مفهوم تروریسم در فناوری نوین سایبر

سیما حاتمی[1]

فتح الله رحیمی[2]

تاریخ دریافت:۱۴۰۲/۰۲/۲۶ تاریخ پذیرش:۱۴۰۲/۰۳/۳۱

چکیده

اقدامات سایبری یا رایا جنگ در بستر اینترنت بعنوان جنگ اطلاعاتی شناخته می شود که با انقلاب اطلاعات بروز پیدا کرده است. امروزه این نوع جنگ با اصطلاح سایبرتروریسم به مجموعه ای از تکنیک ها اطلاق می شود که به قصد ممانعت از دسترسی به اطلاعات و ایجاد اغتشاش و برهم زدن امنیت دولت یا گروه هدف است و مراکز حیاتی، حساس و مهم را تحت تأثیر قرار می دهد. نظر به اهمیت فناوری اطلاعات در عصر حاضر و عدم پایداری بستر اطلاعاتی، این امر به یکی از نقاط بالقوّه آسیب پذیر و خطرناک در جهان بدل شده است. مصون سازی این فناوری از تهدیدات موجود در جهت حفظ امنیت ملّی و حریم شخصی شهروندان در فضای جنگ و مخاصمات بین المللی، مقتضی توجّه و اقدام سریع و در عین حال نظام مند و معقول در این زمینه است. اخیراً حملاتی که به جایگاه های بنزین و سوخت در ایران رخ داد؛ در واقع مبیّن نوعی هشدار به امکان نشانه گرفتن مراکز امنیتی و تأسیسات حیاتی و ایجاد اختلال در شبکه سیاسی، تولیدی، اقتصادی، اجتماعی و حتّی راه های مواصلاتی است که می تواند مانند دومینو یکی بعد از دیگری، شبکه های مختلف کشور را نشانه گرفته و مختل نماید. این مقاله به بررسی سایبر تروریسم با رویکردی انتقادی و تحلیلی در نظام حقوق بین الملل نوین می پردازد و اقدامات کشورها در این حوزه را در تحقق صور نوظهور جرایم مربوط به سایبرتروریسم به چالش می کشد .

واژگان کلیدی : سایبرتروریسم، فناوری اطلاعات، حمله سایبر، سوخت، رایا جنگ

---

۱ . دانش آموخته دانشکده حقوق و علوم سیاسی دانشگاه تهران دکتری حقوق بین الملل عمومی drsimahatami@gmail.com

۲ . عضو هیات علمی دانشگاه آزاد اسلامی rahimif_law@yahoo.com

حادثه ۱۱سپتامبر به عنوان «یکی از بزرگترین زلزله‌ها» تنها و صرفاً محدود به آمریکا نبود، بنا به تعبیری دیگر، این حادثه برای اولین بار آمریکا را وارد کره زمین کرد.(نصری؛ ۱۳۸؛ صص ۶۷۱-۶۹۲) چارچوب حقوق بین الملل پیرامون تروریسم[۳] بسیار قبل تر از اتفاق ۱۱ سپتامبر وجود داشت. از هجده سند بین المللی موجود (شامل اصلاحیه ها و متمم ها[۴]) که از سال ۱۹۶۳ به تصویب رسیده، سیزده سند قبل از سال ۲۰۰۱ وجود داشته است. اگرچه بدیهی به نظر می رسد که حمله به مرکز تجارت جهانی[۵] و سایر رویدادهای داخل ایالات متحده به عنوان کاتالیزور[۶]و عاملی برای تسریع توسعه اسناد جدّی بین المللی عمل کرده؛ لیکن از زمان تصویب کنوانسیون سال ۲۰۰۵ برای سرکوب اقدامات تروریسم هسته ای و استراتژی جهانی ضد تروریسم سازمان ملل متحد در سال ۲۰۰۶[۷]، این اسناد بر اساس مبانی حقوقی قبلی مصوب گردیده اند. از منظر غالب این اسناد بین المللی، جنگ سایبر به عنوان نبردی علیه استفاده از کامپیوترها به عنوان اسلحه و ابزاری برای انجام کارهای خشونت بار و به قصد ارعاب و ترساندن و یا تغییر عقیده یک گروه یا کشور است. جنگ سایبر به قصد کارهای سیاسی و یا آرمانی محقّق می شود و مکان‌ها و تأسیسات حیاتی مانند انرژی، حمل‌ونقل، ارتباطات، سرویس‌های مهم و حیاتی را هدف قرار می‌دهد و از شبکه‌های کامپیوتری به عنوان بستری برای انجام این أعمال خرابکارانه استفاده می‌کند؛ مانند آنچه در رخدادهای أخیر جایگاه های سوخت و بنزین در ایران مشاهده شد.

به رسمیت شناختن حق دفاع یک کشور در پاسخ به یک حمله تروریستی، بطور صریح از سوی شورای امنیت سازمان ملل متحد[۸] در قطعنامه های شماره ۱۳۶۸ و ۱۳۷۳ قابل توجّه است(Derek Jinks; 2003; 32). اگر حمله تروریستی سایبری حداقل به همان آستانه حملات ۱۱ سپتامبر صورت بپذیرد، دلایل جدّی وجود خواهد داشت که به چرایی وجود مبانی حقوقی در دفاع از این رخداد توجّه ویژه شود.

فقدان تعریفی مقبولِ دولتها و عام الشمول از تروریسم، مانعی در توصیف ماهیت آن شده است. بطور کلی، تعیین قطعی وضعیت حقوق عرفی مربوط به استفاده از زور در رابطه با اعمال تروریستی و همچنین جرم انگاری اینگونه أعمال، مقتضی تعریف مشخص از تروریسم است.(Jeff Addicott; 2011; 1) یعنی جلوگیری از تروریسم، محکومیت و مجازات آن(Clive Walker, , 2007 pp 331, 336). شایان ذکر است که تقاضای بین‌المللی و فشارها برای استرداد مجرم یا مجرمین تروریستی بسیار بیشتر از فشارها برای استرداد یک جنایتکار معمولی[۹] است.

---

[3]- Terrorism
[4]- International Legal Instruments to Counterterrorism, U.N. ACTION TO COUNTER TERRORISM, http://www.un.org/terrorism/instruments .shtml (last visited Aug. 21, 2012).
[5]- The World Trade Center
[6]- Catalysts
[7]-The 2005 Convention for the Suppression of Acts of Nuclear Terrorism and 2006 United Nations Global Counter-Terrorism Strategy
[8]- The United Nations Security Council (UNSC) in Resolutions 1368 and 1373
[9]- A Common Criminal.

این موضوع با تعریف توصیه شده توسط هیأت عالی رتبه سازمان ملل[۱۰] در گزارش خود در مورد تهدیدها، چالش ها و تغییرات در سال ۲۰۰۴ پیچیده تر می شود. این هیأت به این نتیجه رسید که جای یک تعریف جامع و مانع در کنوانسیون جامع تروریسم بین المللی خالی است.

تروریسم در واقع به هر گونه اقدام، علاوه بر مواردی که قبلاً در مورد جنبه‌های تروریسم در کنوانسیون‌های ژنو و قطعنامه ۱۵۶۶ (۲۰۰۴) شورای امنیت مشخص شده، اطلاق می شود که به منظور کشتن یا ایجاد یا ورود صدمات جدی بدنی به غیرنظامیان یا غیرنظامیان صورت می پذیرد؛ خصوصاً زمانی که هدف از چنین عملی، بنا به ماهیت یا زمینه آن، ارعاب جمعیت یا مجبور کردن دولت یا سازمان بین المللی به انجام یا خودداری از انجام هر عملی باشد.

کوفی عنان[۱۱] در گزارش سال ۲۰۰۵ «در تبیین آزادی بزرگتر»[۱۲] همین موضوع را تأیید[۱۳] و خاطرنشان کرد، «وقت آن رسیده که بحث‌های به اصطلاح «تروریسم دولتی[۱۴]» را کنار بگذاریم [و] حق مقاومت در برابر اشغال را در معنای واقعی آن در یابیم.» اگرچه هیأت عالی رتبه، صراحتاً خواستار گنجاندن «تعریفی دقیق و جامع» مندرج در قطعنامه ۱۵۶۶ شورای امنیت شده،[۱۵] لیکن قطعنامه ۱۵۶۶ شورای امنیت به وضوح از رویکرد بخشی حمایت می کند، یعنی مستقیماً به کنوانسیون های موجود در مورد تروریسم اشاره أکید دارد.[۱۶]

[10]- The UN's High-Level Panel in its Report on Threats,
[11]- Kofi Annan
[12]- In Larger Freedom
[13]- U.N. Secretary-General, In Larger Freedom, ¶ 91, U.N. Doc. A/59/2005 (Mar. 21, 2005), at ¶ 91.
[14] - State terrorism
[15]- U.N. Secretary-General, A More Secure World: Our Shared Responsibility: Report of the High-level Panel on Threats, Challenges and Change, at ¶ 164(c).
[16]- See S.C. Res. 1566, ¶ 3, U.N. Doc. S/RES/1566 (Oct. 8, 2004) ("Recalls that criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature, and calls upon all States to prevent such acts and, if not prevented, to ensure that such acts are punished by penalties consistent with their grave nature.").

