Public Law Studies Quarterly, Vol. 50, No. 4, Winter 2021
DOI: 10.22059/jplsq.2020.274302.1912

Cyber Espionage in International Law: Attribution of International Responsibility to States in a State of Uncertainty

(Type of Paper: Research Article)

Aramesh Shahbazi [1*], Aida Aghajani Ronaghi [2]

Abstract

The rapid advancement of technology and the unique characteristics of cyberspace have caused change in many of international law's classic concepts, and in most cases, the lack of coherent customary regimes prepared grounds for new interpretation of classic concepts. Cyber espionage is a relatively new concept in international law, and there is no agreement on legal regime governing it. Ambiguity and fear of extending principles and rules governing espionage in traditional sense, to cyberspace, which is generally the domain of soft law practice, has put international law governing this new concept in a state of uncertainty. Therefore, on one hand, the legitimacy of extraterritorial infiltration acts of States through espionage remains controversial, and on the other hand, the use of virtual instruments by States for advancing their extraterritorial infiltration into cyberspace of other States, has fueled ambiguities. The lack of specific international customary and treaty obligations in this regard paves the way for the application of general principles and rules of international law. This article seeks to elucidate the concept and scope of cyber espionage and the international responsibility arising from it, taking into account, State practice and doctrine, to answer this fundamental question that, which principles and rules of international law govern cyber espionage.

Keywords

International Wrongful Acts, Cyber Espionage, International Law, Cyber Space, International State Responsibility.

---

1. Associate Prof., Department of Public and International Law, Faculty of Law and Political Science, University of Allameh Tabataba'i, Tehran, Iran (Corresponding Author).
Email: a.shahbazi@atu.ac.ir
2. Ph.D. Student in International Law, Faculty of Law and Political Science, University of Allameh Tabataba'i, Tehran, Iran. Email: aida_agh.r2002@yahoo.com
Received: January 21, 2019 - Accepted: February 17, 2020

فصلنامهٔ مطالعات حقوق عمومی، دورهٔ ۵۰، شمارهٔ ۴، زمستان ۱۳۹۹: ۱۴۸۷-۱۵۰۳
DOI: 10.22059/jplsq.2020.274302.1912

جاسوسی سایبری در حقوق بین‌الملل: مسئلهٔ انتساب مسئولیت بین‌المللی به دولت در هاله‌ای از ابهام

(نوع مقاله: علمی _ پژوهشی)

آرامش شهبازی [1*]، آیدا آقاجانی رونقی [2]

چکیده

سرعت پیشرفت فناوری و ویژگی‌های منحصربه‌فرد فضای سایبر سبب تغییر بسیاری از مفاهیم سنتی حقوق بین‌الملل شده و در مواردی، شکل نگرفتن رژیم‌های هنجاری منسجم، تنها زمینهٔ تفسیر جدید از مفاهیم سنتی را فراهم کرده است. جاسوسی سایبری در حقوق بین‌الملل، در زمرهٔ مفاهیم نسبتاً جدیدی است که در زمینهٔ رژیم حقوقی حاکم بر آن در حقوق بین‌الملل موجود اتفاق نظری در میان نیست. بیم و ابهام در تسری اصول و قواعد حاکم بر جاسوسی در مفهوم کلاسیک به فضای سایبری که اغلب قلمرو اعمال حقوق نرم است، اضافه شده و حقوق بین‌الملل حاکم بر مفهوم جدید را در هاله‌ای از ابهام قرار داده است، به‌گونه‌ای که از یک‌سو، مشروعیت اقدامات دولت‌ها به نفوذ فراسرزمینی از طریق جاسوسی، همچنان محل تأمل است و از سوی دیگر توسل دولت‌ها به ابزار و ادوات مجازی برای پیشبرد نفوذ فراسرزمینی در قلمرو دولت دیگر در فضای سایبر، بر ابهامات موجود دامن زده است. فقدان تعهدات بین‌المللی عرفی و قراردادی خاص در این خصوص، باب اعمال اصول و قواعد عام حقوق بین‌الملل را باز می‌کند. این مقاله درصدد تبیین و تحلیل مفهوم و قلمرو جاسوسی سایبری و مسئولیت بین‌المللی ناشی از این اقدام از منظر دکترین، مواضع و رویه بین‌المللی دولت‌هاست تا به این پرسش اساسی پاسخ دهد که اصول و قواعد حاکم بر اقدامات دولت‌ها در این زمینه چیست.

کلیدواژگان

اعمال متخلفانهٔ بین‌المللی، جاسوسی سایبری، حقوق بین‌الملل، فضای سایبر، مسئولیت بین‌المللی دولت‌ها.

---

۱. دانشیار، گروه حقوق عمومی و بین‌الملل، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه علامه طباطبایی، تهران، ایران (نویسندهٔ مسئول). Email: a.shahbazi@atu.ac.ir

۲. دانشجوی دکتری حقوق بین‌الملل، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه علامه طباطبایی، تهران، ایران. Email: aida_agh.r2002@yahoo.com

تاریخ دریافت: ۱۳۹۷/۱۱/۰۱ - تاریخ پذیرش: ۱۳۹۸/۱۱/۲۸

مقدمه

عصر اطلاعات که جلوهٔ بارزی از عصر کنونی است، دستاورد پیشرفت بشر در پیدایش نرم‌افزارهای رایانه‌ای جدید و استفاده از اینترنت به‌عنوان محیطی برای اتصال شبکه‌های رایانه‌ای است. در نتیجهٔ اهمیت و جایگاه برخی اطلاعات موجود در این فضا، زمینه‌هایی جدی برای نفوذ در اطلاعات یا حتی جابه‌جایی این اطلاعات با هدف دستکاری یا بهره‌برداری فراهم می‌شود. نمی‌توان انکار کرد که امروزه دولت‌ها با تهدیدهای جدی در زمینهٔ امنیت و حفاظت از اطلاعات، به‌ویژه اطلاعات مهم و طبقه‌بندی‌شده روبه‌رو هستند. از آنجا که هر پدیدهٔ نوظهور می‌تواند در جامعهٔ بین‌المللی مورد استفادهٔ مطلوب یا سوء استفاده قرار گیرد، فضای سایبر نیز بستری برای تسهیل بهره‌برداری از اطلاعات موجود در این فضا فراهم کرده است. با توجه به ویژگی‌های خاص فضای سایبری و گستردگی افعال و اقدامات قابل وقوع در این شبکه، مواجه شدن با پدیدهٔ جاسوسی در این محیط نوظهور نباید چندان عجیب به‌نظر برسد، زیرا وقوع این امر بارها و به‌دفعات در دنیای واقعی محقق شده و فضای مجازی که قابلیت‌های متعددی را برای سارقان اطلاعات فراهم می‌کند، می‌تواند به تسهیل اقدامات ذی‌ربط به بهترین نحو ممکن بینجامد.

از آنجا که استفاده از پدیده‌های نوظهور به‌طور معمول با استقبال کل جامعهٔ بین‌المللی همراه می‌شود، نباید از این نکته غافل شویم که حقوق بین‌الملل به‌عنوان اصول و قواعد حاکم بر جامعهٔ بین‌المللی بر همهٔ اموری که در جامعهٔ بین‌المللی در حال وقوع است حکومت می‌کند. از این‌رو می‌توان در جهت حفظ صلح و ثبات در روابط بین دولت‌ها و حفظ حاکمیت و امنیت داخلی و بین‌المللی دولت‌ها در جامعهٔ بین‌المللی، ضمن تطبیق این اقدامات نوظهور با اصول و قواعد موجود،گام‌های مؤثری در قانونمند کردن این اقدامات به‌طور خاص برداشته شود تا از خطرهای احتمالی در آینده جلوگیری کند یا وقوع آنها را به حداقل رساند.

