دیپلماسی سایبری روسیه برای تحول در رژیم حکمرانی فضای مجازی

سمیه قنبری[1]

کوشش‌های دیپلماتیک وسیع روسیه در حوزه تصدی‌گری و تنظیم مقررات فضای مجازی که از آن تحت عنوان دیپلماسی سایبری نام برده‌می‌شود تا به امروز سه مرحله از توسعه را پشت سر گذاشته‌است. هدف دیپلماسی سایبری روسیه در ابتدا به جلوگیری از نظامی‌سازی فضای سایبر معطوف‌بود، اما با توسعه ابعاد جنگ سایبری و اطلاعات به مرحله متقاعدسازی دولت‌ها برای پذیرش برخی انواع قواعد حاکم بر رفتار دولت‌ها در فضای سایبر واردشد و در ادامه به تلاش برای انعقاد موافقت‌نامه‌های دوجانبه با برخی دولت‌های غربی با هدف منع استفاده نظامی از فناوری‌های اطلاعات و ارتباطات علیه یکدیگر منجرشد. این مقاله با هدف رونمایی از ابتکارها، اولویت‌ها، انگیزه‌ها و پیامدهای دیپلماسی سایبری روسیه در سطوح جهانی، منطقه‌ای و دوجانبه تدوین شده و به‌دنبال ارائه پاسخی مناسب به این پرسش محوری است که «خاستگاه فکری دیپلماسی سایبری روسیه چیست و چه هدفی را دنبال‌می‌کند؟» ریشه دیپلماسی سایبری روسیه برپایه یافته‌های مقاله به فهم این کشور از قلمروی سایبر به‌مثابه ابزار جدید سلطه غرب بازمی‌گردد. هدف غایی مسکو از تلاش‌های دیپلماتیک در سپهر سایبر را نیز رفع تصدی‌گری از موجودیت‌های طرفدار واشنگتن، بروکسل و ناتو بر فضای سایبر با ایجاد حکمرانی جهانی فضای مجازی تشکیل‌می‌دهد. مقاله حاضر از نوع کیفی (توصیفی-تحلیلی) بوده و با استفاده از روش‌شناسی استنتاجی انجام پذیرفته‌است و داده‌های توصیفی و یافته‌های به‌دست‌آمده نیز تحت مفهوم حکمرانی فضای مجازی و ماهیت غیرقطعی و سیال این مفهوم تجزیه‌وتحلیل شده‌اند.

واژگان کلیدی: دیپلماسی سایبری، حکمرانی امنیت سایبری، بی‌طرفی فضای مجازی، حکمرانی جهانی فضای مجازی و آیکان.

---

[1] . نویسنده مسئول، استادیار گروه علوم سیاسی، دانشگاه پیام‌نور، تهران، ایران.
Email: s.ghanbari@pnu.ac.ir

- این مقاله علمی _ پژوهشی می باشد. تاریخ دریافت ۹۸/۱۲/۱ و تاریخ پذیرش ۹۹/۲/۱۴

مقدمه

بحران امروز جهان به پادگویی‌های سیاسی، اقتصادی و نظامی قدرت‌های هم‌آورد بر سر شماری از مسایل قابل‌تقلیل نیست، بلکه مشکی سازمان‌یافته هم‌بسته با روندهای کلی روابط بین‌الملل به‌شمارمی‌آید. موضوع امنیت سایبری و اطلاعات نمونه بارزی از چالش‌های پیش‌روی نظام بین‌الملل معاصر را نشان‌می‌دهد که درپی دگردیسی‌های هم‌پیوند با انقلاب اطلاعات و واگرد جهان به عصر اطلاعات پدیدار شده‌است. انقلاب در فناوری اطلاعات و ارتباطات نه‌تنها با تغییر ماهیت تولید، مصرف و دسترسی به اطلاعات ژرف‌ترین تحول اجتماعی طی دو دهه گذشته را رقم زده‌است، بلکه سیاست، اقتصاد و شیوه‌های فهم جهان را نیز دگرگون ساخته‌است.

چالش‌های متعاقب گذار به عصر اطلاعات بیش از آنکه فنی باشند از ماهیت سیاسی برخوردار هستند و دولت‌ها برای سازواری نظام سیاسی خود با تحولات فناورانه و چگونگی مواجهه با چالش‌های انقلاب اطلاعات شیوه‌های خاص خود را برمی‌گزینند که در قلمروی موضوعی حکمرانی فضای مجازی[۱] (حکمرانی سایبری[۲]) قرارمی‌گیرد. در سطح بین‌المللی نیز درک دولت‌ها از تهدید و جنگ با افزایش و توسعه کارویژه‌های فضای سایبر گسترش‌یافته است و آمادگی برای مقابله با نبردهای غیرنظامی به‌ویژه جنگ اطلاعاتی[۳] و جنگ سایبری[۴] در دستورکار بیشتر دولت‌ها شامل همه قدرت‌های بزرگ قراردارد. در این میان، سوءاستفاده ایالات متحده از اعمال حکمرانی یک‌جانبه سنتی بر فضای مجازی در جهت برآورده‌ساختن منافع خود و تضعیف رقبا بر دغدغه‌های سایبری بازیگران بین‌المللی افزوده‌است.