با اینحال، از منظر حقوقی، بنظر می رسد پیشنهادات دبیرکل سابق ملل متحد بیشتر رویکرد حمایتی دارد تا نوعی رویکرد مبتکرانه؛ زیرا تعریف اصلی و مشابه -که تا حدی شبیه کنوانسیون ۱۹۳۷ برای پیشگیری و مجازات تروریسم است- در پیش نویس کنوانسیون جامع تروریسم بین المللی سال ۲۰۰۱ میلادی وجود دارد که البتّه بدون هرنوع تغییر، مسکوت باقی مانده است. بموجب متن این کنوانسیون، سایبرتروریسم وضعیتی است که «هر مرتکب جرمی در مفهوم کنوانسیون حاضر، به هر وسیله ای غیرقانونی و عمداً باعث بروز موارد زیر شود:

الف) مرگ یا صدمات و جراحات شدید بدنی به هر شخصی؛ یا

ب) آسیب جدّی به اموال عمومی یا خصوصی، از جمله مکان استفاده عمومی، تأسیسات دولتی یا دولتی، سیستم حمل و نقل عمومی، تأسیسات زیربنایی یا محیط زیست؛ یا

ج) آسیب به اموال، مکان‌ها، تأسیسات یا سیستم‌های مذکور که منجر به زیان اقتصادی عمده شده و یا ممکن است منجر به زیان اقتصادی عمده بشود؛ مشروط به آنکه هدف از این رفتار، بنا به ماهیت یا زمینه آن، ارعاب جمعیت مردمی یا مجبور کردن دولت یا یک سازمان بین المللی به انجام یا خودداری از انجام هر کاری باشد.

با اینحال، همچنان این پرسش اساسی وجود دارد که آیا تعریف پیشنهادی سبب نمی شود تا بطور غیرمنطقی رژیم حقوق بین‌الملل موجود، که اقدامات تروریستی را جرم انگاری می‌کند، سست شود؟ این سئوال بطور خاص معطوف به این امر در رابطه با حملات سایبری است. پاسخ به این موارد، مستلزم تحلیل اسناد مربوطه و تبیین صحیح موضوع است.

۱- مفهوم سایبرتروریسم

آنچه تروریسم سایبری را از واژه تروریسم متمایز می کند، استفاده از شبکه های کامپیوتری و وب عمدتاً مبتنی بر اینترنت، است. در اصل، استفاده از پیوندها و شبکه های متصل الکترونیکی بمنظور انجام حملات تروریستی صورت می پذیرد و معمولاً شامل برنامه هایی است که برای این منظور ایجاد می شوند. این برنامه‌ها را می‌توان از طریق اینترنت، وسایل ذخیره‌سازی قابل حمل مانند کارت‌های(USB)، سیگنال‌های رادیویی بی‌سیم یا سایر وسایل مشابه به مقصد رساند؛ لیکن وجود برخی ضعف های ذاتی فناوری ارتباطات، این سامانه را در معرض تهدیدهای امنیتی قرار می دهد. استفاده دولت‌ها از فضای ناامن سایبری، زمینه را برای تهدیدات امنیتی از جمله خرابکاری، اخلال، ترور، جاسوسی و دیگر جرائم مرتبط هموار ساخته است.(صیاد و دیگران؛ ۱۳۹۹؛ صص ۲۹۳-۳۳۰)

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

تروریسم سایبری، باید جدا از استفاده تروریستی از اینترنت و بستر وب مورد مطالعه قرار گیرد.(Elina Noor; 2011; pp 51, 52) در این وضعیت، جنبه های ارتباط، کاربرد و نوع استفاده،[1]تأمین مالی، سازماندهی حملات فیزیکی،[2] تبلیغات (همچنین به شکل «هکتیویسم»[3])، تحریک به تروریسم[4]مورد توجّه قرار خواهد گرفت.(Yaël Ronen; 2010; pp. 645, 654)

اصطلاح «تروریسم سایبری»[5] پیش از ۱۱ سپتامبر وجود داشت(Sam Berner; 2003; 1,1). نظر به تفاوت جرائم سایبر با جنگ سایبری، هرگونه دخل و تصرف غیرمجاز از طریق ورود یا خروج، ضبط و ذخیره، پردازش و کنترل داده ها و نرم افزارهای رایانه ای و ایجاد یا وارد کردن انواع ویروسهای رایانه ای و امثال آن جرم سایبری است. این در حالی است که بلحاظ فقدان تعریف جهانی از «حمله سایبری» و «تروریسم»،[6] هر شخصی، درک جداگانه ای از این اصطلاح دارد(Jahangiri; 2009; 29)؛ و تمایلات نیز بدین جهت است که حملات سایبری جزئی هم اتفاقاً «تروریسم سایبری» توصیف شده و با تمرکز بر ماهیت مخرب و بی‌ثبات سایبری، موضوع فقط به افراد و عاملان غیردولتی محدود گردد(Natasha Solce,; 2008; pp 293, 301).[7]تحقیقاً صِرف تمرکز بر اثرات روانشناختی فاحش مانند ارعاب (ترس)[8] و فرآیند نوشتن بدافزار[9]مفید فایده نخواهد بود؛ بلکه حمله به زیرساخت‌های مهم ملّی و حمله به خود شبکه‌ها است که آسیب زننده و خطرناک است(Gabriel Weimann; 2005; pp 129, 130)؛ همچنین نظراتی وجود دارد دائر بر اینکه اساساً تروریسم سایبری ماهیتاً وجود ندارد، زیرا تروریسم، مستلزم حمله فیزیکی و عینی است و نمی تواند بصورت انتزاعی[10]وجود داشته باشد(Clive Walker; 2007; pp 625, 634).

[1]- Hiring and use
[2]- Physical attacks
[3]- “Hacktivism”3
[4]- Incitement to terrorism
[5]- “Cyberterrorism”
[6]-Cyber-Attack” and “Terrorism”
[7]- The suggestions include those concentrating on the disruptive and destabilizing nature of cyberterrorism, limiting it only to individuals and non-state perpetrators. See Daniel T. Kuehl, The National Information Infrastructure: The Role of the Department of Defense in Defending It, in TRANSNATIONAL THREATS: BLENDING LAW ENFORCEMENT AND MILITARY STRATEGIES 151 (Carolyn W. Pumphrey ed., 2000)
[8]- See Christopher Beggs, Cyber-Terrorism: A Threat to Australia?, in MANAGING MODERN ORGANIZATIONS THROUGH INFORMATION TECHNOLOGY: PROCEEDINGS OF THE 2005 INFORMATION RESOURCES MANAGEMENT ASSOCIATION INTERNATIONAL CONFERENCE 472 (2005); see Maura Conway, Cyberterrorism: Media Myth or Clear and Present Danger? 5 (2004), http://doras.dcu.ie/505/1/media_myth_2004.pdf
[9]- Malware writing process. See Alistair Kelman, The Regulation of Virus Research and the Prosecution for Unlawful Research?, 3 J. INFO. L. & TECH. (1997), available at http://elj.warwick. ac.uk/jilt/compcrim/97-3kelm/, cited in Mathias Klang, A Critical Look at the Regulation of Computer Viruses, 11 INT’L J. L. & INFO. TECH., 162, 167 (2003).
[10]-Abstract

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

در پیش نویس کنوانسیون بین المللی استنفورد برای افزایش حفاظت از جرایم سایبری و تروریسم در سال ۲۰۰۰[1]، تروریسم سایبری عبارت است از «استفاده عمدی یا تهدید به استفاده بدون مجوز قانونی از خشونت، اخلال یا هرگونه مداخله در سیستم‌های سایبری، زمانی که احتمال می‌رود چنین استفاده و کاربردی، منجر به مرگ یا جراحت شخص یا افراد، آسیب قابل توجّه به اموال فیزیکی، اختلالات اجتماعی و یا ورود ضرر فاحش اقتصادی و مالی شود(Abraham D. Sofaer; 2000; 26). برای قرار دادن این تعریف در چارچوب مورد اشاره، ضروری است که مشخص شود عاملان احتمالی چه کسانی هستند و در مورد تروریسم سایبری، چه مواردی احتمالاً هدف قرار می گیرند.