به این ترتیب، به‌نظر می‌رسد که دسترسی به اطلاعات، جابه‌جایی اطلاعات، نقل‌وانتقال قانونمند و گاه غیرقانونی اطلاعات و حتی ربایش اطلاعات از مهم‌ترین موضوعاتی است که لازم است حقوق بین‌الملل در حال توسعه به آن واکنش نشان داده و آن را در زمرهٔ موضوعات مهم و سرنوشت‌ساز خویش قرار دهد.

ازآنجاکه جابه‌جایی اطلاعات در اینترنت فضا و مکان نمی‌شناسد و حتی مسیر ارسال داده‌ها بین دو نقطه از جهان براساس سرعت رسیدن اطلاعات به‌طور خودکار تعیین می شود، نفوذگران یا مهاجمان سایبری می‌توانند با استفاده از چند روش سایبری از جمله یک نشانهٔ «آی‌پی جعلی»[1] «بات نت»[2] یا دیگر روش‌ها، کامپیوترهایی را در نقطهٔ دیگری از جهان

1. IP. Address (Internet Protocol Address)
2. Botnet

به‌عنوان سکوی پرش خود انتخاب کرده و از طریق آنها اقدامات سایبری خود را عملی کرده و به این ترتیب، ماهیت اصلی خود را پنهان کنند (حبیبی، ۱۳۹۶: ۱۶۵). از این‌رو پیچیدگی‌های خاص موضوع، قضیه را با ابهامات عدیده‌ای همراه می‌کند. اما مسئلهٔ اینجاست که آیا این پیچیدگی موجباتی را برای فرار دولت از مسئولیت‌ها و تعهدات بین‌المللی آن فراهم می‌سازد و آیا دستیابی دولت به ابزار و ادوات نوین و به‌ویژه ابهام در انتساب عمل متخلفانه جاسوسی، زمینه‌ای را برای عدم امکان انتساب مسئولیت به دولت فراهم می‌کند؟

روشن است که دولت، به‌عنوان تابع اصیل حقوق بین‌الملل، باید در عرصهٔ حقوق بین‌الملل از بابت هر قسم از اعمال متخلفانهٔ خویش مسئولیت داشته و پاسخگو باشد. وجود خصایصی در پروتکل‌های ارتباطی در فضای سایبری، عملاً شناسایی و ردیابی منبع اصلی نفوذ، جابه‌جایی غیرقانونی و حتی ربایش اطلاعات را دشوار و حتی گاهی ناممکن می‌سازد، اما با دقت در مجموعهٔ قواعد طرح کمیسیون حقوق بین‌الملل دربارهٔ مسئولیت بین‌المللی دولت‌ها و تطبیق آن با جاسوسی سایبری، می‌توان ادعا کرد دولت‌ها در قبال اقدامات متخلفانهٔ خویش در فضای سایبری از جمله جاسوسی سایبری نیز دارای مسئولیت خواهند بود. در همین حال، شناسایی نشدن عامل فرد به‌عنوان جاسوس در جاسوسی سایبری، مسئلهٔ مهم انتساب اقدامات سایبری در چارچوب حقوق مسئولیت بین‌المللی دولت و همچنین ابهام در زمان و مکان وقوع جاسوسی و نقش و تأثیر عوامل مؤثر بر تحقق این پدیده، پرداختن به موضوع این مقاله را با پیچیدگی‌های بیشتری روبه‌رو می‌کند. از این حیث، نخست، به تأملی کوتاه در ماهیت و قلمرو جاسوسی سایبری در حقوق بین‌الملل می پردازیم و آنگاه زمینهٔ لازم برای ورود به مبحث اصلی این نوشته یعنی مسئولیت بین‌المللی ناشی از جاسوسی سایبری را فراهم می‌کنیم.

مفهوم و ماهیت جاسوسی سایبری در حقوق بین‌الملل

جاسوسی سایبری یکی از طرق جاسوسی، دستکاری یا بهره‌برداری غیرقانونی از اطلاعات در فضای مجازی محسوب می‌شود.[۱] این قسم از جاسوسی به دسترسی غیرقانونی یا دزدی اطلاعات محرمانه ذخیره‌شده در فرمت‌های دیجیتال یا کامپیوترها و شبکه‌های اینترنت گفته می‌شود.[۲] دولت‌ها، قوای نظامی، شرکت‌ها و مؤسسات دولتی و خصوصی و حتی در مواردی اشخاص خصوصی نیز می‌توانند هدف جاسوسی سایبری واقع شوند. جاسوس از شبکه‌های کامپیوتر برای دسترسی غیرقانونی یا دزدی اطلاعات محرمانه و حساس یا به‌عبارت دیگر، حفاظت‌شده استفاده

---

۱. با توجه به پرداختن به مفهوم و ماهیت جاسوسی سایبری به‌تفصیل در نوشتاری دیگر، از حیث عدم همپوشی موضوع این نوشته با مطلب فوق‌الذکر، صرفاً به اجمال به بیان مفهوم و ماهیت جاسوسی سایبری خواهیم پرداخت.

2. The MI5, 'Cyber Threats', available at: <https://www.mi5.gov.uk/home/thethreats/cyber.htmlviewed>accessed 12 March 2019 (accessed 12 March 2017)

می‌کند. این اطلاعات حساس می‌تواند مشتمل بر مالکیت معنوی، تحقیقات و داده‌های مربوط به توسعهٔ پروژه‌ها یا هر اطلاعات دیگری شود که برای دارندهٔ اطلاعات مهم و حیاتی است. بنابراین از طریق جاسوسی می‌توان به اطلاعات مهم و طبقه‌بندی‌شده‌ای از یک مکان دور به‌صورت پنهانی، کاملاً ارزان و احتمالاً در مقیاس وسیع نفوذ کرد.[1]

در تعریفی موسع می‌توان جاسوسی را «نسخه‌برداری از اطلاعاتی که در دسترس عموم قرار ندارد و انتقال و ذخیرهٔ آنها به‌صورت بی‌سیم یا به‌صورت موقت در سیستم‌های آی‌تی[2] و شبکه‌های کامپیوتریِ در دسترس که در منطقه یا سرزمین دولت دیگر واقع شده‌اند، دانست که اصولاً این اقدامات توسط یک سازمان یا نمایندهٔ دولتی یا منسوب به دولت، به‌صورت پنهانی با استفاده از الگوهای کاذب و دروغین و بدون کسب اجازه از متصدی سیستم‌های فناوری اطلاعات، شبکه‌های کامپیوتر و دولت سرزمینی صورت می‌گیرد» (آقاجانی، ۳۱:۱۳۹۷).

این قسم از اقدامات می‌تواند توأمان با هدف سرقت اطلاعات مهم از رایانه‌های هدف صورت گیرد که در این زمینه *دریچه‌های تله‌ای*[3] و *ردیاب‌ها*[4] ابزارهایی سودمند برای ربایش و جاسوسی اطلاعات در فضای سایبری به‌شمار می‌روند. دریچهٔ تله‌ای به یک کاربر بیرونی امکان می‌دهد در هر زمان به یک نرم‌افزار دسترسی داشته باشد، بدون آنکه مالک کامپیوتر یا کاربر از حضور و بهره‌برداری وی آگاه باشد. ردیاب‌ها نیز ابزاری برای دزدیدن نام کاربر و کلمهٔ عبورند.

