانه ضروری است، باید میزان

آسیب جانبی به غیرنظامیان در مقابل مزیت نظامی سنجیده شود. اگر آسیب جانبی بیش از حد متعارف باشد، حمله نامشروع است. این معیار در حقوق بین الملل بشردوستانه به «اصل تناسب در آسیب جانبی» معروف است (Henckaerts & Doswald-Beck, 2005, p. 46).

ج) اتخاذ اقدامات احتیاطی: فقه اسلامی تأکید می‌کند که در عملیات نظامی باید اقدامات احتیاطی لازم برای حفاظت از غیرنظامیان اتخاذ شود. در فضای سایبری، این اقدامات شامل استفاده از ابزارهای دقیق، محدود کردن دامنه حمله و هشدار به غیرنظامیان (در صورت امکان) است (مکارم شیرازی، ۱۳۹۲، ص. ۲۸۹).

۶. حفاظت از غیرنظامیان در منازعات سایبری

۶-۱. مفهوم غیرنظامی در فضای سایبری

تعریف «غیرنظامی» در فضای سایبری پیچیده‌تر از جنگ کلاسیک است. در جنگ کلاسیک، غیرنظامیان کسانی هستند که مستقیماً در دشمنی‌ها شرکت ندارند (Henckaerts & Doswald-Beck, 2005, p. 19). اما در فضای سایبری، مرزها مبهم‌تر است. آیا یک برنامه‌نویس غیرنظامی که برای ارتش کار می‌کند، هدف مشروع است؟ آیا یک زیرساخت غیرنظامی که به طور موقت برای مقاصد نظامی استفاده می‌شود، قابل حمله است؟

فقه اسلامی در این زمینه معیار «مشارکت مستقیم در دشمنی‌ها» را مطرح می‌کند. کسانی که مستقیماً در عملیات نظامی شرکت دارند، هدف مشروع هستند، اما کسانی که صرفاً در امور غیرنظامی فعالیت می‌کنند، حتی اگر به طور غیرمستقیم به تلاش جنگی کمک کنند، هدف مشروع نیستند (محقق داماد، ۱۳۹۳، ص. ۴۵۶).

در مورد برنامه‌نویسان و متخصصان فناوری اطلاعات، فقها بر این نظر هستند که اگر این افراد مستقیماً در طراحی و اجرای عملیات سایبری نظامی شرکت داشته باشند، می‌توانند هدف مشروع باشند، اما اگر صرفاً در نگهداری زیرساخت‌های عمومی فعالیت کنند، هدف‌گیری آن‌ها مشروع نیست (آیت‌الله جوادی آملی، ۱۳۹۲، ص. ۲۶۷).

۲-۶. اهداف ممنوعه در جنگ سایبری

فقه اسلامی فهرست روشنی از اهداف ممنوعه در جنگ ارائه می‌دهد که در فضای سایبری نیز قابل اعمال است:

(الف) زیرساخت‌های بهداشتی و درمانی: حمله سایبری به بیمارستان‌ها، مراکز درمانی و سیستم‌های مدیریت دارو، از منظر فقهی حرام است. پیامبر اکرم صلی الله علیه و آله در جنگ‌ها از کشتن زنان، کودکان و بیماران نهی می‌کردند (ابن هشام، ۱۳۷۵ق، ج. ۳، ص. ۲۳۴). حمله سایبری به سیستم‌های بهداشتی که می‌تواند منجر به مرگ بیماران شود، از مصادیق بارز این نهی است.

(ب) اماکن مذهبی و فرهنگی: قرآن کریم می‌فرماید:

«وَلَوْ لَا دَفْعُ اللَّهِ النَّاسَ بَعْضَهُمْ بِبَعْضٍ لَهْدِمَتْ صَوَامِعُ وَبِيعٌ وَصَلَوَاتُ وَمَسَاجِدُ يُذَكَّرُ فِيهَا اسْمُ اللَّهِ كَثِيرًا» (الحج: ۴۰).