۲- عاملان[2] سایبر تروریسم

حملات سایبری بدون فناوری لازم و حداقلِ دانش نسبت به نحوه عملکرد شبکه های الکترونیکی غیرممکن است و غالباً بصورت تیمی و گروهی و بعضاً فوق حرفه ای و شبکه ای صورت می پذیرد.

الف.دولت کشورها

ادعای دخالت مستقیم احتمالی دولتها در اقدامات مرسوم تروریسم، زمانی که در چارچوب فضای سایبری دیده شود، کمتر واقعی بنظر می رسد. علیرغم آنکه پیش نویس کنوانسیون جامع در مورد این موضوع در بن بست باقی مانده[3]، هیچ یک از هجده سند حقوقی موجود، متضمّن بیان مسئولیت دولت در قبال اقدام تروریستی نیست؛ بنابراین ناگزیر برای راهنمایی و تحلیل موضوع باید به حقوق عرفی بین المللی[4] مراجعه کرد.

تروریسم دولتی، که حتّی می تواند به عامل افراط گرایی ضد دولتی مبدّل شود، می تواند در تعریف تروریسم مدنظر باشد؛ زیرا اولاً معنای تاریخی این مفهوم، متحوّل شده و اکنون متفاوت است. ثانیاً، اقدام دولت‌ها در مقایسه با بازیگران غیردولتی به ارتکاب عمل تروریستی، موجب آسیب و تخریب گسترده‌تر

[1]- Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism of 2000
[2]- Potential Perpetrators
[3]- Compare the western draft (“the activities undertaken by the military forces of a State in the exercise of their official duties, inasmuch as they are governed by other rules of international law, are not governed by this Convention”) with the OIC version (“The activities undertaken by the military forces of a State in the exercise of their official duties, inasmuch as they are in conformity with international law, are not governed by this Convention.”). See U.N. Rep. of the Ad Hoc Comm., 6th Sess., Jan. 28–Feb. 1, 2002, U.N. Doc. A/57/37 Annex IV; GAOR, 57th Sess., Supp. No. 37 (2002); see also U.N. Rep. of the Ad Hoc Comm., 14th Sess., Apr. 12–16, 2010, U.N. Doc. A/65/37; GAOR, 65th Sess., Supp. No. 37 (2010). For more information, also see previous and subsequent reports. Note that the Maritime Convention as amended by the 2005 Protocol (Article 2bis(2)), 2005 Nuclear Terrorism Convention (Article 4(2)), 2010 New Civil Aviation Convention (Article 6(2)) and the Unlawful Seizure Convention as amended by the 2010 Protocol (Article 3bis(2)) all use the western wording.
[4]- International customary law for guidance

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

می‌شود. ثالثاً أشکال خاصی از خشونت علیه غیرنظامیان به عنوان بخشی از کمپین های ضد تروریسم رخ می دهد.[1]

تروریسم دولتی را می توان به دو دسته داخلی و خارجی تقسیم کرد. در چارچوب تاریخی، «تروریسم دولتی داخلی» مستلزم استفاده از زور یا توسّل به زور علیه جمعیت غیرنظامی خود برای تضعیف روحیه و از بین بردن تمایل به مقاومت در برابر اراده دولت است؛ در حالیکه «تروریسم دولتی خارجی»، جمعیت های خارجی را هدف قرار می دهد. حملات علیه غیرنظامیان از آن جهت که بسیار ناکارآمد خواهند بود، بسیار بعید است؛ زیرا اولاً، إعمال «مجازات» نسبت به این گروه از افراد بصورت فیزیکی آسان تر است و رعب و ترس بیشتری ایجاد می کند و ثانیاً، بخش قابل توجّهی از زیرساخت های غیرنظامی معمولاً متعلّق به خود دولت است. در شرایطی که دولت‌ها به دلیل اشغال خارجی یا جنگ داخلی، کنترل مؤثری بر بخشی از قلمرو خود ندارند، کنوانسیون‌های ژنو به طور خودکار إعمال می‌شوند و خشونت دولتی[2] باید در چارچوب حقوق بشردوستانه بین‌المللی مورد بررسی قرار گیرد.

ب. بازیگران غیردولتی

بازیگران غیردولتی به عنوان گروه هایی تلقّی می شوند که قادر به انجام اقدامات تروریستی هستند و این وضعیت امروزه، ناشی از حقوق عرفی بین المللی است. این نکته در تعدادی از اسناد شورای امنیت سازمان ملل متحد، به ویژه قطعنامه ۱۵۲۶ مکرراً مطرح شده است.[3] محکومیت شبکه القاعده[4] و سایر گروه های تروریستی مرتبط با آن در قطعنامه ۱۵۳۰ بعلّت ارتکاب اقدام تروریستی جنایتکارانه، محکومیت حملات گروه تروریستی ETA در بمب گذاری در شهر مادرید، قطعنامه های۱۹۸۹ و ۱۹۶۳ در ابراز نگرانی راجع به افزایش حواد-ث آدم ربایی و گروگانگیری توسط گروه های تروریستی جملگی مؤید رویکرد این نهاد بین المللی نسبت به موضوع است.

در جهان مدرن معاصر، بیش از صد سازمان تروریستی بین‌المللی از گروه‌های کوچکی نظیر فیانا عایران، حرکت‌الجهاد الاسلامی، مجاهدین خلق ایران، که توسط چند کشور تعیین شده‌اند تا گروه‌هایی

[1]- By the 2010 Protocol (Article 3bis (2)) all use the western wording. See RICHARD JACKSON, LEE JARVIS, JEROEN GUNNING & MARIE BREEN SMYTH, TERRORISM: A CRITICAL INTRODUCTION (2011)
[2]- State violence
[3]- See S.C. Res. 1989, U.N. Doc. S/RES/1989 (June 17, 2011); S.C. Res. 1988, U.N. Doc. S/RES/1988 (June 17, 2011); S.C. Res. 1963, U.N. Doc. S/RES/1963 (Dec. 20, 2010); S.C. Res. 1904, U.N. Doc. S/RES/1904 (Dec. 17, 2009); S.C. Res. 1822, U.N. Doc. S/RES/1822 (June 30, 2008); S.C. Res. 1735, U.N. Doc. S/RES/1735 (Dec. 22, 2006); S.C. Res. 1617, U.N. Doc. S/RES/1617 (July 29, 2005); S.C. Res. 1530, U.N. Doc. S/RES/1530 (Mar. 11, 2004); S.C. Res. 1526, U.N. Doc. S/RES/1526 (Jan. 30, 2004); S.C. Res. 1455, U.N. Doc. S/RES/1455 (Jan. 17, 2003); S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001).
[4]- Al-Qaida network

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

بزرگی نظیر القاعده، لشکر طیبه، اسباط الانصار، داعش و غیره، که بطور گسترده به عنوان سازمان تروریستی شناخته می‌شوند، وجود دارند که پناهگاه امن سایبری زیادی ایجاد نمودند تا بتوانند بدون ترس از انتقام‌جویی مستقیم، در آنجا فعالیت کنند.(Kenneth Geers; 2010; 547)[1]به همین جهت، موفقیت در عملیات ضد تروریستی نیز احتمالاً این بازیگران غیردولتی را به روی آوردن به تروریسم سایبری ترغیب می کند و برخی گروه ها که پناهگاه فیزیکی خود را در مناطق کلیدی و مهم از دست داده اند، به پناهگاه فضای مجازی روی آورده اند.(Gabriel Weimann; 2004, at 1, 11)

ج. شرکت ها

شرکت‌ها[2]،مدت‌هاست که هدف حملات سایبری قرار گرفته‌اند. این موضوع اکنون منجر به نوعی ناامنی فناوری اطلاعات شده و متقابلاً به نوبه خود منجر به تمایل شرکتها به استفاده از پیشرفته‌ترین قابلیت‌های دفاع سایبری و احیاناً حمله سایبری متقابل گردید که بسیار فراتر از امنیت دفاعی کشورها است. امروزه با دور شدن از «دولت‌گرایی[3]»، دانش فنّی، استقلال نسبی عملیات، بودجه قابل توجّه و تیمی ساختاریافته از کارشناسان و متخصصان، شرکت‌ها را به عامل بالقوّه اقدامات تروریستی سایبری تبدیل کرده است.[4] اگرچه حملات سایبری آنها احتمالاً رقبا را هدف قرار می دهد،[5] معذالک به ویژه شرکتهای چندجانبه ممکن است برای کسب سود بیشتر، علاقه مند به بی ثبات کردن اقتصاد کشورها و یا حتّی اقتصاد کل جهان باشند. بعضاً نیز احتمال می رود که برخی شرکتها حتّی تحت دیدگاه های افراطی رهبری خود هدایت شده و مبادرت به ارتکاب حملات تروریستی نمایند.