۱. حقوق بین‌الملل حاکم بر جاسوسی

رژیم حقوقی حاکم بر جاسوسی در حقوق بین‌الملل، به دو قسم از جاسوسی در زمان جنگ و صلح دسته‌بندی می‌شود. درحالی‌که در حقوق بشر دوستانهٔ بین‌المللی، جاسوسی به‌عنوان یک تکنیک جنگی ممنوع نشده است (اصلانی و رنجبریان، ۲۶۰:۱۳۹۴) و گرچه برخی معتقدند که به‌طور کلی، جاسوسی در زمان صلح در حقوق بین‌الملل ممنوع قلمداد می‌شود، برخی دیگر معتقدند اصلی اساسی در حقوق بین‌الملل وجود دارد که براساس آن در صورت فقدان ممنوعیت خاص و مصرح در حقوق بین‌الملل عمومی و مشروعیت جاسوسی در دوران مخاصمات مسلحانه، در دوران صلح نیز جاسوسی برمبنای عملکرد همهٔ دولت‌ها در این زمینه و در راستای دفاع مشروع و حفظ توازن قدرت در عرصهٔ جوامع بین‌المللی صورت می‌گیرد (زارع و قره‌باغی، ۶۱۸:۱۳۹۴-۶۱۱). به‌نظر نمی رسد این رویکرد مدافعانی جدی در حال حاضر داشته باشد و به‌ویژه با درنظر گرفتن اقسام مختلف جاسوسی در قالب جاسوسی نظامی،

1. Ibid
2. Information Technology (IT)
3. Doors Trap
4. Sniffers

اقتصادی، سیاسی، فرهنگی، زیست‌محیطی و ... تجویز کلی مشروعیت یا عدم مشروعیت جاسوسی در حقوق بین‌الملل دشوار و عمدتاً تابعی از ممنوعیت کلی ناشی از اصل عدم مداخله در امور داخلی دولت‌ها و لزوم احترام به حاکمیت ارضی و استقلال سیاسی دولت‌هاست که در منشور ملل متحد پیش‌بینی شده است و از سوی دیگر، اینکه اقسام مختلف جاسوسی به انحای گوناگون می‌تواند به اختلال در نظم داخلی کشورها بینجامد.

۲. آثار و تبعات جاسوسی سایبری

در واقع در چارچوب حقوق بین‌الملل، جاسوسی سایبری مجموعهٔ اقداماتی را در بر می‌گیرد که هرچند ماهیتاً با سرقت اطلاعات، فیشینگ، هکینگ و امثالهم ارتباط و سنخیت دارد، به لحاظ ماهوی، عملی مستقل محسوب می‌شود و به‌ویژه از حیث اهمیت اطلاعات و حفاظت از منافع ملی، دولت‌ها به آن واکنشی جدی از خود نشان می‌دهند. برای مثال، در قانون ایران جاسوسی سایبری، شنود و دسترسی غیرمجاز که از طریق آن نفوذگران از بدافزارهای گوناگونی برای دستیابی به اطلاعات محرمانه و حیاتی استفاده می‌کنند، به‌ویژه در مادهٔ ۳ قانون جرایم رایانه‌ای ممنوع اعلام شده و برای آن مجازات‌هایی در نظر گرفته شده است (قدیری،کاظمی، ۱۳۹۸:۲۴۰). با این‌حال، هرچند دولت‌ها در قوانین ملی عمدتاً به جرم‌انگاری جاسوسی در قوانین ملی مبادرت کرده و برای آن مجازاتی در نظر گرفته‌اند، در چارچوب حقوق بین‌الملل قضیه بسیار پیچیده است. برخی معتقدند این امر در حقوق بین‌الملل با محدودیتی جدی همراه نیست، چراکه رویهٔ بین‌المللی مؤید آن است که دولت‌ها مکرراً مبادرت به جاسوسی سایبری می‌کنند (Sulmasy & Yoo, 2007: 625) و دستهٔ دیگری این امر را مداخله در امور داخلی، نقض حاکمیت و تمامت ارضی تلقی کرده و آنرا ممنوع قلمداد می‌کنند (Garcia-Mora, 1964:79-80). به هر حال، این امر به‌ویژه در مواردی که ماهیت جاسوسی سیاسی یا اقتصادی است، نمودی جدی یافته است و دولت ایالات متحده و برخی همفکرانش به‌شدت درصدد شکل‌دهی یک رژیم حقوقی صریح در جهت ممنوعیت جاسوسی سایبری با ماهیت اقتصادی از طریق توسل به توجیهاتی سیاسی مانند نقض اصل ممنوعیت مداخله در امور داخلی سایر دولت‌ها هستند.[1] به هر حال، در این مقاله با پذیرش ممنوعیت جاسوسی سایبری به‌عنوان اقدامی که ناقض اصل منع مداخله در امور داخلی دولت‌هاست، به تأملی در مسئولیت بین‌المللی ناشی از جاسوسی بین‌المللی می‌پردازیم.

1. See Aaron Shull, Cyber Espionage and International Law, available at: file:///C:/Users/ Majid %20Reza/Desktop/SSRN-id2809828.pdf (09/21/2019).

مسئولیت بین‌المللی ناشی از جاسوسی سایبری

مسئولیت بین‌المللی از مهم‌ترین و اساسی‌ترین نهادهای حقوقی بین‌المللی است، زیرا اصولاً هر گونه تعهد حقوقی بین‌المللی که از سوی تابعان حقوقی بین‌المللی نادیده انگاشته و نقض شود، بلافاصله موضوع مسئولیت بین‌المللی آنها پیش می‌آید (Schwarzenberger, 1976: 17).

وقوع هر عمل ناقض تعهد بین‌المللی یک دولت می‌تواند موجب طرح مسئولیت ناشی از اقدمات ذی‌ربط یا مسئولیت ترکیبی ناشی از یکایک اقدامات متخلفانهٔ موردنظر باشد.[۱]

طرح مسئلهٔ مسئولیت بین‌المللی در قلمرو تهدیدهای سایبری یا در زمینهٔ رمایش اطلاعات در فضای سایبر که از قابلیت انعطاف زیادی برخوردار است و می‌تواند سلسله اقدامات متخلفانه‌ای را در برگیرد از اهمیت ویژه‌ای برخوردار است. به‌ویژه باید این نکته توجه شود که اقدام یا اقدامات صورت‌گرفته در این زمینه بسیار به یکدیگر مرتبط و درهم‌تنیده است و تفکیک اجزای اقدامات به‌منظور احراز تحقق یک عمل متخلفانه در این موارد کار بسیار دشواری است. از جمله اینکه تهدیدهای صورت‌گرفته از طریق شبکه‌های کامپیوتری به‌دلیل حذف احتمالی یا نامشخص بودن برخی از عناصر وقوع تهدید مثل عامل نفوذکننده یا زمان و مکان وقوع ممکن است احراز مسئولیت بین‌المللی دولت‌ها را دچار مشکلاتی کند. به هر روی، از آنجا که بیشتر اصول و قواعد حقوق بین‌الملل حاکم بر مسئولیت بین‌المللی، به‌ویژه در طرح کمیسیون حقوق بین‌الملل راجع به مسئولیت بین‌المللی دولت ناشی از اقدامات متخلفانهٔ بین‌المللی (۲۰۰۱) تجلی یافته است، در این مقاله با استناد به مواد این طرح به مسئولیت بین‌المللی دولت و امکان تسری اصول و قواعد عام مسئولیت بین‌المللی به اقدامات مشتمل بر جاسوسی سایبری می‌پردازیم. البته شایان ذکر است که هرچند گسترهٔ وسیعی از اقداماتی که می‌توانند تحت عنوان جاسوسی سایبری در حقوق بین‌الملل طبقه‌بندی شوند، می‌توانند توسط هکرهای معمولی یا نهادها و ارگان‌های غیردولتی صورت پذیرد و عملاً منتسب به دولت نباشد، از این‌رو، در این نوشتار به مقولهٔ جاسوسی در مواردی خواهیم پرداخت که عمل منحصراً توسط دولت یا ارگان‌های دولتی صورت می‌پذیرد.