این آیه بر حرمت تخریب اماکن عبادی تأکید دارد (طباطبایی، ۱۳۷۴، ج. ۱۴، ص. ۴۵۶). در فضای سایبری، این حکم شامل حمله به پایگاه‌های داده و سیستم‌های دیجیتال مربوط به این اماکن نیز می‌شود.

(ج) زیرساخت‌های آموزشی: مدارس، دانشگاه‌ها و مراکز آموزشی از اهداف ممنوعه هستند. حمله سایبری به سیستم‌های آموزشی که می‌تواند منجر به اختلال در تحصیل دانش‌آموزان و دانشجویان شود، از منظر فقهی نامشروع است (مکارم شیرازی، ۱۳۹۲، ص. ۳۰۱).

(د) زیرساخت‌های حیاتی غیرنظامی: سیستم‌های تأمین آب، برق، گاز و سایر خدمات حیاتی که صرفاً برای غیرنظامیان استفاده می‌شوند، از اهداف ممنوعه هستند. حمله به این زیرساخت‌ها می‌تواند منجر به رنج گسترده غیرنظامیان شود که با اصل «نهی از فساد فی الارض» در تعارض است (نجفی، ۱۴۰۴ق، ج. ۲۱، ص. ۱۷۸).

۳-۶. اعمال اصل تناسب در آسیب جانبی

یکی از پیچیده‌ترین مسائل فقهی در جنگ سایبری، سنجش آسیب جانبی به غیرنظامیان است. در حقوق بین‌الملل بشردوستانه، اصل تناسب ایجاب می‌کند که آسیب جانبی به غیرنظامیان

نباید «بیش از حد» (excessive) در مقایسه با مزیت نظامی مستقیم و مشخص باشد (Henckaerts & Doswald-Beck, 2005, p. 46).

فقه اسلامی نیز معیار مشابهی دارد. فقها بر این نظر هستند که اگر یک عملیات نظامی منجر به آسیب قابل توجه به غیرنظامیان شود، باید میزان این آسیب در مقابل مصلحت نظامی سنجیده شود. اگر آسیب بیش از حد متعارف باشد، عملیات نامشروع است (آیت الله خامنه‌ای، ۱۳۹۵، ص. ۲۳۴).

در فضای سایبری، این سنجش بسیار دشوار است، زیرا:

۱. پیش‌بینی آثار حمله سایبری دشوار است: یک حمله سایبری به یک زیرساخت دوگانه می‌تواند آثار غیرمنتظره‌ای داشته باشد. برای مثال، حمله به شبکه برق ممکن است نه تنها تأسیسات نظامی، بلکه بیمارستان‌ها را نیز تحت تأثیر قرار دهد.
 ۲. ماهیت به هم پیوسته فضای سایبری: در فضای سایبری، سیستم‌ها به شدت به هم متصل هستند و یک حمله به یک بخش می‌تواند به بخش‌های دیگر سرایت کند.
 ۳. دشواری سنجش کمی آسیب: برخلاف جنگ کلاسیک که تعداد تلفات قابل شمارش است، در جنگ سایبری، آسیب ممکن است به صورت اختلال در خدمات، از دست رفتن داده‌ها یا آسیب اقتصادی باشد که سنجش کمی آن دشوار است.
- فقها در این زمینه توصیه می‌کنند که در صورت تردید، باید از اصل احتیاط پیروی کرد و از عملیاتی که احتمال آسیب قابل توجه به غیرنظامیان دارد، خودداری نمود (شهید ثانی، ۱۴۱۳ق.، ج. ۲، ص. ۲۸۹).

۴-۶. اقدامات احتیاطی در عملیات سایبری

فقه اسلامی تأکید می‌کند که در عملیات نظامی باید تمام اقدامات احتیاطی ممکن برای حفاظت از غیرنظامیان اتخاذ شود. امام علی علیه السلام در نهج البلاغه می‌فرماید:

«وَلَا تُقَاتِلُوا إِلَّا مَنْ قَاتَلَكُمْ» (نهج البلاغه، خطبه ۱۴، ص. ۷۸).