با این وجود، برخلاف سازمان‌های تروریستی، شرکت‌ها اغلب در اجرای اصل شفافیت نسبت به عملکرد مربوطه[6]و حفظ شخصیت حقوقی در کشور میزبان، اغلب تحت فشار قرار می‌گیرند تا شفاف‌تر باشند. اگرچه این امر مانع رفتار مجرمانه و ارتکاب اعمالی چون سایبرتروریسم در بستر وب نمی شود؛ لیکن آنها را به دسته خاصی از بازیگران غیردولتی («هر شخص»[7]) تبدیل می کند که می توانند از نظر قانونی

---

[1]- Also See, Gabriel Weimann, Cyberterrorism: How Real Is the Threat?, U.S. INST. OF PEACE, Dec. 2004, at 1, 11. AND. Stuart H. Starr, Towards and Evolving Theory of Cyberpower, in THE VIRTUAL BATTLEFIELD: PERSPECTIVES ON CYBER WARFARE, 18, 34 (Christian Czosseck & Kenneth Geers eds., 2009).
[2]- Corporations
[3]-Statecentrism
[4]- PST), http://www.zdnet.com/news/security-guru-lets-secure-the-net/120859. 78. Toby Blyth, Cybertrrorism and Privet Corporations: New Threat Models and Risk Management Implications 24 (1999).
[5]- Id. At 105.
[6]- United Nations Conference on Trade and Development, Geneva, Switz., 2004, Disclosure of the Impact of Corporations on Society: Current Trends and Issues, UNCTAD/ITE/TEB/2003/7 (Aug. 26, 2004).
[7]- Any Person

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

مسئول جرائمی قلمداد شوند که در کنوانسیونهای ضد تروریسم موجود، جرم شناخته شده اند. به عبارت دیگر، جدای از رهبری شرکت و اعضای تیم فناوری اطلاعات که مستقیماً در تروریسم سایبری دخالت داشتند، در صورت اجازه سیستم های قانونی مربوطه، می توان خود شرکت را تحت پیگرد[1] قانونی قرار داد.

د.افراد

در نظام فعلی حقوق بین الملل، امروزه افراد نیز بعنوان تابعان حقوق بین الملل شناخته می شوند(اکهرست؛۱۳۷۳؛ صص ۹۹ ـ ۹۸) و ممکن است همانند گروه‌های مجرم سایبری مستقل، در صورت وجود انگیزه هایی مادی یا معنوی مثل پول، اعتبار یا ایدئولوژی، در فضای مجازی مأخوذ به اینترنت مرتکب اقدامات تروریستی شوند[2]. لازمه این امر برای انجام حملات آنلاین یا به تنهایی است(Sean M. Condron; 2007; pp 404, 406) و مانند همتایان کمتر پیچیده خود، می توان آنها را به دسته هایی که البتّه انگیزه های آنها را نیز آشکار می کند تقسیم کرد.

تروریست های ذهنی و عقیدتی (افرادی که به دنبال رضایت در نیاز به کنترل هستند)، تروریست های مذهبی و سیاسی قومی–جغرافیایی (مبارزه برای یک «علّت گروهی»)، و تروریست‌های انتقام‌جو (افرادی که علیه خود، خانواده یا جامعه خود متحمّل جنایت شده‌اند) و یا «شورشیان[3]» (که به کل نظم جهانی اعتراض می کنند؛ این دسته شامل مجرمان سایبری نوجوان نیز می شود)(Raymond H; 2004; 174)

آنچانکه بیان شد، از منظر رژیم معاهده ای موجود در مورد تروریسم، امکان پیگرد قانونی افراد به دلیل تروریسم (و تروریسم سایبری به عنوان زیرمجموعه آن) وجود دارد. البتّه باید توجّه داشت که اگر این تروریست‌های سایبری در راستای منافع دولت عمل کنند، دولت‌ها ممکن است منافعی در اجتناب از پیگرد تروریست‌های سایبری «با استعداد»[4] داشته باشند؛ بگونه ای که حتّی می توان آنها را به دلیل کمبود متخصصان سایبری، به عنوان دارایی های محدود دولتی محسوب نمود.(Jeffery Carr; 2009; 29). اگرچه این رویکرد دولتها، در واقع مغایر روح قانون اساسی کشورها و نقض تعهّدات بین المللی آنها می باشد و احتمالاً می تواند به عنوان حمایت دولتی از تروریسم سایبری تلقّی شود.

۳. دلایل تروریسم سایبری در جهان معاصر

[1]- Prosecute the Company
[2]- Like Cyber-Breiviks
[3]- Rebels
[4]- Talented” Cyberterrorists

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

افراط گرایان برای توسّل به تروریسم سایبری، دلایل ثانویه زیادی دارند که به تضعیف قابلیت های عملیاتی «دشمن» کمک کرده و اعتبار یک سازمان، ملّت یا اتّحادیه بین المللی را از بین می برد و نشان می دهد که قادر به وارد کردن صدمات قابل توجّه به اهداف خود هستند و حتّی افراد مورد حمله را متقاعد می کند که وابستگی خود را تغییر دهند.(Abdul Jalil; 2003). در تروریسم سایبری، اهدافی نظیر کنترل‌های ترافیک هوایی و رایانه‌های ناوبری در هواپیماها و کشتی‌های تجاری، نیروگاه‌های اتمی و تأسیسات غنی‌سازی مواد هسته‌ای ممکن است مستعد حمله باشند. حملات متعارف علیه این اهداف توسط بازیگران غیردولتی در حال حاضر کاملاً در کنوانسیونهای ضد تروریسم موجود و پروتکل های مربوط، جرم انگاری شده است. پست های برق، شبکه های تامین آب و کارخانه های آماده سازی خودکار مواد غذایی، شبکه های حمل و نقل «هوشمند»، بانک ها و بورس ها، سدها، ماشین ها و موتورهای کامپیوتری، خطوط لوله گاز و نفت، کنترل های ناوبری فضایی، موسسات پزشکی و تجهیزات پزشکی در زمره سایر اهداف آسیب پذیرند و حمله سایبری علیه این اهداف ممکن است منجر به حدوث اثرات تروریستی شود و به ایجاد تشویش اذهان عمومی در بین مردم بیانجامد.

تبیین موضوع در قالب مصادیقی که می تواند علیرغم آنکه موضوع و هدف حملات سایبری باشد؛ لیکن به جهت تمهید بسترهای مطمئن و پدافندی، مانع حمله سایبری شده و نتیجتاً از بروز حوادث و آثار بسیار خطرناکی برای کشوری که در معرض این حملات قرار می گیرد، مصون بماند، می تواند به شناخت بیشتر موضوع رهنمون گردد؛ لذا بطور اجمال به بررسی آنها پرداخته می شود.

الف. ساخت مواد منفجره

وفق ماده ۲ کنوانسیون مواد منفجره پلاستیک(۱۹۹۱)[1] ساختن مواد منفجره بدون علامت، ممنوع و جرم است. از لحاظ تکنیکی، اگر رایانه‌های موجود در تأسیسات ساخت مواد منفجره، به نحوی اشتباه درگیر فرآیند آماده‌سازی باشند و نقص برنامه، منجر به علامت‌گذاری اشتباه روی مواد شود، مواد منفجره ساخته شده قبل از اینکه برای فروش یا استفاده رها شوند، بطور کامل توسط کارکنان بررسی و کنترل می‌شوند. علاوه بر این، از آنجاکه فرآیند ساخت هم توسط همان افرادی که حملات سایبری را انجام می دهند، انجام نمی شود، لذا مسئولیت کیفری به دلیل عدم وجود آگاهی نسبت به موضوع، منتفی است.

ب. بمباران

[1]- ICAO, 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection, June 21, 1988, ICAO Doc. S/22393, 30 I.L.M. 721.

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

وفق مفاد کنوانسیون ۱۹۹۷ بمباران تروریستی،[1] تحویل غیرقانونی و عمدی، در معرض قرار دادن، یا منفجر کردن هرگونه مواد منفجره یا سایر وسایل کشنده در داخل یک مکان عمومی یا تأسیسات دولتی، سیستم حمل و نقل عمومی یا تأسیسات زیربنایی یک کشور، ممنوع و جرم است. مطابق بند ۳ ماده ۱ این کنوانسیون، «منفجره یا سایر وسایل کشنده» به معنای؛ الف) سلاح یا وسیله ای منفجره یا آتش زا است که برای مرگ، ایراد صدمات جدی بدنی یا آسیب مادی قابل توجه طراحی شده یا توانایی ایجاد آنرا دارد. ب) سلاح یا وسیله ای که از طریق انتشار، انتشار یا تأثیر مواد شیمیایی سمی، عوامل بیولوژیکی یا سموم یا مواد مشابه یا تشعشعات یا مواد رادیواکتیو برای مرگ، ایراد صدمات جدی بدنی یا آسیب مادی قابل توجّه طراحی شده یا توانایی ایجاد آنرا دارد.