در این زمینه، دو سند بین‌المللی را مدنظر قرار می‌دهیم. نخست، طرح مسئولیت بین‌المللی دولت ناشی از اعمال متخلفانهٔ بین‌المللی (۲۰۰۱)، به‌ویژه مادهٔ ۲ طرح و همچنین مواد راهنمای تالین ۲[۲]در زمینهٔ اقدامات سایبری که به آستانهٔ توسل به زور نظامی نرسیده‌اند و از

---

۱. علاوه‌بر مسئولیت بین‌المللی ناشی از نقض تعهد، قسمی از مسئولیت بین‌المللی نیز به اعمال منع‌نشده در حقوق بین‌الملل اختصاص دارد که موضوع این مقاله نیست.

۲. بعد از انتشار راهنمای تالین ۱ که توسط جمعی از حقوقدانان و کارشناسان بین‌المللی در سال ۲۰۱۳ و در چارچوب ناتو تهیه شد و به قواعد قابل اعمال بر توسل به زور سایبری و همچنین قواعد قابل اعمال در

جمله، به جاسوسی سایبری نیز تسری‌پذیرند. به این ترتیب، نخست بحث وقوع عمل متخلفانه و سپس انتساب مسئولیت بین‌المللی ناشی از نقض تعهد یا تخلف بررسی می‌شود.

۱. احراز مسئولیت بین‌المللی دولت ناشی از اقدامات سایبری

انتساب عمل متخلفانه به دولت در فضای سایبری به دو علت از ویژگی‌های خاصی برخوردار است: نخست آنکه اقداماتی که در فضای مجازی صورت می‌گیرد، ملموس نیست و هرچند تبعات خارجی و ملموسی به‌همراه دارد، از حیث مادی در مواردی قابل رهگیری و رصد نیست. همچنین، پیوستگی اطلاعات در دنیای مجازی به‌نحوی است که اثر عمل یک دولت در گوشه‌ای از جهان در بسیاری از نقاط دیگر دنیا قابل رؤیت و اثربخش خواهد بود و البته ممکن است بخشی هم همیشه پنهان بماند یا سال‌ها بعد مشخص شود. به‌طور مثال، کشوری که «سرور اصلی» ارتباطی در سرزمین آن مستقر است می‌تواند با قطع آن موجب قطع اینترنت در بخشی از جهان شود یا دولتی با پراکندن اخبار و جملات تحریک‌آمیز به هدایت و واداشتن دیگران به نسل‌کشی یا تبعیض نژادی در فضای سایبر بپردازد و تمام کاربران دنیای واقعی را تحت تأثیر قرار دهد. دوم اینکه، آثار و پیامدهای عمل متخلفانهٔ انجام‌گرفته از طریق فضای سایبر، در فضای واقعی قابل رؤیت است، اما ریشهٔ این عمل متخلفانه و عامل آن در شبکهٔ عنکبوتی اینترنت به‌سختی قابل ردیابی است (ضیایی، ۱۳۹۲: ۵۳). ماهیت ویژهٔ فضای سایبر ایجاب می‌کند که عوامل مختلفی از قبیل اطلاعات فنی، فضای سیاسی، سابقهٔ فعالیت‌های سایبری دولت‌ها و غیره برای انتساب جاسوسی سایبری در نظر گرفته شود؛ برای مثال، دربارهٔ حملات سایبری آمریکا مؤلفه‌هایی چون روابط میان دو کشور، سابقهٔ اقدامات دولت مظنون در زمینهٔ 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 حامیِ» حملات مد نظر قرار می‌دهد (خلیل‌زاده و همکاران، ۱۳۹۳: ۵۲). باید به این نکته توجه داشت که در عالم واقع نیز، انتساب عمل متخلفانه به دولت، در مواردی با محدودیت‌هایی همراه است و از دشوارترین اجزای طرح مسئولیت بین‌المللی دولت تلقی می‌شود. با پیدایش

مخاصمات مسلحانهٔ سایبری و حملات سایبری در مخاصمات مسلحانه در مفهوم رایج و سنتی آن اختصاص داشت، در سال ۲۰۱۷، گروهی از کارشناسان بین‌المللی راهنمای دیگری را تدوین کردند که در همان چارچوب سازمانی تهیه و منتشر شد که به‌عنوان راهنمای تالین ۲ شناخته می‌شود. راهنمای تالین ۲ به بررسی اقدامات سایبری در ارتباط با موضوعاتی چون حاکمیت دولت‌ها، مسئولیت بین‌المللی، حقوق بشر، حقوق هوا و فضا و حقوق دریاها می‌پردازد. اگرچه دستورالعمل تالین ۲ صرفاً دیدگاه‌هایی از کارشناسان بین‌المللی را ارائه می‌دهد، از حیث دکترین از اهمیت چشمگیری برخوردار است و تا پیش از شکل‌گیری قواعد الزام‌آوری برای بازیگران بین‌المللی می‌تواند به‌منظور کنترل رفتار در فضای سایبری مدنظر قرار گیرد.

فضای سایبر و انجام و امکان انجام اقدامات متخلفانه بین در این فضا بر دشواری‌های انتساب اقدام به دولت می‌افزاید. فرایند انتساب عملیات سایبری در فصل چهارم راهنمای تالین ۲ با عنوان "حقوق مسئولیت بین‌المللی" بررسی و بیان شده است. این راهنما به نقد وضعیت کنونی حقوق مربوط به انتساب اقدامات سایبری در سطح بین‌المللی می‌پردازد. راهنمای تالین ۲ اهمیت حقوق بین‌الملل عرفی را در خصوص انتساب عملیات سایبری به‌طور خلاصه شرح می‌دهد. انتساب اقدامات سایبری، هنگامی‌که یک دولت مظنون به دست داشتن در آن است، دشوار و اغلب زمان‌بر است. به همین دلیل، حقوق بین‌الملل در پاسخ به تهدیدهای سایبری که متضمن اعمال زور نیستند، در موضعی دشوارتر قرار می‌گیرد، چراکه بدون توسل به ابزاری نظامی، عملی متخلفانه صورت می‌گیرد و دولت بی‌آنکه متجاوز شناخته شود، با مداخله یا حمایت از اقدام غیرقانونی در فضای سایبری، به مقصود نامشروع خود دست می‌یابد.

نباید از یاد برد که جاسوسی سایبری مدنظر این مقاله، از سوی ارکان دولتی به‌طور مستقیم یا از سوی اشخاص خصوصی که تحت حمایت و هدایت دولت خارجی هستند محقق می‌شود، در هریک از این دو حالت انتساب جاسوسی سایبری به یک دولت محرز است. تنها اعمال و رفتاری را می‌توان در سطح بین‌المللی به دولت نسبت داد که این اعمال از جانب ارگان‌های دولتی آن کشور یا سایر کارمندان تحت حمایت و کنترل مستقیم ارگان‌های عامل دولت صورت گرفته باشد (Brownlie, 1983: 132; Caron, 1998: 76). در مرحلهٔ اول، هر دولت مسئول اعمال و رفتار اشخاص و ارگان‌هایی است که به نوعی نمایندهٔ آن دولت محسوب می‌شوند. علت اصلی مفید و کارامد بودن این موضوع این است که براساس آن هر کدام از دستگاه‌ها و ارگان‌های دولتی می‌توانند در تهدیدهای صورت‌گرفته از طریق شبکه‌های کامپیوتری نقش داشته باشد، در واقع هر دولت مسئول اعمال و رفتار همهٔ ارگان‌های خود و نحوهٔ عملکرد و ظرفیت رسمی نهادها و افرادی است که تحت هدایت و کنترل آن دولت قرار دارند. از این‌رو برای تبیین انتساب اقدام سایبری به دولت، در ادامهٔ بحث به تحقق عمل متخلفانه و معیارهای انتساب مسئولیت عملیات سایبری که به آستانهٔ توسل به زور نظامی نمی‌رسند، می‌پردازیم.

