University of Zanjan
The Journal of
Ethical Reflections
Original Research
Vol.2, Issue 3, Autumn, 2021, pp. 49-76.
Online ISSN: 2717-1159 / Print ISSN: 2676-4810
http://jer.znu.ac.ir

Application of the Just War Theory in Cyberwarfare and Ethical Solutions to the Use of Cyber Weapons

Zeinab Alebouye,[1] Alireza Alebouyeh [2]

Abstract

Cyberspace has provided new possibilities for the exchange of information that can be considered a key element for the development of life. On the other hand, it has become a new weapon and a suitable platform for war. Some argue that one of the features of cyberwarfare is that it can be more ethical than traditional warfare because it causes less damage and the resulting damage is easily compensable. In recent years, due to the expansion of the use of cyber weapons, new and serious ethical issues have arisen in this area. The ethics of using cyber weapons and whether the theory of just war also applies to cyberwarfare is a serious question. In this article, in addition to examining the application of the just war theory in cyberwarfare, strategies for the ethical use of cyber weapons are addressed. Such solutions include: using the just war theory in accordance with cyber warfare, designing reversible attacks, designing and using controllable cyber weapons, training cyber army experts, non-arbitrary participation of civilians in cyberwarfare, mobilization of people, teaching ethical issues of cyberwarfare, and moral education from childhood. According to studies, the just war theory is necessary for cyberwarfare, but it is not enough, and governments and the international community should seek to establish ethical and legal principles specific to cyberwarfare.

Keywords: IT Ethics, War Ethics, Cyberspace, Cyber Warfare, Cyber Weapons, Just War.

Received: 03 Jan. 2022 | **Accepted**: 24 Jan. 2022 | **Published**: 19 Feb. 2022

1. Corresponding Author, Ph.D Student at IT (Electronic Commerce), Qom University, z.alebouyeh@gmail.com

2. Assistant Professor, Islamic Sciences and Culture Academy, a.alebouyeh@isca.ac.ir

دانشگاه زنجان
فصلنامه تأملات اخلاقی
دورهٔ دوم، شمارهٔ سوم، پاییز ۱۴۰۰، صفحات ۴۹-۷۶.
شاپا الکترونیکی: ۱۱۵۹-۲۷۱۷
شاپا چاپی: ۴۸۱۰-۲۶۷۶

مقالهٔ پژوهشی

کاربرد نظریهٔ جنگ عادلانه در جنگ سایبری و راهکارهای اخلاقی استفاده از سلاح‌های سایبری

زینب آل‌بویه،[۱] علیرضا آل‌بویه[۲]

چکیده

فضای سایبری امکانات جدیدی را برای تبادل اطلاعات فراهم کرده است که می‌تواند به عنوان رکنی اصلی برای توسعهٔ زندگی در نظر گرفته شود. از طرف دیگر، همین فضا به منزلهٔ سلاحی جدید و بستری مناسب برای جنگ تبدیل شده است. برخی معتقدند یکی از ویژگی‌های جنگ سایبری این است که نسبت به جنگ‌های سنتی می‌تواند اخلاقی‌تر باشد؛ زیرا آسیب‌های کمتری ایجاد کرده و خسارت‌های ناشی از آن به راحتی قابل جبران است. در سال‌های اخیر به دلیل گسترش استفاده از سلاح‌های سایبری مسائل اخلاقی جدید و مهمی در این حوزه به وجود آمده است. اخلاقی بودن استفاده از سلاح‌های سایبری و اینکه آیا نظریهٔ جنگ عادلانه در مورد جنگ سایبری نیز کاربرد دارد یا نه، یک سؤال جدی است. در این مقاله علاوه بر بررسی کاربرد نظریهٔ جنگ عادلانه در جنگ سایبری، به راهکارهای استفاده اخلاقی از سلاح‌های سایبری پرداخته می‌شود. راه‌کارها عبارتند از: استفاده از نظریهٔ جنگ عادلانه متناسب با جنگ سایبری، طراحی حمله‌های برگشت‌پذیر، طراحی و استفاده از سلاح‌های سایبری قابل کنترل، تربیت نیروهای خبره ارتش سایبری، عدم شرکت خود سرانه غیرنظامیان در جنگ سایبری، تشکیل بسیج مردمی، آموزش مسائل اخلاقی جنگ سایبری و تربیت اخلاقی از کودکی. با توجه به بررسی‌های انجام شده، نظریهٔ جنگ عادلانه برای جنگ سایبری لازم است، اما کافی نیست و دولت‌ها و جوامع بین‌المللی باید به دنبال تدوین اصول اخلاقی و قانونی مخصوص جنگ‌های سایبری باشند.

واژگان کلیدی: اخلاق فناوری اطلاعات، اخلاق جنگ، فضای سایبری، جنگ سایبری، جنگ عادلانه.

تاریخ دریافت: ۱۴۰۰/۱۰/۱۳ | **تاریخ پذیرش**: ۱۴۰۰/۱۱/۰۴ | **تاریخ انتشار**: ۱۴۰۰/۱۱/۳۰

۱. نویسندهٔ مسئول، دانشجوی دکتری فناوری اطلاعات (تجارت الکترونیک)، دانشگاه قم، z.alebouyeh@gmail.com

۲. استادیار پژوهشگاه علوم و فرهنگ اسلامی، a.alebouyeh@isca.ac.ir

مقدمه

رشد روزافزون فناوری اطلاعات و فضای سایبری امکانات وسیع و غیرقابل تصوری را در اختیار کاربران قرار داده است. در کنار قابلیت‌ها و مزایای بی‌شمار فناوری اطلاعات و فضای سایبری، به دلیل ویژگی‌ها و ساختاری که این فضا دارد، تهدیدها و خطرات نیز روز به روز در حال افزایش بوده و این فضا را به سلاحی جدید و بستری مناسب برای جنگ تبدیل کرده و میدان نبرد جدیدی را شکل داده است.

جنگ اطلاعاتی، سلاح‌های سایبری، ارتش سایبری و دفاع سایبری واژگان نسبتاً جدیدی هستند که در سال‌های اخیر به واژه‌نامه اصطلاحات نظامی اضافه شده‌اند. جنگ سایبری جنگی است که در آن از نرم‌افزارها و بسترهایی مانند اینترنت به عنوان سلاح‌هایی برای حمله و آسیب زدن به سیستم‌های رایانه‌ای، پایگاه‌های داده، شبکه‌ها و در بسیاری از موارد زیر ساخت‌های مهم و حیاتی کشورها استفاده می شود. جنگ بدون خسارت همیشه رؤیای طراحان و برنامه‌ریزان ارتش بوده است. به گفته سون تزو[1] بالاترین هنر در جنگ این است که بتوان کشور دشمن را دست نخورده و کامل تصرف کرد. به عقیدهٔ او، یک رهبر مدبّر شرایط را به‌گونه‌ای فراهم می‌کند که در کوتاه‌ترین مدت، با کمترین تلفات انسانی و با حداقل صدمه به دشمن، به پیروزی برسد (Tzu, 2005, p. 46). به اعتقاد برخی، رؤیای پیروزی در جنگ بدون خونریزی و تلفات با جنگ سایبری میسر می‌شود (Rid, 2013, p. viii). در واقع تصور این بود که جنگی را که سون تزو همواره آرزویش را داشت می‌توان در کالبد جنگ سایبری جست‌وجو کرد.

در سال‌های اخیر جنگ سایبری به دلیل هزینه کمتر و عدم وجود خطر حمل و نقل تجهیزات و اعزام سربازان به خاک دشمن، نسبت به اقدامات نظامی متعارف جذاب‌تر شده است و به همین دلیل، امنیت سایبری به عنوان یکی از مؤلفه‌های مهم و جدی برنامه امنیت ملی کشورها مدنظر قرار گرفته است (Evans et-al., 2014, p. 17). در ژوئن ۲۰۰۹ وزیر دفاع آمریکا فرمان ایجاد فرماندهی سایبری ایالات متحده را به عنوان جزئی از سازمان امنیت ملی آمریکا صادر کرد و فرماندهی آن به کیث بی. آلکساندر[2] واگذار شد (US Department of Defense U.S., 2010, p. 1) وجود ژنرال چهار ستاره[3] ارتش آمریکا در فرماندهی سایبری نشان می‌دهد که پنتاگون[4] حساب ویژه‌ای روی جنگ‌های سایبری باز کرده است. در سال‌های اخیر فرماندهی‌های مشابهی هم در روسیه، چین و کشورهای دیگر تشکیل شده است (Clarke et-al., 2012, p. 6).

در سال‌های اخیر به دلیل گسترش استفاده از جنگ‌ها و سلاح‌های سایبری مسائل اخلاقی جدید و جدی‌ای در این حوزه به وجود آمده است. به دلیل گسترش استفاده از جنگ‌های سایبری و چالش‌های منحصر به فردی که این جنگ‌ها در حوزهٔ

1 . Sun Tzu
2 . Keith B. Alexander
3 . https://en.wikipedia.org/wiki/Keith_B._Alexander
4 . Pentagon

اخلاق جنگ به‌وجود آورده‌اند، بررسی آن به لحاظ اخلاقی ضروری به نظر می‌رسد. این پرسش جدی مطرح است که آیا جنگ سایبری با جنگ سنتی به لحاظ اخلاقی تفاوت جدی دارد و آیا نظریهٔ جنگ عادلانه در مورد جنگ سایبری نیز کاربرد دارد یا نه؟ در این مقاله علاوه بر بررسی کاربرد نظریه جنگ عادلانه در جنگ سایبری و اثبات اینکه گرچه نظریهٔ جنگ عادلانه لازم است، ولی کافی نیست، به راه‌کارهای استفاده اخلاقی از سلاح‌های سایبری پرداخته می‌شود.

۱. جنگ سایبری

ریچارد کلارکز، متخصص امنیت سایبری، تعریف جامعی از جنگ سایبری ارائه داده است: «جنگ سایبری مجموعهٔ اقداماتی است که توسط ملت یا دولتی صورت می‌گیرد تا به رایانه‌ها و شبکه‌های ملت دیگری نفوذ کند؛ به آنها آسیب رساند یا در عملکرد آنها اختلال ایجاد کند» (Clarke et-al., 2012, p. 11). هدف جنگ‌های سایبری همانند جنگ‌های سنتی می‌تواند مواضع نظامی، صنعتی و حتی غیرنظامی باشد. از جنگ سایبری نیز باید همانند جنگ سنتی ترسید؛ زیرا سطح خشونت آن ممکن است به شدت افزایش پیدا کند و صدمات فیزیکی و جانی جبران‌ناپذیری را موجب شود؛ برای مثال، حمله‌ای سایبری که سیستم کنترل هوایی نظامی را در دست می‌گیرد و منجر به سقوط هواپیما می‌شود (Taddeo, 2012, p. 211)، طبیعتاً موجب تخریب فیزیکی و حتی مرگ غیرنظامیان خواهد شد. جنگ سایبری به همان میزان که می‌تواند موجب تخریب دارایی‌های غیرفیزیکی از جمله اطلاعات گردد، به همان میزان هم می‌تواند آسیب‌های فیزیکی به دنبال داشته باشد. پس اهداف جنگ‌های سایبری می‌تواند هر دو زمینه فیزیکی و غیرفیزیکی را شامل شود. در واقع، جنگ سایبری نشان می‌دهد که فضای جدیدی برای جنگ وجود دارد که دارایی‌های فیزیکی و غیرفیزیکی به اندازه هم ارزشمند هستند؛ فضایی که جنگ در آن می‌تواند هم خشونت‌آمیز باشد و هم غیرخشونت‌آمیز؛ و میزان خسارت‌ها و خشونت‌ها بستگی به اهداف مورد نظر و نوع سلاح‌های سایبری‌ای دارد که در جنگ به کار برده می‌شوند.