در فضای سایبری، اقدامات احتیاطی شامل موارد زیر است:

الف) استفاده از ابزارهای دقیق: باید از ابزارهای سایبری استفاده شود که قابلیت

هدف‌گیری دقیق دارند و احتمال آسیب جانبی را به حداقل می‌رسانند. این امر مستلزم سرمایه‌گذاری در تحقیق و توسعه فناوری‌های دقیق است (Schmitt, 2013, p. 156).

ب) محدود کردن دامنه حمله: حملات سایبری باید به گونه‌ای طراحی شوند که دامنه آن‌ها محدود به اهداف نظامی باشد و به سیستم‌های غیرنظامی سرایت نکند. این امر نیازمند برنامه‌ریزی دقیق و آزمایش‌های گسترده قبل از اجرا است.

ج) هشدار به غیرنظامیان: در صورت امکان، باید قبل از حمله سایبری به زیرساخت‌های دوگانه، به غیرنظامیان هشدار داده شود تا بتوانند اقدامات احتیاطی لازم را انجام دهند. البته این امر همیشه ممکن نیست، زیرا ممکن است مزیت نظامی را از بین ببرد، اما در مواردی که امکان‌پذیر است، باید انجام شود (مکارم شیرازی، ۱۳۹۲، ص. ۳۱۲).

د) نظارت مستمر بر آثار حمله: پس از اجرای حمله سایبری، باید آثار آن به طور مستمر نظارت شود و در صورت مشاهده آسیب غیرمنتظره به غیرنظامیان، اقدامات اصلاحی فوری انجام شود.

۵-۶. مسئولیت جبران خسارت

فقه اسلامی بر اصل «الإتلاف یوجب الضمان» (تلف کردن مال دیگری موجب ضمان است) تأکید دارد (نجفی، ۱۴۰۴ق، ج. ۳۷، ص. ۸۹). این اصل در مورد خسارات وارده به غیرنظامیان در جنگ سایبری نیز قابل اعمال است.

اگر یک حمله سایبری دفاعی منجر به آسیب به اموال یا جان غیرنظامیان شود، حتی اگر حمله در چارچوب دفاع مشروع بوده باشد، مسئولیت جبران خسارت وجود دارد. این مسئولیت بر عهده دولتی است که حمله را انجام داده است (محقق داماد، ۱۳۹۳، ص. ۵۶۷). البته در مواردی که آسیب ناشی از اقدامات دشمن باشد (مانند استفاده از غیرنظامیان به عنوان سپر انسانی)، مسئولیت بر عهده دشمن است. اما در مواردی که آسیب ناشی از عدم رعایت اقدامات احتیاطی یا خطای عملیاتی باشد، مسئولیت بر عهده مهاجم است.

۷. چارچوب فقهی - حقوقی یکپارچه برای پاسخ دفاعی مشروع

۷-۱. تلفیق اصول فقهی و حقوق بین الملل بشردوستانه

یکی از اهداف اصلی این پژوهش، ارائه چارچوب یکپارچه‌ای است که اصول فقه دفاعی اسلامی را با هنجارهای حقوق بین الملل بشردوستانه تلفیق کند. این چارچوب می‌تواند به عنوان راهنمایی برای تصمیم‌گیرندگان نظامی و سیاسی در کشورهای اسلامی مورد استفاده قرار گیرد.