۲. وقوع عمل متخلفانهٔ بین‌المللی در جاسوسی سایبری

اثبات وقوع عمل متخلفانه در فضای سایبری در عمل با معضلاتی همراه است. دربارهٔ عملیات سایبری قهری با شدتی کمتر از توسل به زور نظامی، دولت در صورتی مسئولیت بین‌المللی خواهد داشت که علاوه‌بر قابل انتساب بودن آن به دولت، آن اقدام نقض یک تعهد حقوقی بین‌المللی محسوب شود (Tallin Manual, 2017: 84, Rule14). این‌گونه اقدامات می‌تواند نقض یک قاعدهٔ معاهداتی یا حقوق بین‌الملل عرفی، یا اصلی از "اصول کلی حقوقی" باشد

(Tallin Manual, 2017: 84, Rule14). این قسم از اقدامات که دامنهٔ گسترده‌ای از اقدامات متخلفانه را در بر می‌گیرد، به‌واسطهٔ نقض اصل منع مداخله در امور داخلی دولت‌های دیگر، در زمرهٔ مجموعهٔ اعمال متخفانه حقوق بین‌الملل قرار می‌گیرند (Tallin Manual, 2017: 312). براساس اصول ناظر بر برابری حاکمیت دولت‌ها و منع مداخله در امور داخلی دولت‌های دیگر، به‌کارگیری روش‌های سایبری که به آستانهٔ توسل به زور نظامی می‌رسند و متضمن مداخلهٔ قهرآمیز در امور داخلی دولت دیگر می‌شوند ممنوع است (Tallin Manual, 2017: 313). با این‌حال، راهنمای تالین ۲ اقدامات سایبری علیه دولت‌های دیگر را به‌صِرف «زیانبار، قابل نکوهش یا به‌نحوی دیگر غیردوستانه» بودن، موجد مسئولیت بین‌المللی برای دولت نمی‌داند، مگر اینکه نقض تعهدی بین‌المللی تلقی شوند (Tallin Manual, 2017: Rule 14, para.7)؛ بنابراین برای غیرقانونی انگاشتن یک عملیات سایبری، ایجاد خسارت فیزیکی لازم نیست، مگر اینکه ورود خسارت جزو عوامل اصلیِ متخلفانه انگاشتن آن عمل باشد. از سوی دیگر، وجود سوء نیت نیز لازمهٔ متخلفانه محسوب شدن یک عمل به‌موجب حقوق بین‌الملل محسوب نمی‌شود. همچنانکه نقض قانون داخلی یک کشور نیز نمی‌تواند به‌تنهایی پایه و اساس وقوع یک عمل متخلفانه بین‌المللی باشد، زیرا حدود و ثغور تعهد حقوقی و نقض آن تنها توسط حقوق بین‌الملل تعیین می‌شود (Crawford, 2002: 881).

جاسوسی سایبری توسط دولت‌ها اغلب با دستور وزارت دفاع، وزارت اطلاعات یا ارکان و مؤسسات دولتی انجام می‌گیرد. دولت‌ها همچنین ممکن است از نمایندگان، برای مثال در شکل افراد یا گروه‌های به لحاظ فنی ماهر، استفاده کنند (Shoshan, 2015:16). این عاملان، یا به‌صورت کاملاً مستقیم از سوی دولت حمایت می‌شوند، مانند مواردی که دولت آنها را از لحاظ مالی تأمین می‌کند یا از سوی دولت مستقیماً برای این عمل استخدام می‌شوند یا حمایت دولت از آنها به‌شکل غیرمستقیم انجام می‌گیرد. مثال برای حمایت غیرمستقیم، موردی است که دولت آگاهانه از دخالت در اعمال اشخاص غیردولتی جاسوس خودداری می‌کند، درحالی‌که کاملاً از ماهیت عمل آنان آگاه است. در هر حال، شیوه‌های مختلفی موجود است که براساس آنها دولت‌ها می‌توانند با اشخاص غیردولتی فعال در جاسوسی سایبری ارتباط برقرار کنند، با وجود این به‌نظر می‌رسد پذیرش داوطلبانهٔ چنین مسئولیتی از سوی دولت‌ها بسیار بعید باشد.

مسئلهٔ انتساب مسئولیت به دولت

قواعد ۱۵ تا ۱۸ راهنمای تالین ۲، انتساب عملیات سایبری را به‌دقت و با بیان تفصیلی جزئیات توضیح می‌دهد. طبق قاعدهٔ ۱۵ این سند، «عملیات سایبری که توسط ارگان‌های یک دولت یا اشخاص یا نهادهایی انجام می‌شوند که به موجب حقوق داخلی اختیار اِعمال اقتدار حکومتی را

دارند، قابل انتساب به آن دولت هستند». به این ترتیب، در صورتی که از ابزار و ادوات سایبری یا از فضای مجازی به‌نحوی علیه دولت دیگر استفاده شود که آثار عمل صورت‌گرفته به ارکان این دولت منتسب باشد، جاسوسی سایبری به دولت ذی‌ربط قابل انتساب است.

براساس قاعدهٔ ۱۶ راهنمای تالین: «عملیات سایبری که توسط ارگان یک دولت که در اختیار دولت دیگری قرار گرفته است، انجام می‌شود، قابل انتساب به دولت اخیر در موردی است که ارگان مزبور در اِعمال عناصر اقتدار حکومتیِ دولتی عمل می‌کند که در اختیار آن قرار گرفته است» (Tallin Manual, 2017: 16). همچنین براساس قاعدهٔ ۱۷ همان راهنما، عملیات سایبری که توسط کُنشگری غیردولتی انجام می‌شود، هنگامی قابل انتساب به یک دولت است که: الف) طبق دستورات، هدایت یا تحت کنترل آن انجام شده باشد؛ ب) آن دولت عملیات مزبور را به‌عنوان عملیات خود تصدیق نموده و بپذیرد» (Tallin Manual, 2017: 94, Rule 17). به‌عبارت دیگر، دولت‌ها نمی‌توانند با ارتکاب جرایم سایبری از طریق یافتن جایگزین‌ها یا با تغییر دادن آدرس اصلی خود از انتساب عمل به خود بگریزند. پاسخگویی دولت در قبال اعمال کنشگران خصوصی که تحت کنترل آن دولت مبادرت به عملیات سایبری می‌کنند، محرک اصلی تدوین این قواعد بوده است. به‌نظر می‌رسد که در این موراد، نفوذ معیار «کنترل مؤثر» مصرح در رأی دیوان بین‌المللی دادگستری در دو پروندهٔ نیکاراگوئه و اعمال کنوانسیون منع و مجازات جرم نسل‌کشی (I.C.J. Rep,1986: para.115; I.C.J. Rep,2007: para. 400). مشهود است. باید به این نکته نیز توجه داشت که یکی از عواملی که انتساب عملیات کنشگران غیردولتی به دولت‌ها را در کانون توجه قرار می‌دهد، این است که اعمال خارج از اختیارات قانونی آنها معمولاً قابل انتساب به دولت نیست (Tallin Manual, 2017: 97). برای مثال، یک دولت به یک کنشگر غیردولتی دستور می‌دهد تا یک بدافزار را وارد شبکه‌های کامپیوتری دولت دیگر کند، و آن کنشگر غیردولتی از آن بدافزار برای هدف قرار دادن یک دولت سوم استفاده می‌کند. در اینجا، عمل این کنشگر قابل انتساب به دولت نخست نیست. زیرا کنشگر غیردولتی طوری آن دستور را اجرا کرده که خارج از اختیارات قانونی او بوده است (Tallin Manual, 2017: 98, paras. 12 and 13 of the commentary to Rule 17).