۲. سلاح‌های سایبری

در ژوئن سال ۲۰۱۰ کرمی رایانه‌ای با نام استاکس‌نت، با منشأ ناشناخته، در سراسر جهان منتشر شد. هزاران رایانه در کشورهای سراسر دنیا از جمله ایران، هند و ایالات متحده آمریکا آلوده به این کرم رایانه‌ای شدند(Evans et-al., 2014, p. 17; Farwell, 2011, p.1). به دلیل اینکه حدود ۶۰ درصد از قربانیان این کرم رایانه‌ای در ایران بود، بسیاری از متخصصان استنباط کردند که یا ایران دفاع سایبری ضعیفی دارد که این امر موجب آسیب‌پذیری بیشتر سیستم‌های آن شده است یا اینکه کرم از ابتدا سیستم‌های ایران را هدف قرار داده است. البته بعدها در برخی گزارشات ذکر شد که هدف اصلی این کرم تجهیزات هسته‌ای ایران بوده است. (Singer, 2015, p. 3)

استاکس‌نت در واقع سلاحی جدید بود که با ابزارهای سایبری موجب صدمات فیزیکی می شد (Singer, 2015, p. 7). استاکس‌نت بهترین مثال از بدافزاری است که برای اولین بار به عنوان سلاح علیه کشوری مورد استفاده قرار گرفت (Knopová et-al., 2014, p. 5). به گفته سردار جلالی، رئیس پدافند غیرعامل ایران، «استاکس‌نت یک ویروس یا کرم نیست؛ بلکه سلاحی سایبری است و جزء اولین سلاح‌های سایبری‌ای محسوب می شود که به صورت رسمی علیه ایران به کار گرفته شد» (به گزارش فارس‌نیوز).[1]

در حال حاضر هیچ اجماع بین المللی در خصوص تعریف سلاح‌های سایبری وجود ندارد. به طور کلی، سلاح سایبری کدی رایانه‌ای است که برای آسیب رساندن فیزیکی به ساختارها، عملکرد سیستم‌ها و موجودات زنده به کاربرده می شود (Rid et-al., 2012, p.2). در واقع، سلاح‌های سایبری نرم‌افزارهایی هستند که برای حمله به نرم‌افزارهای دیگر و یا داده‌های ذخیره شده در سیستم‌های رایانه‌ای استفاده می‌شوند (Evans et-al. , 2014, p. 17; Rowe, 2010, p. 2; Mele, 2013, p. 9). برای نمونه نرم‌افزاری که ترافیک شبکه‌ای غیر ضروری تولید کرده و به سمت وب سرور بانکی ارسال می‌کند تا بانک نتواند به کاربران خود خدمات ارائه دهد، سلاحی سایبری به شمار می‌آید و یا نرم‌افزاری که برای کپی‌کردن اطلاعات محرمانه کاربر بدون اطلاع و اجازه وی طراحی شده است نیز سلاحی سایبری است؛ زیرا محرمانگی داده‌های سیستم را نقض می‌کند (Lorentset-al., 2010, p.139). آسیب‌های سلاح‌های سایبری فقط به فضای سایبری محدود نمی‌شود و می‌تواند صدمات جبران‌ناپذیری را در فضای واقعی و بر روی موجودات زنده بر جای گذارد؛ برای نمونه، بدافزاری که به سیستم رایانه‌ای تصفیه آب آشامیدنی شهری نفوذ کرده و میزان کلر وارد شده به آب را دستکاری می‌کند، سلاحی سایبری است که با تغییر داده‌های دیجیتال موجب آسیب دیدن انسان‌ها می‌گردد. همانند سلاح‌های متداول، سلاح‌های سایبری نیز می‌توانند علیه اهداف متنوع و در شرایط متنوع و با محدوده وسیعی از تخریب و تلفات جانی به کاربرده شوند.

۳. ویژگی‌های جنگ‌ها و سلاح‌های سایبری

جنگ‌های سایبری در مقایسه با جنگ‌های سنتی لزوماً به کشته شدن انسان‌ها منجر نمی شوند و حالت‌های نرم و بدون خونریزی آنها می‌توانند به عنوان راه‌کاری برای اجتناب از صدمات جانی جنگ‌های سنتی مناسب باشند؛ اما جنگ‌های سایبری در مقایسه با جنگ‌های سنتی، ویژگی‌های منحصر به فردی دارند که موجب چالش‌های جدیدی در خصوص اخلاق نبرد شده‌اند؛ از جمله این ویژگی‌ها می‌توان به موارد زیر اشاره کرد:

۳-۱. انتقال سریع، آسان و کم هزینه سلاح‌ها

انتقال سلاح‌های سایبری به سیستم‌های هدف راحت، سریع و کم هزینه است؛ زیرا این سلاح‌ها برنامه‌هایی هستند که به

1 . http://www.farsnews.com/printable.php?nn=13900726000534، ۹۵/۹/۲۲

سادگی کپی و منتقل می شوند و زمانی که حمله‌کننده به هدف خود بر سد، می‌تواند به راحتی آنها را از سیستم قربانی پاک کند. این ویژگی سبب می شود که به‌طور قابل توجهی نظارت بر انتقال سلاح‌های سایبری نسبت به سلاح‌های هسته‌ای، شیمیایی و بیولوژیکی سخت‌تر باشد.

۳-۲. مخفی بودن تحرکات و انتقال تجهیزات

در جنگ‌های سنتی در بسیاری از مواقع تحرکات دشمن و انتقال تجهیزات و نیروهای نظامی نشان می‌دهد که به زودی جنگی در حال وقوع است و کشور قربانی می‌داند که قرار است مورد حمله قرارگیرد؛ پس می‌تواند تا حدودی خود را آماده نبرد کند؛ اما در جنگ سایبری شرایط متفاوت است و قربانی کاملاً با حملات غافلگیر می‌شود؛ زیرا انتقال سلاح‌ها به صورت مخفیانه و بدون اثر روی دنیای واقعی صورت گرفته و نیاز به جابه‌جایی نیروهای نظامی نیز نیست.

۳-۳. امکان انجام حملات غیرفعال

حمله سایبری می‌تواند به صورت غیرفعال انجام شود؛ یعنی هیچ اثری روی سیستم قربانی باقی نگذارد. در چنین حملاتی چون اختلالی در شبکه و سیستم ایجاد نمی شود، قربانی حتی ممکن است متوجه نشود که مورد حمله قرار گرفته است. نمونه‌ای از این حملات حمله شنود است که منجر به سرقت اطلاعات محرمانه سیستم‌ها می شود؛ اما در چنین حمله‌ای آسیبی به اطلاعات محرمانه وارد نمی‌شود؛ بلکه فقط یک نسخه از این اطلاعات دست دشمن می‌افتد.

۳-۴. قابلیت فعال‌سازی و کنترل سلاح‌ها از راه دور و نزدیک

از دیگر ویژگی‌های این سلاح‌ها این است که هم می‌توان آنها را از راه دور و از طریق اینترنت فعال و کنترل کرد و هم می‌توان به صورت داخلی و با دسترسی فیزیکی به سیستم‌ها از آنها استفاده کرد (Rowe, 2010a, pp. 3-4)؛ برای مثال، حمله‌کننده می‌تواند از طریق اینترنت به سیستم قربانی دسترسی پیدا کند و عملیات خود را از راه دور انجام دهد یا در حالتی حمله‌کننده می‌تواند با دسترسی فیزیکی به شبکه سازمان یا با اتصال یک حافظه جانبی آلوده به رایانه‌ها، به سرورهای آن حمله کند و صدمات جبران‌ناپذیری را موجب شود.

۳-۵. دشوار بودن ارزیابی صدمات

تخمین میزان صدمات ناشی از حملات سایبری بسیار مشکل است؛ به دلیل اینکه بسیاری از صدمات درون داده‌ها مخفی است. یکی از مشکلات جنگ سایبری این است که تعیین اینکه کسی تحت حمله سایبری قرار گرفته است یا نه دشوار است؛ زیرا حملات سایبری ممکن است مشهود و علنی نباشند و تا مدت‌ها قربانی متوجه نشود و طبیعتاً تا زمانی که قربانی متوجه حمله به سیستم خود نشود، تلاشی هم برای از خنثی کردن آن نخواهد کرد. به این ترتیب، آسیب‌های بسیار زیاد و پنهانی در طول زمان به سیستم و داده‌های آن وارد خواهد شد.

۶-۳. دشوار بودن مشخص کردن منبع حمله

مشخص کردن منبع حمله‌ای که با سلاح سایبری صورت گرفته است، بسیار دشوار است و دفاع کننده برای اینکه بتواند عکس‌العمل و پاسخی درست به حملات دهد، باید کشور حمله کننده را تا حدودی بشناسد (Evans et-al., 2014, p. 18)؛ زیرا در بسیاری از موارد، حمله‌کننده در فضای سایبری می‌تواند اقداماتی انجام دهد که هویت خود را مخفی و رد پای خود را نیز از سیستم‌ها پاک کند؛ در صورتی که در جنگ‌های سنتی در اغلب موارد قربانی متوجه می‌شود که از کجای دنیا و توسط چه کسانی مورد حمله قرار گرفته است؛ بنابراین، به راحتی می‌تواند عکس‌العمل مناسبی نشان دهد. با این حال، در بسیاری از موارد ردیابی حملات سایبری روی سیستم قربانی و شبکه‌ها دشوار اما امکان‌پذیر است.

۷-۳. کاهش آستانه درگیری نظامی میان حکومت‌ها

سلاح‌های سایبری آستانه درگیری نظامی و جنگ‌های سنتی میان حکومت‌ها را به شدت کاهش می‌دهند. بسیاری از دولت‌ها به دلیل آسیب‌های کمتر سلاح‌های سایبری و همچنین هزینه‌های مالی و جانی کمتر این سلاح‌ها، در مواقع تنش ترجیح می‌دهند به جای استفاده از سلاح‌های سنتی تا جایی که امکان دارد و آنها را به اهداف سیاسی خود نزدیک می‌کند، از سلاح‌های سایبری استفاده کنند و درگیر جنگ نظامی نشوند. به‌واسطه استفادهٔ مکرر و بی‌رویه از این سلاح‌ها، به‌طور بالقوه حالت‌های خطرناک‌تری از درگیری‌های سایبری به‌وجود می‌آید (Evans et-al., 2014, p. 18). بنابراین، به دلیل اینکه اقدام به جنگ سایبری آسان‌تر، کم هزینه‌تر و به ظاهر بی‌خطرتر است، به‌مرور زمان، ممکن است تمایل دولت‌ها به جنگ سایبری بیشتر شود و تعداد جنگ‌ها از نظر کمّی افزایش پیدا کند و به تبع آن، از نظر کیفی نیز آسیب‌های وارده به شدت گسترش یابد.

۸-۳. افزایش احتمال درگیرشدن غیرنظامیان و آسیب رسیدن به آنها

استفاده از سلاح های سایبری احتمال اینکه افراد غیرنظامی هدف این سلاح ها قرار گیرد و قربانی حملات به زیرساخت‌های مشترک شوند، افزایش می‌دهد. مشکل اینجاست که تمایز میان سیستم‌های اطلاعاتی نظامی و غیرنظامی خیلی مشخص نیست و بعضاً بسیار دشوار است؛ به دلیل اینکه استفاده نظامی از زیرساخت‌های غیرنظامی همه‌جا فراگیر است (Evans et-al., 2014, p. 18). در جنگ‌های سنتی مرز میان نظامیان و غیرنظامیان کاملاً مشخص است و اگر هدف حمله‌کننده فقط مناطق غیرمسکونی و حمله و آسیب زدن به نظامیان باشد، تا حد زیادی دست‌یابی به آن ممکن است؛ اما در جنگ‌های سایبری زمانی که به سیستم‌های اطلاعاتی و زیرساختی آسیب وارد می شود، حتی اگر هدف حمله‌کننده صرفاً صدمه به سیستم‌های نظامی باشد، باز هم نمی‌توان تضمین کرد که آسیبی جدی به غیرنظامیان وارد نشود؛ زیرا بسیاری از زیرساخت‌ها و سیستم‌های اطلاعاتی مشترک بوده و آسیب به سیستمی ظاهراً نظامی ممکن است

اثرات جانبی برگشت‌ناپذیری بر روی سیستم‌های غیرنظامی بگذارد.