روسیه به‌دلیل هم‌آوردی راهبردی طولانی‌مدت با ایالات متحده احتمالا بیش از هر دولت دیگری از جنبه‌های شناختی پدیده سایبر به اندازه جنبه‌های فنی آن نگران است. به همین دلیل مسکو در مقایسه با تمرکز پایتخت‌های غربی بر امنیت سایبری شبکه-محور فنی، رویکردی متفاوت، جامع‌تر و یکپارچه‌تر نسبت به امنیت اطلاعات اتخاذ کرده‌است.

---

[۱]. عبارت حکمرانی فضای مجازی (Internet Governance) در فارسی به "راهبری فضای مجازی" و "زمام‌داری فضای مجازی" نیز ترجمه شده‌است. اما در این مقاله به‌دلیل اهمیت مقابله دو مفهوم حکمرانی (Governance) و حکومت (Government) در تدوین پایه‌های مفهومی حاکم بر بحث از معادل‌های شبیه به‌هم برای استفاده شده‌است.

[2]. Cyber Governance

[3]. Information Warfare

[4]. Cyberwarfare (Cyber Warfare)

چگونگی پیاده‌سازی این چشم‌انداز در آموزه‌ها و راهبردهای فنی، سیاسی و نظامی این کشور آشکار بیان‌شده‌اند. رهنامه امنیت اطلاعات فدراسیون روسیه[1] در سال ۲۰۱۶ تازه‌ترین و فراگیرترین سندی است که به راهبرد روسیه در فضای مجازی به‌ویژه پیرامون شناسایی و مقابله با تهدیدهای سایبری، جنگ سایبری و جنگ اطلاعاتی اختصاص‌دارد.

همچون دیگر کشورها جهان، موضوع امنیت سایبری و اطلاعات در روسیه به ثبات داخلی و جلوگیری از مداخله‌های بیرونی با هدف پاسداری از منافع ملی پیوند خورده‌است و بنابراین بخش مهمی از راهبرد امنیت ملی این کشور را تشکیل‌می‌دهد. رهبران روسیه قویا بر این باور هستند که غرب و در رأس آن ایالات متحده از ظرفیت‌های جنگ اطلاعاتی به‌ویژه در فضای سایبر برای پیشبرد اهداف و نیات خصمانه خود علیه مسکو در سطح وسیعی بهره‌می‌برد و حتی بخشی از دلایل فروپاشی اتحاد جماهیر شوروی را به گمراه‌سازی افکار عمومی بلوک شرق در اثر جنگ اطلاعاتی و رسانه‌ای غرب نسبت‌می‌دهند. این دیدگاه نزد کرملین با وقوع رویدادهای بی‌ثابت‌ساز دو دهه گذشته در خارج نزدیک روسیه شامل انقلاب‌های رنگی در صربستان (۲۰۰۰)، گرجستان (۲۰۰۳)، اوکراین (۲۰۰۴) و قرقیزستان (۲۰۰۵)، پیوستن تعداد زیادی از دولت‌های پساشوروی و اعضای پیمان ورشو (۱۹۹۱-۱۹۵۵) به ناتو و اتحادیه اروپایی و برکناری ویکتور یانوکویچ، رئیس‌جمهور هوادار روسیه در اوکراین طی انقلاب ۲۰۱۴ هواداران اروپا در این کشور و همچنین خیزش‌های ۲۰۱۰-۲۰۱۱ جهان عرب در جنوب غربی آسیا و شمال آفریقا تقویت نیز شده‌است.

وقایع و برداشت‌هایی از این دست طی سال‌های گذشته بر احساس آسیب‌پذیری روسیه در فضای سایبر افزوده و توجیهاتی برای نظارت و کنترل گسترده داخلی بر فضای مجازی به‌منظورجلوگیری از نفوذ بیرونی، دسترسی غیرمجاز به اطلاعات، سرقت داده‌های طبقه‌بندی‌شده و نیز انتشار اطلاعات نادرست و گمراه‌کننده با هدف تأثیرگذاری بر افکار عمومی فراهم آورده‌است. الگوی حکمرانی امنیت سایبری روسیه در درجه نخست برپایه جلوگیری از خدشه‌دارشدن امنیت ملی این کشور از رهگذر تهدیدهای بیرونی در فضای مجازی شکل گرفته‌است و بنابراین برهم‌کنش‌های بین‌الدولی را نیز دربرمی‌گیرد.