بنابراین به‌زعم بانیان راهنمای تالین ۲ «حقوق بین‌الملل عرفی نتوانسته است معیار معقولی برای انتساب عمل به دولتی که اقدامات سایبری را انجام داده است، تعیین کند». نتیجه گیری نهایی این گروه از کارشناسان این بود که «دولت‌ها می‌توانند با هم در مورد یک قاعدهٔ خاص برای احراز مسئولیت بین‌المللی ناشی از اقدامات سایبری توافق کنند» (Tallin Manual, 2017: 80, para.5). و با تأیید اینکه در حال حاضر، چنین قواعد یا توافقی در میان دولت‌ها وجود ندارد، عدم قطعیت دربارهٔ انتساب عملیات سایبری را پذیرفتند و توافق کردند که به‌عنوان یک مسئلهٔ کلی، دولت‌ها باید چنان عمل کنند که دولت‌های معقول در همان شرایط یا در

شرایط مشابه، واکنشی یکسان از خود ناشی می‌دهند (Tallin Manual, 2017: 81, para.10).

به این ترتیب، با توجه به مفاد راهنمای تالین در این زمینه می‌توان مدعی شد که «رویهٔ دولتی و عنصر معنوی کافی وجود ندارد تا نتیجه گرفته شود که مبنای تثبیت‌شده‌ای به‌موجب حقوق بین‌الملل برای تعهد به افشای اقداماتی که می‌تواند به انتساب عمل به دولت بینجامد، وجود دارد. بنابراین عملاً اقدام متقابل از سوی دولت قربانی غیرممکن می‌شود. ممکن است راه‌های سیاسی یا دیپلماتیک برای متهم کردن دولت خاصی برای جاسوسی سایبری وجود داشته باشد، اما تهیه ادلهٔ کافی برای انتساب مورد مشخصی از جاسوسی سایبری یا به‌طور کلی هر عمل سایبری به یک دولت دشوار است.

تأملی در رویهٔ بین‌المللی در زمینهٔ جاسوسی سایبری

در زمینهٔ ممنوعیت یا جواز جاسوسی در حقوق بین‌الملل، نه تنها از حیث نظری، بلکه در رویهٔ بین‌المللی نیز اختلاف نظری جدی موجود است. از آنجا که این ممنوعیت به‌نحوی مطلق مورد قبول قبول نگرفته و توافقی عام در این زمینه موجود نیست، نمی توان به قطعیت اظهار نظر کرد، برخی با توسل به فقدان یک رژیم ممنوعیتی خاص، ممنوعیتی در این زمینه قائل نمی‌شوند (Cohen-Janathon, 1960: 239-242). برخی نیز این قسم از اقدامات را زمینه‌ساز نقض حق حاکمیت و اصل عدم مداخله در امور سایر دولت‌ها تلقی می‌کنند و مغایر با اصول حقوق بین‌الملل موجود می‌دانند و از این منظر پیوسته درصددند تا با اعلام موضعی مبنی بر ممنوعیت این اقدامات، مانع شکل‌گیری یک رژیم عرفی مبتنی بر تجویز جاسوسی در حقوق بین‌الملل شوند (Deeks, 2015: 314). با این‌حال، واقعیت این است که توسل به این قسم از اقدامات در حقوق بین‌الملل رو به تزاید به‌نظر می‌رسد و دستیابی به توافقی جدی در این زمینه در آینده نزدیک ضروری است (Katharina Ziolkowski, 2013: 425-427).

ابهام در رویه و عملکرد بین‌المللی دولت‌ها در زمینهٔ جاسوسی در حقوق بین‌الملل، با ظهور اینترنت و با کاربرد رو به رشد استفاده از فناوری‌های نوین در توسل به این اقدامات تشدید شده است (شهبازی، ۱۳۹۶: ۲۲۲-۲۲۰). به این ترتیب، در حالی که فضای سایبر، کمکی به شکل‌گیری رژیم حقوقی در زمینهٔ جاسوسی در حقوق بین‌الملل نکرده، بر چالش‌های عملی دولت‌ها در این زمینه نیز افزوده است. امکانات و تسهیلاتی که فضای سایبر در اختیار افراد و دولت‌ها قرار می‌دهد، زمینه‌ای را برای توسل به اقدامات جاسوسی فراهم می‌کند و همزمان که سرعت، دقت و سهولت در این زمینه، به ارتکاب جاسوسی کمکی جدی می‌کند، به بهترین نحو، موجباتی را برای مخفی شدن در فضای مجازی فراهم می‌آورد. همین موضوع سبب می‌شود تا هم در شناسایی مصادیق رویهٔ بین‌المللی موجود در این زمینه، اختلاف نظر حاصل

شود و هم زمینه‌های مساعدی برای فرار از مسئولیت بین‌المللی پیش روی مرتکبان جاسوسی سایبری قرار گیرد. استفاده از میزان قابل ملاحظهٔ اطلاعات به‌طور همزمان از کانال‌های مختلف که در آن فاصلهٔ میان مکان و زمان حذف شده، استفاده از آدرس‌های مجعول و ساختگی، حذف سریع راه‌های پیگیری و جابه‌جایی اطلاعات در زمانی اندک، هرچند توسل به جاسوسی سایبری را همواره کرده، تعیین مصادیق جاسوسی سایبری را نیز دشوار ساخته است (Kilovaty, 2016: 66-69).