۹-۳. حمله آسان و کم هزینه در برابر دفاع دشوار و هزینه‌بر

یکی دیگر از ویژگی‌های جنگ سایبری این است که همانند جنگ‌های رایج، پیشگیری و دفاع در برابر چنین حملاتی بسیار هزینه‌بر است و امکان شکست در آن وجود دارد. در حالی که حمله با سلاح سایبری به دلایل مختلفی ارزان‌تر و آسان‌تر است (Dipert, 2010, p. 385)، ولی دفاع سایبری بسیار پرهزینه است. حمله در فضای سایبری با سرعت بسیار زیادی صورت می‌گیرد و سیستم دفاعی را تحت فشار زیادی قرار می‌دهد. مهاجم تنها یک بار نیازمند موفقیت در حمله است، در حالی که سیستم امنیتی در طول زمان باید همیشه به درستی و به‌طور موفقیت‌آمیزی عمل کند. همچنین، پیچیدگی فضای سایبری باعث افزایش هزینه‌های دفاعی می‌شود. دیگر اینکه، محل جغرافیایی در فضای سایبری معنایی ندارد و حملات از هر نقطه‌ای از دنیا می‌توانند صورت گیرند (Rid et-al., 2012, p. 25)؛ بنابراین، محافظت از مرزهای جغرافیایی زمینی، هوایی و دریایی برای دفاع دیگر معنایی ندارد؛ زیرا سیستم‌ها از هر نقطه‌ای از دنیا ممکن است مورد حمله قرار گیرند و طبیعتاً دفاع در چنین شرایطی بسیار دشوار و هزینه‌بر خواهد بود. البته ذکر این مطلب به این معنا نیست که همیشه دفاع سایبری پر هزینه‌تر از حمله سایبری است؛ بلکه هدف از بیان این مطالب این است که یکی از جذابیت‌های حملات سایبری و تمایل به انجام این حملات این است که خیلی از انواع این حملات می‌تواند هزینه کمتری نسبت به حملات سنتی داشته باشد. باید به این نکته نیز توجه کرد که هزینه‌های حمله و دفاع سایبری در نهایت، بر اساس پیچیدگی اهداف حمله و دفاع شکل می‌گیرد و گاهی ممکن است هزینه حمله سایبری هم بسته به نوع حمله زیاد باشد؛ برای مثال، دستیابی به حملاتی که اثرات مخرب فیزیکی بر جای می‌گذارند، بسیار پرهزینه است همان‌طور که تجزیه و تحلیل استاکس‌نت نشان داده است که آسیب‌رساندن به زیرساخت‌های فیزیکی بسیار پرهزینه‌تر از نفوذ ساده به شبکه‌های اطلاعاتی است (Slayton, 2017, p. 2).

۴. نظریهٔ جنگ عادلانه[1]

در طول دو دهه گذشته، ثابت شده است که فناوری اطلاعات و ارتباطات می‌تواند ابزاری مفید و مناسب برای ایجاد نوع جدیدی از جنگ باشد. نگرانی از افزایش تمایل به جنگ سایبری منحصر به ارتش و سازمان‌های نظامی نیست، بلکه نگرانی عالمان اخلاق و سیاست‌گذاران نیز هست (Taddeo, 2012a, pp. 209-210). اعلان و استفاده از جنگ سایبری نیاز به قوانین اخلاقی و بین‌المللی جدی‌ای دارد که عدالت آن را تضمین کند. در مجامع بین‌المللی هرگاه صحبت از مشروعیت و عدالت در جنگ مطرح می‌شود، پای «نظریهٔ جنگ عادلانه» به میان می‌آید. به همین دلیل برای

1 . Just war theory

بررسی اخلاقی بودن جنگ‌های سایبری، در این بخش، به بررسی این نظریه پرداخته می‌شود؛ هر چند با توجه به ویژگی‌های منحصر به فردی که جنگ سایبری دارد، برای تحلیل اخلاقی آن، نظریهٔ جنگ عادلانه لازم است، اما کافی نیست؛ به طور مثال، شرکت در جنگ سایبری برخلاف جنگ سنتی می‌تواند خودسرانه انجام شود؛ زیرا برای شرکت در جنگ نیاز به حضور فیزیکی و تجهیزات نظامی نیست و این شرکت خودسرانه در جنگ می‌تواند تبعات جبران‌ناپذیری را در پی داشته باشد؛ پس باید تمهیداتی اندیشیده شود که از شرکت خودسرانه افراد در جنگ سایبری جلوگیری شود. بخش اصلی قوانین و هنجارهای بین‌المللی، برای مثال کنوانسیون‌های ژنو و لاحه در ابتدا از نظریهٔ جنگ عادلانه گرفته شده‌اند و در طی سال‌ها و بر حسب شرایط مختلف به تکامل رسیده‌اند (Dower, 2009, p. 81). بخشی از نظریهٔ جنگ عادلانه در خصوص حق جنگ است که در این قسمت به بررسی آن خواهیم پرداخت.

۱-۴. حق جنگ (عدالت در آغاز کردن جنگ)[1]

توسل به جنگ تحت چه شرایطی به لحاظ اخلاقی درست است؟ یک کشور تحت چه شرایطی می‌تواند جنگی را علیه کشوری دیگر آغاز کند؟ نظریهٔ جنگ عادلانه در بخش «حق جنگ» به سؤالاتی از این قبیل پاسخ می‌دهد و مشخص می‌کند که شروع جنگ تحت چه شرایطی می‌تواند اخلاقی و درست باشد. در این بخش شش معیار برای عادلانه بودن آغاز جنگ ارائه شده است (Lazar, 2020).

۱) علت عادلانه: شروع جنگ باید علتی عادلانه داشته باشد. در خصوص اینکه چه چیزی علت عادلانه را شکل می دهد اختلاف نظر است. دفاع از خود، دفاع از دیگران در برابر حملات تهاجمی و حفاظت از مردم بی‌گناه در مقابل رژیم تهاجمی نمونه‌هایی از علت‌های عادلانه برای آغاز جنگ هستند. قابل ذکر است که تنها دولت مشروع می‌تواند جنگی با علتی عادلانه را شروع کند و برای مشروع بودن، دولت باید از سوی شهروندان خود و دیگر کشورها به رسمیت شناخته شده باشد (Dower, 2009, p. 82 ; Department of Defense, 2015, p. 40). نکته اخیر که «تنها دولت مشروع می‌تواند جنگی با علتی عادلانه را آغاز کند» به صورت مطلق درست به نظر نمی‌رسد؛ چون از جمله موارد علت عادلانه آغاز کردن جنگ، دفاع از خود و دفاع از دیگران در برابر حملات تهاجمی و حفاظت از مردم بی‌گناه در مقابل رژیم تهاجمی نام برده شده است. در چنین مواردی نمی‌توان به‌طور مطلق حکم کرد که کسی حق دفاع در مقابل رژیم متجاوز را ندارد، مگر اینکه دولت مشروع آغاز جنگ دفاعی را اعلان کند؛ چون بر این اساس، دولتی که مشروعیت ندارد، حق اعلان آغاز جنگ دفاعی را ندارد. چنین حکمی درست به نظر نمی‌رسد و شهروندان نیز در چنین مواردی گرچه حکومت مرکزی را به رسمیت نشناسند، ولی در مقابلِ مهاجمان با حکومت در دفاع از کشور شان همکاری و آن را حق اخلاقی خود تلقی می‌کنند. در نتیجه، دولت نامشروع در این کارش به لحاظ اخلاقی درست عمل می‌کند. همچنین، در مواردی

1. jus ad bellum (right to war)

که به مرزهای کشوری تهاجم صورت می‌گیرد، مرزنشینان برای دفاع از جان و مال و نیز خاک وطن خود نیازی به دستور دولت مرکزی ندارند و خود به‌لحاظ اخلاقی موظف به دفاع هستند. نه تنها دلیل عقلی بر این شرط دلالت دارد، بلکه آیات قرآن نیز مؤید آن است از جمله تعدی در مقابل تعدی دشمن (بقره/ ۱۹۴)، جنگیدن در مقابل کسانی که با شما می‌جنگند (بقره/ ۱۹۰) و رخصت به جهاد در مقابل کسانی که جنگ را تحمیل کرده اند (حج/ ۳۹-۴۰)

۲) نیت صواب: شروع جنگ باید با نیت صواب باشد. نیت دولت‌ها برای جنگیدن فقط باید علت عادلانه باشد. تنها داشتن علت عادلانه برای شروع جنگ کافی نیست؛ بلکه انگیزهٔ واقعی توسل به جنگ نیز باید از نظر اخلاقی مناسب باشد. انگیزه‌های پنهان، مانند: کسب قدرت، اشغال اراضی، به دست آوردن منافع مادی، انتقام و یا نفرت قومی از جمله نیت‌های ناصوابی هستند که عدالت جنگ را با چالش مواجه می‌کنند (Department of Defense, 2015, p. 40; Lacewing, 2010, p.1; Dower, 2009, p. 82) و در مقابل، ورود در جنگ در کشور دیگری که ظالمانه به آنها تهاجم شده است و آنها نیز یاری طلبیده‌اند، با نیت کمک به آنان در مقابل مهاجمان، از جمله نیت‌های صواب تلقی می شود. نیت صواب در آموزه های اسلامی امر روشنی است و در آیات قرآن نیز معمولاً هر گاه سخن از جهاد رفته است مقید به در راه خدا بودن شده است؛ از جمله در بقره/۱۹۰ و نساء/۷۶. همچنین، روایات بسیاری در این زمینه نقل شده است از جمله سخن مشهور رسول خدا صلی الله علیه وآله که فرمود: «نیةُ المُؤمنِ خیرٌ مِن عَمَلِهِ» (مجلسی، ۱۴۰۳، ج ۶۷، ص. ۲۰۶)

۳) مرجع ذی‌صلاح و اعلان عمومی: مراجع ذی‌صلاح تصمیم‌گیرندگان مشروع حکومت‌ها هستند که می‌توانند شامل: سران دولت‌ها، حاکمان، پادشاهان، روسای جمهور، نخست‌وزیران، نهادهای قانون‌گذار و غیره باشند. تصمیم آغاز جنگ باید توسط مراجع ذی‌صلاح اتخاذ شود و با اعلان عمومی همراه باشد (Department of Defense, 2015, p. 40؛ Lacewing, 2010, p.1 ؛ Dower, 2009, p. 82). گرچه در دفاع از کشور افراد نباید درنگ کنند و به نظر می‌رسد حکم مرجع ذی صلاح لازم نیست، ولی اگر هر کسی سر خود عمل کند و هیچ گونه سازماندهی میان آنها و نیز هماهنگی با مسئولان مربوطه و حکومت مرکزی شکل نگیرد، نتیجه مطلوب حاصل نخواهد شد و جز هرج و مرج چیزی در پی نخواهد داشت؛ اما در جنگ ابتدایی مسلماً نیاز به مرجع ذی صلاح است و در اسلام جنگ ابتدایی باید به اذن امام معصوم علیه السلام باشد (امام خمینی، ۱۳۹۰، ج ۱، ص ۴۸۲).

٤) گزینه آخر: اعلان جنگ باید آخرین راه حل باشد و پس از به‌کارگیری تمام گزینه‌های قابل قبول برای حل و فصل درگیری اتخاذ شود (Department of Defense, 2015, p. 40؛ Lacewing, 2010, p. 1 ؛ Dower, 2009, p. 83). به دلیل هزینه‌های بسیار سنگین مالی، جانی و روحی و پیامدهای جبران‌ناپذیر جنگ تا جایی که ممکن است باید از شروع جنگ و خونریزی خودداری کرد. اعلان جنگ تنها در صورتی باید صورت گیرد که تمامی راه‌کارهای صلح‌آمیز و غیرنظامی ممکن برای رفع اختلاف، از جمله راه‌های سیاسی، مذاکرات دیپلماتیک، تحریم‌های هدفمند و غیره بسته

شده باشد و تنها راه حل ممکن برای حل تعارض جنگ باشد. مضمون آیه شریفه اگر دشمن تمایل به صلح داشت شما نیز پذیرای آن باشید (انفال/۶۱) شاهد خوبی برای این شرط است.

۵) احتمال موفقیت: اعلان جنگ تنها در صورتی عادلانه است که دولت حمله‌کننده احتمال موفقیت در حل و فصل درگیری را از طریق جنگ پیش‌بینی کند. توسل به خشونت بدون احتمال دستیابی به موفقیت نمی‌تواند عادلانه باشد (Dower, 2009, p. 83 ؛ Lacewing, 2010, p. 1). زمانی که احتمال موفقیت و رسیدن به هدف در جنگ پایین باشد، توسل به جنگ معقول به نظر نمی‌رسد. در چنین شرایطی که دولت حمله‌کننده پیش‌بینی می‌کند که احتمال شکست قوی است، نباید جان انسان‌ها و دارایی‌های آنها را به خطر انداخته و منابع مالی را به هدر دهد.