نگرانی روسیه نسبت به سوءستفاده دولت‌های غربی از ابزارهای سایبری برای تحقق نیات سیاسی، نظامی و امنیتی خود طی دو دهه گذشته به کوشش‌های دیپلماتیک وسیع این

[1]. Russian Federation Doctrine of Information Security

کشور در حوزه تصدی‌گری و تنظیم مقررات فضای مجازی در سطوح جهانی، منطقه‌ای و دوجانبه منجر شده‌است که می‌توان از آن تحت عنوان دیپلماسی سایبری[۱] روسیه نام‌برد. دیپلماسی سایبری روسیه از چشم‌انداز دولت‌ها، نهادها، تحلیلگرها و رسانه‌های غربی اغلب به‌مثابه تلاشی همه‌جانبه از سوی حکومت روسیه برای به‌دست‌گرفتن ابتکارعمل مدیریت شهروندان این کشور در فضای مجازی برپایه ایجاد هنجارهای جدید بین‌المللی کنترل سایبری با کمک برخی دیگر از دولت‌های هم‌فکر[۲] تعبیر می‌شود. این نگاه بیش از آنکه تقلیل‌گرایانه باشد، مغرضانه است. حتی دولت‌های اروپایی نیز به‌رغم وجود نهادهای بین‌المللی گوناگون در مدیریت جهانی فضای مجازی از نمایشی‌بودن این‌گونه نهادها و یکه‌تازی ایالات متحده در فضای سایبر گلایه‌مند هستند.

دیپلماسی سایبری مسکو بیش‌وپیش از آنکه به‌دنبال تثبیت حاکمیت (حق‌حاکمیت)[۳] دولت بر فضای سایبری روسیه یا کنترل بر دسترسی شهروندان این کشور در فضای مجازی باشد، ظرفیت هنجاری خود برای به‌چالش‌کشیدن نظم بین‌المللی سایبری شکل‌گرفته برپایه قواعد لیبرال را به‌نمایش گذاشته‌است. بی‌شک، روسیه در این مسیر تنها نیست و دولت‌های به‌لحاظ جهانی و منطقه‌ای قدرتمند فراوانی ازجمله اتحادیه اروپایی، چین، هند، برزیل، ایران، ترکیه، آفریقای جنوبی نیز هدف مشابهی را دنبال‌می‌کنند که وجه مشترک همه آنها را می‌توان در کوشش برای ایجاد حکمرانی جهانی فضای مجازی[۴] برپایه دموکراسی، انحصارزدایی و شفافیت خلاصه‌کرد.

دیپلماسی سایبری روسیه تا به امروز نقش برجسته‌ای در بسیج نارضایتی‌های جهانی علیه هنجارهای به طور عمده یک‌جانبه ایجادشده حاکم بر رژیم حکمرانی فضای مجازی در سطح‌بین‌المللی داشته‌است. به‌جز دولت‌های اروپایی که دغدغه آنها بیشتر منحصر به جایگزینی هنجارهای یک‌جانبه آمریکایی با هنجارهای لیبرال غربی است، اغلب دولت‌های جهان از ایده مسکو مبنی بر همگانی‌سازی حکمرانی فضای مجازی برپایه اصل دموکراسی میان همه دولت‌ها پشتیبانی می‌کنند و خواستار احترام به حق‌حاکمیت ملت‌ها در فضای مجازی هستند. حکمرانی سایبری در درون کشورها برحسب ویژگی‌های سیاسی، قومی و

---

1. Cyber Diplomacy
2. Like-minded
3. Sovereignty
4. Global Governance of the Internet

مذهبی و هندسه مناسبات جامعه، حکومت و فرهنگ شکل‌می‌گیرد و در سپهر داخلی دولت‌ها قراردارد. پشتیبانی از کوشش‌های دیپلماتیک روسیه برای همگانی‌سازی و انحصارزدایی از حکمرانی جهانی فضای سایبر نیز موضوعی جدا از نظام مدیریت سایبری این کشور در داخل است. با این همه، تدقیق در سیاست‌ها و رهنامه‌های روسیه در حوزه امنیت اطلاعات و حکمرانی فضای مجازی برای شناخت انگیزه‌های دیپلماسی سایبری این کشور ضروری است.