با این‌حال، در عمل، از این منظر که دولت‌ها جاسوسی سایبری را چونان شمشیری دولبه تلقی می‌کنند که در صورت موضع نگرفتن در مقابل آن، می‌تواند آنها را به‌عنوان قربانی بالقوه‌ای در مقابل مخاطرات آتی قرار دهد، در موارد متعددی، دست‌کم در اظهار نظر خویش، توسل به جاسوسی سایبری را عموماً زمینه‌ساز نقض حقوق بین‌الملل و نه یک استثنای امنیتی برای حفاظت از منافع ملی تلقی می‌کنند. برای مثال، همزمان با افشای اقدامات نظارتی سازمان امنیت ملی آمریکا توسط ادوارد اسنودن در سال ۲۰۱۳، مرکز ارتباطات دولت بریتانیا اعلام کرد که چنین برنامه‌هایی که می‌توانند مصادیقی از جاسوسی سایبری تلقی شوند، موجب نقض برخی از اصول اساسی حقوق بین‌الملل می‌شود. وزیر خارجهٔ مکزیک نیز در طی اظهاراتی در یکی از رسانه‌ها، اقدامات نظارتی ایالات متحده در خصوص دولت و رئیس‌جمهور مکزیک را محکوم کرد و بیان داشت که این اقدامات غیرقابل قبول، غیرقانونی و خلاف قوانین مکزیک و حقوق بین‌الملل است. اندونزی نیز اقدامات نظارتی فرامرزی ایالات متحده و برخی از همفکرانش را زمینه‌ساز نقض حقوق بین‌الملل تلقی کرد. چنین رویکردهایی زمینه‌ساز طرح این پرسش کلیدی می شود که اصول اساسی نظیر حفظ تمامیت ارضی، حق حاکمیت و احترام به مقررات ملی دولت‌ها در عمل به چه معناست؟ آیا این ادعا که مصالح امنیتی دولت‌ها می‌تواند توجیهی قابل قبول برای توسل به جاسوسی سایبری باشد، پذیرفتنی است؟ برخی معتقدند دست‌کم در قضیهٔ اسنودن، توسل به برخی اطلاعات ("توسل" در اینجا به چه معناست؟ آیا به‌معنای جمع‌آوری و بهره‌برداری از برخی اطلاعات است؟)، نه‌تنها در زمینهٔ تأمین امنیت ملی ایالات متحده مفید نبوده، بلکه در مقابل، ازآنجاکه حسن نیتی در بهره‌برداری از اطلاعات فراهم نبوده، زمینه‌ای را برای نظارت بیشتر بر افراد فراهم کرده و لذا نه‌تنها در راستای حمایت از حقوق بشر و اهداف انسان‌دوستانهٔ امنیتی قابل تفسیر نیست، بلکه می‌تواند به نقض حقوق بشر نیز بینجامد (Barrie Sander, 2019: 12).

رئیس‌جمهور وقت برزیل، دیلما روسف نیز با همین رویکرد، برنامهٔ نظارتی سازمان امنیت ملی آمریکا را اقدامی خواند که در آن آزادی‌های شهروندی و حقوق بشر افراد به‌شکلی جدی پایمال شده است و با صراحت ابراز داشت که با پایمال کردن حقوق بشر شهروندان کشورهای دیگر، حق امنیت برای شهروندان یک کشور تضمین‌شدنی نیست (Barrie Sander, 2019: 13).

از این منظر، علی‌رغم قلت رویهٔ بین‌المللی و ابهام در تعیین مصادیق جاسوسی سایبری در حقوق بین‌الملل، به‌نظر می‌رسد که دست‌کم با توجه به جایگاه متعالی هنجارهای حقوق بشری در حقوق بین‌الملل و روند انسانی‌تر شدن حقوق بین‌الملل که به محدودیت‌هایی جدی در اعمال بی‌قیدوشرط حاکمیت ملی در حقوق بین‌الملل انجامیده است، مواضع و اظهارات دولت‌ها و تفسیر موسع از مفهوم و جایگاه حقوق بشر در مقابل منافع مبتنی بر امنیت ملی دولت‌ها، از غلبهٔ رویکرد مبتنی بر ممنوعیت جاسوسی سایبری در عملکرد بین‌المللی دولت‌ها حکایت دارد.

نتیجه‌گیری

توسعهٔ فناوری و استفادهٔ بشر از فناوری، خیره‌کننده است. تبعات مثبت این توسعه در کمک به تدوین و توسعهٔ برخی از هنجارهای حقوقی انکارناپذیر است، با این حال، فاصلهٔ زیادی میان شکل‌گیری یک رژیم حقوقی منسجم و واقعیات فناورانهٔ امروزی وجود داردکه همین امر، خود می‌تواند زمینهٔ ایجاد خلأ جدی را در اجرای حقوق و تکالیف دولت‌ها فراهم کند.

جاسوسی در حقوق بین‌الملل از جمله مقوله‌های کلاسیکی است که هرچند عموماً دولت‌ها در قلمرو حقوق ملی خود نسبت به آن واکنشی جدی نشان می‌دهند و به‌طور معمول با جرم‌انگاری و اعمال مجازات‌های سنگین، مرتکبان را به کیفر می‌رسانند، در حقوق بین‌الملل همچنان محل تشتت و معرکهٔ آراست. هرچند جاسوسی در زمان جنگ عملاً در شرایطی با ممنوعیت قانونی همراه نیست، لکن در زمان صلح، با دیدگاه‌های مخالف و موافق مواجه بوده است. در این میان، نبود قواعد صریح و معینی دربارهٔ ممنوعیت جاسوسی در حقوق بین‌الملل، زمینهٔ اعمال اصول کلی از جمله منع مداخله در امور داخلی دولت‌ها یا قداست اصل حاکمیت ارضی دولت‌ها را فراهم کرده و از این منظر با واکنش دولت‌های قربانی همراه بوده است. با این‌حال، زمانی که اقدام به جاسوسی از طریق فضای مجازی صورت می‌پذیرد، ابهام در مسئلهٔ وقوع عمل متخلفانه و به‌ویژه انتساب عمل جاسوسی به دولت جاسوس یا ارکان و ارگان‌های دولت مذکور بر ابهام بیشتر قضیه دامن می‌زند و فقدان قواعد بین‌المللی معاهداتی یا عرفی سبب می‌شود که از مفاد طرح مسئولیت بین‌المللی دولت‌ها ناشی از اعمال متخلفانهٔ بین‌المللی (۲۰۰۱) و راهنمای تالین ۲ (که البته ماهیتی الزام‌آور ندارد) برای تعیین شاخص‌های مسئولیت بین‌المللی دولت استفاده شود.

پیچیدگی مقولهٔ انتساب عمل متخلفانه به دولت در فضای سایبر، درهم‌تنیدگی مجموعهٔ اقداماتی که می‌توانند به تحقق مسئولیت بین‌المللی دولت منجر شوند، تعیین میزان مشارکت، مباشرت و معاونت در تحقق اقداماتی که به جاسوسی سایبری در حقوق بین‌الملل منجر می‌شوند و از طرفی قلت رویهٔ بین‌المللی، تشتت در تعیین مصادیق جاسوسی سایبری در حقوق

بین‌الملل و ابهام در قواعد بین‌المللی الزام‌آور در این مورد، مانع شکل‌گیری رویه‌ای یکنواخت و مستمر درخصوص مسئولیت بین‌المللی دولت در زمینهٔ جاسوسی سایبری در حقوق بین‌الملل شده است. البته به نظر می‌رسد که تا زمان شکل‌گیری رژیم حقوقی حاکم بر این قسم از اقدامات در فضای سایبر و حل معمای انتساب اقدامات ذی‌ربط به دولت، که مسیری ناهموار به‌نظر می‌رسد، حسب مورد تنها می‌توان به اعمال قواعد بین‌المللی ذی‌ربط موجود در معاهدات، حقوق بین‌الملل عرفی یا اصول کلی حقوق بین‌الملل اکتفا کرد.

منابع

۱. فارسی

الف) کتاب‌ها

۱. خلیل‌زاده، مونا (۱۳۹۳)، *مسئولیت بین‌المللی دولت در قبال حملات سایبری*، تهران: مجمع علمی فرهنگی مجد.

۲. زمانی، سید قاسم (۱۳۸۴)، *حقوق سازمان‌های بین‌المللی: شخصیت، مسئولیت، مصونیت*، تهران: مؤسسهٔ مطالعات و پژوهش‌های حقوقی.

۳. کمیسیون حقوق بین‌الملل سازمان ملل متحد (۱۳۹۱)، *متن و شرح مواد کمیسیون حقوق بین‌الملل راجع به مسئولیت دولت*، ترجمهٔ علی‌رضا ابراهیم‌گل، تهران: شهر دانش.

ب) مقالات

۴. اصلانی، جبار؛ رنجبریان، امیرحسین (۱۳۹۴)، «بررسی تطبیقی و تحلیل تعریف حملهٔ سایبری از منظر دکترین، رویه- کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل»، *تحقیقات حقوقی*، ش ۷۱.