اصول بنیادین چارچوب:

۱. اصل مشروعیت دفاع: دفاع در برابر تجاوز، حق طبیعی و شرعی هر کشور است، اما باید در چارچوب اصول فقهی و حقوقی انجام شود.
۲. اصل تمیز: در تمام عملیات سایبری باید بین اهداف نظامی و غیرنظامی تمایز قائل شد و حمله به غیرنظامیان ممنوع است.
۳. اصل تناسب: پاسخ دفاعی باید متناسب با تجاوز باشد و از حد دفع تجاوز فراتر نرود.
۴. اصل ضرورت: باید از حداقل زور لازم برای دفع تجاوز استفاده شود و اقدامات غیرتخریبی بر اقدامات تخریبی اولویت دارند.
۵. اصل احتیاط: باید تمام اقدامات احتیاطی ممکن برای حفاظت از غیرنظامیان اتخاذ شود.
۶. اصل مسئولیت: مسئولیت شرعی و حقوقی عملیات سایبری بر عهده تصمیم‌گیرندگان انسانی است، نه سامانه‌های خودمختار.
۷. اصل جبران خسارت: در صورت ورود خسارت به غیرنظامیان، مسئولیت جبران خسارت وجود دارد.

۷-۲. فرآیند تصمیم‌گیری برای پاسخ سایبری دفاعی

بر اساس چارچوب فوق، فرآیند تصمیم‌گیری برای پاسخ سایبری دفاعی باید شامل مراحل زیر باشد:

مرحله اول: تأیید تجاوز و انتساب

- جمع‌آوری شواهد فنی و اطلاعاتی

- تحلیل شواهد توسط متخصصان
- دستیابی به اطمینان قوی نسبت به وقوع تجاوز و هویت متجاوز
- مشورت با مراجع فقهی در مورد کفایت شواهد
- مرحله دوم:** ارزیابی گزینه‌های پاسخ
- بررسی گزینه‌های غیرتخریبی (دفاع، دیپلماسی)
- در صورت ضرورت پاسخ تخریبی، شناسایی اهداف نظامی مشروع
- ارزیابی آثار احتمالی هر گزینه بر غیرنظامیان
- سنجش تناسب هر گزینه با تجاوز
- مرحله سوم:** تصویب فقهی-حقوقی
- ارائه طرح عملیات به کمیته تخصصی فقهی-حقوقی
- بررسی انطباق طرح با اصول فقهی و حقوقی
- اخذ مجوز شرعی و حقوقی
- مرحله چهارم:** اجرا با نظارت
- اجرای عملیات با رعایت دقیق اقدامات احتیاطی
- نظارت لحظه‌ای بر آثار عملیات
- آمادگی برای توقف یا تعدیل عملیات در صورت آسیب غیرمنتظره به غیرنظامیان
- مرحله پنجم:** ارزیابی پس از عملیات
- ارزیابی آثار عملیات
- شناسایی خسارات وارده به غیرنظامیان
- اتخاذ تصمیم در مورد جبران خسارت
- استخراج درس‌آموخته‌ها برای عملیات آینده

۳-۷. نقش مراجع فقهی در تصمیم‌گیری‌های دفاعی

یکی از ویژگی‌های منحصربه‌فرد نظام اسلامی، نقش محوری مراجع فقهی در تصمیم‌گیری‌های

مهم است. در حوزه دفاع سایبری نیز، مشورت با مراجع فقهی و اخذ نظر آن‌ها در مورد مشروعیت عملیات، اهمیت حیاتی دارد.

پیشنهاد می‌شود که در ساختار نیروهای مسلح کشورهای اسلامی، کمیته‌های تخصصی فقهی - حقوقی تشکیل شود که متشکل از فقهای مجتهد، حقوقدانان بین‌المللی و متخصصان فناوری اطلاعات باشند. این کمیته‌ها وظیفه دارند:

۱. بررسی مشروعیت فقهی و حقوقی عملیات سایبری پیشنهادی

۲. ارائه راهنماهای عملیاتی مبتنی بر اصول فقهی

۳. نظارت بر رعایت موازین شرعی در عملیات

۴. پاسخگویی به سؤالات فقهی نیروهای عملیاتی

۵. تدوین و به‌روزرسانی فقه دفاعی نوین

۸. نتیجه

این پژوهش نشان داد که اصول بنیادین فقه دفاعی اسلامی، با وجود شکل‌گیری در دوران جنگ‌های کلاسیک، قابلیت انطباق با منازعات نوین سایبری و هوشمند را دارند. اصول تمیز، تناسب، ضرورت و نهی از فساد فی‌الارض، چارچوب محکمی برای ارزیابی مشروعیت عملیات سایبری دفاعی فراهم می‌کنند.

