مقاله

مجلهٔ

پژوهشهای حقوقی

علمی ـ ترویجی

شماره ۲۳

هزار و سیصد و نود و دو ـ نیمسال اول

شهر دانش

مؤسسه مطالعات و پژوهشهای حقوقی

http://jlr.sdil.ac.ir/article_32830.html

مجله پژوهشهای حقوقی (علمی ـ ترویجی)، شماره ۲۳، نیمسال اول ۱۳۹۲
صفحات ۸۷ الی ۱۱۲، تاریخ وصول: ۱۳۹۱/۶/۳، تاریخ پذیرش: ۱۳۹۱/۹/۲۲

مسؤولیت بین‌المللی دولت ناشی از حملات سایبری

سید یاسر ضیایی* ـ مونا خلیل‌زاده**

چکیده: حملات سایبری به عنوان یکی از جلوه‌های نوین مداخلات سایبری مورد شناسایی قرار گرفته است. حملات سایبری اقداماتی است که از سوی یک دولت برای هدف قرار دادن زیرساخت‌های اساسی یک دولت از جمله سیستم بانکی، انرژی و حمل و نقل عمومی که به شبکه رایانه‌ای متصل هستند صورت می‌پذیرد. حملات سایبری اگر مصداقی از تجاوز یا توسل به زور محسوب نشوند می‌تواند به عنوان مداخله در امور داخلی دولت یک تخلف بین‌المللی تلقی شود. در صورت انتساب این تخلف بین‌المللی به دولت طرح مسؤولیت بین‌المللی دولت امکانپذیر خواهد بود. حمله سایبری توسط افراد خصوصی در صورتی که در استخدام دولت یا تحت کنترل دولت باشند به دولت منتسب می‌شود و حمله سایبری با همکاری شرکت‌های ارائه‌دهنده خدمات اینترنتی تا جایی که در چارچوب اقتدار عمومی یا تحت کنترل دولت عمل می‌کنند به دولت منتسب می‌شود. اعمال نظریه تقصیر در حملات سایبری موجب می‌شود تا با شناسایی «مقصر» حمله سایبری «مرتکب» حمله سایبری نیز شناسایی شود. در این صورت امکان جبران خسارت به روش‌های مختلف اعم از توقف عمل متخلفانه، پرداخت غرامت و جلب رضایت وجود خواهد داشت.

* استادیار گروه حقوق بین‌الملل و عمومی دانشکده حقوق دانشگاه قم Email: yaserziaee@gmail.com
** دانشجوی کارشناسی ارشد حقوق بین‌الملل دانشگاه آزاد واحد مرکز

کلیدواژه‌ها: فضای سایبر، حملات سایبری، انتساب عمل متخلفانه بـه دولـت، مسؤولیت بین‌المللی، جبران خسارت.

۱- مقدمه

یکی از اصطلاحاتی که به دوران امروزی اطلاق می‌شود «عـصر اطلاعـات» اسـت. ایـن عبارت متضمن روش‌های نوین جابه‌جایی اطلاعات و اهمیت اطلاعات برای اداره امور دولت است. بـا پیـدایش نـرم‌افزارهـای رایانـه‌ای امکـان بهـره‌گیـری از ایـن پدیـده در بخش‌های مختلف دولتی خصوصاً زیرسـاخت‌هـای اساسـی فـراهم گردیـد. بـا ظهـور اینترنت به عنوان محیطی برای اتصال شبکه‌های رایانه‌ای بـا یکـدیگر ایـن امـر تـسهیل گردید. تحقق دولت الکترونیک نتیجـه ایـن پیـشرفت بـوده اسـت. بـا ایـن حـال ایـن دستاوردهای بشری آسیب‌پذیری خود را به زودی نشان داد و امکان مداخلـه نامـشروع در فعالیت‌های دولت در عرصه‌های مختلف از طریق شبکه‌های اینترنتی مطـرح گردیـد. جامعه بین‌المللی شاهد حملاتی به اطلاعات رایانه‌ای در عرصـه‌هـای بـانکی، انـرژی و هوانوردی بوده است. از این حملات نوین می‌توان تحت عنوان «حملات سـایبری» نـام برد. با توجه به گستردگی، پیچیدگی و منـافع ناشـی از ایـن حمـلات عمومـاً کنتـرل و هدایت یک دولت در این حملات مفروض است. طرح مسؤولیت دولتـی کـه مرتکـب حمله سایبری شده است اولاً منوط به اثبات نامشروع بودن این حملـه از منظـر حقـوق بین‌الملل و ثانیاً منتسب بودن حمله سایبری به دولت می‌باشد. ماده ۲ طرح پـیش‌نـویس مسؤولیت بین‌المللی دولت‌ها مورخ ۲۰۰۱ در این رابطـه بیـان مـی‌دارد «فعـل متخلفانـه بین‌المللی دولت هنگامی محقق می‌شود که رفتاری اعم از فعل یا تـرک فعـل الـف) بـه موجب حقوق بین‌الملل قابل انتساب به آن دولت باشد و ب) نقض تعهد بین‌المللـی آن دولت تلقی شود». لذا ابتدا به جایگاه حمله سایبری در حقوق بین‌الملل اشاره می‌شود و سپس قابلیت انتساب آن به دولت بررسی می‌شود تا از این طریـق بتـوان روش جبـران خسارات ناشی از حملات سایبری را از منظر حقوق مسؤولیت بین‌المللـی دولـت‌هـا را مشخص نمود.

۲- جایگاه حمله سایبری در حقوق بین‌الملل

در ادبیات رسانه‌ای و رایانه‌ای مفاهیم مشابهی در حوزه حملات سایبری عنوان می‌شـود که پیش از بررسی مشروعیت حملات سـایبری از منظـر حقـوق بـین‌الملـل لازم اسـت

تفاوت آن‌ها از نقطه نظر حقوقی مشخص شود. در اینجا به برخی از این مفاهیم اشاره می‌شود.

۲-۱- مفاهیم مرتبط با حملات سایبری

در این قسمت به تفاوت میان تروریسم سایبری، جرایم سایبری، جنگ اطلاعاتی و حمله سایبری اشاره می‌شود.

۲-۱-۱- تروریسم سایبری

تروریسم سایبری به معنی حملات از پیش طراحی شده با انگیزه سیاسی است که توسط گروه‌های تحت حمایت کشورها یا عوامل خرابکار علیه سیستم‌های رایانه‌ای و اطلاعاتی، برنامه‌های رایانه‌ای و داده‌ها انجام می‌شود، به نحوی که منجر به خشونت علیه اهداف غیرنظامی می‌شود.[۱] در تروریسم سایبری برخلاف حملات سایبری هدف نظامی مشخصی وجود ندارد و صرفاً تأثیرگذاری بر تمام ساکنین دنبال می‌شود.[۲] لذا در تروریسم سایبری هدف حملات اصولاً غیرنظامی است و ارتکاب آن نیز لزوماً با هدایت دولت نیست.[۳]

۲-۱-۲- جنگ اطلاعاتی

جنگ اطلاعاتی با انقلاب اطلاعات ظهور پیدا کرده است. این انقلاب به دلیل دامنه وسیع و تأثیرات گسترده آن می‌تواند سبک نوینی از جنگ را ارائه بدهد. جنگ اطلاعات عبارت است از حمله برنامه‌ریزی شده توسط دولت یا عوامل آن‌ها علیه سیستم‌ها و برنامه‌های رایانه‌ای و اطلاعاتی که با هدف تحمیل خسارت به کشور دشمن صورت می‌پذیرد.[۴] سازمان همکاری شانگهای رویکرد موسع‌تری نسبت به تعریف جنگ اطلاعاتی دارد و معتقد است «جنگ اطلاعاتی مواجهه دو یا چند دولت در فضای اطلاعاتی است با این هدف که موجب صدمه به نظام اطلاعاتی، روندها، منابع و ساختارهای بسیار مهم یکدیگر شوند و موجب تضعیف نظام‌های سیاسی، اقتصادی و اجتماعی یکدیگر شده که منجر به حملات روانی علیه مردم و بی‌ثباتی جامعه و دولت می‌شود و دولت را مجبور به اتخاذ تصمیماتی می‌نماید که در راستای منافع دشمن است».[۵] تفاوت عملی بین دو اصطلاح تروریسم سایبری و جنگ اطلاعاتی این است که

---

۱. برای مطالعه بیشتر، نک: جلالی فراهانی، «تروریسم سایبری».

2. Janczewski & Colarik, *Cyber warfare and cyber terrorism*, p. xiv.

3. See Shiryaev, "Cyberterrorism in the Context of Contemporary International Law", p. 139.

4. Hamelink, "Human Rights in Cyberspace".

5. Agreement Between The Governments of The Member States of The Shanghai Cooperation ←

در تروریسم سایبری هدف صرفاً ایجاد ترس و آسیب‌رسانی در افراد جامعه است درحالی که هدف از جنگ اطلاعات تأثیرگذاری بر منافع یک دولت است.[۶] امروزه جنگ اطلاعاتی مترادف با حمله سایبری مورد استفاده قرار می‌گیرد.

۲-۱-۳- جرایم سایبری

جرایم سایبری شامل جرایمی است که توسط اشخاص در محیط سایبر ارتکاب می‌یابند. جرائمی همچون کلاهبرداری رایانه‌ای، جعل رایانه‌ای، جاسوسی رایانه‌ای، تخریب و اخلال‌گری (سابوتاژ) رایانه‌ای، دستیابی و شنود غیرمجاز رایانه‌ای از جمله جرایم سایبری هستند. به نظر می‌رسد ویژگی خاص فضای سایبر موجب می‌شود تا همان‌گونه که افراد مرتکب جرایم سایبری می‌شوند دولت‌ها نیز بتوانند مرتکب جرایم سایبری شوند. در واقع در این فضا برخی دولت‌ها علاوه برجنگ، به جرم و تروریسم دست می‌زنند در حالی که افراد علاوه بر جرم و تروریسم به جنگ نیز دست می‌زنند.[۷] سازمان همکاری و توسعه اقتصادی، جرایم سایبری را سوء استفاده از رایانه شامل هر نوع رفتار غیرقانونی، غیراخلاقی یا غیرمجاز که مربوط به پردازش اتوماتیک و انتقال داده‌ها می‌باشد تعریف می‌کند.[۸]

۲-۱-٤- حمله سایبری

امروزه اینترنت در زمینه‌های مختلف دولتی مانند دولت الکترونیک، نیروگاه‌های هسته‌ای، بخش انرژی، سامانه کنترل هوانوردی و بانکداری آنلاین وارد شده است که میزان آسیب‌پذیری دولت‌ها را افزایش داده است. لذا گسترش شبکه‌های الکترونیکی می‌تواند اشکال جدیدی از تجاوز را محقق کند. ایجاد تغییرات در رکوردهای مالیاتی در بازار سهام،[۹] ارسال پیغام خطا به سیستم‌های بخش انرژی که به طور مثال می‌تواند منجر به خاموش شدن رآکتورهای هسته‌ای شود،[۱۰] باز کردن سد،[۱۱] ایجاد اختلال در سیستم ترافیک هوایی که منجر به تصادم هواپیماها می‌شود از جمله این اقدامات است. در سال‌های اخیر حملات سایبری به استونی (۲۰۰۷)، گرجستان (۲۰۰۸) و جمهوری

Organization on Cooperation In The Field of International Information Security, 61st Plenary Meeting (Dec. 2, 2008).