٦) تناسب هزینه و دست‌آورد: سودی که از طریق جنگ حاصل می‌شود، نسبت به زیان آن بایدبیشتر باشد. در این محاسبه دولت حمله‌کننده نه تنها باید هزینه‌ها و منافع خود را درنظر بگیرد، بلکه باید هزینه‌ها و منافع تمامی کسانی که درگیر این جنگ می‌شوند را نیز به حساب آورد حتی تلفات دشمن خود را (Lacewing, 2010, p. 1 ؛ Dower, 2009, p. 83). معقولیت این شرط نیز روشن است و ضابطه هزینه- فایده را باید در انجام دادن تمامی کارها از جمله جنگ سایبری مدنظر قرار داد.

۲-۴. جنگ سایبری و نظریهٔ جنگ عادلانه

نظریهٔ جنگ عادلانه سال‌ها قبل از به وجود آمدن جنگ‌های سایبری مطرح شده است و به نظر می‌رسد که این نظریه در جنگ‌های سایبری نیز کاربرد دارد؛ زیرا وارد مباحث فنی جنگ نشده و کاری به نوع جنگ و فناوری‌های جنگی ندارد. علاوه بر این، افزودن شروط دیگری نیز امکان‌پذیر است؛ برای مثال، در جنگ‌های سنتی افراد خودسرانه نمی‌توانند وارد جنگ شوند؛ اما در جنگ‌های سایبری چون شرکت در جنگ نیاز به ابزار جنگی خاصی ندارد و فقط از طریق یک دستگاه رایانه و مهارت فنی حمله صورت می‌گیرد، افراد می‌توانند خودسرانه و به راحتی حمله‌های سایبری را نسبت به مواضع دشمن انجام دهند. بنابراین حکومت‌ها اخلاقاً موظف‌اند جلوی حمله خودسرانه شهروندان خود را در حمله‌های سایبری بگیرند.

برخی معتقدند به دلیل اینکه جنگ‌های سایبری با جنگ‌های سنتی متفاوت بوده و لزوماً خشونت‌آمیز و مخرب نیستند، اعمال برخی از اصول نظریهٔ جنگ عادلانه به این نوع جنگ‌ها با مشکلاتی مواجه است که در این راستا سه مسئله مطرح می‌شود: ۱) جنگ به عنوان آخرین راه حل، ۲) سود بیشتر از زیان و ۳) مصونیت غیرنظامیان (Taddeo, 2012a, p. 212).

الف) جنگ به عنوان آخرین راه حل: زمانی که صحبت از جنگ سایبری به میان می‌آید، اصل «جنگ به عنوان آخرین راه حل» تضعیف می‌شود؛ زیرا این نوع جنگ‌ها لزوماً خشونت فیزیکی و خونریزی به همراه ندارند؛ پس در چنین شرایطی ممکن است استفاده از اصل «جنگ به عنوان آخرین راه حل» ضرورت کمتری پیدا کند؛ برای مثال،

حالتی را تصور کنید که روابط دو کشور دچار مشکل شده و این تنش تنها در صورتی برطرف خواهد شد که یکی از این دو کشور تصمیم بگیرد جنگ سایبری را علیه زیرساخت‌های اطلاعاتی کشور دیگر شروع کند. این حمله سایبری می‌تواند طوری طراحی شود که بدون خونریزی بوده و هیچ تلفات جانی نداشته باشد. این حمله همچنین می‌تواند تنش بین دو کشور را برطرف کرده و از امکان وقوع جنگ سنتی در آینده نزدیک جلوگیری کند. بر اساس نظریهٔ جنگ عادلانه استفاده از جنگ به عنوان اولین اقدام در برخورد با دشمن نادرست است؛ اما با شرایط ذکر شده در این مثال، اگر دولت جنگ سایبری را آغاز نکند، به احتمال زیاد در آینده مجبور به شرکت در جنگی خونین خواهد شد. از طرف دیگر، اگر دولت اجازهٔ شروع جنگ سایبری را بدهد، اصل «جنگ به عنوان آخرین راه حل» را نقض کرده و مرتکب عملی غیراخلاقی شده است و احتمالاً ممکن است توسط قوانین بین‌المللی تحریم شود (Taddeo, 2012a, p. 212).

اما به نظر می رسد این سخن درست نیست، چون با اقدام به جنگ سایبری نمی‌توان پیامدهای احتمالی آن را به دقت محاسبه کرد. چه بسا چنین اقداماتی نتایجی بسیار زیان‌بار در پی داشته باشد. نباید با تصور اینکه برخی از انواع جنگ‌های سایبری صدمات فیزیکی و جانی به دنبال ندارند، به راحتی به عنوان گزینه مناسب برای حل اختلافات سیاسی مدنظر قرار گیرد؛ زیرا این‌گونه حملات ممکن است در شرایطی منجر به ضد حمله با سلاح‌های واقعی گردد و نهایتاً جنگی سنتی را رقم بزند؛ زیرا برخی از کشورها حمله به زیرساخت‌های حیاتی و حساس خود را به منزله حمله به خاک خود تلقی می‌کنند و برای دفاع از مرزهای سایبری کشور اقدام به مقابله می‌کنند. بنابراین، در هر تنشی که بین دولت‌ها رخ می‌دهد، نباید بلافاصله جنگ سایبری را آغاز کرد. حرکت به سمت جنگ سایبری باید در صورتی انجام شود که مذاکرات و گفتگوهای سیاسی و بین‌المللی برای رفع تنش جواب نداده باشد.

ب) سود بیشتر نسبت به زیان: طبق چنین اصلی، اعلان جنگ توسط دولت تنها زمانی توجیه‌پذیر است که سود حاصل از آن بیشتر از زیان آن باشد. این تعادل در مورد جنگ‌های سنتی به راحتی قابل ارزیابی است؛ زیرا در این جنگ‌ها زیان عمدتاً به صورت تلفات و خسارت‌های فیزیکی و جانی است؛ اما محاسبه سود و زیان در خصوص جنگ سایبری به این راحتی نیست. جنگ سایبری در بسیاری از موارد به احتمال زیاد یا تلفات فیزیکی و جانی ندارد یا تلفات آن بسیار کم است. بنابراین، اگر تنها معیار برای ارزیابی آسیب‌ها در جنگ، صدمات فیزیکی باشد، همه موارد غیر خشونت‌آمیز جنگ سایبری به طور پیش‌فرض از این اصل تبعیت می‌کنند. بنابراین، تخریب پایگاه داده دیجیتالی یا پاک کردن آرشیوی دیجیتال که شامل سوابق تاریخی مهم یک ملت است، طبق نظریهٔ جنگ عادلانه اعمالی اخلاقی تلقی خواهند شد؛ زیرا موجب صدمات فیزیکی نمی‌شوند (Taddeo, 2012a, p. 213). این مسئله بدان معنا نیست که در شروع جنگ‌های سایبری اصل «سود بیشتر نسبت به زیان» قابل اعمال نیست و این اصل باید نادیده گرفته شود؛ بلکه نشان‌دهندهٔ این است که معیارهای محاسبهٔ سود و زیان در جنگ‌های سنتی، برای ارزیابی جنگ‌های سایبری کافی نیستند و در مواجه با این نوع

جنگ‌ها باید معیارهای جدیدی ارائه شوند؛ زیرا از یک طرف، چون در فضای سایبری بسیاری از سیستم‌ها از طریق شبکه و اینترنت به هم متصل و وابسته هستند، از کارافتادن یک شبکه و یا اخلال در یک سامانه می‌تواند در سامانه‌های دیگر هم اختلال به‌وجود آورد؛ برای نمونه، اختلال در اینترنت یک منطقه می‌تواند موجب اختلال در سیستم‌ها و تجهیزات بیمارستانی و حتی موجب مرگ بیماران شود. از طرف دیگر، در فضای سایبری دارایی‌ها و سرمایه‌های غیرفیزیکی مانند اطلاعات به اندازه دارایی‌ها و سرمایه‌های فیزیکی ارزشمند هستند و حتی در بسیاری از موارد ارزش دارایی‌های غیرفیزیکی بسیار بیشتر از دارایی‌های فیزیکی است. البته این نکته نیز باید در نظر گرفته شود که سود و زیان در جنگ‌های سنتی هم مختص ضرر جانی و فیزیکی نیست. آسیب‌های روانی و اجتماعی ناشی از جنگ هم از پیامدهایی است که هم در جنگ های سنتی و هم در جنگ های سایبری گریبان گیر عموم مردم می‌شود که بسته به نوع و شدت جنگ میزان آن متفاوت خواهد بود. از تأثیرات اجتماعی و روانی جنگ می‌توان به اضطراب، نگرانی، خشم، عصبانیت، افسردگی و غیره اشاره کرد. اما در جنگ های سایبری علاوه بر آسیب‌های مشترکی که با جنگ های سنتی دارند (آسیب جانی، فیزیکی، روانی و اجتماعی)، با آسیب‌های جدیدی هم مواجه هستیم که در جنگ‌های سنتی با آن روبرو نبوده‌ایم؛ مثل آسیب به داده‌ها و اطلاعات که به طور فیزیکی نامحسوس هستند؛ اما ارزش آنها ممکن است حتی بیشتر از دارایی‌های فیزیکی باشد. بنابراین، در محاسبه سود و زیان جنگ‌های سایبری این نوع آسیب‌ها هم باید مدّ نظر گرفته شوند.

ج) اصل مصونیت غیرنظامیان: هدف این اصل کاهش خونریزی و جلوگیری از هر نوع خشونت و صدمه‌ای به غیرنظامیان است. کاربرد این اصل در خصوص جنگ سایبری بسیار دشوار است. در جنگ‌های سنتی تمایز میان رزمنده و غیررزمنده منعکس‌کننده تمایز بین جامعه نظامی و غیرنظامی است. اما در جنگ سایبری این تمایز به راحتی امکان‌پذیر نیست (Taddeo, 2012a, p. 213). در جنگ سایبری هر سیستم رایانه‌ای یک سلاح سایبری بالقوه است و هر فردی که توانایی هک و نفوذ به سیستم‌ها را داشته باشد یک جنگنده بالقوه به شمار می‌رود و نمی‌توان به راحتی مرز مشخصی میان نظامیان و غیرنظامیان قائل شد. حتی تمایز میان سیستم‌ها و پایگاه‌های داده نظامی و غیرنظامی نیز در فضای سایبری بسیار مشکل است، زیرا بسیاری از منابع اطلاعاتی و زیرساخت‌های رایانه‌ای میان نظامیان و شهروندان مشترک هستند. در فضای سایبری بخشی از تجهیزات و سیستم‌ها مخصوص سازمان‌های نظامی است که حمله به این سیستم‌ها فقط به سازمان‌های نظامی آسیب می‌رساند، مانند حمله به سیستم‌های رایانه‌ای، شبکه و سرورهای داخل یک سازمان نظامی؛ اما یک سری از تجهیزات و زیرساخت‌ها هستند که بین نظامیان و غیرنظامیان مشترکند مثل تاسیسات برق، آب ، تلفن و غیره. ممکن است حمله به برخی از این زیرساخت‌ها از دید حمله‌کننده فقط هدف نظامی داشته باشد؛ مثلا مهاجم می‌خواهد برق یک منطقه نظامی را قطع کند، اما به دلیل اینکه خیلی از تجهیزات مشترک هستند و ممکن است حمله‌کننده ساختار دقیق اتصالات و شبکه‌ای این زیرساخت‌ها را نداند، موجب آسیب رساندن به غیرنظامیان شود. علاوه بر مشترک بودن تأسیسات زیرساختی

مانند: آب، برق و تلفن، تجهیزات الکترونیکی مانند: تجهیزات زیر ساخت اینترنت، مسیریاب‌های شبکه و سایر تجهیزات شبکه‌ای هم گاهی اوقات بین نظامیان و غیرنظامیان مشترک است؛ برای مثال، حمله به زیر ساخت اینترنت با هدف مختل کردن عملکرد یک سازمان نظامی خاص، ممکن است در عرضه خدمات حیاتی به غیرنظامیان اختلال ایجاد کند و آسیب‌های زیادی به آنها برساند؛ پس در حمله سایبری هنگام حمله به زیرساخت‌هایی که مشترک هستند، باید دقت زیادی شود که به غیرنظامیان آسیب رسانده نشود. هر چند آسیب غیرمستقیم به غیرنظامیان، مانند آسیب‌های اجتماعی و روانی ناشی از جنگ، چه در جنگ های سنتی و چه در جنگ‌های سایبری، غیرقابل اجتناب است، حملات باید به گونه‌ای طراحی شود که این نوع آسیب‌ها برای غیرنظامیان به کمترین حد خود برسد.