«تحویل» و «قرار دادن/ در معرض قراردادن » این سلاح‌ها یا وسایل، یک عمل فیزیکی است که از طریق فضای مجازی قابل انجام نیست. آنها بندرت قبل از «تحویل» توسط یک عامل قانونی مجاز به تخلیه و انفجار، مسلح و بندرت از طریق وسایل الکترونیکی منفجر می شوند؛ بلکه بجای آن، از محرک های شیمیایی، مکانیکی یا الکتریکی استفاده می شود. لذا موارد مذکور نمی توانند مورد حمله سایبری قرار بگیرند.

واقعه حمله سایبری به خط لوله گاز طبیعی ترانس سیبری در سال ۱۹۸۲[2]، تفسیر جامع تری از کلمه «دستگاه»[3] در کنوانسیون مطرح کرد. این واقعه، ثابت کرد حمله سایبری علیه یک دستگاه غیرنظامی که بخشی از زیرساخت انرژی نفت و گاز است، می تواند منجر به انفجار شود. اما آنچه در چنین حالتی «منفجر می شود» و «تخلیه می شود»، گاز یا بنزین است؛ بنابراین، خود وسیله مورد بهره برداری، ظرفیت انفجار را ندارد؛ زیرا در آن مواد منفجره بکار نرفته است. معذالک، رایانه‌های موجود در راکتورهای هسته‌ای و آزمایشگاه‌های

---

[1] – کنوانسیون بین المللی برای سرکوب بمب گذاری های تروریستی، ماده. ۲(۱)، ۱۵ دسامبر ۱۹۹۷، «هر شخصی مرتکب جرمی در مفهوم این کنوانسیون می شود اگر آن شخص به طور غیرقانونی و عمدی یک ماده منفجره یا سایر وسایل کشنده را در، داخل یا علیه یک مکان استفاده عمومی، یک تأسیسات دولتی یا دولتی، یک سیستم حمل و نقل عمومی یا یک تأسیسات زیربنایی تحویل، جاگذاری، تخلیه یا منفجر می کند: الف. به قصد ایجاد مرگ. یا صدمات جدی بدنی؛ یا ب) به قصد ایجاد تخریب گسترده در چنین مکان، تأسیسات یا سیستمی، در صورتی که چنین تخریبی منجر به خسارات اقتصادی عمده شود یا احتمالاً منجر به آن شود. ر.ک.http://treaties.un.org/doc/db/Terrorism/english-18-9.pdf

[2]- Cyber-attack on the Trans-Siberian natural gas pipeline in 1982

[3]- “Device”

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

بیولوژیکی ممکن است مشمول تعریف ماده ۱ (۳) (ب) قرار گیرند(Aviv Cohen, L; 2010; 1, 27-28. Also. Id. at 28).

در این ماده، دستگاهی که توانایی ایجاد مرگ، آسیب و آسیب از طریق انتشار سموم یا تشعشعات را دارد، مدنظر است و از این جهت، این رایانه ها، سطح «دما، رطوبت، تشعشع و سایر داده هایی که برای ایمنی بسیار مهم است» را کنترل می کنند و اگر مورد حمله سایبری قرار گیرند، می توانند فرمان انفجار بدهند؛ لذا در صورت ارتکاب یک اقدام تروریستی سایبری، می توانند باعث فاجعه مهیب انسانی گردند.

اگرچه کوهن در تبیین نظر خود با استناد به ماده ۳۱ کنوانسیون وین در مورد حقوق معاهدات، معتقد است کلمات کنوانسیون بمب گذاری تروریستی، باید در پرتو هدف آن تفسیر شود؛ لیکن باید توجّه داشت که مطابق بند ۱ ماده ۳۱ کنوانسیون وین، بهنگام تفسیر متن هر معاهده ای، باید به «شرایط معاهده»، «معنای عادی» داد و متن معاهده را در سیاق عبارات و معنای متداول کلمات مربوط، در پرتو هدف معاهده تفسیر نمود. ضمن آنکه به اقتضای شرایط زمانی تصویب کنوانسیون بمب‌گذاری تروریستی، وفق بند «الف» ماده ۳۲ کنوانسیون وین شرایط نتیجه گیری موضوع بحث، با توجّه به هدف و روح کنوانسیون مذکور، جلوگیری از بمب گذاری های سنّتی است، نه تروریسم سایبری؛ لذا موقعیتی برای تروریست های سایبری فراهم نیست تا أعمال ارتکابی آنان نقض کنوانسیون بمب گذاری تروریستی تلقّی شود.(SIMON CHESTERMAN; 2001; 48)

ج. افراد محافظت شده و گروگانگیری

وفق کنوانسیون ۱۹۷۳ ماموران دیپلماتیک[1]، ارتکاب عمدی «قتل، آدم ربایی یا هر حمله به شخص یا آزادی یک فردِ تحتِ حمایت بین المللی یا حمله خشونت آمیز به اماکن رسمی، مسکن و حریم خصوصی یا وسایل حمل و نقل بین المللی» جرم است.[2]به خطر انداختن تمامیت جسمانی یا آزادی شخص محافظت شده، اعم از قتل یا جرح و هر حمله دیگر، رفتار ممنوعه ای است که وابسته به وسیله مورد استفاده نیست و می تواند به شکل تخریب وسایل حمل و نقل آن شخص، از کار انداختن کامپیوتر بیمارستان، آلوده کردن دستگاه پزشکی، انفجار کامپیوتری یا یک عمل مُضِرّ مشابه باشد.

نظر به اینکه صدمات وارده باید پیامد مستقیم یک حمله سایبری باشد تا «عمدی» تلقّی گردد، أعمالی مانند مسمومیت عمومی با غذا یا آب از طریق وسایل سایبری، مشمول موارد ممنوعه مقرر در این کنوانسیون

[1]- The 1973 Diplomatic Agents Convention
[2]- Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, art. 2(1), Dec. 14, 1973, 1035 U.N.T.S. 167.

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

نمی شود.[1]همین اصل در مورد حملات سایبری علیه اماکن، محل سکونت یا وسایل حمل و نقل نیز صدق می کند. این حملات باید مستقیم باشند و جان فرد محافظت شده را تهدید کنند تا تروریسم سایبری محقق شود. ربودن مقامات دولتی و اعضای خانواده‌های آنها به دلایلی مشابه با گروگان‌گیری معمولی، در زمره تروریسم قرار نمی گیرد؛ اگرچه به دام انداختن افراد محافظت‌شده در ماشین یا آسانسور رایانه‌ای از مصادیق «هر حمله دیگری به آزادی[2]» محسوب می‌شود.

وفق کنوانسیون گروگانگیری(۱۹۷۹)[3]؛ «هر فردی که به منظور اجبار شخص ثالث.....انجام یا خودداری از انجام هر عملی به عنوان شرط صریح یا ضمنی برای آزادی گروگان....شخص دیگری را دستگیر یا بازداشت و تهدید به کشتن، مجروح کردن یا ادامه بازداشت کند.....مستوجب مجازات متناسب است».

البتّه امکان گروگان گرفتن افراد از طریق حملات سایبری «محض» تقریباً غیرممکن است و تروریست‌ها، در موارد نادری، ممکن است بتوانند فردی را در یک ابزار با تکنولوژی پیشرفته مانند آسانسور یا ماشین کامپیوتری دستگیر کنند، اما احتمال زخمی کردن یا ادامه بازداشت او امری بسیار بعید است. آسانسورهای هیدرولیک و سایر آسانسورها از وسایل مکانیکی (از جمله ترمز) استفاده می کنند و هرگونه خطر فیزیکی ناشی از حملات سایبری را از بین می برند و می توان با شکستن شیشه های وسایل نقلیه و یا باز کردن و درهای آسانسور به صورت دستی، اشخاص گرفتار را نجات داد.

د.کشتی های دریایی

در وضعیت فعلی پیشرفتهای تکنولوژیکی، فنآوری دریانوردی کشتیهای دریایی[4]، بگونه ای است که امکان کنترل کامل یک کشتی[5] از طریق حملات سایبری وجود ندارد و حتّی اگر یک خرابکار سایبری در کشتی از درایو فلش یو اس بی آلوده به ویروس استفاده کند، این دستگاه یو اس بی نیست که ناوبری ایمن را به خطر می اندازد، بلکه خود برنامه و در واقع یک شی مجازی آلوده می شود، نه سیستم ناوبری و دستگاه، بعنوان شیء فیزیکی. بنابراین، نقض ماده ۱۰۴ کنوانسیون نیز عملاً غیر ممکن است.