٦. برای مطالعه بیشتر، نک: مورکیان علی‌آباد، «جنگ اطلاعات از منظر حقوق بین الملل».

See Greenberg, Goodman & Soo Hoo, *Information Warfare and International Law.*

7. Hamelink, "Human Rights in Cyberspace".

۸. خداقلی، جرائم کامپیوتری، ص ۲۹.

9. Hollis, "Why States Need an International Law for Information Operations", p.1042.

10. Antolin-Jenkins, "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places", p. 140.

11. Gellman, "Cyber Attacks by al Qaeda Feared".

اسلامی ایران (۲۰۱۱) هدف شدیدترین حملات سایبری بوده‌اند به نوعی که برخی از این دوران به دوران «جنگ سرد سایبری» تعبیر کرده‌اند.[۱۲] تعریف حملات سایبری مقدمه تعیین اقدامات مشروع در برابر آن است.

میشل هایدن[۱۳] مدیر سابق آژانس اطلاعاتی امریکا[۱۴] و ناسا[۱۵] معتقد است که حملات سایبری تلاش عمدی برای غیرفعال کردن و یا از بین بردن شبکه‌های رایانه‌ای یک کشور دیگر میباشد.[۱۶] مارتین لیبیکی[۱۷] کارشناس فنی سایبری، جنگ سایبری را حملات و آسیب‌های دیجیتالی دانسته است که موجب می‌شود سیستم رایانه‌ای در ظاهر طبیعی عمل کند در حالی که جواب‌های مغایر با واقعیت ارائه می‌دهد.[۱۸] اما به نظر می‌رسد تعریف صحیح‌تر از سوی ریچارد ای. کلارک[۱۹] ارائه شده باشد که جنگ سایبری را اقدامات انجام شده توسط یک دولت که به منظور نفوذ و یا ایجاد اختلال در کامپیوتر و یا شبکه‌های رایانه‌ای دیگر دولت‌ها صورت می‌پذیرد، می‌داند.[۲۰] «دولتی بودن» هدف حملات محور این تعریف است. لذا هر حمله‌ای از طریق شبکه‌های اینترنتی حمله سایبری نیست، بلکه صرفاً حملات علیه اهداف دولتی مصداق حملات سایبری هستند؛ در غیر این صورت با تروریسم سایبری یا جرایم سایبری روبه رو خواهیم بود.

در مجموع می‌توان این تعریف را از حملات سایبری ارائه نمود «اقداماتی که از سوی یک دولت یا افراد تحت کنترل دولت برای هدف قرار دادن زیرساخت‌های اساسی دولت دیگر از جمله سیستم بانکی، بخش انرژی و حمل و نقل عمومی و غیره که به شبکه رایانه‌ای متصل هستند صورت می‌پذیرد». لازم به ذکر است که هرچند به علت ماهیت خاص فضای سایبر امکان توسل اشخاص خصوصی به این‌گونه اقدامات نیز وجود دارد اما منظور از حملات سایبری در اینجا حملاتی است که از سوی دولت یا با حمایت دولت صورت می‌پذیرد، چه آنکه صرفاً این‌گونه حملات می‌تواند مسؤولیت بین المللی دولت را به دنبال داشته باشد.

12. Willson, "Cyberwar or Cyber Cold War?".
13. Michael Hayden
14. The Central Intelligence Agency (CIA) is an independent US Government agency responsible for providing national security intelligence to senior US policymakers.
15. The National Aeronautics and Space Administration (NASA) is the agency of the United States government that is responsible for the nation's civilian space program and for aeronautics and aerospace research.
16. Gjelten, "Extending the Law of War to Cyberspace".
17. Martin Libicki
18. Libicki, *What is Information Warfare?*, p. 77.
19. Richard A.Clarke
20. See "More Than Firewalls: Three Challenges to American Cyber Security".

۲-۲- حمله سایبری به مثابه عمل متخلفانه بین‌المللی

آیا حملات سایبری اصل منع توسل به زور را نقض می‌کند؟ برای پاسخ به این سوال لازم است تا به مفاهیم مرتبط با «توسل به زور»[۲۱] یعنی «تجاوز»[۲۲] و «حمله مسلحانه»[۲۳] در حقوق بین‌الملل رجوع شود. با مرور اسناد بین‌المللی مشخص می‌شود که مفهوم توسل به زور اعم از تجاوز است و تجاوز اعم از حمله مسلحانه است.[۲۴] به عبارت دیگر یکی از اشکال توسل به زور، تجاوز است و یکی از اشکال تجاوز، حمله مسلحانه است.

طبق ماده ۵۱ منشور ملل متحد «در صورت وقوع حمله مسلحانه علیه یک عضو ملل متحد تا زمانیکه شورای امنیت اقدام لازم برای حفظ صلح و امنیت بین‌المللی را به عمل آورد هیچیک از مقررات این منشور به حق ذاتی دفاع از خود، خواه فردی یا دسته جمعی لطمه‌ای وارد نخواهد کرد». باید توجه داشت که این ماده دفاع مشروع را به «حمله مسلحانه» محدود کرده است که شامل استفاده از ادوات نظامی علیه دولت دیگر می‌شود در حالی که اینترنت به عنوان ابزار نظامی در نظر گرفته نمی‌شود. لذا حمله سایبری نمی‌تواند متضمن دفاع مشروع مورد نظر ماده ۵۱ باشد و برخلاف بیانیه‌های متعددی که از سوی برخی مقامات دفاعی ملی منتشر شده است حمله سایبری نمی‌تواند موجبی برای توسل به دفاع مشروع باشد.[۲۵]

حملات سایبری همچنین مصداقی از تجاوز نیستند. معتبرترین سند در تعریف تجاوز قطعنامه ۳۳۱٤ مجمع عمومی در خصوص تعریف تجاوز است.[۲۶] طبق این قطعنامه تجاوز عبارت است از «به کارگیری زور به صورت مسلحانه توسط یک دولت علیه حاکمیت یا تمامیت ارضی یا استقلال سیاسی دولت دیگر یا به هر نحو دیگر که با اهداف سازمان ملل متّحد ناسازگار باشد». با توجه به مصادیق ذکر شده در این قطعنامه از تجاوز مشخص می‌شود که از نظر مجمع عمومی به کارگیری زور صرفاً ناظر بر بکارگیری نیروی مسلحانه است و مسایلی نظیر تهاجم فرهنگی، ایدیولوژیک و یا

21. use o force
22. aggression
23. armed attack

۲٤. مقدمه قطعنامه مجمع عمومی در تعریف تجاوز بیان می‌دارد که «تجاوز جدی‌ترین و خطرناک‌ترین شکل توسل به زور است». از سوی دیگر حمله مسلحانه تنها یکی از اشکال تجاوز است که می‌تواند دفاع مشروع را طبق ماده ۵۱ به دنبال داشته باشد.

25. Waxman, "Cyber Attack and the Use of Force".
26. Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX).

اقتصادی را شامل نمی‌شود. بنابراین مطابق با قطعنامه شماره ۳۳۱٤ نمی‌توان حمله به زیرساخت‌های کلیدی از طریق شبکه‌های الکترونیکی را تجاوز بین‌المللی دانست، چراکه در این میان هیچ تجاوز فیزیکی به قلمرو کشور صورت نگرفته است. با این حال اگر حمله سایبری به زیرساخت‌های نظامی یک دولت صورت بگیرد شاید بتوان آن را با حملات نظامی قابل قیاس دانست، چرا که در هر دو حمله نتیجه یکسانی حاصل می‌شود. لذا هر عمل برون سرزمینی که پیامدهای اقتصادی، سیاسی و امنیتی بین‌المللی به دنبال داشته باشد نمی‌تواند تجاوز تلقی شود مگر اینکه اثرگذاری بر بخش نظامی دشمن باشد.[۲۷]

اما آیا حمله به پایگاه‌های داده‌های ملی، امنیت سایبری و زیرساخت‌های الکترونیکی مصداق توسل به زور خواهد بود؟ مطابق بند ٤ ماده ۲ منشور ملل متحد کلیه اعضا ملزم هستند در روابط بین‌المللی خود از تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی هر کشوری یا از هر روش دیگری که با مقاصد ملل متحد مباینت داشته باشد خودداری نمایند. استفاده از عبارت استقلال سیاسی در کنار تمامیت ارضی حاکی از این است که آنچه ممنوع شده است صرفاً حمله نظامی نیست بلکه تحت تأثیر قرار دادن استقلال سیاسی دولت از طریق زور نیز ممنوع است.[۲۸] با این حال برخی معتقدند که در سراسر منشور منظور از کابرد زور «حمله مسلحانه» بوده است[۲۹] که در این صورت حمله سایبری اصل منع توسل به زور را نیز نقض نمی‌کند.[۳۰]

باید توجه داشت حتی اگر حمله سایبری مصداقی از توسل به زور تلقی نشود، می‌تواند اصل منع مداخله در امور داخلی دولت‌ها را نقض نماید. حمله سایبری مصداقی از اعلامیه عدم مداخله مجمع عمومی مورخ ۱۹۸۱ است؛ آنجا که در بند ۳ پاراگراف اول بیان می‌دارد «حق دولت و مردم در دسترسی آزاد به اطلاعات حق توسعه سیستم‌های اطلاعاتی و رسانه جمعی و استفاده از رسانه‌های اطلاعاتی بدون مداخله و با این هدف که منافع سیاسی، اقتصادی و فرهنگی خود را توسعه دهند».[۳۱] دیوان بین المللی دادگستری در قضیه «فعالیت‌های نظامی و شبه نظامی در نیکاراگوئه و علیه

27. Synovitz, "Georgian Government Accuses Russia of Waging 'Cyberwarfare'"; & Shachtman, "Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It".