۵. راه‌کارهای اخلاقی استفاده از جنگ سایبری

مطرح شدن مشکلات فوق بدان معنا نیست که اصول نظریهٔ جنگ عادلانه در خصوص جنگ سایبری کارایی ندارد و در این نوع جنگ‌ها نباید به این نظریه توجه کرد؛ بلکه باید با توجه به ویژگی‌های منحصر به فرد جنگ سایبری به دنبال چگونگی پیاده‌سازی اصول اخلاقی در مورد این جنگ‌ها بود تا بتوان پاسخی درخور به مسائل و معضلات نوظهور این نوع جنگ ارائه داد. در این قسمت راه‌کارهایی اخلاقی برای استفاده از جنگ‌های سایبری مطرح می‌شود.

۵-۱. استفاده از شروط نظریهٔ جنگ عادلانه متناسب با جنگ سایبری

ممکن است در نگاه نخست به نظر برسد که جنگ سایبری از خونریزی و درگیری انسان‌ها جلوگیری می‌کند و در نتیجه، مقامات سیاسی نیازی به توجیه اقدامات نظامی برای افکار عمومی ندارند؛ اما واقعیت این است که باید از جنگ سایبری به همان اندازه جنگ سنتی ترسید؛ زیرا این نوع جنگ نیز می‌تواند منجر به خشونت و پیامدهای تخریبی زیادی شود. بنابراین، اعلان و استفاده از جنگ سایبری به قواعد اخلاقی جدی‌ای نیاز دارد که عدالت آن را تضمین کند (Taddeo, 2012a, p. 212). عدم وجود قواعد اخلاقی و قوانین بین‌المللی در حوزه جنگ سایبری موجب شده تا هر کشوری به خود اجازه بدهد تا با کوچکترین تنش و اختلافی، بدون رعایت اصول اخلاقی بر ضد کشوری دیگر وارد جنگ سایبری شود. بسیاری از قوانین بین‌المللی در خصوص جنگ‌های سنتی بر اساس قواعد اخلاقی نظریهٔ جنگ عادلانه نوشته شده است؛ اما بسیاری از این قانون‌ها و قواعد اخلاقی نمی‌تواند در خصوص جنگ‌های سایبری کاربرد داشته باشد. ممکن است گمان شود با توجه به اینکه برخی قواعد نظریهٔ جنگ عادلانه در جنگ سایبری کاربرد ندارد، در جنگ سایبری نباید توجهی به نظریهٔ جنگ عادلانه داشت؛ اما نظریهٔ جنگ عادلانه و بسیاری از اصول اخلاقی آن در مورد انواع جدید جنگ نیز می‌تواند معتبر باشد و با اندکی تغییر در روش‌های نوین جنگی به‌کار گرفته شوند. برای جلوگیری از گسترش بی‌رویه جنگ‌های سایبری و کاهش آستانه درگیری میان دولت‌ها باید چارچوبی اخلاقی برای قانونمند ساختن جنگ سایبری با تکیه بر شروط نظریهٔ جنگ عادلانه مانند: علت عادلانه، نیت صواب، جنگ سایبری به

عنوان آخرین راه‌حل فراهم کرد تا بتواند پاسخگوی پدیده‌های اخلاقی نوظهور این نوع جنگ‌ها باشد.

۲-۵. طراحی حمله‌های برگشت‌پذیر

یکی از معیارهای مهم در استفاده اخلاقی از سلاح‌ها و روش‌های جنگی قابلیت برگشت‌پذیری آنها است. قابلیت برگشت‌پذیری به این معنا است که پس از پایان جنگ و برطرف شدن خصومت میان دولت‌ها، بتوان تا حد زیادی خسارت‌های واردشده را جبران کرد و شرایط را به سرعت به حالت عادی برگرداند. میزان برگشت‌پذیری در جنگ تا حد زیادی بستگی به نوع سلاح‌های به کاررفته دارد. برخی سلاح‌ها ذاتاً قابلیت برگشت‌پذیری ندارند؛ زیرا خسارت‌های وارد شده توسط این سلاح‌ها قابل کنترل نبوده و به حدی سنگین هستند که به هیچ عنوان جبران نمی‌شوند، مانند: سلاح‌های اتمی، شیمیایی و بیولوژیکی؛ اما در مقابل، برخی سلاح‌ها و روش‌های جنگی قابلیت برگشت‌پذیری دارند و می‌توان پس از پایان جنگ تا حد زیادی خسارت‌های وارد شده را جبران کرد.

طبق بیان برخی متخصصان و طرفداران جنگ سایبری، سلاح‌های سایبری می‌توانند به لحاظ اخلاقی نسبت به سلاح‌های سنتی برتری داشته باشند؛ زیرا این سلاح‌ها برگشت‌پذیری بیشتری دارند. این قابلیت برگشت‌پذیری در حوزه جنگ سایبری به این دلیل است که تخریب سیستم‌های رایانه‌ای و یا اطلاعات نسبت به صدمات فیزیکی راحت‌تر قابل جبران است (Lin et-al., 2012; Shulman, 1999, p. 964). برگشت‌پذیری می‌تواند عامل بسیار مهمی در استفاده اخلاقی از سلاح‌های سایبری باشد. قابل ذکر است که همه جنگ‌های سایبری برگشت‌پذیر نیستند و در حوزه جنگ سایبری نیز برخی حملات سایبری به لحاظ اخلاقی نسبت به برخی دیگر ارجحیت دارند؛ زیرا صدماتی که ایجاد می‌کنند و اثراتی که بر جای می‌گذارند قابل برگشت است (Rowe, 2010b, pp. 1-2)؛ مانند حملاتی که در آنها به طور موقت داده‌ها رمزگذاری می‌شوند تا قابل استفاده نباشند و پس از پایان درگیری از حالت رمز خارج می‌شوند، بدون اینکه صدمه‌ای به آنها وارد شود. درست است که سلاح‌های سایبری نسبت به سلاح‌های سنتی قابلیت برگشت‌پذیری بیشتری دارند و صدمه به برنامه‌ها و داده‌ها می‌تواند با کپی داده‌های اصلی روی داده‌های آسیب‌دیده جبران شود، اما در خصوص استفاده از سلاح‌های سایبری باید به چند نکته مهم توجه کرد:

بازیابی برنامه‌ها و داده‌ها توسط قربانی ممکن است زمان‌بر باشد و نیاز به کاربران تعلیم دیده داشته باشد (Dorf et-al., 2007) که این شرایط همیشه در دسترس نیست. حمله‌کننده باید این نکته را مدنظر داشته باشد که همیشه قربانی دانش و ابزار کافی برای برگرداندن اطلاعات را ندارد؛ پس باید حمله سایبری را به‌گونه‌ای طراحی کند که پس از جنگ یا خود حمله‌کننده بتواند سیستم‌ها و اطلاعات را به حالت اولیه برگرداند و یا ابزارهای لازم را برای برگرداندن اطلاعات در اختیار قربانی قرار دهد.

باید به این نکته نیز توجه داشت که جنگ‌های سایبری ممکن است به اندازه صدمات فیزیکی و تخریب اطلاعات،

موجب آسیب‌های روان شناختی هم بشود و آسیب‌های روان شناختی قربانیان به سادگی قابل بازگشت نیست (Rowe, 2010b, p. 2). پس صرف بازگرداندن اطلاعات و سیستم‌ها به حالت اولیه دلیل برگشت‌پذیر بودن سلاح‌های سایبری نیست و برای استفاده اخلاقی از این سلاح‌ها باید همه شرایط و خسارت‌های وارد شده از جمله خسارت‌های روحی و روانی را نیز درنظر گرفت.

حمله به سیستم‌هایی که فعالیت‌های آنها حساس به زمان است، ممکن است قابل برگشت نباشد؛ برای مثال، زمانی که بیماری در بیمارستان زیر ماسک اکسیژنی است که توسط رایانه کنترل می‌شود، تأخیر در عملکرد رایانه می‌تواند موجب مرگ بیمار شود (Rowe, 2010b, p. 2). در این حالت شاید سلاح به کاررفته از نوع سلاح‌های برگشت‌پذیر باشد و بتوان سیستم و اطلاعات آن را به حالت اولیه بازگرداند، اما چون در چنین سیستم‌هایی زمان حرف اول را می‌زند، حتی صدم ثانیه‌ای تأخیر در عملکرد سیستم می‌تواند آثار مرگبار و غیرقابل جبرانی را به دنبال داشته باشد. استفاده از سلاح‌های برگشت‌پذیر سایبری در سیستم‌های حساس به زمان مانند سیستم‌های کنترل صنعتی، سیستم‌های حوزه بهداشت و درمان، و سامانه‌های حمل و نقل باید با دقت بسیار بیشتری صورت گیرد.

۱-۲-۵. روش‌هایی برای طراحی جنگ سایبری برگشت‌پذیر

برای طراحی جنگ‌های سایبری برگشت‌پذیر روش‌های مختلفی وجود دارد که به برخی از این روش‌ها اشاره می‌شود.

الف) حملات رمزنگاری

رمزنگاری روشی برای مخفی کردن اطلاعات است. از آنجایی که در جنگ سایبری اطلاعات هدف اصلی است، مخفی کردن آن می‌تواند یک حمله باشد. اگر در جنگ سایبری از رمزنگاری اطلاعات استفاده شود، پس از پایان جنگ می‌توان با رمزگشایی آنها را به حالت اولیه بازگرداند. در حملات رمزنگاری حمله‌کننده می‌تواند داده‌ها و برنامه‌های اصلی سیستم قربانی را با کلیدی که فقط در اختیار خودش است، رمز کند و در صورت پایان خصومت با کلید مربوطه داده ها را از حالت رمز خارج کند (Rowe, 2010b, p. 3; Lin et-al., 2012). یک نمونه از فعالیت های سایبری برگشت‌پذیر باج‌افزارها هستند که داده‌های سیستم قربانی را رمزنگاری می‌کنند؛ این بدان معنا است که فقط حمله‌کننده قادر به رمزگشایی اطلاعات است که وی نیز این کار را در ازای دریافت هزینه انجام خواهد داد. دولت‌ها می‌توانند از باج‌افزارها و سیستم‌های رمزنگاری برای طراحی سلاح‌های سایبری برگشت‌پذیر استفاده کنند. البته باید دقت شود که هدف فقط مواضع نظامی باشد و انتشار باج‌افزار قابل کنترل باشد زیرا در صورت انتشار باج‌افزارها به سیستم‌های عمومی صدمات جبران‌ناپذیری برای عموم مردم بوجود خواهد آمد برای مثال اگر باج‌افزار وارد سیستم‌های درمانی شود می‌تواند جان بیماران را به خطر بیاندازد.

ب) حملات به ساختار داده‌ها و سیستم‌ها

سیستم‌های رایانه‌ای با دقت بسیار زیادی طراحی شده‌اند که اگر بتوان ساختار و نظم منطقی آنها را مختل کرد به راحتی از کار خواهند افتاد. در حملات سایبری می‌توان داده‌ها و یا ساختار سیستم را به گونه‌ای تغییر داد که سیستم به طور موقتی به طور کلی از کار بیافتد و یا درست کار نکند (Rowe, 2010b, p. 3). رایانه‌ها به حدی دقیق‌اند که کوچکترین تغییر در داده‌ها و یا ساختار منطقی آنها می‌تواند عملکرد درست آنها را مختل کند. حمله‌کننده در هنگام جنگ برای مختل کردن موقتی عملکرد سیستم می‌تواند داده‌ها را تغییر دهد؛ داده‌هایی را به سیستم اضافه کند یا تغییراتی را در برنامه‌ها و فایل‌های سیستم‌عامل ایجاد کند؛ سپس در پایان جنگ باید تمامی تغییرات داده شده را به حالت اولیه بازگرداند. طراحی چنین حملاتی می‌تواند گامی مناسب برای حملات سایبری برگشت‌پذیر باشد؛ زیرا در پایان جنگ می‌توان تغییرات انجام شده روی سیستم قربانی را به حالت اول بازگرداند. درنتیجه، آن سیستم مجدداً به عملکرد صحیح خود ادامه خواهد داد.