یافته‌های اصلی پژوهش عبارتند از:

۱. **قابلیت انطباق اصول فقهی:** اصول فقه دفاعی با اجتهاد نوین و تفسیر دقیق مفاهیم، قابل اعمال در فضای سایبری هستند. اگرچه ابزار و فضای جنگ تغییر کرده، اما اصول اخلاقی و شرعی حاکم بر جنگ ثابت مانده‌اند.

۲. **معیارهای مشروعیت حملات سایبری:** حملات سایبری دفاعی زمانی مشروع هستند که: (الف) در پاسخ به تجاوز واقعی یا قریب‌الوقوع باشند، (ب) انتساب قابل اعتماد وجود داشته باشد، (ج) راه‌حل‌های مسالمت‌آمیز جواب نداده باشند، (د) متناسب با تجاوز باشند، (ه) به حداقل زور لازم محدود شوند، و (و) اصل تمیز را رعایت کنند.

۳. حفاظت از غیرنظامیان: حفاظت از غیرنظامیان در منازعات سایبری، اولویت مطلق است. حمله به زیرساخت‌های صرفاً غیرنظامی حرام است و در مورد زیرساخت‌های دوگانه، باید آسیب جانبی به غیرنظامیان در مقابل مزیت نظامی سنجیده شود.
۴. چالش سامانه‌های هوشمند: استفاده از سامانه‌های کاملاً خودمختار که قادر به رعایت قابل اعتماد اصل تمیز نیستند، از منظر فقهی مشکل‌ساز است. مسئولیت شرعی و حقوقی این سامانه‌ها بر عهده طراحان، برنامه‌نویسان و فرماندهان است.
۵. نیاز به اجتهاد نوین: با وجود قابلیت انطباق اصول بنیادین، مفاهیم کلاسیک فقه دفاعی مانند «هدف نظامی»، «غیرنظامی»، «خسارت جانبی» و «تناسب» نیازمند بازتعریف و تفسیر نوین در بستر فضای سایبری هستند.
۶. همگرایی فقه و حقوق بین‌الملل: اصول فقه دفاعی اسلامی و حقوق بین‌الملل بشردوستانه، همگرایی قابل توجهی دارند. این همگرایی می‌تواند زمینه‌ساز مشارکت فعال فقه اسلامی در شکل‌دهی هنجارهای بین‌المللی جنگ سایبری باشد.

کتابنامه

متون دینی

قرآن کریم

نهج البلاغه

صحیح بخاری

صحیح مسلم

الكافی (كلینی)

وسائل الشيعة (حر عاملی)

منابع فارسی

آیت الله جوادی آملی، عبدالله. (۱۳۹۲). *فقه و حقوق در جهان معاصر*. قم: انتشارات اسراء.

آیت الله خامنه‌ای، سیدعلی. (۱۳۹۵). *احکام دفاع و جهاد*. تهران: دفتر حفظ و نشر آثار

حضرت آیت الله العظمی خامنه‌ای.

آیت الله سیستانی، سیدعلی. (۱۳۹۴). *منهاج الصالحین* (جلد ۱). قم: دفتر آیت الله سیستانی.

ابن قدامه، موفق الدین. (۱۳۸۸ق.). *المغنی* (جلد ۱۰). بیروت: دار الفکر.

ابن هشام، عبدالملک. (۱۳۷۵ق.). *السيرة النبوية* (جلد ۳). بیروت: دار الکتب العلمیة.