28. See Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", p. 420.

29. Heselhaus, "International Law and the Use of Force".

۳۰. در مقابل، برخی از مفهوم نوین «توسل به زور سایبری» (Use of Cyber Force) سخن به میان آورده‌اند.

D'Souza, "Cyber Warfare and State Responsibility: Developments in International Law".

31. A/RES/36/103, Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States 91st plenary meeting, 9 December 1981.

نیکاراگوئه»[۳۲] مورخ سال ۱۹۸٦ مداخله را در صورت وجود چند شرط غیرقانونی دانست: «اولاً آن که مداخله در اموری باشد که هر کشور در نتیجه اصل حاکمیت مجاز به انجام آن‌هاست، ثانیاً روش مورد استفاده کشور مداخله‌گر زورمندانه و قهرآمیز باشد و ثالثاً در مداخله‌ای که به طور قهرآمیز و با استفاده از زور صورت گرفته است لازم است عنصر زور و اجبار امری بارز و آشکار باشد».[۳۳] همچنین اعلامیه اصول حقوق بین‌الملل راجع به روابط دوستانه و همکاری میان کشورها، هر نوع مداخله مستقیم یا غیرمستقیم در امور داخلی یا خارجی کشور دیگر را به منزله نقض تعهدات بین‌المللی می‌داند. ماده ۳۲ قطعنامه منشور حقوق و تکالیف اقتصادی دولت‌ها[۳۴] نیز تأکید کرده است که هیچ کشوری حق استفاده ابزاری از امکانات سیاسی و اقتصادی و غیره به منظور دستیابی به اعمال حق حاکمیت خود را ندارد. از مجموع این تعهدات بر می‌آید که حمله سایبری می‌تواند در خوشبینانه‌ترین حالت نقض اصل منع مداخله در امور داخلی تلقی شود.

۳- انتساب حمله سایبری به دولت

انتساب عمل متخلفانه به دولت در فضای سایبر به دو علت از ویژگی خاصی برخوردار است: اول اینکه دنیای مجازی در دنیایی خارج از دنیای مرسوم و متعارف واقعی به حیات خود ادامه می‌دهد و پیوستگی اطلاعات در این فضا به نحوی است که اثر عمل یک دولت در گوشه‌ای از دنیا قابل رؤیت و اثربخش در بسیاری از نقاط دیگر دنیا خواهد بود. به طور مثال کشوری که سرور ریشه‌ای[۳۵] در سرزمین وی مستقر است می‌تواند با قطع آن به قطع اینترنت در بخش وسیعی از جهان دامن زند و یا دولتی با پراکندن اخبار و جملات تحریک‌آمیز به نسل‌کشی یا تبعیض نژادی در فضای مجازی، تمام کاربران دنیای واقعی را تحت تأثیر قرار دهد.[۳۶] دوم اینکه برخلاف دنیای واقعی که اصولاً عامل نقض قابل شناسایی است، ریشه عمل نقض و عامل آن در شبکه

32. *ICJ Reports*, "Military and Paramilitary Activities in and against Nicaragua",1986.
33. *Ibid*, paras. 227 to 238.
34. See General Assembly Res. 3281, 1974.
35. See http://www.root-servers.org/

۳٦. پروتکل الحاقی به کنوانسیون جرایم سایبری اینگونه اقدامات را ممنوع اعلام کرده‌اند.

See Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, 28.01.2003, available at http://conventions.coe.int/Treaty/EN/Treaties/html/189.htm

عنکبوتی اینترنت به سختی قابل ردیابی است.[۳۷] ماهیت ویژه فضای سایبر ایجاب می‌کند تا عوامل مختلفی از قبیل اطلاعات فنی، فضای سیاسی، سابقه فعالیت‌های سایبری دولت‌ها و غیره برای انتساب حملات سایبری در نظر گرفته شود.[۳۸] وزارت دفاع امریکا مؤلفه‌هایی چون روابط میان دو کشور، سابقه اقدامات دولت مظنون در حملات رایانه‌ای، ماهیت سیستم‌های مورد حمله، ماهیت و پیچیدگی روش‌ها و ابزار مورد استفاده، آثار حملات [سایبری] گذشته و خسارات احتمالی در آینده را برای تعیین «دولت حامی»[۳۹] حملات سایبری در نظر گرفته است.[۴۰]

۳-۱- مسؤولیت ناشی از فعل اشخاص خصوصی

هرچند در گذشته صرفاً دولت‌ها با توسل به ادوات نظامی می‌توانستند آغازگر یک جنگ باشند امروزه افراد نیز می‌توانند به کمک یک لپ‌تاپ حمله‌ای را علیه اهداف نظامی دولت خارجی سازمان‌دهی کنند.[۴۱] لذا برای طرح مسؤولیت بین‌المللی دولت ناشی از حملات سایبری بسیار اهمیت دارد که حمله سایبری صورت گرفته از سوی اشخاص خصوصی به دولت منتسب گردد.

در حقوق بین‌الملل معیارهای مختلفی برای انتساب عمل بازیگر غیردولتی (اشخاص خصوصی) به دولت مطرح شده‌اند، مانند دکترین کنترل مؤثر در آرای دیوان بین‌المللی دادگستری در قضایای نیکاراگوئه،[۴۲] نسل‌کشی[۴۳] و کنگو علیه اوگاندا،[۴۴] دکترین کنترل عمومی در دیوان کیفری بین‌المللی کیفری برای یوگسلاوی سابق در قضیه تادیچ،[۴۵] دکترین حمایت مالی و پناه دادن به تروریست‌ها در قطعنامه‌های ۱۳۶۸ (۲۰۰۱) و ۱۷۰۳ (۲۰۰۶) شورای امنیت،[۴۶] دکترین ارتباط کافی[۴۷] در سازمان جهانی تجارت[۴۸] و سایر موارد مذکور در مواد ٤ تا ۱۱ طرح مسؤولیت کمیسیون حقوق بین‌الملل برای مسؤولیت بین‌المللی دولت‌ها. در حملات سایبری معیار نوین «ماهیت

۳۷. ضیایی، «حمایت از حقوق بشر در فضای سایبر».

38. Blog of the European Journal of International Law, "The Tallinn Manual on the International Law applicable to Cyber Warfare".

39. State Sponsorship

40. http://www.au.af.mil/au/awc/awcgate/army/jaoac-io.pdf U.S. Department of Defense Report.

41. http://www.au.af.mil/au/awc/awcgate/army/jaoac-io.pdf Nikhil D'Souza, op. cit.

42. *ICJ Reports*, 1984.

43. *ICJ Reports*, 1999.

44. *ICJ Reports*, 2005.

45. The Prosecutor *v.* Duško Tadic, 1997.

46. Security Council Resolution 1368 (2001), 1703 (2006).

47. sufficient involvement

48. Villalpando, "Attribution of Conduct to the State: How the Rules of State Responsibility may be Applied Within the WTO Dispute Settlement System", pp. 393-420.

عمل» قابل طرح است که طبق آن چنانچه حملات سایبری از وسعتی برخوردار باشد که بدون حمایت دولتی امکانپذیر نباشد آن حمله به دولتی منتسب خواهد شد که حملات از آنجا انجام شده است. به طور مثال مرکز مطالعات دانشگاه دفاع ملی سوئد معتقد بود ماهیت حملات سایبری به گرجستان در پی جنگ روسیه و گرجستان[۴۹] به گونه‌ای است که تحقق آن بدون حمایت دولت روسیه غیرقابل تصور است.[۵۰] ویژگی‌های انتساب عمل بازیگران غیردولتی در فضای سایبر که شامل افراد خصوصی و شرکت‌های خصوصی ارائه‌کننده خدمات اینترنتی می‌شود، متفاوت خواهد بود.

۳-۱-۱- مسؤولیت ناشی از فعل افراد خصوصی

اصل کلی در حقوق بین‌الملل این است که دولت مسؤول اعمال اشخاص خصوصی نیست. با این حال از نظر کمیسیون حقوق بین‌الملل استثناآتی بر این اصل وجود دارد. طبق ماده ٤ طرح پیش‌نویس کمیسیون حقوق بین‌الملل در خصوص مسؤولیت بین‌المللی دولت‌ها مورخ ۲۰۰۱ رفتارهای متخلفانه ارگان‌های دولتی قابل انتساب به آن دولت خواهد بود. چنانچه افرادی که در حملات سایبری نقش‌آفرینی می‌کنند در استخدام دولت باشند و مشروط بر اینکه در سمت رسمی خویش عمل کرده باشد انتساب آن‌ها به دولت مفروض خواهد بود. کمیسیون حقوق بین‌الملل در تفسیر شماره ۷ ماده ٤ تأکید می‌کند که ارگان دولتی صرفاً محدود به مقامات مافوق نمی‌شود بلکه «هیچ تمایزی میان اعمال مأموران مافوق و مادون به عمل نیامده است مشروط بر اینکه آن‌ها در سمت رسمی خویش عمل کرده باشند».[۵۱] همچنین کمیسیون‌های مختلط بعد از جنگ جهانی دوم اغلب به مسائل ناشی از رفتارهای ارگان‌های سطح پایین دولت همچون مدیران اموال دشمن، شهرداران و مأموران پلیس پرداخته است و اعمال این اشخاص را به دولت قابل انتساب دانسته است. لذا چنانچه حملات سایبری توسط هکرهایی صورت پذیرد که در استخدام دولت هستند و بدین منظور فعالیت می‌کنند انتساب به دولت مفروض خواهد بود.

در این حالت اقدام هکر دولتی اقدام دولت تلقی خواهد شد. استفاده از عبارت کارگزار یا نماینده[۵۲] در تفاسیر طرح مسؤولیت دولت‌ها نیز به همین دلیل است، چرا که

49. Tikk et al., *Cyber Attacks Against Georgia Legal Lessons Identified*, pp. 18-25.

50. Swedish Defense University with preliminary conclusions on 'Cyberattack against Georgia', August 2008.

۵۱. ابراهیم‌گل، متن و شرح مواد کمیسیون حقوق بین‌الملل در خصوص مسؤولیت بین‌المللی دولت، ص ٤٨.