۵. حبیبی، همایون؛ بذّار، وحید (۱۳۹۶)، «حملات سایبری و ممنوعیت توسل به زور»، *فصلنامهٔ تعالی حقوق*، دورهٔ جدید، ش ۱۹.

۶. خلیل‌زاده، مونا؛ شعبانی، امید؛ اقبالی، میثم (۱۳۹۳)، «جایگاه اقدامات متقابل در برابر حملات سایبری از منظر حقوق بین‌الملل»، *فصلنامهٔ مطالعات بین‌المللی پلیس*، سال پنجم، ش ۱۷.

۷. خلیلی، رضا (۱۳۸۲)، «عوامل و مراحل تدوین، اجرا و ارزیابی استراتژی ملی»، *مجلهٔ راهبرد*، ش ۲۸.

۸. زارع، محسن؛ قره‌باغی، ونوس (۱۳۹۴)، «تعارض میان جاسوسی و آزادی اطلاعات از منظر حقوق بین‌الملل بشر»، *مطالعات حقوق عمومی*، دورهٔ ۴۵، ش ۴.

۹. شهبازی، آرامش (۱۳۹۶)، «در تکاپوی توسعه حقوق بین‌الملل اینترنت»، پژوهش‌های حقوق عمومی، ش ۵۴.

۱۰. ضیایی، سید یاسر (۱۳۹۲)، «حمایت از حقوق بشر در فضای سایبر»، *مجلهٔ پژوهش‌های حقوقی*، ش ۲۱.
۱۱. قدیری، محسن؛ کاظمی فروشانی، حسین (۱۳۹۸)، «بررسی تطبیقی حقوق کیفری ایران با اسناد بین‌المللی در زمینهٔ مقابله و پیشگیری از وقوع تروریسم سایبری»، *مجلهٔ حقوقی بین‌المللی*، ش ۶۰.

ج) پایان‌نامه‌ها

۱۲. آقاجانی رونقی، آیدا (۱۳۹۷)، *جاسوسی سایبری از دیدگاه حقوق بین‌الملل*، پایان‌نامهٔ کارشناسی ارشد رشتهٔ حقوق بین‌الملل عمومی، دانشگاه علامه طباطبایی.

۲. انگلیسی

A) Books

13. Becker, T., (2006), *Terrorism and the state: rethinking the rules of state responsibility*, Bloomsbury Publishing.
14. Crawford, J., & James, C., (2002), *The International Law Commission's articles on state responsibility: introduction, text and commentarie,* Cambridge University Press.
15. Parry, C., Grant, J. P., & Barker, J. C., (2009), *Parry & Grant encyclopaedic dictionary of international law*. Oxford University Press.
16. Schmitt, M. N. (Ed.), (2017), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press.
17. Schwarzenberger, G., & Brown, E. E. D., (1976), *Manual of International Law*. Fred B. Rothman &Company.
18. Ziolkowski, K., (2013), *Peacetime Cyber Espionage–New Tendencies in Public International Law*, Peacetime Regime for State Activities in Cyberspace; International Law, International Relations and Diplomacy. CCDCOE.

B) Articles

19. Banks, W., (2016), "State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0", *Tex. L. Rev.*, Vol. 95, No. 7.
20. Brownlie, Ian, (1983), "System of the Law of Nations: State Responsibility" (Part I), Vol. 79, No.2
21. Calabresi, Massimo (2016), "The hide hidtory of US 2016 election", *Time Mgazine*.
22. Carlin, J. P., (2015), "*Detect, Disrupt, Deter:* A Whole-of-Government Approach to National Security Cyber Threats", *Harvard National Security Journal*, Vol. *7*.
23. Caron, D. D., (1998), "The basis of responsibility: attribution and other trans-

substantive rules", in Lillich, R. B. and Magraw, D. B. (eds.), *The Iran-United States claims tribunal: its conclusions to state responsibility*,
24. Clark, D. D., & Landau, S. (2011), "Untangling attribution", *Harv. Nat'l Sec. J., 2*
25. Cohen-Jonathan, Gérard & Robert Kovar (1960), "L'espionnage en temps de paix", Annuaire Français de Droit International 6.1
26. Crawford, J., (2002), "The ILC's articles on responsibility of states for internationally wrongful acts: a retrospect", *American Journal of International Law*, Vol. 96, No. 4.
27. Deeks, A. (2015), "An International Legal Framework for Surveillance', *Virginia Journal of International Law,*Vol. 55, No.2.
28. Egan, B. J., (2017), "International Law and Stability in Cybershpace", *Berkeley Journal of International Law,* Vol. 35, No. 1. *nt'l L., 35,* 169.
29. Glenn Sulmasy & John Yoo, (2007), "Counterintuitive: Intelligence Operations and International Law", *MICH. J. INT'L L.28.*
30. Heupel, M. (2018), "How do States Perceive Extraterritorial Human Rights Obligations? Insights from the Universal Periodic Review", *Human Rights Quarterly*, Vol. *40*, No.3.
31. Katharina Ziolkowski, (2013), "Peacetime Cyber Espionage – New Tendencies in Public International Law", in Katharina Ziolkowski (ED.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO CCD COE).
32. Kilovaty, I. (2016), "World Wide Web of Exploitations-The Case of Peacetime Cyber Espionage Operations under International Law: Towards a Contextual Approach", *Colum. Sci. & Tech. L. Rev., 18*.
33. Cahin, G., (2010), "The responsibility of other entities: Armed bands and criminal groups", in Crawford, J., Pellet, A., Olleson, S. (eds.), *The Law of International Responsibility*, Oxford: Oxford University Press.
34. Manuel R. Garcia-Mora, (1964), "Treason, Sedition and Espionage as Political Offenses under the Law of Extradition", 26 U. PITT. L. REV. 65.
35. Sander, B. (2019, May), "The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations", In *2019 11th International Conference on Cyber Conflict (CyCon),* Vol. 900, pp. 1-21, IEEE.

C) Cases

36. Application of the Convention on the Prevention and Punishment of the Crime of Genocide, (Bosn. & Herz. v. Serb. & Montenegro), I.C.J., Report 2007.
37. Big Brother Watch & Others v. The United Kingdom, Application Nos 58170/13, 62322/14 and 24960/15, ECtHR, Judgment, 13 September 2018, para. 271.
38. Gabcikovo- Nagymaros Project,)Hongary v. Slovakia), I. C. J., Report 1997.
39. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, I.C.J., Report 1986.

40. Phosphates in Morocco, (It. v. Fr.), Preliminary Objections, P.C.I.J., Report 1938, (ser. A/B), No. 74.
41. United States Diplomatic and Consular Staff in Tehran, I. C. J., Report 1980.

D) Documents:
42. Report of the Group of Governmental Experts on Developments in the Field of *Information and Telecommunications in the Context of International Security*, U.N. Doc. A/70/174, 22 July 2015.

E) Thesis:
43. Shoshan, E., (2015), «Applicability of International Law on Cyber Espionage Intrusions», Faculity of Law, *Stockholm University.*

F) Electronic resources
44. DEP'T OF DEF., THE DEPARTMENT OF DEFENSE CYBER STRATEGY, Avaiable at:,https://www.defense.gov/Portals/1/features/ 2015/0415_cyber-strategy/Final_2015_DoD_CYBER _STRATEGY_for _web.pdf
45. Lipton, E., Sanger, D. E., & Shane, S. (2016). «The perfect weapon: how Russian cyberpower invaded the US». *The New York Times*, Avaiable at: https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html