ج) حملات از دسترس خارج کردن اطلاعات

از دیگر حملات برگشت‌پذیر حملاتی هستند که داده‌ها را پنهان کرده و یا اصطلاحاً از دسترس خارج می‌کنند. این عمل مشابه محاصره کردن در جنگ نیروی دریایی و یا پارازیت انداختن در جنگ الکترونیک است که هر دوی آنها تقریباً مزیت برگشت‌پذیری آسیب‌ها را دارند. برای مثال پارازیت انداختن در جنگ الکترونیک سینگنال‌ها را از بین نمی‌برد بلکه فقط موجب می‌شود که در بازه‌ای از زمان سینگنال‌های رادیویی به درستی به دست گیرنده نرسند و هر زمان که ار سال پارازیت متوقف شود گیرنده مجدداً می‌تواند پیام‌ها را به در ستی دریافت کند. پس این نوع حملات سرویس‌ها را از بین نمی‌برند بلکه فقط برای مدت زماتی سرویس‌های مورد نیاز را از دسترس خارج می‌کنند. حملات از کارانداختن سرویس[1] نمونه‌ای از این گونه حملات است که در این روش با ارسال حجم زیادی از داده‌های اشتباه به سمت سرور از خدمات رسانی سرور به کاربران جلوگیری می‌شود. (Rowe, 2010b, p. 4) برای مثال، در چنین حمله‌ای حمله‌کننده با ار سال حجم انبوهی از بسته‌های اطلاعاتی بیهوده به سمت سرورهای بانکی موجب می شود حجم کاری سرور بانک به قدری بالا رفته که سرور عملاً از کار افتاده و دیگر قادر به سرویس‌دهی به کاربران نباشد. در این نوع حملات هیچ آسیبی به داده‌های کاربران و اطلاعات ذخیره شده در سرورها نمی‌رسد و به محض اینکه حمله‌کننده ارسال بسته‌های اطلاعاتی به سرورهای بانک را متوقف کند بانک مجدداً قادر خواهد بود به کاربران خود خدمات لازم را ارائه دهد.

موارد ذکر شده فقط نمونه‌هایی از حملات سایبری برگشت‌پذیر هستند. استفاده از حملات برگشت‌پذیر گامی درست به سمت هدایت مسئولانه جنگ سایبری است. (Rowe, 2010b, p. 3) دولت‌هایی که خود را ملزم به رعایت اصول

1 . Denial of Services (DoS)

اخلاقی می‌دانند می‌توانند سلاح‌های سایبری‌ای را طراحی کنند که اثرات آن به سرعت قابل برگشت باشد. در مورد حملات برگشت‌پذیر نکته‌ای که باید مورد توجه قرار گیرد این است که برگشت‌پذیر بودن حملات نباید باعث شود که چنین حملاتی به اطلاعات حساس به زمان و یا سیستم‌هایی که برای ارائه خدمات حیاتی به مردم است مورد چنین حملاتی قرار گیرد. در حملات سایبری هدف مستقیم فقط باید مواضع نظامی باشد و سعی شود کمترین آسیب به غیرنظامیان وارد شود. نکته‌ای که وجود دارد این است که باید محرکی وجود داشته باشد که بتواند دولت‌ها را به سمت استفاده از سلاح‌های برگشت‌پذیر سوق دهد. بهترین محرک برای استفاده از حملات برگشت‌پذیر توسط دولت‌ها این است که در جوامع بین‌المللی حمله‌کننده مجبور باشد برای جبران خسارت‌های جنگ به قربانی هزینه بپردازد. در این صورت برای کاهش هزینه‌های خود به استفاده از حملات برگشت‌پذیر روی خواهد آورد. محرکی دیگر برای استفاده از حملات برگشت‌پذیر این است که زمانی که حمله‌کننده از حملات برگشت‌پذیر استفاده می‌کند احتمال اینکه قربانی نیز در پاسخ از این نوع حملات علیه حمله‌کننده استفاده کند افزایش پیدا می‌کند.

۳-۵. طراحی و استفاده از سلاح‌های سایبری قابل کنترل

جنگ سایبری نشان داده است که متفاوت از جنگ سنتی بوده و لزوماً خشونت‌آمیز و مخرب نیست. اما این واقعیت انکارناپذیر است که بسیاری از سلاح‌های سایبری برای ایجاد صدماتی فراتر از صدمات ساده نرم‌افزاری طراحی شده‌اند و علی‌رغم تصور عموم مردم این سلاح‌ها می‌توانند آسیب‌های فیزیکی و مرگباری را به دنبال داشته باشند. طراحان سلاح‌های سایبری به لحاظ اخلاقی موظف هستند سلاح‌هایی را طراحی کنند که از راه دور قابل کنترل بوده و در صورت پایان خصومت به راحتی قابل توقف باشند. ادامه حملات بعد از تسلیم دشمن و یا پس از پایان خصومت، غیراخلاقی است؛ یعنی حملات باید در صورت ضرورت قابلیت توقف از راه دور را داشته باشند و این امر برای حملات سایبری که به صورت خودکار انجام می‌شوند، نسبتاً دشوار است. سلاح سایبری‌ای که فعالیت آن قابل کنترل نباشد، مانند سلاح شیمیایی و یا سلاح اتمی است که ممکن است اثرات مخرب غیرقابل کنترل و جبران‌ناپذیری را موجب شود. برای مثال فرض کنید دشمن بدافزاری را وارد سیستم کنترل صنعتی نیروگاه‌های کشوری کرده است. این بدافزار به محض ورود به یکی از سیستم‌های نیروگاه، خود را در کلیه شبکه توزیع برق کشور تکثیر کرده و همه سیستم‌ها را آلوده می‌کند. اگر در چنین شرایطی خصومت میان طرفین برطرف شود، به دلیل اینکه این بدافزار به طور خودکار خود را در سراسر شبکه پخش کرده است، ممکن است دشمن نتواند عملکرد آن را کنترل و به راحتی آن را متوقف کند و اختلال در عملکرد سیستم نیروگاهی کشور می‌تواند موجب خسارت‌های گسترده شده و در پی آن درگیری میان آنها را افزایش دهد. علاوه بر اینکه سلاح سایبری باید قابلیت کنترل داشته باشد، چنین سلاح‌هایی نباید با ایجاد تخریب‌های فیزیکی در مواضع نظامی موجب به خطر افتادن جان مردم عادی و یا آسیب برگشت‌ناپذیر به محیط

زیست شوند؛ مثلا سلاح سایبری که موجب انفجار در تأسیسات هسته‌ای کشور دشمن شود می‌تواند اثرات جبران‌ناپذیری را تا سال‌های متمادی برای محیط زیست و سلامت افراد دا شته با شد. در صورت ا ستفاده از این نوع سلاح‌ها، حتی در صورت پشیمانی جلوی منتشر شدن و عملکرد آنها را نمی‌توان گرفت. تشعشعات رادیواکتیو برخی از مواقع تا شعاع ده‌ها کیلومتری از منطقه حادثه وجود دارد و هوا، آب و خاک را آلوده می‌کند و این آثار مخرب تا سال‌های طولانی در منطقه باقی خواهد ماند و منطقه مورد حمله را غیرقابل استفاده خواهد کرد. این پرتوها باعث پیدایش انواع سرطان‌ها، نقص عضوها و سندروم‌های غیرقابل درمان و حتی تغییرات ژنتیکی در نسل‌های آینده می‌شود و عواقب وحشتناک آنها قابل کنترل و جبرانا‌پذیر نیستند.

برای بیان پیامدهای حادثه‌های اتمی می‌توان به انفجار در نیروگاه برق هسته‌ای چرنوبیل در سال ۱۹۸۶ اشاره کرد. البته این حادثه جنگ سایبری نبوده و در اثر آزمایش ایمنی در یکی از رآکتورهای نیروگاه رخ داده است، ولی عواقب ناگوار و برگشت‌ناپذیر آن می‌تواند نشان دهد که تأسیسات هسته‌ای از حساسیت ویژه‌ای برخوردار هستند و هنگام جنگ نباید به بهانه جلوگیری از ساخت سلاح هسته‌ای کشور د شمن موجب حوادث جبران‌ناپذیری شد. محققان بیان کرده بودند که رادیواکتیو آزاد شده در حادثه چرنوبیل هرگز به طور کامل در محیط زیست زمین از بین نخواهد رفت. افزایش سرطان خون، افزایش سقط جنین و تولد کودکانی با ناهنجاری‌های ژنتیکی از پیامدهای این حادثه وحشتناک بود. کمتر از ۶ سال پس از حادثه افزایش صد درصدی سرطان های تیروئید در بلاروس، روسیه و اکراین رخ داد.[۱]

۴-۵. تربیت نیروهای خبره ارتش سایبری

یکی از وظایف اخلاقی مسئولان و دولت‌ها تربیت نیروهای ارتش سایبری برای مقابله با تهدیدها و جنگ‌های سایبری است. دولت‌ها باید توانایی لازم برای شناخت سریع حمله‌های سایبری را داشته باشند و همیشه با جدیدترین روش‌های حمله و نفوذ آشنا باشند؛ زیرا حمله‌کنندگان همیشه بهترین و جدیدترین راه‌های حمله را انتخاب می‌کنند. اگر کشوری ارتش سایبری قوی داشته باشد، زمانی که با حملات سایبری گسترده مواجه می‌شود، نه تنها می‌تواند به خوبی از زیرساخت‌ها و اطلاعات خود دفاع کند؛ بلکه می‌تواند از ضد حمله سایبری برای دفع و کاهش حملات استفاده کند و دیگر نیازی به ضد حمله سنتی ندارد. اگر دشمن جنگ سایبری را علیه کشوری آغاز کند، بهتر است قربانی نیز با رعایت ملاحظات اخلاقی نظریۀ جنگ عادلانه با همان سلاح‌های سایبری پاسخ حملات را بدهد. در واقع، با همان ابزاری که د شمن می‌جنگد، ما هم باید به جنگ د شمن برویم؛ همان‌طور که خداوند در قرآن می فرماید: «فَمَنِ اعْتَدَى عَلَيْكُمْ فَاعْتَدُواْ عَلَيْهِ بِمِثْلِ مَا اعْتَدَى عَلَيْكُمْ».[۲] شاید یک تفسیر این آیه آن باشد که با همان ابزاری که به جنگ شما

---

۱ برای جزئیات بیشتر در خصوص حادثه چرنوبیل به کتاب «نیایش چرنوبیل» نوشته سوتلانا آلکساندرونا الکسیویچ مراجعه شود.