52. agent

نماینده، جانشین اصیل محسوب می‌شود و تمام اقداماتش به نام و حساب دیگری است.[۵۳] به‌علاوه هدف حقوق مسؤولیت بین‌المللی در وهله اول جبران خسارت است، در حالی که افراد به ندرت توانایی جبران خساراتی وارده را دارند. البته در خصوص جنایات بین‌المللی طرح مسؤولیت موازی دولت و فرد محتمل است. چرا که واکنش دولت‌ها در سطح بین‌المللی علیه دولت متخلف و در سطح داخلی علیه جنایتکاران بین‌المللی نشان از شکل‌گیری این رویه در خصوص جنایات بین‌المللی دارد. علت این امر ماهیت دوگانه جنایات بین‌المللی است که به صورت همزمان و اتوماتیک‌وار مسؤولیت بین‌المللی کیفری و غیرکیفری را دامن می‌زند.[۵۴] لذا احاله مسؤولیت بازیگر غیردولتی به دولت به معنای عدم مسؤولیت «کیفری» افراد به صورت جداگانه نیست و آنچه گفته شد در خصوص مسؤولیت بین‌المللی غیرکیفری دولت است.[۵۵] در حال حاضر طرح مسؤولیت کیفری هکر تحت عناوین مجرمانه‌ای چون سابوتاژ (خرابکاری) در نظام حقوق داخلی دولت قربانی امکانپذیر خواهد بود.[۵۶]

طبق ماده ۸ طرح پیش‌نویس کمیسیون حقوق بین‌الملل در خصوص مسؤولیت

---

۵۳. با این حال در حقوق داخلی پذیرفته شده که اگر نمایندگی نماینده برای ثالث پنهان مانده باشد (undisclosed principal) طرف عمل یا واقعه حقوقی، نماینده است و نه اصیل و مسؤولیت آن با نماینده است.
Martin, *Dictionary of Law*, p. 23.

۵٤. طرح پیش‌نویس کمیسیون حقوق بین‌الملل در مورد مسؤولیت دولت‌ها پس از احصای اصول و قواعد حقوق مسؤولیت بین‌المللی دولت‌ها، در مواد پایانی طرح مقرر می‌دارد که این مواد به هرگونه مسأله مربوط به مسؤولیت فردی شخص به موجب حقوق بین‌الملل که از طرف دولت عمل می‌کند خدشه‌ای وارد نمی‌سازد (ماده ۵۸).

۵۵. قاضی وین‌گارت در نظریه مخالف خود در قضیه یرودیا در دیوان بین‌المللی دادگستری (کنگو علیه بلژیک) معتقد بود که ارتکاب جنایات بین‌المللی توسط مقامات دولتی تنها جنبه خصوصی دارد و چنین شخصی صرفاً به ابتکار (از قِبَل) خود عمل کرده است و قابل انتساب به دولت نیست تا مسؤولیت دولت مطرح باشد.
ICJ Reports, Congo *v.* Belgium, 2002, Dissenting Opinion by Judge Van Den Wyngaert, Para 36.
در مقابل، حقوقدانان دیگر از جمله آنتونیو کاسسه بر این اعتقادند که مقامات رسمی می‌توانند در سمت خود مرتکب جنایات بین‌المللی شوند و از این طریق موجب طرح مسؤولیت بین‌المللی دولت هم شوند. نک:
Spinedi, "State Responsibility *v.* Individual Responsibility for International Crimes: Tertium Non Datur?", pp. 895-899.
اما در هر صورت حمله سایبری را چنانچه مصداق تجاوز ندانیم یک جنایت بین‌المللی نیست و امکان انتساب آن به دولت وجود دارد.

۵٦. با این حال رسیدگی به جنبه کیفری جرم تجاوز علیه اشخاص خصوصی در محاکم ملی با تردید مواجه بوده است.
See Scharf, "Universal Jurisdiction and the Crime of Aggression", p. 358.
همچنین، نک: سازمان ملل، نشریه بین‌المللی سیاست جنائی، ص ۳۲.

بین‌المللی دولت‌ها مورخ ۲۰۰۱ رفتارهای متخلفانه اشخاص خصوصی تحت هدایت یا کنترل دولت نیز به دولت منتسب می‌شود. کمیسیون حقوق بین‌الملل در تفسیر شماره ۹ ماده ۸ بیان می‌دارد که این ماده ناظر به «شخص یا گروهی از اشخاص» است و دولت می‌تواند اقدامی را از طریق مجموعه‌ای از اشخاص یا گروه‌هایی انجام دهد که فاقد شخصیت حقوقی هستند اما با این وجود به صورت جمعی عمل می‌کنند.[۵۷] لذا چنانچه دولت برای حمله سایبری خود به هکرهای خصوصی رهنمود داده یا آن‌ها را برای حمله سایبری تحریک و ترغیب نموده است حمله سایبری فعل دولت تلقی می‌شود.[۵۸] به طور مثال بسیاری از هکرهایی که از طرف روسیه اقدام می‌کنند از افراد آموزش دیده‌ای هستند که بیکار بوده و در استخدام دولتی نیز نیستند.[۵۹] باید توجه داشت چنانچه افراد خصوصی ابتدائاً اقدام به حمله سایبری کرده باشند و دولت صرفاً به آن‌ها کمک کرده باشد این اقدام منتسب به دولت نخواهد بود و دولت صرفاً از جهت کمک به یک عمل متخلفانه بین‌المللی مسؤولیت خواهد داشت.[۶۰]

۳-۱-۲- مسؤولیت ناشی از شرکت‌های خصوصی ارائه‌کننده خدمات اینترنتی

حملات سایبری هرچند به کمک افراد متخصص انجام می‌شود اما تحقق آن نیازمند همکاری عمل شرکت‌های ارائه‌کننده خدمات اینترنتی می‌باشد. انتساب عمل شرکت‌های خصوصی ارائه‌کننده خدمات اینترنتی به دولت در دو حالت اتفاق می‌افتد: زمانی که دولت کنترل مؤثر بر نهاد مذکور داشته باشد (ماده ۸ طرح مسؤولیت بین‌المللی دولت‌ها) و زمانی که نهاد مذکور طبق حقوق داخلی یک کشور اعمال اقتدار عمومی می‌کند (ماده ۵ طرح مسؤولیت بین‌المللی دولت‌ها).

آنچه که دیوان بین‌المللی کیفری برای یوگسلاوی سابق از کنترل عمومی برای

---

۵۷. ابراهیم‌گل، پیشین، ص ۷۰.

۵۸. اکهرست، حقوق بین‌الملل نوین.

59. Karatgozianni, "Blame It on the Russians: Tracking the Portrayal of Russian Hackers during Cyber Conflict Incidents", p. 130.

60. Melzer, "Cyberwarfare and International Law".

به طور مثال در ماه آوریل سال ۲۰۰۷ زیرساخت‌های الکترونیکی استونی هدف حمله هماهنگ تعدادی از هکرها قرار گرفت، بنا به گزارش‌های موجود اولین حمله از داخل خاک کشور روسیه صورت گرفته است. به گزارش مقامات روسی این حملات از سوی سازمان جوانان «نازسی» و با حمایت کرملین صورت گرفته است. با این حال بیانیه انتشار یافته از سوی یکی از نزدیک‌ترین همکاران پوتین، نخست‌وزیر روسیه این حملات را به مقامات روسی نسبت می‌دهد.

Wired Magazine, August 21 2007, Available at http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

انتساب اقدامات بازیگران غیردولتی به دولت سخن به میان آورد برای انتساب اقدامات یک گروه (و نه اقدامات یک فرد) به دولت است. از نظر این دادگاه هرچند برای انتساب اعمال بازیگران غیردولتی غیرسازمان‌یافته (افراد) به دولت به احراز کنترل مؤثر نیاز داریم اما برای انتساب اعمال بازیگران غیردولتی سازمان‌یافته (شرکت) به دولت، احراز کنترل عمومی کافی است.[۶۱] کمیسیون حقوق بین‌الملل با نادیده گرفتن این تفاوت در طرح سال ۲۰۰۱ خود در ارتباط با مسؤولیت بین‌المللی دولت‌ها در ماده ۸ بیان می‌دارد که دولت مسؤول اقدامات «فرد یا گروهی» از افراد است در صورتی که این فرد یا گروه حقیقتاً طبق دستور،[۶۲] هدایت[۶۳] یا کنترل[۶۴] آن دولت عمل کرده باشد. هرچند منظور کمیسیون از عبارت دستور، هدایت و کنترل به خوبی معلوم نیست، اما برخی معتقدند که کمیسیون در این ماده به دکترین نیکاراگوئه (کنترل مؤثر) صحه گزارده است.[۶۵]

در خصوص کنترل دولت بر شرکت‌های ارائه‌کننده خدمات اینترنتی باید توجه داشت که باید میان دو نقش شرکت‌های ارائه‌کننده خدمات اینترنتی قائل به تفکیک شد. زمانی این شرکت‌ها در نقش ناشر اطلاعات ظاهر می‌شوند و زمانی نقش توزیع‌کننده این اطلاعات را دارند. در واقع وقتی اطلاعات توزیع می‌شوند مانند مبادلات الکترونیکی و یا کالا این شرکت‌ها مسؤولیت کمی دارند و مسؤولیت اصلی متوجه کاربران است، چرا که متصدی سیستم نه اجازه و نه امکان بررسی اطلاعات را دارد،[۶۶] اما زمانی که شرکت، ناشر اطلاعات است انتساب اعمال به شرکت آسان‌تر است.[۶۷] چنانچه دادگاه امریکا در پرونده هندریکسون علیه شرکت ای‌بی (eBay) مطرح کرد، شرکت‌ها در قبال ارائه خدمات اینترنتی که از تخلف و تخطی کاربران بی‌اطلاع است،

---

۶۱. زمانی و ضیایی، «تعمیم نظام مسؤولیت بین‌المللی به بازیگران غیردولتی با تأکید بر مسؤولیت بین‌المللی جدایی‌طلبان»، صص ۸۳-۵۵.

62. instruction
63. direction
64. control
65. Mohan, "Terrorism and Asymmetric Warfare: State Responsibility For The Acts of Nonstate Entities - *Nicaragua, Tadic*, and Beyond".
66. Shackelford, "From Nuclear War To Net War: Analogizing Cyber Attacks In International Law", p. 234.

۶۷. در مواردی شرکت‌های واسط و ارائه‌کننده خدمات اینترنتی در نقض حقوق بشر با دولت همکاری می‌کنند مانند همکاری یک شرکت اینترنتی در انگلستان با پلیس انگلستان در نقض کنوانسیون اروپایی حقوق بشر. نک: استون، حقوق بشر و اینترنت، ص ۱۹۷.