مجروح کردن یا کشتن یک فرد به قصد انجام یک حمله تروریستی در کشتی، در ماده ۳ کنوانسیون[6] ممنوع شده و جرم محسوب می گردد. هر «اقدام خشونت آمیزی هم علیه هر شخص در کشتی، در صورتیکه

[1]- *See* Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents, at art. 1(1)(a) (describing protected persons)
[2]- Other attack upon liberty."
[3]- International Convention Against the Taking of Hostages, art. 1(1) & 2, Dec. 17, 1979, 1316 U.N.T.S. 207.
[4]- *Maritime Vessels*
[5]- *See id*. at art. 1(1)(a) (explaining that warships, naval auxiliary ships, vessels of customs or police authorities and ships withdrawn from navigation are not covered by the Maritime Convention).
[6]- Article 3(1)(b)

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

این عمل ناوبری ایمن را به خطر اندازد، نوعی حمله تروریستی محسوب می گردد. بنظر می رسد آستانه حمله موضوع بند(ب) جزء ۱ ماده ۳ کنوانسیون[1] شامل حمله علیه همه افراد دارای دانش حیاتی و یا اقدام به روشی است که بخش مهم مورد نیازِ ناوبری ایمنِ کشتی را ویران کند. در اینصورت، چنین أعمالی، مصداق تروریسم مورد نظر کنوانسیون تلقّی خواهد شد که در واقع یک چشم انداز تقریباً غیرممکن است.

این وضعیت در مورد احتمال بعید آسیب به کشتی یا محموله آن از طریق حملات سایبری، که در ماده ۳ (۱) (ج)[2] ممنوع شده، نیز صدق می کند. همچنین ارسال اطلاعات نادرست برای به خطر انداختن ایمنی کشتی تحت عنوان جنایت ارتکابی مندرج در بند ۱ ماده ۳ (و)[3] از طریق حملات سایبری، در مواردی که کشتی، جدید است، بسیار محتمل است؛ معذالک، نظر به اینکه کشتی های جدید برای ناوبری به شدّت به فناوری رایانه متّکی می باشند، تحقّق این امر تقریباً غیر محال نیست.

۷.تروریسم هسته ای[4]

از جمله أعمال جرم انگاری شده در جزء ۷ بند (۱) ماده ۱۱۳ کنوانسیون مواد هسته ای مصوب ۱۹۸۰(اصلاح شده در سال ۲۰۰۵)، دریافت، تملّک، استفاده، انتقال، تغییر، دفع، سرقت، اختلاس، تحصیل و ربایش با قصد متقلّبانه، حمل، ارسال یا جابجایی مواد هسته ای است؛ لیکن تلقّی این أعمال بعنوان تروریسم سایبری، هرچند امری غیرممکن نیست، اما بعید است؛[5] کمااینکه در مورد کنوانسیون مواد هسته ای[6] نیز برخی أعمال فیزیکی مانند در اختیار داشتن مواد رادیواکتیو، ساخت یا در اختیار داشتن یک وسیله هسته ای یا استفاده از دستگاه هسته ای، بموجب ماده ۲ (۱) کنوانسیون تروریسم هسته ای ۲۰۰۵[7]، از چارچوب تروریسم سایبری مستثنی هستند. با اینحال، در این کنوانسیون، وفق بند (ب) جزء ۱ ماده ۲، آسیب رساندن به تأسیسات هسته‌ای و یا استفاده از آن به نحوی که خطر انتشار آن را به دنبال داشته و یا منجر به انتشار مواد رادیواکتیو گردد، ممنوع شده است.

برخلاف بند (ه) ماده ۷ اصلاحی کنوانسیون تروریسم هسته ای، جنایت، در صورتیکه توأم با قصد ایجاد مرگ، جراحت یا خسارت ارتکاب یافته باشد، یک اقدام تروریستی خواهد بود. وادار کردن یک

---

[1]- *See id*. at art. 3(1)(b), which reads: "performs an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of that ship.". *See id*. at art. 3(1)(c), which reads: "destroys a ship or causes damage to a ship or to its cargo which is likely to endanger the safe navigation of that ship."
[2]- By Article 3(1)(c).
[3]- *See id*. at art. 3(1)(f), which reads: "communicates information which he knows to be false, thereby endangering the safe navigation of a ship."
[4]- Nuclear Terrorism
[5]- Consider if the US B-52H bomber, that was mistakenly transferring nuclear warheads in 2007, was connected to the internet and hijacked by cyberterrorists.
[6]- Nuclear Materials Convention
[7]- Article 2(1) of the 2005 Nuclear Terrorism Convention

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

شخص حقیقی یا حقوقی و یا یک سازمان بین المللی یا یک دولت، به انجام یا خودداری از انجام هر اقدامی در اینخصوص، در این تعریف می گنجد.[۱]

حمله سایبری تحت عنوان استاکس نت[۲]، علیرغم آسیب جزئی، از آن جهت که متضمّن تخریب سانتریفیوژها و خطر انتشار مواد رادیواکتیو ولو در مقادیر کم بود، در زمره این مفهوم تروریسم در کنوانسیون قرار می گیرد؛ زیرا بنظر می رسد یکی از اهداف حمله مذکور، آن بوده که جمهوری اسلامی ایران برنامه هسته ای خود را تعطیل نماید. بنابراین، استفاده از استاکس نت علیه تأسیسات هسته ای ایران، نقض تعهّدات مقرر در کنوانسیون تروریسم هسته ای بوده و در اصل، اولین اقدام سایبری تروریسم هسته ای در دوران معاصر نظام بین المللی است. با این وجود، این موضوع، تنها از منظر از نقطه نظر استنباط حقوقی از مفاد کنوانسیون و از لحاظ عرفی صادق است؛ زیرا نه ایران و نه «مظنونین» بالقوّه – اسرائیل و ایالات متحده – تا سال ۲۰۱۱ کنوانسیون تروریسم هسته ای را تصویب و امضا نکرده بودند؛ لذا از این جهت، موضوع از منظر حقوقی قابل تعقیب نبود؛ لیکن این امر بمنزله عدم انطباق رفتار ارتکابی با منطوق و مفهوم مقررات کنوانسیون نیست و اخلاقاً سبب مبرا بودن تروریستها از مسئولیت کیفری نیست.

۸.هواپیماها

تروریسم سایبری در ارتکاب جرایم علیه هواپیماها[۳] نیازمند حضور شخص در هواپیما بهنگام پرواز نیست. حملات سایبری علیه هواپیماها بیشتر از طریق شبکه‌های الکترونیکی و یا حداقل با نصب برنامه‌های مُضرّ قبل از پرواز صورت می پذیرد؛ زیرا شخص تروریست که بنحوی خودش را به کابین خلبان می‌رساند، می‌تواند هواپیما را بدون هیچ برنامه‌ای سریع‌تر ساقط کند. امروزه بدلیل استفاده از دستگاههای مخابراتی بی‌سیم، جنایتکاران قادر به کنترل یک هواپیمای معمولی سرنشین دار نیستند. علاوه بر این، جنایتکاران و تروریستها این احتمال را می دهند که وسایل مشکوک داخل هواپیما، بطور معمول ممکن است توسط خدمه هواپیما کشف و مصادره و یا نابود شوند. لذا این موارد مشمول کنوانسیون تصرف غیرقانونی ۱۹۷۰[۴] بوده و از عنوان حملات سایبری مستثنی هستند.

---

[۱] – ماده ۲ (۱) (ب).(i i i)

[2]- Stuxnet

[3]- Aircrafts

[4]- Convention for the Suppression of Unlawful Seizure of Aircraft, supra note 26, at art 1 (criminalizing the act of seizing and exercising control over an aircraft).

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

بطور کلی، وفق ماده ۶ (۱) کنوانسیون هوانوردی ۱۹۶۳[1] فرمانده هواپیما اجازه دارد اقدامات معقولی را نسبت به افرادی که مظنون به خطر انداختن ایمنی در هواپیما هستند؛ از جمله کسانی که سعی در انجام یک حمله سایبری دارند، إعمال کند. از سوی دیگر، وفق ماده ۱ (۱) کنوانسیون توقیف غیرقانونی[2]، که در پروتکل ۲۰۱۰[3] آن گنجانده شده، حضور شخص در داخل هواپیمای در حال پرواز الزامی نیست و توقیف هواپیما «به هر وسیله فنّی» از جمله حمله سایبری، جرم محسوب می شود. پروتکل ۲۰۱۰ در مواد ۱ و ۳ عبارت «هواپیمای در حال پرواز» را با عبارت «هواپیمای در حال خدمت»[4] که در واقع شامل مرحله آماده سازی هواپیما تا بیست و چهار ساعت پس از فرود می شود، جایگزین کرده است. لذا حکم مقرر درباره عدم لزوم حضور مظنون به ارتکاب جنایت در داخل هواپیمای در حال پرواز، در خصوص این گروه از هواپیماها نیز صادق است.