۲ . بقره آیه ۱۹٤، «هر کس به شما تجاوز کرد، همانند آن بر او تعدی کنید»

می‌آیند، باید به جنگ دشمنان اسلام رفت؛ لذا پاسخ مبارزهٔ علمی، مبارزهٔ علمی است؛ پاسخ جنگ سخت، جنگ سخت است و پاسخ تهدید سایبری، مقابله سایبری است و یا در جای دیگری از قرآن آمده است: «وَأَعِدُّواْ لَهُم مَّا اسْتَطَعْتُم مِّن قُوَّةٍ»،[1] این آیه به این مسئله اشاره دارد که ما باید از تمامی ظرفیت‌های ممکن خود در جنگ استفاده کنیم. پس دولت اسلامی به لحاظ اخلاقی برای دفاع از خود و مقابله با حملات دشمن مسئولیت تربیت نیروهای خبره ارتش سایبری را بر عهده دارد، زیرا در سال‌های اخیر فضای سایبری تبدیل به فضای جدیدی برای جنگ شده است. لازم به ذکر است که از آنجایی آموزش جنگ و دفاع سایبری مستلزم آموزش مهارت هک کردن و نوشتن بدافزارها است و به دلیل ماهیت خطرناکی که این مهارت‌ها دارند، ممکن است موجب به وجود آمدن مسائل اخلاقی و قانونی در جامعه شود که برای جلوگیری از تبعات این آموزش‌ها باید به مسائل اخلاقی آن نیز توجه ویژه‌ای شود.[2]

۵-۵. عدم شرکت خودسرانه غیرنظامیان در جنگ سایبری

در دنیای فناوری اطلاعات هر سیستم رایانه‌ای یک سلاح سایبری بالقوه است و هر کسی با دانش پیشرفته سیستم‌های اطلاعاتی یک جنگنده بالقوه به شمار می‌رود (Dipert, 2010, p. 3). در حال حاضر از یک طرف اجزای لازم برای جنگ‌های سایبری، برای مثال سیستم رایانه‌ای و ارتباط اینترنتی، به سهولت در دسترس اغلب افراد هست و از طرف دیگر افراد در فضای سایبری می‌توانند هویت متفاوتی را شکل دهند و ممکن است کارهایی را انجام دهند که معمولا در دنیای واقعی انجام نمی‌دهند؛ چون در فضای سایبری کمتر احساس آسیب‌پذیری می‌کنند و علاوه بر این، افراد احساس می‌کنند در فضای سایبری کمتر دیده و ردیابی می‌شوند و از طرف دیگر پیامدهای برخی از اقدامات یا فعالیت‌های آنلاین برای افراد در دنیای آفلاین کاملا ملموس نباشد؛ بنابراین ممکن است در فعالیت‌هایی شرکت کنند که در غیر اینصورت انجام نمی‌دادند. یکی از این اقدامات شرکت خودسرانه در جنگ سایبری است. زمانی که به کشوری حمله سایبری صورت می‌گیرد برخی مواقع علاوه بر ارتش سایبری آن کشور، هکرها و افرادی که توانایی نفوذ به سیستم‌های رایانه‌ای را دارند به صورت خودسرانه و در اغلب موارد به دلیل احساس مسئولیت، عرق ملی و مذهبی و احساسات و عواطف نسبت به هموطنان خود، وارد جنگ شده و به‌طور گسترده به سیستم‌های کشور متجاوز حمله می‌کنند. باید تدبیری اندیشیده شود که کسانی که عضو ارتش رسمی سایبری کشور نیستند، به‌طور خودسرانه وارد جنگ سایبری میان دولت‌ها نشوند؛ چون چنین افرادی ممکن است به علت عدم آگاهی لازم از پیامدها و صدمات ناشی از حمله‌های سایبری موجب نقض اصول اخلاقی جنگ شده و علاوه بر وارد کردن آسیب‌های جبران ناپذیر، موجب تشدید خصومت میان دولت‌ها شده

---

۱ . انفال آیه ٦٠، «هر نیروئی در قدرت دارید برای مقابله با آنها (دشمنان) آماده سازید»

۲ . برای مطالعه بیشتر نک: آل بویه، علیرضا و آل بویه، زینب (۱۳۹۷) « بررسی اخلاقی آموزش نوشتن بدافزارها و مهارت هک و نفوذ به سیستم ها». پژوهش‌های فلسفی - کلامی, ش ٧٦، ص ٧١-٩٤.

و باعث شوند کنترل جنگ و پیامدهای ناشی از آن از دست مسئولان و دولت‌ها خارج شود و علاوه بر طولانی‌تر شدن جنگ، عواقب جبران‌ناپذیری را نیز بر جای بگذارد. بسیاری از افرادی که خودسرانه وارد جنگ سایبری می‌شوند با هدف ایجاد اختلال در دولت کشور دشمن، مواضع دولتی دشمن را هدف قرار می‌دهند و در شبکه و سیستم‌های دولتی اختلال ایجاد می‌کنند که این امر باعث می شود به غیرنظامیان آ سیب وارد شود که این کار یکی از ا صول اولیه جنگ عادلانه را نقض می‌کند؛ مثلا حمله به بانک‌های دولتی ممکن است موجب آسیب‌های جبران‌ناپذیری به مردم عادی شود؛ به‌طور مثال بیماری که قرار است پس از واریز وجه به حساب بیمارستان تحت عمل جراحی قلب قرار بگیرد، اگر به علت اختلال در شبکه بانکی نتواند وجه را واریز کند ممکن است جانش به خطر بیافتد. پس باید تدابیری اندیشیده شود که از شرکت خودسرانه افراد در جنگ‌های سایبری جلوگیری شود.

۶-۵. تشکیل بسیج مردمی و ساماندهی افراد آشنا به امنیت و حملات سایبری

در حال حاضر با توجه به گستردگی و سهولت دسترسی به ابزارهای امنیتی و ضد امنیتی فضای سایبری، بسیاری از افراد به راحتی دانش و مهارت نفوذ به سیستم‌های رایانه‌ای و در مقابل آن حفاظت از سیستم در مقابل حملات سایبری را فراگرفته‌اند. در زمان وقوع جنگ سایبری، ممکن است بسیاری از افراد عادی جامعه مهارت دفاع سایبری و حملات سایبری را داشته باشند؛ اما همان‌طور که گفته شد شرکت خودسرانه آنها در جنگ سایبری بین کشورها به لحاظ اخلاقی نادر ست ا ست؛ اما از طرف دیگر، این افراد دانش و مهارتی دارند که بی شک می‌تواند در شرایط جنگ و بحران به دفاع و امینت سایبری کشور کمک کند. طبیعتاً استفاده نکردن از این نیروی‌های بالقوه برای دفاع و جنگ سایبری درست نیست. بهترین راه حل برای استفاده درست و اخلاقی از این نیروهای بالقوه، تشکیل بسیج مردمی در حوزه امنیت سایبری و ساماندهی آنها است که می‌تواند موجب ارتقاء امنیت ملی کشور شده و توان دفاعی کشور را بالا ببرد و در مواقع جنگ سایبری می‌توان از حداکثر دانش و مهارت این افراد برای دفاع از کشور و حمله استفاده کرد. اگر بسیج سایبری به درستی راه‌اندازی و ساماندهی شود می‌تواند همانند بسیج مردمی در فضای واقعی تاثیرگذار و کارآمد باشد.

۷-۵. آموزش مسائل اخلاقی حوزه جنگ سایبری

دا شتن مهارت و دانش فنی برای جنگ سایبری کافی نیست و افرادی که در این حوزه آموزش می‌بینند و کسب مهارت می‌کنند، باید در کنار مسائل فنی با مسائل اخلاقی این حوزه نیز آشنا شوند. قطعاً یکی از وظایف اخلاقی مسئولان و دانشگاه‌ها این است که مسائل اخلاقی این حوزه را به افراد آموزش دهند و آنها را نسبت به پیامدهای اعمال خود آگاه کنند؛ مثلاً دانشگاه‌هایی که دوره‌های تخصصی جنگ سایبری برگزار می‌کنند، بهتر است چند واحد اخلاق این حوزه را نیز به دانشجویان تدریس کنند. آموزش اخلاق، افراد را برای اتخاذ تصمیم‌های درست و اخلاقی آماده می‌کند. گاهی اوقات هنگام وقوع جنگ سایبری برخی افراد ممکن است، به علت عِرق ملّی و از روی حس وطن‌پرستانه، خودسرانه وارد

جنگ سایبری شوند. چنین افرادی از عواقب عمل خود آگاه نیستند و ممکن است تبعات ناخواسته جبران ناپذیری را برای منافع ملی کشور به‌وجود آورند. بنابراین، آموزش اخلاق جنگ سایبری می‌تواند منجر به استفاده درست و اخلاقی از مهارت های فنی افراد شود. با توجه به فقر منابع در زمینه اخلاق جنگ سایبری به زبان فارسی، تولید منابع و تالیف کتاب‌هایی در این زمینه نیز می‌تواند برای دادن بینش اخلاقی درست به افراد بسیار راهگشا باشد.

البته باید توجه داشت که معرفت‌بخشی در حوزهٔ مباحث اخلاقی نباید منحصر به آموزشِ یک سری مباحث اخلاقی ناظر به جنگ سایبری و کدهای اخلاقی در این باره شود؛ بلکه باید دربارهٔ کارکرد اخلاق، چرایی زیست اخلاقی و انگیزش اخلاقی نیز معرفت‌های لازم ارائه گردد؛ برای مثال، نوعاً تصور بر آن است که اخلاق تنها کارکردی بیرونی دارد و تنها روابط میان انسان‌ها را تنظیم کرده و انسان‌ها با زیست اخلاقی اجتماع سالمی خواهند داشت و همگان از زندگی در جامعه‌ای سالم سود می‌برند. به همین وِزان رواج اخلاق در سطح بین المللی نیز می‌تواند روابط میان کشورها را سالم‌سازی کرده و همه کشورهای می‌توانند در سایه زیست اخلاقی جهانی بهتر و دل‌انگیزتری را رقم بزنند. این سخن فی نفسه سخنی درست و لازم است ولی کافی نیست؛ چرا که اخلاق علاوه برکارکرد و نقشی که در جامعه ایفا می‌کند کارکردی درونی دارد و هویت انسانی را شکل می‌دهد. البته بیشتر نظریه‌های اخلاقی مطرح در غرب مانند پیامدگرایی و حتی برخی از تقریرها وظیفه‌گرایانه توجهی به چنین کارکردی اصلاً ندارند؛ برای مثال، سودگرایی اخلاقی که رواج بیشتری در فلسفه اخلاق غرب دارد، با تقریرهای گوناگون در پی بیشترین غلبه خیر (لذت) بر شر (الم) برای بیشترین افراد است. در چنین نظریه‌هایی اصلاً سخن از نقشی که اخلاق می‌تواند در شکل‌گیری هویت آدمی ایفا کند دیده نمی‌شود؛ اما در اندیشه اخلاق اسلامی آنچه مهم است علاوه بر کارکرد بیرونی اخلاق و نقشی که اخلاق در سلامت اجتماع ایفا می‌کند، کارکرد درونی اخلاق است.

از منظر قرآن انسان جایگاه بسیار ویژه و والایی دارد، به گونه‌ای که روح الهی در او دمیده شده و به مقام خلیفه‌اللهی نائل و شایستگی سپرده شدن امانت الهی به خود را یافته است و در پیشِ روی خود زندگی جاودانه‌ای را در پیش دارد که چگونگی زیست در آن در گرو پاسداشت ارزش‌های اخلاقی در مراتب گوناگون آن در دنیا است. هدف از زیست اخلاقی در اسلام تشبه به خداست و در سایه شباهت وجودی با خداست که انسان به مقام انسانیت واقعی نایل می‌شود. از همین روست که در برخی روایات آمده است که «تخلقوا باخلاق الله» یا «تشبهوا به اخلاق الله». کوتاه سخن آنکه معرفت‌بخشی در کارکرد درونی اخلاق و تبیین مقدمات چنین معرفتی از جمله دوگانگی روح و بدن و اصالت داشتن روح می‌تواند زمینه زیست اخلاقی را تا حدودی بهتر فراهم آورد

۸-۵. ضرورت تربیت اخلاقی

همان‌گونه که گذشت تفاوت جدی در جنگ سایبری و جنگ سنتی وجود دارد و در جنگ سنتی اقدام خود سرانه و انفرادی افراد حتی با انگیزه‌های صحیح وجود ندارد؛ ولی در جنگ سایبری کاملاً بر عکس است و تک‌تک افراد اگر

آموزش‌های لازم هک کردن و نفوذ در سیستم‌های رایانه‌ای را آموخته باشند، از هر جا و مکانی و در هر زمانی می‌توانند علیه منافع کشورهای متخاصم دست به کار شوند. نکته مهم اینکه در آموختن هک کردن نیازی به آموزش‌های کلاسیک نیز نیست و افراد به صورت تجربی با گذرندان دوره‌هایی می‌توانند مهارت هک را به خوبی بیاموزند. از این رو، برای اینکه چنین وقایعی رخ ندهد عوامل بازدارنده درونی بسیار راهگشا است و قوانین حقوقی و جزایی کافی به نظر نمی‌رسد. به‌خصوص با توجه به اینکه هکرها و حمله‌کنندگان سایبری اصولاً به‌گونه‌ای عمل می‌کنند که قابل شناسایی نبوده و ردیابی آنها به سهولت امکان‌پذیر نیست؛ پس آموزه‌های اخلاقی در اینجا نقش مهمی را می‌توانند ایفا کنند؛ چون ضمانت اجرای اخلاق درونی است، برخلاف حقوق که ضمانت اجرای آن بیرونی است (آل‌بویه، ۱۳۹۴، ص ۱۰۸). برای القای اهمیت اخلاق و درونی ساختن آن، علاوه بر آموزش اخلاق، باید تربیت اخلاقی را از خانواده شروع کرد و خانواده نقش بسیار مهمی در این زمینه ایفا می‌کند و بعد از خانواده مقاطع گوناگون آموزش در دوران کودکی، نوجوانی و جوانی نیز اهمیت بسزایی دارند. روشن است که دانشگاه نیز از این امر مستثنا نیست.