مسؤولیت ثانوی ندارند.[۶۸] لذا کنترل مؤثر دولت بر شرکت ارائه‌کننده خدمات اینترنتی که در حمله سایبری مشارکت دارد در چارچوب وظایف نشر اطلاعات و نه توزیع اطلاعات قابل اثبات خواهد بود.[۶۹]

رفتار شخص یا نهادی که ارگان دولتی محسوب نمی‌شود اما به موجب قانون آن دولت مجاز به اعمال اقتدارات دولتی است به موجب حقوق بین‌الملل فعل آن دولت محسوب می‌شود مشروط بر آنکه شخص یا نهاد مزبور در قضیه ذیربط در این سمت عمل کرده باشد. ارائه خدمات اینترنتی اقدامی حاکمیتی است که دولت‌ها آن را به بخش خصوصی واگذار کرده‌اند. این پرسش مطرح می‌شود که همکاری یک شرکت خصوصی ارائه‌کننده خدمات اینترنتی در حمله سایبری موجب انتساب آن عمل به دولت می‌شود؟ همان‌طور که کمیسیون حقوق بین‌الملل در تفسیر شماره ۲ ماده ۵ بیان کرده است که این نهادها شامل «شرکت‌های خصوصی هستند مشروط بر اینکه در هر مورد آن نهاد به موجب قوانین داخلی آن دولت مجاز به اعمال کارکردها و اشتغالاتی با ماهیت عمومی باشد که معمولاً توسط ارگان‌های دولتی اعمال می‌شود». بر این اساس مشارکت عامدانه عمل شرکت‌های خصوصی ارائه‌کننده خدمات اینترنتی در حملات سایبری منتسب به دولت خواهد بود مگر آنکه دولت تلاش مقتضی برای جلوگیری از آن را به عمل آورد.

یکی از مشکلات مربوط به انتساب حمله سایبری به دولت در زمانی اتفاق می‌افتد که چند شرکت اینترنتی واسط وجود داشته باشد. زمانی که حمله سایبری توسط یک دولتی در بالادست صورت می‌پذیرد (دولتی که میزبان سرور ریشه‌ای است) دولت قربانی برای یافتن مسؤول نهایی چاره‌ای ندارد جز آنکه به دولت پایین‌دست‌تر از کشور میزبان سرور ریشه‌ای که انتساب به آن مسلم است رجوع نماید، سپس کشور میزبان آن شرکت به شرکت بعدی که پشتیبان شرکت قبلی است رجوع کند. روش عقب پریدن[۷۰] ادامه پیدا خواهد کرد تا شرکت یا کشوری که مسؤول نهایی است مشخص شود. اما

68. Hendrickson v. eBay Inc., 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

۶۹. ممکن است که مسؤولیت شرکت‌های اینترنتی از جهت حملات سایبری اشخاص خصوصی حقیقی (هکرها) مطرح شود. اصل مسؤولیت نیابتی در بسیاری از کشورها از جمله آمریکا وجود دارد که طبق آن مدیر مسؤول نظارت بر کار زیردستانش است و اگر در انجام وظیفه خود کوتاهی و غفلت کرده باشد موجب مسؤولیت مدیر خواهد شد. این رویه باری را بر دوش بخش‌های خصوصی که کنترل عمومی بر اینترنت دارند می‌گذارد که بر سازه‌های تحت مدیریتشان نظارت پلیسی داشته باشند تا از تخلفات مهم و بالقوه جلوگیری کنند.

70. hop back

این روش به علت زمان‌بر بودن و همچنین به علت نیاز به همکاری کشورهای دیگر موجب جبران خسارت فوری برای قربانی نمی‌شود. برای همین برخی به اعمال اصل تعقیب فوری[۷۱] در فضای سایبر اشاره کرده‌ان که طبق آن دولت قربانی می‌تواند بدون کسب اجازه از کشورهای پایین‌دست، از حوزه صلاحیتی آن‌ها عبور نموده و دست به تعقیب فوری زده و علیه شرکت یا کشور متخلف دست به اقدام متقابل بزند.[۷۲]

لازم به ذکر است که برخی از شرکت‌های ارائه‌کننده خدمات اینترنتی دولتی هستند. باید توجه داشت که صرف دولتی بودن این شرکت‌ها حمله سایبری خودبه‌خود به دولت منتسب نمی‌شود. همان‌طور که کمیسیون حقوق بین‌الملل در تفسیر شماره ٦ ماده ٨ بیان می‌دارد «اینکه شرکتی ابتدائاً خواه به موجب قانون خاص یا به هر طریق دیگر توسط دولت تأسیس شده است دلیل کافی برای انتساب رفتارهای بعدی آن به دولت تلقی نمی‌شود».[۷۳] علت این امر اهمیت شخصیت حقوقی مستقل شرکت است. با این حال در مواردی که کنترل دولت بر اقدامات آن شرکت محرز باشد و یا آن شرکت در چارچوب وظایف اقتدار عمومی خویش عمل کرده باشد انتساب عمل به دولت مفروض خواهد بود.

۳-۲- مسؤولیت ناشی از عمل ارگان‌های دولتی

به موجب ماده ٤ طرح کمیسیون حقوق بین‌الملل رفتار هر ارگان دولتی به موجب حقوق بین‌الملل فعل آن دولت تلقی می‌شود فارغ از اینکه آن ارگان کارکرد تقنینی، قضائی، اجرایی یا کارکردی دیگر داشته باشد و اعم از اینکه ارگان مذکور در سازمان دولتی چه موقعیتی دارد. از آنجا که اصولاً حملات سایبری از گستره‌ای برخوردار است که بدون هماهنگی بخش‌های دولتی امکان آن دور از ذهن است بیشترین اتهام در حملات سایبری متوجه ارگان‌های دولتی است. تشکیل پدافند سایبری، ارتش سایبری و سرویس اطلاعاتی سایبری از سوی برخی کشورها احتمال انتساب حملات سایبری به آن‌ها را قوت می‌بخشد.[۷۴] همچنین احتمال انتساب حملات سایبری به دولتی که انحصار ارائه خدمات اینترنتی را در دست دارد بیش از دولتی است که ارائه خدمات اینترنتی خود را به شرکت‌های خصوصی واگذار کرده است.

71. hot pursuit
72. Todd, "Armed attack in cyberspace: deterring asymmetric warfare with an asymmetric definition".
۷۳. ابراهیم‌گل، پیشین، ص ٦٨.
74. See Heickero, "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations".

چنانچه حملات سایبری با سایر فشارهای بین المللی همراه باشد احتمال انتساب آن به دولت متخاصم بیشتر خواهد بود. به طور مثال در سال ۲۰۰۸ حمله سایبری به گرجستان با حمله ارتش روسیه به این کشور همزمان شده بود و این احتمال را قوت بخشید که عامل اصلی و مجری حمله سایبری به گرجستان، روس‌ها بوده‌اند. بررسی‌های بعدی نشان داد که حملات سایبری از رایانه‌های متعلق به کاربران خانگی در کشورهای مختلف صورت گرفته است که از این حملات بی‌خبر بوده‌اند؛ به این ترتیب که هکرها و مهاجمان سایبری ابتدا با نفوذ به رایانه‌های این افراد و در اختیار گرفتن کنترل آن‌ها، یک ارتش مخفی از رایانه‌ها ساخته و به وسیله آن‌ها به سوژه‌های مورد نظر خود حمله می‌کنند.[۷۵] با این حال برخی دولت‌ها در حملات سایبری بدنام هستند به نوعی که در بیشتر مواقع انگشت اتهام به سمت آن‌ها نشانه می‌رود. چین از جمله کشورهایی است که در حملات سایبری متعددی نقش آفرینی مستقیم آن‌ها به اثبات رسیده است.[۷۶]

همچنین ممکن است مبادرت افراد خصوصی به یک حمله سایبری بتواند برای دولت ایجاد مسؤولیت کند از آن جهت که طبق اصل تلاش معقول برای پیشگیری[۷۷] دولت موظف به پیشگیری و اتخاذ تصمیمات لازم برای مقابله با آن بوده است[۷۸] و در صورت کوتاهی نه از باب انتساب رفتار فرد خصوصی به دولت بلکه به سبب نقض تعهد به پیشگیری موجب طرح مسؤولیت بین‌المللی آن دولت خواهد بود.[۷۹] اولین تعهد دولت‌ها ناشی از این اصل تعهد به قانونگذاری برای جلوگیری از حملات سایبری از سوی شهروندان است[۸۰] که در چارچوب جرایم سایبری و تحت عنوان مجرمانه سابوتاژ (خرابکاری اینترنتی) جرم‌انگاری می‌شود. دیوان بین‌المللی دادگستری در قضیه گروگانگیری بیان داشت که هرچند عمل قابل انتساب به دولت نیست اما امهال در جلوگیری موجب طرح مسؤولیت دولت می‌شود.[۸۱] همان‌گونه که دیوان بین‌المللی

75. Tikk and other, *op. cit.*

76. Creekman, "A Helpless America? An Examination of the Legal Options Available to the United States in Response", p. 641. to Varying Types of Cyber-Attacks from China.

77. Due diligence

۷۸. بند ۳ ماده ١٤ طرح پیش‌نویس کمیسیون به طور ضمنی به این تعهد اشاره می‌کند «نقض تعهد بین‌المللی که دولت را ملزم به پیشگیری از واقعه خاصی می‌کند به هنگام وقوع واقعه محقق می‌شود و به کل دوره‌ای که آن واقعه تداوم داشته و مطابق تعهد نیست توسعه می‌یابد».

79. Shackelford, *op. cit.*, p. 234.

80. Kulesza, *op. cit.*, p. 151.

81. *ICJ Reports*, 1980, p. 3.