بهرحال، آنچنانکه ذکر شد، هیچ حمله سایبری نمی تواند کنترل مؤثری بر هواپیمای سرنشین دار ایجاد کند. با اینحال، بر اساس متن اصلاح شده کنوانسیون، امکان ارتکاب یک عمل تروریستی سایبری با در دست گرفتن کنترل وسایل نقلیه هوایی بدون سرنشین وجود دارد. کمااینکه هواپیماهایی مانند پهپادهای هدایت شونده از راه دور[5] که برای اهداف مختلف در بیش از پنجاه کشور مورد استفاده قرار می‌گیرند، بعلّت آنکه ایستگاه‌های کنترل آنها در معرض حمله تروریستی قرار گرفته و آلوده شده باشند، ممکن است «ربوده شوند»(Jack M. Beard; 2009; 409, 444)[6]. معذالک، از آنجاکه بند ۲ ماده ۳ کاربرد کنوانسیون توقیف غیرقانونی را برای هواپیماهای نظامی، گمرکی و پلیس[7] مستثنی می کند، وقوع تروریسم سایبری تحت این سند، تنها در صورت إعمال کنترل غیرقانونی بر پهپادهای تجاری، غیر نظامی و علمی امکان پذیر است.

طبق ماده ۱ کنوانسیون ۱۹۷۱ هواپیمایی کشوری، قرار دادن یا در معرض گذاردن هر وسیله یا شیء مستعد ارتکاب عمل خرابکارانه در هواپیما، جرم است. انجام این عمل از طریق فضای سایبری غیرممکن

[1]- Article 6(1) of the 1963 Aviation Convention
[2]- See Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft, at art. II, which reads: "Any person commits an offence if that person unlawfully and intentionally seizes or exercises control of an aircraft in service by force or threat thereof, or by coercion, or by any other form of intimidation, or by any technological means."
[3]- Article 1(1)124 of the Unlawful Seizure Convention, included in its 2010 Protocol
[4]- Article 3(1) of the Amended Unlawful Seizure Convention reads: "For the purposes of this Convention, an aircraft is considered to be in service from the beginning of the pre-flight preparation of the aircraft by ground personnel or by the crew for a specific flight until twenty-four hours after any landing. In the case of a forced landing, the flight shall be deemed to continue until the competent authorities take over the responsibility for the aircraft and for persons and property on board." Id. at art. V.
[5]- Unmanned Aerial Vehicles (UAVs).
[6]- These countries include the USA, Russia, China, France, Germany, Georgia, India, Israel, Pakistan, Egypt, and others.
[7]- See also Noah Shachtman, Computer Virus Hits US Predator and Reaper Drone Fleet, ARS TECHNICA (Oct. 7, 2011), http://arstechnica. com/business/news/2011/10/exclusive-computer-virus-hits-drone-fleet.ars.

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

است. همانطور که در کنوانسیون توقیف غیرقانونی و پروتکل ۲۰۱۰ آن، انجام یک عمل خشن سایبری علیه یک شخص در هواپیمای در حال خدمت، به نحوی که ایمنی هواپیما را به خطر بیندازد، نیازمند حضور مرتکب در هواپیما نیست، در اینجا نیز ممکن است مرتکب با استفاده از وسایل الکترونیکی، یک کلید کنترل کننده ناوبری هواپیما را هدف قرار دهد. معذالک، نظر به حرکت مداوم هواپیما در ارتفاعات بالا، انجام حمله سایبری از زمین دشوار است و بنظر می رسد، حمله سایبری از سوی یکی از مسافران و بصورت مخفیانه میسّر باشد. با اینحال، شانس موفقیت آمیز بودن حمله سایبری از داخل هواپیما کم است.[1]

انجام عمل تروریستی علیه یک فرد خاصی که سوار بر هواپیما است، می تواند از طریق تخریب یا ایجاد خسارت قابل توجّه به کل هواپیما هم انجام بپذیرد. وفق ماده ۱ کنوانسیون در زمینه تروریسم سایبری، چنین آسیبی می تواند در نتیجه یک نقص فنّی ناشی از یک حمله سایبری (مثلاً انفجار سوخت هواپیما) یا در اثر برخورد هواپیما با زمین، به دلیل تداخل سایبری در عملکرد تاسیسات ناوبری آن هواپیما رخ دهد. همچنین می تواند با ارسال اطلاعات اشتباه به خلبانان و یا مسئول کنترل ترافیک هوایی (در مورد هواپیمای سرنشین دار) و یا به ایستگاه های کنترل پهپادها صورت بپذیرد[2]؛ لیکن آنچه اهمّیت دارد، شمول صدق عنوان تروریسم سایبری به چنین عمل جنایتکارانه ای است که سبب تخریب هواپیما و احیاناً قتل و یا آسیب جسمانی اشخاص می گردد.

نتیجه

با توجّه به ظهور و تحوّل روزافزون فناوری های نوین در حوزه بین الملل و جهانی شدن پدیده تکنولوژی مدرن، این امر در حوزه تروریسم نیز تغییراتی را در تبیین تعریف آن ایجاد نموده، بگونه ای که أشکال نوظهور سایبرتروریسم با احتمالات قریب الوقوع در بستر وب امکانپذیر است.

آنچنانکه بیان شد، تحلیل ماهیت سایبرتروریسم در دنیای پُست مدرن، دغدغه جنگ اطلاعاتی را به مثابه نبرد رایانه ای گوشزد می نماید. سایبر تروریسم، بعنوان یکی از تهدیدات امنیتی که در حوزه داخل و خارج

[1]- See Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, supra note 2, at art. 1(1)(c), which reads: "Any person commits an offence if he unlawfully and intentionally . . . [p]laces or causes to be placed on an aircraft in service, by any means whatsoever, a device or substance which is likely to destroy that aircraft, or to cause damage to it which renders it incapable of flight, or to cause damage to it which is likely to endanger its safety in flight." 129. Id. at art 1(1)(a), which reads: "performs an act of violence against a person on board an aircraft in flight if that act is likely to endanger the safety of that aircraft

[2]- Id. at art. 1(1) (b), which reads: "destroys an aircraft in service or causes damage to such an aircraft which renders it incapable of flight or which is likely to endanger its safety in flight." ALSO Id. at art. 1(1) (d), which reads: "destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight." SEE ALSO Id. at art. 1(1) (e), which reads: "communicates information which he knows to be false, thereby endangering the safety of an aircraft in flight."

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

به دولت ها آسیب وارد می نماید، عمدتاً متضمّن عملیات پیچیده با دانش فنِی و اطلاعاتی بالایی است که واجد پیامدهای بسیار زیان آوری می باشد. استفاده از فضای سایبر برای انجام این نوع عملیات خرابکارانه و مجرمانه، شکل نوینی از فناوری را در قالب تروریسم با حمله الکترونیکی به زیرساختهای حیاتی و بسترهای الکترونیکی هدف در وب در جهان مدرن ظاهر ساخته و با نفوذ بر بخش اطلاعات نیروهای نظامی و مراکز مهم حیاتی کشورها، می توانند اطلاعات نادرستی را جایگزین کرده و یا در اختیار آنها قراردهند تا بر مبنای آن، متولیان امر و یا سیستم های هوشمند الکترونیکی، فریب خورده و تصمیمی مغایر وضعیت عادی و مقتضی شرایط مطلوب، اتخاذ کنند.

قطع برق وگازطبیعی و سوخت و حتّی خرابی سیستم های رایانه ای و ایجاد اختلال در سیستم حمل و نقل و ترابری زمینی، هوایی و دریایی، نیروگاهها و سدها، شبکه انتقال آب، بانک ها و بخش اقتصاد و امدادرسانی و پلیس، بیمارستانها و.... می توانند علاوه بر آسیب به وضعیت عادی جریان اداره امور در یک کشور، با قصد ایجاد رعب و وحشت در بین مردم، سبب شورش شده و منجر به سقوط نظام سیاسی یک کشور شوند که بی شک نمادی از تروریسم نوین را به نمایش می گذارد.