امام خمینی، روح الله. (۱۴۲۱ق.). *تحریر الوسیلة* (جلد ۱). قم: مؤسسه تنظیم و نشر آثار امام خمینی.

رضایی، محمد؛ احمدی، علی؛ و حسینی، حسن. (۱۳۹۹). جنگ سایبری و چالش‌های فقهی آن.

فصلنامه مطالعات فقه و حقوق اسلامی، ۱۲(۴۵)، ۷۸-۱۰۲.

سیوطی، جلال الدین. (۱۴۱۱ق.). *الأشباه و النظائر* (جلد ۱). بیروت: دار الکتب العلمیة.

شهید اول، محمد بن مکی. (۱۴۱۰ق.). *اللمعة الدمشقية* (جلد ۲). قم: دار الفکر.

شهید ثانی، زین الدین بن علی. (۱۴۱۳ق.). *مسالك الأفهام* (جلد ۲). قم: مؤسسة المعارف الإسلامية.

شهید مطهری، مرتضی. (۱۳۶۸). *جهاد*. تهران: انتشارات صدرا.

طباطبایی، محمدحسین. (۱۳۷۴). *المیزان فی تفسیر القرآن* (جلدهای ۲، ۵، ۱۴). قم: دفتر

انتشارات اسلامی.

شیخ طوسی، محمد بن حسن. (۱۳۸۷ق.). *المبسوط فی فقه الإمامیة*. تهران: المكتبة المرتضوية.

- مکارم شیرازی، ناصر. (۱۳۷۴). *تفسیر نمونه* (جلد ۱۴). تهران: دار الکتب الإسلامية.
- _____ (۱۳۹۲). *فقه دفاع و جهاد*. قم: مدرسه امام علی بن ابی طالب.
- محقق داماد، سیدمصطفی. (۱۳۹۳). *حقوق بین الملل اسلامی*. تهران: مرکز نشر علوم اسلامی.
- نجفی، محمدحسن. (۱۴۰۴ق.). *جواهر الکلام فی شرح شرائع الإسلام* (جلدهای ۲۱، ۳۷، ۴۰). بیروت: دار إحياء التراث العربی.

منابع عربی

- ابن قدامه، موفق الدین. (۱۳۸۸ق.). *المغنی* (جلد ۱۰). بیروت: دار الفکر.
- الماوردی، علی بن محمد. (۱۴۱۹ق.). *الأحكام السلطانية*. بیروت: دار الکتب العلمیة.
- الغزالی، محمد بن محمد. (۱۴۱۳ق.). *إحياء علوم الدين* (جلد ۲). بیروت: دار المعرفة.
- الصدر، محمد باقر. (۱۴۰۳ق.). *اقتصادنا*. بیروت: دار التعارف للمطبوعات.

منابع انگلیسی

- Arkin, R. C. (2009). *Governing lethal behavior in autonomous robots*. Boca Raton, FL: CRC Press.
- Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. New York, NY: HarperCollins.
- Henckaerts, J.-M., & Doswald-Beck, L. (2005). *Customary international humanitarian law* (Vol. 1). Cambridge: Cambridge University Press.
- Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3), 49-51. <https://doi.org/10.1109/MSP.2011.67>
- Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, CA: RAND Corporation.
- Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1-2), 4-37. <https://doi.org/10.1080/01402390.2014.977382>
- Sardar, Z. (2010). Welcome to postnormal times. *Futures*, 42(5), 435-444. <https://doi.org/10.1016/j.futures.2009.11.028>
- Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge: Cambridge University Press.
- Sharkey, N. (2012). The evitability of autonomous robot warfare. *International Review of the Red Cross*, 94(886), 787-799. <https://doi.org/10.1017/S1816383112000732>
- Singer, P. W. (2009). *Wired for war: The robotics revolution and conflict in the 21st century*. New York, NY: Penguin Press.
- Walzer, M. (2015). *Just and unjust wars: A moral argument with historical illustrations* (5th ed.). New York, NY: Basic Books.