دادگستری در قضیه کانال کورفو بیان داشت تعهد به پیشگیری و تلاش معقول برای جلوگیری از وقوع تخلفات بین‌المللی به وسیله امکانات دولتی باعث شده تا در حقوق بین‌الملل هیچ دولتی حق نداشته باشد اجازه دهد تا از قلمرو آن جهت ایجاد ضرر و خسارت به سایر دولت‌ها استفاده شود. هرگاه با وجود کنترل و مراقبت خاص، عمل خلاف حقوق بین‌الملل واقع شد و موجب ضرر و زیان دولت خارجی یا اتباع آن گردید، نخستین وظیفه دولتی که جرم در قلمرو آن واقع شده این است که مرتکب جرم را تعقیب و مجازات کند.[۸۲] همچنین باید مقصر را ملزم به جبران خسارت نماید و به عبارت دیگر، باید از خسارت دیدگان رفع خسارت نماید در غیر این صورت موجب مسؤولیت بین‌المللی دولت خواهد شد.[۸۳]

لذا در حمله سایبری سازمان ناسزی[۸۴] به استونی هرچند انتساب عمل به دولت روسیه اثبات نشد اما خودداری دولت روسیه در جلوگیری از حملات سایبری از کشورش مسؤولیت بین‌المللی این دولت را می‌تواند به دنبال داشته باشد در حالی که تعقیب و مجازات عاملین حمله سایبری طلوع خورشید شمسی[۸۵] توسط رژیم صهیونیستی مسؤولیت را از این دولت مرتفع کرده است.[۸۶] همچنین طبق اصل تلاش معقول برای پیشگیری در حملات سایبری دولت‌های محل استقرار سرورهای بالادستی ملزم هستند تا برای یافتن متخلف همکاری لازم را داشته باشند که در غیر این صورت مسؤولیت آن‌ها از جهت معاونت در تخلف قابل طرح خواهد بود.

٤- جبران خسارت در حملات سایبری

در خصوص مسؤولیت بین‌المللی دولت سه نظریه وجود دارد: نظریه خطا، خطر و مسؤولیت ناشی از اعمال منع نشده. در نظریه خطا لازم است تا تخلف دولت و تقصیر دولت اثبات شود، در نظریه خطر لازم است تا فقط تخلف دولت اثبات شود و در نظریه مسؤولیت ناشی از اعمال منع نشده (یا مسؤولیت ناشی از اعمال خطرناک) صرفاً

---

۸۲. باید توجه داشت که صرف استقرار رایانه‌ای که حملات سایبری از آن صورت گرفته است در سرزمین یک دولت به معنای انتساب آن حمله به دولت نخواهد بود و دولت به جهت تعهد به تعقیب و مجازت مسؤولیت خواهد داشت.

D'Souza, *op. cit.*
83. Brerly,1963: 289.
84. Naszi organization
85. Solar Sunrise
86. Kulesza, "State responsibility for cyber-attacks on international peace and security", p. 150.

لازم است تا ورود خسارت اثبات شود حتی اگر تخلفی رخ نداده باشد. نتیجه اتخاذ هر یک از این سه رویکرد نیز متفاوت خواهد بود: در حالی که دولت مسؤول در رویکرد اول و دوم موظف به جبران خسارت کامل (اعم از اعاده وضع به حال سابق، توقف عمل متخلفانه، تضمین به عدم تکرار عمل متخلفانه و پرداخت غرامت) است، دولت مسؤول در رویکرد سوم تنها موظف به پرداخت غرامت خواهد بود.

مسأله اصلی در طرح مسؤولیت دولت ناشی از حملات سایبری به علت پیچیدگی شبکه‌های اینترنتی و بازیگران اینترنتی، «مرتکب» حمله سایبری است و تکیه بر نظریه خطر نمی‌تواند اهداف این نظریه را تأمین نماید. به عبارت دیگر نظریه خطر در جایی کارآیی دارد که مرتکب مشخص باشد. از سوی دیگر احراز تقصیر می‌تواند در انتساب عمل به دولت کمک‌کننده باشد. در واقع از طریق احراز تقصیر می‌توان دولت مسؤول در حمله سایبری را یافت. تقصیر در این مورد در احراز انتساب عمل، طریقیت خواهد داشت و اثبات تقصیر می‌تواند یکی از راه‌های احراز انتساب باشد؛ کما اینکه در حقوق داخلی نیز برخی قائل به طریقیت تقصیر در اثبات رابطه سببیت هستند.[۸۷] لذا تأکید بر تقصیر یا سوء نیت می‌تواند تا حدودی این اطمینان را حاصل کند که با یافتن «مقصر» در اصل «مرتکب» را نیز یافته‌ایم. لذا نظریه تقصیر برای طرح مسؤولیت دولت ناشی از حملات سایبری مناسب‌تر به نظر می‌رسد.

باید توجه داشت که ابتنای مسؤولیت بین‌المللی دولت ناشی از حملات سایبری بر نظریه «تقصیر» موجب می‌شود تا نتیجه مسؤولیت صرفاً به پرداخت غرامت محدود نشود بلکه دولت متخلف ملزم به توقف و عدم تکرار نقض تعهد خود نیز گردد.[۸۸] طبق ماده ۳٤ طرح پیش‌نویس مسؤولیت بین‌المللی دولت‌ها جبران کامل زیان ناشی از فعل متخلفانه بین‌المللی اعاده وضع به حال سابق، غرامت و جلب رضایت است که منفرداً یا مجتمعاً برطبق مقررات این فصل صورت می‌گیرد.

٤-۱- توقف و عدم تکرار

ماده ۳۰ طرح مسؤولیت بین‌المللی دولت‌ها دولت مسؤول را متعهد می‌داند که الف) در صورت تداوم فعل، آن را متوقف کند و ب) در صورتی که شرایط ایجاب نماید اطمینان و تضمینات مناسبی برای عدم تکرار آن ارائه نماید. تعهد به متوقف ساختن

۸۷. انتظاری و محقق‌داماد، «نقش اتلاف و تسبیب در مسؤولیت مدنی زیست محیطی»، ص ٤۸.

88. International Law Commission, *The Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries (2001)*, Arts. 30-31.

عمل نادرست تا زمانی باقی است که عمل نادرست وجود یا ادامه داشته باشد. در حملات سایبری دولت صدمه دیده در هر لحظه می‌تواند از دولت متحاجم درخواست توقف عمل نادرست را بنماید. در این صورت دولت مسؤول با شناسایی عوامل متجاوز یا قطع اینترنت لازم است به تعهد خود مبنی بر توقف عمل متخلفانه عمل نماید. برای تضمین به عدم تکرار در مواردی دولت‌ها درخواست می‌کنند دستورات خاصی صادر شود یا رفتارهای خاصی اتخاذ شود.[۸۹] در حملات سایبری که ناشی از فعل اشخاص خصوصی بوده باشد با اصلاح قوانین ناظر بر ارائه خدمات اینترنتی و جرایم اینترنتی، تضمین به عدم تکرار امکانپذیر است.

٤-۲- اعاده وضع به حال سابق

اصولاً خسارات وارد شده باید به صورت کامل جبران شود.[۹۰] بدین ترتیب که تا آنجایی که ممکن است تمامی آثار ناشی از عمل متخلفانه را از بین برده و دوباره وضعیتی را برقرار کند که با وجود تمام احتمالات می‌توانست در صورت عدم وقوع آن عمل غیرحقوقی وجود داشته باشد.[۹۱] نخستین روش جبران خسارت در ماده ۳۱ طرح مسؤولیت بین‌المللی دولت‌ها اعاده وضع به حال سابق است، این روش بر پرداخت غرامت اولویت دارد.[۹۲] بدین معنا که ابتدا دولت زیان‌زننده از طریق اعاده به وضعیت سابق خسارات وارده را جبران کند و اگر این امر میسر نشد یا کفایت نکرد، از روش‌های دیگری برای جبران استفاده نماید. دولت مسؤول، در صورتی مکلف به اعاده به وضع سابق است که این اعاده به لحاظ مادی غیرممکن نبوده و یا به طورکلی نامناسب نباشد.[۹۳]

در حملات سایبری با فرض اینکه این خسارات غیرمادی هستند آیا برای دولت مسؤول این امکان فراهم خواهد شد تا سیستم‌های مورد نفوذ قرار گرفته را به حالت سابق اعاده کند؟ در اکثر مواقع این خود سیستم‌ها نیستند که مورد حمله قرار میگیرند، بلکه اطلاعات سری و امنیتی آن‌هاست که مورد نفوذ و تغییرات قرار می‌گیرد و نیاز دارند که مجدداً کدبندی شوند. به نظر می‌رسد در این شرایط دولت قربانی حملات سایبری نمی‌تواند بار دیگر به دولت حمله‌کننده اعتماد کرده و سیستم‌های خود را برای

89. *Ibid*, Commentary No. 13.
90. *Ibid*, Art. 31(1).
91. Factory of Chorzow, Merits, 1928, P.C.I.J, Series A No. 17, p. 47.
92. International Law Commission, *op. cit.*, p. 238.
93. *Ibid*, Art. 35.

بازیابی در اختیار آن دولت قرار دهد، چرا که امکان این وجود دارد که دولت حمله‌کننده راه‌های نفوذ بی‌دردسری برای حملات آتی خود در سیستم‌ها ایجاد کند. لذا در حملات سایبری اعاده وضعیت به حالت سابق به طور عملی تقریباً غیرممکن است.

٤-۳- غرامت

پرداخت غرامت[۹۴] رایج‌ترین روش جبران خسارات قلمداد شده است. در این خصوص ماده ۳٦ طرح مسئوولیت بین‌المللی دولت‌ها بیان می‌دارد که دولت مسؤول در نتیجه ارتکاب عمل نامشروع موظف است که با پرداخت غرامت، خساراتی را که به وسیله اعاده وضع سابق قابل جبران نمی‌باشند، جبران نماید. خسارات اعم از خسارات مادی و معنوی است[۹۵] و دولت زیان‌زننده ملزم به جبران هر دو زیان است. برای پرداخت غرامت، حتماً باید ضرری به دولت صدمه دیده وارد شده باشد و صرف نقض حقوق بدون ورود خسارت، هر چند که موجب مسئوولیت دولت است از طریق پرداخت غرامت جبران نخواهد شد.[۹۶] لذا می‌توان گفت که پرداخت غرامت جنبه تنبیهی ندارد بلکه ویژگی اصلی آن ترمیمی بودن آن است. تنها خساراتی مشمول پرداخت غرامت میشود که قابل ارزیابی مالی باشند. این خسارت ممکن است به خود دولت یا اتباعش وارد آید که خسارات وارد بر آن‌ها هم ممکن است شخصی یا مالی باشد.[۹۷]