منابع

الف. فارسی

۱) اکهرست، مایکل؛(۱۳۷۳)؛ «حقوق بین الملل نوین»؛ مهرداد سیدی(مترجم)؛ تهران؛ دفتر خدمات حقوقی بین المللی

۲) صیاد، محمد کاظم و دیگران(۱۳۹۹)؛ «تهدیدهای سایبری و اقدامات امنیتی در فضای مجازی؛ بررسی رویکردهای ایالات‌متحده آمریکا و جمهوری اسلامی ایران»، فصلنامه علمی امنیت ملّی، مقاله ۱۰، دوره ۱۰، ش ۳۸، صص ۲۹۳-۳۳۰

۳) طیبی فرد، امیرحسین(۱۳۸۴)؛ «مبارزه با تأمین مالی تروریسم در اسناد بین المللی»؛ مجلهٔ حقوقی، نشریهٔ دفتر خدمات حقوقی بین المللی؛ شمارهٔ ۳۲؛ صص ۳۰۵-۲۸۹

۴) نصری، قدیر(۱۳۸۱)؛ «حادثه ۱۱ سپتامبر: نظریه‌ها و تفاسیر»؛ فصلنامه مطالعات راهبردی ، دوره ۵؛ شماره پیاپی ۱۷؛ صص۶۷۱-۶۹۲

ب.لاتین

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

5) Abraham D. Sofaer et al., A Proposal for an International Convention on Cyber Crime and Terrorism 26 (Aug. 2000)
6) Addicott, Jeff Terrorism Law: Materials, Cases, Comments, 6th Edition, CENTER FOR TERRORISM LAW ISSUES FOR DISCUSSION: CYBER SECURITY 1 (2011).
7) Aviv Cohen, Cyberterrorism: Are We Legally Ready? 9 J. INT'L BUS. & L. 1, 27-28 (2010) (discussing international responses to terrorism). Also. Id. at 28.
8) Beard, Jack M. Law and War in the Virtual Era, 103 AM. J. INT'L L. 409, 444 (2009).
9) Beggs, Christopher Cyber-Terrorism: A Threat to Australia? In MANAGING MODERN ORGANIZATIONS THROUGH INFORMATION TECHNOLOGY: PROCEEDINGS OF THE 2005 INFORMATION RESOURCES MANAGEMENT ASSOCIATION INTERNATIONAL CONFERENCE 472 (2005);
10) Berner, Sam Cyber-Terrorism: Reality or Paranoia? 5 S. AFR. J. INFO. MGMT. 1, 1 (2003).
11) BLYTH, TOBY CYBERTERRORISM AND PRIVATE CORPORATIONS: NEW THREAT MODELS AND RISK MANAGEMENT IMPLICATIONS 24 (1999).
12) CARR, JEFFREY INSIDE CYBER WARFARE 29 (2009).
13) CHESTERMAN, SIMON JUST WAR OR JUST PEACE? HUMANITARIAN INTERVENTION AND INTERNATIONAL LAW 48 (2001).
14) Clive Walker, The Legal Definition of "Terrorism" in United Kingdom Law and Beyond, 2007 PUB. L. 331, 336 (2007).
15) Cohen, Aviv Cyberterrorism: Are We Legally Ready? 9 J. INT'L BUS. & L. 1, 27-28 (2010) (discussing international responses to terrorism). Also. Id. at 28.
16) Condron, Sean M. Getting it Right: Protecting American Critical Infrastructure in Cyberspace, 20 HARV. J.L. & TECH. 404, 404-06 (2007)
17) Derek Jinks, September 11 and the Laws of War, 28 YALE J. INT'L. L. 32 (2003).
18) Gabriel Weimann, Cyberterrorism: How Real Is the Threat?, U.S. INST. OF PEACE, Dec. 2004, at 1, 11.

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

19) Geers, Kenneth Cyber Weapons Convention 26 COMPUTER L. & SEC. REV. 547 (2010).
20) Elina Noor, The Problem with Cyber Terrorism, 2 SOUTHEAST ASIA REGIONAL CTR. FOR COUNTER-TERRORISM 51, 52 (2011).
21) Hamden, Raymond H. The Retributional Terrorist: Type 4, in 2 THE PSYCHOLOGY OF TERRORISM: CLINICAL ASPECTS AND RESPONSES 174 (Chris E. Stout ed., Greenwood 2002).
22) Jahangiri, Ali Cyberspace, Cyberterrorism and Information Warfare: A Perfect Recipe for Confusion, WORLDWIDE SECURITY CONFERENCE 6: BACKGROUND MATERIALS AND SELECTED SPEAKERS NOTES 29 (2009).
23) Jeff Addicott, Terrorism Law: Materials, Cases, Comments, 6th Edition, CENTER FOR TERRORISM LAW ISSUES FOR DISCUSSION: CYBER SECURITY 1 (2011), available at www.stmarytx.edu/law/pdf/CLEAddicott.pdf.
24) Jinks, Derek September 11 and the Laws of War, 28 YALE J. INT'L. L. 32 (2003).
25) Klang, Mathias. A Critical Look at the Regulation of Computer Viruses, 11 INT'L J. L. & INFO. TECH., 162, 167 (2003).
26) Kelman, Alistair The Regulation of Virus Research and the Prosecution for Unlawful Research?, 3 J. INFO. L. & TECH. (1997),
27) Kenneth Geers, Cyber Weapons Convention 26 COMPUTER L. & SEC. REV. 547 (2010.
28) Kuehl, Daniel T. The National Information Infrastructure: The Role of the Department of Defense in Defending It, in TRANSNATIONAL THREATS: BLENDING LAW ENFORCEMENT AND MILITARY STRATEGIES 151 (Carolyn W. Pumphrey ed., 2000)
29) Noor, Elina. The Problem with Cyber Terrorism, 2 SOUTHEAST ASIA REGIONAL CTR. FOR COUNTER-TERRORISM 51, 52 (2011).
30) Rajeev C. Puran, Beyond Conventional Terrorism. . . The Cyber Assault (Feb). 2003
31) Raymond H. Hamden, The Retributional Terrorist: Type 4, in 2 THE PSYCHOLOGY OF TERRORISM: CLINICAL ASPECTS AND RESPONSES 174 (Chris E. Stout ed., Greenwood 2002.

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

32) Ronen, Yaël Incitement to Terrorist Acts and International Law, 23 LEIDEN J. INT'L L., 645, 654 (2010)
33) Sam Berner, Cyber-Terrorism: Reality or Paranoia? 5 S. AFR. J. INFO. MGMT. 1, 1 (2003).
34) Shamsuddin Abdul Jalil, Counting Cyber Terrorism Effectively: Are We Ready to Rumble? (June 2003
35) Sean M. Condron, Getting it Right: Protecting American Critical Infrastructure in Cyberspace, 20 HARV. J.L. & TECH. 404, 404-06 (2007)
36) Shachtman, Noah Computer Virus Hits US Predator and Reaper Drone Fleet, ARS TECHNICA (Oct. 7, 2011)
37) Shamsuddin Abdul Jalil, Counting Cyber Terrorism Effectively: Are We Ready to Rumble? (June 2003)
38) SIMON CHESTERMAN, JUST WAR OR JUST PEACE? HUMANITARIAN INTERVENTION AND INTERNATIONAL LAW 48 (2001).
39) Singh Arun Kr. & Siddiqui, Ahmad T. New Face of Terror: Cyber Threats, Emails Containing Viruses, 1 ASIAN J. TECH. & MGMT. RES. (2011) (discussing the new face of terror).
40) Sofaer Abraham D.et al., A Proposal for an International Convention on Cyber Crime and Terrorism 26 (Aug. 2000) (paper presented at the Stanford Conference at Stanford University), available at http://iis-db.stanford.edu/pubs/11912/sofaer goodman.pdf.
41) Solce, Natasha The Battlefield of Cyberspace: The Inevitable New Military Branch: The Cyber Force, 18 ALB. L.J. SCI. & TECH. 293, 301 (2008)
42) Stuart H. Starr, Towards and Evolving Theory of Cyberpower, in THE VIRTUAL BATTLEFIELD: PERSPECTIVES ON CYBER WARFARE, 18, 34 (Christian Czosseck & Kenneth Geers eds., 2009).
43) Walker, Clive The Legal Definition of "Terrorism" in United Kingdom Law and Beyond, 2007 PUB. L. 331, 336 (2007).
44) Weimann, Gabriel Cyberterrorism: The Sum of All Fears? 28 STUD. IN CONFLICT & TERRORISM 129, 130 (2005)
45) Yaël Ronen, Incitement to Terrorist Acts and International Law, 23 LEIDEN J. INT'L L., 645, 654 (2010)

Websites

فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف
سال ششم، شماره بیستم، بهار ۱۴۰۲

46) http://www.un.org/terrorism/instruments.shtml (last visited Aug. 21, 2012).
47) www.stmarytx.edu/law/pdf/CLEAddicott.pdf
48) www.stmarytx.edu/law/pdf/CLEAddicott.pdf
49) http://arstechnica. com/business/news/2011/10/exclusive-computer-virus-hits-drone-fleet.ars.
50) http://www.zdnet.com/news/security-guru-lets-secure-the-net/120859.
51) http://treaties.un.org/doc/db/Terrorism/english-18-9.pdf