در بند قبلی سخن از ضرورت آموزش اخلاق جنگ سایبری بود و در اینجا سخن از ضرورت تربیت اخلاقی است. از نظر سقراط یگانه فضیلت معرفت است. او می‌گفت اگر کسی معرفت اخلاقی داشته باشد، عمل اخلاقی نیز خواهد کرد و لذا کافی است به انسانها معرفت اخلاقی بدهیم. به اعتقاد او شکافی میان معرفت و عمل اخلاقی وجود ندارد، اما غالباً اندیشمندان بعدی حتی افلاطون و ارسطو به او اشکال کرده و سخن او را نپذیرفته‌اند. به گفته‌ها آنها، با انسانهای بسیاری مواجه می‌شویم که معرفت اخلاقی دارند ولی به دانسته‌های اخلاقی خود عمل نمی‌کنند. دست‌کم ما خود را این گونه می‌یابیم و در موارد گوناگونی به دانسته‌های اخلاقی خود عمل نمی‌کنیم. از جمله عواملی که برخی از روان‌شناسان اخلاق نام برده‌اند ضعف اراده، نداشتن الگوی اخلاقی، و عمق‌بخشی به معرفت اخلاقی است. بنابراین، به نظر می‌رسد علاوه بر خانواده‌ها، مراکز آموزشی در سطوح مختلف علاوه بر معرفت‌بخشی درباره اخلاق و از جمله اخلاق جنگ سایبری و پیامدهای دخالت خودسرانه در چنین اموری، به تربیت اخلاقی نیز توجه ویژه داشته باشند.

نتیجه‌گیری

در سال‌های اخیر به دلیل افزایش وابستگی سازمان‌ها و دولت‌ها به زیرساخت‌های اطلاعاتی و ارتباطی نمی‌توان به سادگی از کنار سلاح‌های سایبری گذشت و آنها را نادیده گرفت؛ زیرا بسیاری از سلاح‌های سایبری برای ایجاد صدماتی فراتر از صدمات ساده نرم‌افزاری طراحی شده‌اند و می‌توانند همانند سلاح‌های سنتی خطرناک بوده و آسیب‌های جبران‌ناپذیری را وارد کنند. با توجه به ویژگی‌های منحصر به فرد جنگ سایبری باید به دنبال کشف اصول جدیدی برای اخلاقی بودن این جنگ‌ها بود تا بتوان پاسخی درخور به مسائل و معضلات نوظهور این نوع جنگ ارائه داد. تبیین اصول اخلاقی و تدوین قوانین مخصوص جنگ سایبری در سطح بین المللی، طراحی حملات برگشت‌پذیر،

طراحی و استفاده از سلاح‌های سایبری قابل کنترل، تربیت نیروهای خبره ارتش سایبری، عدم شرکت خودسرانه غیرنظامیان در جنگ سایبری و تشکیل بسیج سایبری، آموزش مسائل اخلاقی جنگ سایبری و تربیت اخلاقی از کودکی از راه‌کارهای اخلاقی‌ای هستند که کمک می‌کنند عواقب و معضلات جنگ‌های سایبری کمتر شود. در مقایسه جنگ سنتی و جنگ سایبری، اگر معیارهای نظریهٔ جنگ عادلانه رعایت شود و اصول اخلاقی و قوانین مخصوص جنگ‌های سایبری نیز محقق شود، در جایگاه انتخاب، جنگ سایبری می‌تواند انتخاب مناسب‌تر و اخلاقی‌تری نسبت به جنگ سنتی بوده و تلفات جانی و خسارت‌های جبران‌ناپذیر کمتری را موجب شود. و این طبیعتاً مستلزم آن است که دولت‌ها و جوامع بین‌المللی به دنبال تدوین اصول اخلاقی مخصوص جنگ‌های سایبری باشند و در کنار آن ضمانت‌ها و اهرم‌های اجرایی لازم نیز برای الزام دولت‌ها به مراعات این اصول تعیین شوند تا بتوان آسیب‌ها و عواقب این گونه جنگ‌ها را کاهش داده و از مزایای آنها بهره گرفت.

منابع

قرآن کریم.

آل‌بویه، علیر ضا؛ آل‌بویه، زینب. (۱۳۹۴). هک کردن و نفوذ به سیستم‌های رایانه‌ای از منظر اخلاقی، *فصلنامه علمی-پژوهشی نقد و نظر*. ۲(۲۰): ۱۲۸-۱۰۴.

مجلسی، محمدباقر. (۱۴۰۳ ق). *بحار الانوار*، ج ۶۷، بیروت: دار احیاء التراث العربی.

امام خمینی، سیدروح الله، (۱۳۹۰ ق). *تحریر الوسیله*، ج ۱. الطبعه الثانیه، النجف الاشرف: مطبعه آلاداب.

Anonymos, "Department of defense law of war manual", United States (2015). Department of Defense, Available at: https://www.defense.gov/Portals/1/Documents/DoD_Law_of_War_Manual-June_2015_Updated_May_2016.pdf. (Accessed on: 6 Apr 2017)

Australia. Department of the Prime Minister and Cabinet, (2013), "Strong and Secure: A Strategy for Australia's National Security". Available at: yun.ir/sj1gs6, Canberra The Department of the Prime Minister and Cabinet. (Accessed on: 7 May 2016).

Boylan, Michael. (2013). Can there be a Just Cyber War? *Journal of applied ethics and philosophy*, vol 5: 10-17.

Clarke, Richard A., and Knake, Robert K. (2012). *Cyber War The Next Threat to National Security and What to Do About It*, New York: HarperCollins, Routledge.

Cohen-Almagor, Raphael. (2011). Internet History. *International Journal of Technoethics*. USA. IGI Publishing Hershey: 2(2): 45-64.

Denning, Dorothy E. (2008). The Ethics of Cyber Conflict' in: *The Handbook of Information and Computer Ethics* (eds K. E. Himma and H. T. Tavani). John Wiley & Sons, Inc., Hoboken, NJ, USA.

Denning, Dorothy E. and Strawser, Bradley J. (2014). Moral Cyber Weapons. *The Ethics of Information Warfare*. Volume 14 of the series Law, Governance and Technology Series. Springer: 85-103.

Dipert, Randall. (2010). The Ethics of Cyberwarfare. *Journal of Military Ethics*. London, Routledge: Vol. 9, 4, 384-410.

Dorf, J. and Johnson, M.. (2007). Restoration Component of Business Continuity Planning. in Tipton, H. and Krause, M. (Eds.). *Information Security Management Handbook.* Sixth Edition. CRC Press: pp. 645-654.

Dower, Nigel.(2009). The ethics of war and peace, *Polity Press*.

Estrella, Iceal Averroes E. (2012). On the Ethics of War. KRITIKE: *An Online Journal of Philosophy*. Vol. 6 Issue 1: 67-84.

Evans, Nicholas and Ford, Shannon B. and Gastineau, Adam & Henschke, Adam & West, Levi. (2014) Cybersecurity: Mapping the Ethical Terrain. National Security College Occasional Paper, Available at: yun.ir/nndbz, (Accessed on: 4 May 2017).

Fred Schreier. (2015). On Cyberwarfare. DCAF HORIZON 2015 WORKING PAPER No. 7, Available at: http://docplayer.net/4159538-Dcaf-horizon-2015-working-paper-no-7-on-cyberwarfare-fred-schreier.html. (Accessed on: 2 Aug 2017).

Green, Leslie C. (1993). *The Contemporary Law of Armed Conflict*, Canada, Manchester University Press.

Hubert, Don & Weiss, Thomas G. et al. (2001). The Responsibility to Protect: Supplementary Volume to the Report of the International Commission on Intervention and State Sovereignty, Canada, International Development Research Centre.

Johnson, James Turner. (1981). *Just War Tradition and the Restraint of War: A Moral and Historical Inquiry*. New Jersey. Princeton University Press.

Just war theory, routledge, cw.routledge.com/textbooks/alevelphilosophy/data/A2/Politcal/JustWarTheory.pdf

Knopová, Martina & Knopová, Eva. (2014). The Third World War? In The Cyberspace. Cyber Warfare in the Middle East, *Acta Informatica Pragensia.* 3(1).23–32.

Lazar, Seth. (2020). War. The Stanford Encyclopedia of Philosophy (Spring 2020 Edition), Edward N, Zalta. (ed.) URL = <https://plato.stanford.edu/archives/spr2020/entries/war/>.

Lin, Patrick & Rowe, Neil & Allhoff, Fritz. (2012). "s It Possible to Wage a Just Cyberwar? Available at: https://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/. (Accessed on: 7 Jun 2017).

Lin, Patrick & Allho, Fritz & Rowe, Neil C. (2012). War 2.0: Cyberweapons and Ethics. *Communications of the ACM*. New York, ACM: vol. 55, no. 3, 24-26.

Lorents, Peeter & Ottis, Rain. (2010) Knowledge Based Framework for Cyber Weapons and Conflict. *Conference on Cyber Conflict*. Available at: https://ccdcoe.org/uploads/2018/10/Lorents-et-al-Knowledge-Based-Framework-for-Cyber-Weapons-and-Conflict.pdf. (Accessed on: 23 Mar 2017).

Lucas, George. (2014). Permissible Preventive Cyberwar: Restricting Cyber Conflict to Justified Military Targets. *The Ethics of Information Warfare*, Law, Governance and Technology Series, vol 14. Springer: 73-83.

Mele, Stefano. (2013). Cyber-weapons: legal and strategic aspects (version 2).Available at: http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf. (Accessed on: 3 Jun 2017).

Nasir Mohd, Zin, Ahmad and Yunos, Zahri. (2003). Computer Virus: Future Cyber Weapons. National ICT Security and Emergency Response Centre (NISER). Available at: http://www.cybersecurity.my/data/content_files/13/73.pdf. (Accessed on: 9 Jul 2016).

Ohlin, Jens David & Finkelstein, Claire Oakes & Govern, Kevin. (2015). *Cyberwar: Law and Ethics for Virtual Conflicts*, Oxford University Press.

Park, Ji Min. (2015). Finding effective responses against cyber attacks for divided nations. Unpublished master's thesis, Naval Postgraduate School.

Rid, Thomas & McBurney, Peter. (2012). Cyber-Weapons. *The RUSI Journal*, vol.157. NO.1: 6-13.

Rid, Thomas. (2013). *Cyber War Will Not Take Place*, Oxford University Press.

Rowe, Neil C. (2010a). "The Ethics of Cyberweapons in Warfare". *International Journal of Cyberethics*. USA, IGI Publishing Hershey: Vol. 1, No. 1: 20-31.

Rowe, Neil C. (2010b). Towards Reversible Cyberattacks. *Proc. 9th European Conference on Information Warfare and Security*. Thessaloniki, Greece [ECIW].

Shulman, M. (1999). Discrimination in the Laws of Information Warfare. *Columbia Journal of Transnational Law.* Vol. 37. 939-968.

Singer, P.W. (2015). Stuxnet And Its Hidden Lessons On the Ethics Of Cyberweapons. *Case Western Reserve Journal of International Law*. 47, 79-86.

Slayton, Rebecca. (2017). Why Cyber Operations Do Not Always Favor the Offense. Policy File.1–7. Yun.ir/64n61e.

Taddeo, Mariarosaria. (2012a). An Analysis For A Just Cyber Warfare. *4th International Conference on Cyber Conflict (CYCON 2012)*. NATO CCD COE Publications, Tallinn.

Taddeo, Mariarosaria. (2012b). Information Warfare: a Philosophical Perspective. *Philosophy and Technology*. 25(1): 105-120.

Tzu, Sun. (2005). *The art of war*. Thomas Cleary, Shambhala.

US Department of Defense U.S. Cyber Command Fact Sheet, May 25. (2010). Available at: http://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf. (Accessed on: 26 Jun 2017).

Michael, Lacewing. (2010). Just war theory. New York: Routledge, Available at: http://documents.routledge-interactive.s3.amazonaws.com/9781138793934/A2/Political/JustWarTheory.pdf. (Accessed on: 10 Apr 2017).