شاید بتوان خساراتی که در اثر برخی حملات سایبری وارد می‌شود را به دو دسته خسارات مادی و معنوی تقسیم نمود. خسارات وارده به تأسیسات زیرساختی مانند بانک‌ها، سدها، تأسیسات هسته‌ای، سیستم حمل و نقل و غیره خساراتی مادی تلقی می‌شوند اما چون نتیجه مستقیم حملات نیستند ممکن است به جهت فقدان رابطه سببیت میان حمله و خسارت مشمول غرامت نگردد. به طور مثال حملات سایبری به وب‌سایت‌های مهم دولتی استونی در سال ۲۰۰۷ موجب نافرمانی مدنی وسیع و آشوب‌هایی شد که منجر به زخمی شدن ۱۵۰ نفر و کشته شدن یک تبعه روسی گردید.[۹۸] میان صدمات و تلفات انسانی و حملات سایبری به استونی رابطه سببیت

94. Compensation
95. *Ibid*, Art. 31(2).
96. *Ibid*, Art. 36, para. 4, p. 12.
97. *Ibid*, para. 5, p. 12.
98. "Putin Warns Against Belittling War Effort", Radio Free Europe, May 9, 2007. Available at: http://www.rferl.org/featuresarticle/2007/05/704c2d80-9c47-4151-ab76-

در ۲۷ آوریل ۲۰۰۷ استونی مورد حمله اینترنتی قرار گرفت. طی چند ساعت شبکه‌های اینترنتیِ بانک‌های اصلی استونی از کار انداخته شده و انتشار تمام روزنامه‌های اصلی متوقف شد. ارتباطات دولتی مختل گردید. ←

نزدیکی وجود ندارد و لذا دریافت غرامت از این جهت با مشکل مواجه خواهد شد. همچنین خسارات معنوی مانند خسارات به اطلاعات و دستاوردهای اطلاعاتی دولت جنبه معنوی دارد که محاسبه میزان صدمه به این بخش آسان نخواهد بود.

برای جبران این نقیصه می‌توان روش خسارت تنبیهی[۹۹] در حملات سایبری در نظر گرفته شود. خواستگاه اصلی این خسارت در حقوق کامن‌لا میباشد. با توجه به اینکه محاسبه خسارت وارد شده در اثر حملات سایبری اعم از خسارات مادی و معنوی ممکن و دقیق نیست و در اکثر مواقع حتی مبهم است و حتی ممکن است بعدها آسیب‌های وارد شده مشخص شوند این روش به انصاف نزدیک‌تر است.

٤-٤- جلب رضایت

جبران خسارت به این روش میتواند به شکل تأیید نقض تعهد، ابراز تأسف، معذرت خواهی رسمی یا دیگر اشکال مناسب صورت پذیرد.[۱۰۰] اصولاً جلب رضایت در ارتباط با زیان‌هایی که به لحاظ مادی قابل ارزیابی نمی‌باشند به کارگرفته می‌شود. این روش جبران خسارت را نمی‌توان ابزاری مناسب برای جبران خسارت دانست. به همین دلیل است که ماده ۳۱ طرح مسئوولیت بین‌المللی دولت‌ها زمانی دولت مسؤول را وادار به استفاده از جلب رضایت می‌کند که نتواند از اعاده وضع به حال سابق یا پرداخت غرامت استفاده کند.[۱۰۱]

در حملات سایبری ممکن است اظهار ندامت روش مناسبی برای جبران باشد، چه آنکه در بسیاری از موارد حمله سایبری با هک سایت‌های اساسی دولت قربانی همراه است. این سایت‌ها که زمانی از سوی دولت مهاجم هک شده بودند مکان مناسبی برای انتشار عذرخواهی همان دولت است. البته ممکن است اظهار ندامت هیچگاه روش متناسبی با خسارات وارده مانند از دست رفتن اطلاعات امنیتی و ملی دولت تلقی نشود، اما می‌توان جلب رضایت را یک روش مبتنی بر نزاکت بین‌المللی پس از حمله سایبری دانست.

←
کشور استونی با تأسیس دولت الکترونیک نود درصد از خدمات بانکی و حتی انتخابات پارلمانی را توسط اینترنت تحت پوشش قرار داده بود. استونی مالیات‌ها را به طور آنلاین دریافت می‌کرد و از سیستم تلفن همراه برای خرید و پرداخت پول پارکینگ استفاده می‌کرد. شاکل فورد، «از جنگ هسته‌ای تا جنگ اینترنتی: مشابهت‌سازی حملات سایبری در حقوق بین‌الملل».

99. Punitive Damages
100. International Law Commission, *op. cit.*, p. 262, para. 5.
101. *Ibid*, para. 1, p. 12.

۵- نتیجه گیری

در دورانی که اصل منع توسل به زور به عنوان یک قاعده آمره بین‌المللی از سوی دولت‌های عضو جامعه بین المللی به رسمیت شناخته شده است کمتر دولتی به خود این جرأت را می‌دهد تا از طریق حمله نظامی منویات خود را دولت دیگر تحمیل نماید. امروزه دولت‌ها تلاش می‌کنند تا از طریق سایر اشکال فشارهای بین‌المللی اعم از اقتصادی، فرهنگی و سیاسی دیگر دولت‌ها را وادار به پذیرش مطالبات خود نمایند. یکی از این اشکال نوین فشارهای سایبری است. مداخلات سایبری برخلاف سایر اشکال اقتصادی، فرهنگی و سیاسی واجد ویژگی گمنامی[۱۰۲] است. دولت‌ها می‌توانند در پوشش عناوین مختلف و با گذر از سرورهای اینترنتی مختلف رد پای خود را از این اقدامات پاک نمایند. لذا اثبات انتساب این‌گونه اقدامات به دولت از پیچیدگی خاصی برخوردار است.

تبیین چارچوب حقوقی مناسب در رابطه با مسؤولیت بین‌المللی دولت ناشی از حملات سایبری گامی برای جلوگیری از حملات سایبری و جبران خسارات وارده ناشی از آن است. خسارات ناشی از حملات سایبری از جمله در سیستم‌های بخش انرژی و حمل و نقل بعضاً آنقدر وسیع است که آقای شاکلفورد آن‌ها را با جنگ هسته‌ای مقایسه نموده است. برای طرح مسؤولیت دولت‌ها در حملات سایبری لازم است اولاً مشخص شود حمله سایبری منطبق با کدام یک از اقدامات متخلفانه بین‌المللی است و ثانیاً حمله سایبری به کدام دولت قابل انتساب است.

جز در صورتی که اینترنت به عنوان یک جنگ‌افزار در نظر گرفته شود نمی‌توان حملات سایبری را مصداق «حمله مسلحانه» موضوع بند ٤ ماده ۲ منشور ملل متحد دانست. همچنین حملات سایبری جز در موارد استثنائی نمی‌تواند مصداقی از «تجاوز» و «توسل به زور» تلقی شود، اما در این تردیدی وجود ندارد که حملات سایبری مصداقی از «مداخله در امور داخلی دولت» است. لذا دولت قربانی می‌تواند با تأسی به نظام حقوق مسؤولیت بین‌المللی جبران خسارت کافی از این حملات را بخواهد.

از آنجا که ماهیت فضای سایبر این امکان را فراهم آورده که اشخاص خصوصی نیز دست به حملات سایبری بزنند انتساب عمل به دولت اهمیت دوچندان می‌یابد. حملات سایبری از سوی افراد خصوصی در صورتی به دولت منتسب خواهد شد که

102. anonymous

این افراد در استخدام دولت و یا تحت هدایت و کنترل دولت بوده باشند. همکاری شرکت‌های خصوصی ارائه‌کننده خدمات اینترنتی نیز در صورتی که در چارچوب اقتدار عمومی (امور مخابراتی) عمل کرده باشد مسؤولیت دولت را به دنبال خواهد داشت و در غیر این صورت تنها در مواردی که شرکت در چارچوب نشر اطلاعات فعالیت می‌کند و دولت کنترل مؤثری بر آن داشته است مسؤولیت دولت قابل طرح خواهد بود. باید توجه داشت اتکا به نظریه تقصیر در مسؤولیت بین‌المللی دولت‌ها ناشی از حملات سایبری می‌تواند خطرات ناشی از ابهام در دولت مسؤول را کمرنگ کند؛ چرا که در این حالت یافتن «مقصر» به یافتن «مرتکب» منجر خواهد شد.

پیوستگی روزافزون شبکه‌های اینترنتی و ضرورت بهره‌برداری دولت از اینترنت از جمله تشکیل دولت الکترونیک موجب شده است تا نگرانی دولت‌ها راجع به حملات سایبری نیز روزافزون شود. این نگرانی در صورتی تعدیل خواهد شد که نظام مسؤولیت بین‌المللی دولت به عنوان ضامن اجرای قواعد حقوقی بین‌المللی کارآمد باشد. در غیر این صورت دولت‌ها به سمت اتخاذ تدابیری یکجانبه نظیر دفاع پیشدستانه و تجاوز تلقی کردن حملات سایبری خواهند رفت. به طور مثال راسموسن،[۱۰۳] دبیرکل ناتو با تنظیم برنامه‌ای جدید، استراتژی پیمان نظامی ناتو در قرن بیست و یکم را به کشورهای عضو ارائه داده که در آن بر اهداف مهمی همچون دفاع مشترک در مقابل حملات سایبری و همکاری نزدیک با روسیه تأکید کرده است.[۱۰۴] پیمان آتلانتیک شمالی (ناتو) بر آن است که خود را در برابر حملات و تهدیدات سایبری مجهز سازد. یکی از مهم‌ترین خطرات جدید به گفته راسموسن حملات سایبری است که این خطر به معنای ساده، حمله گسترده به سیستم‌های کامپیوتری در کشورهای عضو است.[۱۰۵] مشخص است که عدم تقویت مبانی نظام مسؤولیت بین المللی دولت ناشی از حملات سایبری می‌تواند به همه‌گیر شدن این رویکرد در سایر دولت‌ها و سازمان‌های بین‌المللی منجر شود. لذا لازم است نظام حقوق مسؤولیت بین‌المللی دولت در خصوص حملات سایبری با در نظر داشتن ویژگی‌های خاص فضای سایبر خود را با تحولات نوین منطبق نماید.

---

103. Anders Fogh Rasmussen

۱۰۴. روزنامه آلمانی «زود دویچه» به نقل از دبیر کل ناتو گزارش می‌دهد که از این پس پیمان ناتو نه تنها علیه حملات نظامی، بلکه در مقابل حملات اینترنتی نیز موظف به دفاع و مبارزه مشترک است.

105. Hughes, "NATO and Cyber Defence: Mission Accomplished?".

فهرست منابع

ابراهیم گل، علیرضا. ***متن و شرح مواد کمیسیون حقوق بین‌الملل در خصوص مسؤولیت بین‌المللی دولت***، نشر شهر دانش، ۱۳۸۸.

استون، هیک. ***حقوق بشر و اینترنت***، ترجمه و تحقیق سید قاسم زمانی و مهرناز بهراملو، نشر خرسندی، چاپ اول، ۱۳۸٦

اکهرست، مایکل. ***حقوق بین‌الملل نوین***، ترجمه مهرداد سیدی، چاپ اول، تهران: دفتر خدماتی حقوقی بین‌المللی جمهوری اسلامی ایران،۱۳۷۳.

انتظاری، علیرضا، و سید مصطفی محقق داماد، نقش اتلاف و تسبیب در مسؤولیت مدنی زیست محیطی، ***مجله مطالعات اسلامی***، شماره ۸۹، ۱۳۹۱.

ثریانی آذر، حسین. ***حقوق بین‌الملل عمومی***، چاپ اول،تهران: قوس،۱۳۸۲

جلالی فراهانی، امیر حسین. تروریسم سایبری، نشریه فقه و حقوق، شماره ۱۰، ۱۳۸۵

خداقلی، زهرا. ***جرائم کامپیوتری***، انتشارات آریان، چاپ اول، سال ۱۳۸٤

زمانی، سیدقاسم، و سید یاسر ضیایی، تعمیم نظام مسؤولیت بین‌المللی به بازیگران غیردولتی؛با تأکید بر مسؤولیت بین‌المللی جدایی‌طلبان، ***مجله حقوقی بین‌المللی***، شماره ٤٥، ۱۳۹۱

سازمان ملل، ***نشریه بین‌المللی سیاست جنائی***، ترجمه دبیرخانهٔ شورای عالی انفورماتیک، سازمان برنامه و بودجه کشور، ۱۳۷٦

شاکل فورد، اسکات جی. ***از جنگ هسته‌ای تا جنگ اینترنتی: مشابهت‌سازی حملات سایبری در حقوق بین‌الملل***، ترجمه سید یاسر ضیایی، قابل دسترسی در http://diplomatist.blogfa.com/post-145.aspx

ضیایی، یاسر. حمایت از حقوق بشر در فضای سایبر، ***مجله پژوهشهای حقوقی***، شماره ۲۱، ۱۳۹۲.

مورکیان علی آباد، محمود. ***پایان‌نامه جنگ اطلاعات از منظر حقوق بین‌الملل***، دانشگاه علامه طباطبایی، ۱۳۸۵

A/RES/36/103, Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States 91st plenary meeting, 9 December 1981.

Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, 28.I.2003, available at

Agreement Between The Governments Of The Member States Of The Shanghai Cooperation Organization On Cooperation In The Field Of International Information Security, 61st Plenary Meeting (Dec. 2, 2008)

available at http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

Barton Gellman, ***Cyber Attacks by al Qaeda Feared***, Washington Post, 2002, available at http://ellen-bomer.com/Osama/Cyber-Attacks.html

Barton Gellman, Cyber Attacks by al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say, ***Washington Post***, June 27, 2002, at A1.

Blog of the European Journal of International Law, ***The Tallinn Manual on the International Law applicable to Cyber Warfare***, 2013, available at http://www.ejiltalk.org/the-tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/

Cees Hamelink, Human Rights in Cyberspace, available at http://www.religion-online.org/showarticle.asp?title=283

Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX).

Draft articles on Responsibility of States for Internationally wrongful Acts (2001)

Duncan B. Hollis, Why States Need an International Law for Information Operations, 11 Lewis & Clark Law Review. 1023, 1042 (2007).

Duncan B. Hollis, Why States Need an International Law for Information Operations, Lewis & Clark Law Review, No. 11, 2007, p.1042.

Elizabeth A. Martin, ***Dictionary of Law***, Oxford University Press, sixth edition, 2006

Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul, Cyber ***Attacks Against Georgia Legal Lessons Identified***, Tallinn: NATO Cooperative Cyber Defence Center of Exellence, 2008

Factory of Chorzow, Merits, 1928,P.C.I.J, Series A No.17, p.47

General Assembly Res. 3281, 1974.

Graham H. Todd, Armed attack in cyberspace: deterring asymmetric warfare with an asymmetric definition, ***Air Force Law Review***, 2009

http://conventions.coe.int/Treaty/EN/Treaties/html/189.htm

http://www.au.af.mil/au/awc/awcgate/army/jaoac-io.pdf U.S. Department of Defense Report.

http://www.rferl.org/content/Georgian_Government_Accuses_Russia_Of_Cyberwar/1190477.html

http://www.root-servers.org/

http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

http://www.wired.com/dangerroom/2009/03/georgia-blames/

ICJ Rep. Congo v. Belgium, 2002, Dissenting Opinion by Judge Van Den Wyngaert, Para 36.

ICJ Rep. Military and Paramilitary Activities in and against Nicaragua,1986

Joanna Kulesza, State responsibility for cyber - attacks on international peace and security, Polish Yearbook of International Law, 2009, p. 150.

Kiran. Mohan. V., Terrorism And Asymmetric Warfare: State Responsibility For The Acts Of Non-State Entities Nicaragua, Tadic, And Beyond, ***Journal of the Institute of Justice and International Studies***, 2008.

Lawrence T. Greenberg, Seymour E. Goodman, Kevin J. Soo Hoo, ***Information Warfare and International Law***, Natl Defense Univ Pr, 1997.

Lech J. Janczewski, Andrew Michael Colarik, ***Cyber warfare and cyber terrorism***, Idea Group Inc (IGI), 2008, p. xiv.

Libicki, Martin C., ***What is Information Warfare***? (Washington, D.C.: National Defense University Press, 1995).

Marina Spinedi, State Responsibility v. Individual Responsibility for International Crimes: Tertium Non Datur?, ***European Journal of International Law***, Vol. 13, No. 4, 2002

Matthew C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), The Yale Journal Of International Law, Vol. 36, p.420.

Matthew C.Waxman, Cyber Attack And The Use of Force, ***Yale Journal of International Law***, Vol. 36, 2011.

Michael P. Scharf, Universal Jurisdiction and the Crime of Aggression, ***Harvard International Law Journal***, Vol. 53, 2012, p. 358.

More Than Firewalls: Three Challenges to American Cyber Security, Asymmetric Threat (Aug. 2011), available at http://asymmetricthreat.net/docs/ snapshot2011_08.pdf (citing Clarke's definition); Understanding Cyber Warfare.

N. Shachtman, Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It, Wired Magazine, March 11, 2009,

Nikhil D'Souza, ***Cyber Warfare and State Responsibility: Developments in International Law***, Working Paper, 2011, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1842984

Nils Melzer, ***Cyberwarfare and International Law***, United Nations Institute for Disarmament Research, 2011, available at

Putin Warns Against Belittling War Effort, Radio Free Europe, May 9, 2007. Available at: http://www.rferl.org/featuresarticle/2007/05/704c2d80-9c47-4151-ab76-

R.Synovitz, Georgian Government Accuses Russia Of Waging 'Cyberwarfare', ***Radio Free Europe***, August 12, 2008,

Rex B. Hughes, *NATO and Cyber Defence: Mission Accomplished?*, ATLANTISCH PERSPECTIEF (Apr. 2009), *available at* http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf

Ronald Heickero, ***Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations***, Swedish Defence Research Agency, Defence Analysis, 2010, available at http://www.foi.se

Santiago M. Villalpando, Attribution of Conduct to the State: How the Rules of State Responsibility may be Applied Within the WTO Dispute Settlement System, ***Journal of International Economic Law***, 2002, 5(2)

Scott J. Shackelford, From Nuclear War To Net War: Analogizing Cyber Attacks In International Law, ***Berkeley Journal of International Law***, Vol. 27, 2008

Sebastian Heselhaus, ***International Law and the Use of Force***, in: A. Schwabach/A. Cockfield (Hrsg.), The Role of International Law and institutions, Kap. 1.36.1.7., in: Encyclopedia of Life Support Systems (EOLSS), EOLSS-Publishers under the auspices of UNESCO, Oxford, 2002.

Security Council Resolution 1368 (2001), 1703 (2006).

Swedish Defense University with preliminary conclusions on 'Cyberattack against Georgia', August 2008.

The Central Intelligence Agency (CIA) is an independent US Government agency responsible for providing national security intelligence to senior US policymakers.

The National Aeronautics and Space Administration (NASA) is the agency of the United States government that is responsible for the nation's civilian space program and for aeronautics and aerospace research.

The Prosecutor v. Duško Tadic, 1997

Tom Gjelten, Extending the Law of War to Cyberspace, ***National Public Radio*** (Sept. 22, 2010), available at http://www.npr.org/templates/story/story.php?storyId=130023318 (last visited Apr. 18, 2012).

Tom Gjelten, ***Extending the Law of War to Cyberspace***, National Public Radio, 2010, available at http://www.npr.org/templates/story/story.php?storyId=130023318

Vida M. Antolin-Jenkins, Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places, ***51 Naval Law Review*** . 132, 140 (2005).

Vida M. Antolin-Jenkins, Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places, ***Naval Law Review***, No. 51, 2005, p. 140.

Wired Magazine, August 21 2007,

Yaroslav Shiryaev, Cyberterrorism in the Context of Contemporary International Law, ***San Diego International Law Journal***, Vol. 14, 20102, p. 139.

International Responsibility of State in Cyber Attacks

Seyed Yaser ZIAEE (Ph.D.)
Assistant Professor of International Law, University of Qom
Mona KHALILZADEH
LL.M. Student in International Law, IAU, Central Tehran branch

Cyber attacks are recognized as a new form of cyber interventions. Cyber attacks are targeting basic installations like governmental bank, energy, transportation systems which connected to cyber networks. Although cyber attacks aren't kinds of use of force, aggression or armed attack but they are kinds of intervention in internal affairs of State which are a breach of international law. A state would be responsible if the attack attributes to that State. Cyber attack can be done by individuals who are employed by State and by Internet Service Provider Companies in to extent which these cyber attacks are done in public authority of that state. In this way it is necessary that that Draft Convention on International Responsibility of State be amended in relation to cyber attack requirements.

Keywords: cyber space, cyber attack, attribution of wrongful Act to a state, international responsibility, compensation.

ISSN 1682-9220

Journal of LEGAL RESEARCH

VOL. XII, No. 1 2013-1

S. D. I. L.
The S.D. Institute of Law
Research & Study