این مقاله با هدف رونمایی از ابتکارها، اولویت‌ها، انگیزه‌ها و پیامدهای دیپلماسی سایبری روسیه در سطوح دوجانبه، منطقه‌ای و بین‌المللی تدوین شده و به‌دنبال ارائه پاسخی مناسب به این پرسش محوری است که «خاستگاه فکری دیپلماسی سایبری روسیه چیست و چه هدفی را دنبال‌می‌کند؟» فرضیه به‌آزمون گذاشته‌شده این است که «ریشه دیپلماسی سایبری روسیه به فهم این کشور از قلمروی سایبر به‌مثابه ابزار جدید سلطه غرب بازمی‌گردد و هدف مسکو، رفع تصدی‌گری از موجودیت‌های طرفدار واشنگتن، بروکسل و ناتو بر فضای سایبر با ایجاد حکمرانی جهانی فضای مجازی است». فرض روسیه در فضای سایبر بر پیوستگی غرب است و بنابراین (اتحادیه) اروپا را جدای از (ایالات متحده) آمریکا نمی‌داند. همچنین، شناسایی قلمروی سایبر ازسوی روسیه به‌عنوان میدان جدید نبرد غرب علیه این کشور به‌معنای تهدید قلمدادکردن سلطه سایبری غرب هم برای نظم بین‌المللی دموکرات و هم حق‌حاکمیت داخلی دولت‌ها ازجمله روسیه است.

مقاله حاضر از نوع کیفی (توصیفی-تحلیلی) بوده و با استفاده از روش‌شناسی استنتاجی انجام پذیرفته‌است. داده‌ها نیز به‌شیوه کتابخانه‌ای از راه مطالعه اسناد ملی روسیه، اظهارنظرها و بیانیه‌های رسمی، کتاب‌ها، مقاله‌ها، تارنماها و خبرگزاری‌های معتبر گردآوری شده‌اند. داده‌های توصیفی و یافته‌های به‌دست‌آمده نیز تحت مفهوم حکمرانی فضای مجازی و ماهیت غیرقطعی و سیال این مفهوم تجزیه‌وتحلیل شده‌اند.

چارچوب مفهومی

برخلاف پیش‌بینی‌های زودهنگام در مورد ماهیت بدون‌مرز و تقریبا بی‌قانون فضای مجازی، نشانه‌های حکمرانی و اعمال حق‌حاکمیت بر فضای مجازی به‌تدریج پدیدار شد (Satola, 2007:49). رابطه میان فضای مجازی و حق‌حاکمیت از دهه ۹۰ میلادی با

ورود به ادبیات دانشگاهی، پژوهشگران و اندیشمندان را بـه‌خـود معطـوف‌داشـت و از رهگـذر دگردیسی سیاست بین‌الملل تحت شرایط جهانی‌سازی پیشرفت قابل‌تـوجهی نمـود. ماهیـت فراملی فضای مجازی در تجزیه‌وتحلیل‌هـای اولیـه بـه‌دلیـل قابلیـت درنوردیـدن قلمروهـای سرزمینی مجزا و عبور از مرزهای فیزیکی کـشورها در جهـت فرسـایش اصـل حـق‌حاکمیـت دولت‌ها تفسیرمی‌شد. علاوه بر این، قلمروی مجازی به‌مثابه فضایی بنیادشکن دارای حاکمیت منحصربه‌فرد و مخصوص به‌خود فرض‌می‌شد کـه فراتـر از اقتـدار یـا کنتـرل دولـت‌هـا قـرار دارد (Zeng et al., 2017:3).

در حقیقت، توانایی ورود افراد بـه دنیـای مجـازی دیگـران، عبـور بـدون‌مـانع داده‌هـا و اطلاعات از مرزها و به‌ویژه تغییر بازیگران به‌گونه‌ای ماهیت حق‌حاکمیـت سـنتی دولـت‌هـا را به‌چالش کشیده‌بود (جعفری، ۱۳۹۸: ۱۱۷) که اعمال حاکمیت دولت بر فضای سایبر در نگاه نخست دشوار به نظر می‌رسید. با این همه، تجزیه‌وتحلیل‌های بعـدی در تـلاش بـرای کـشف دقیق‌تر چگونگی تأثیر فضای مجازی بـر نظریـه و رویـه حاکمیـت بـه مفهـوم چنـدمعنایی[1] حاکمیت آوردند (Krasner 2001:233). به عنوان مثال، بتـز[2] و اسـتیونز[3] (74-55 :2011) به ایـن نتیجـه رسـیدند، فـضای مجـازی بـه‌لحـاظ بـین‌المللـی چـالش مـستقیمی در برابـر حق‌حاکمیت قانونی دولت‌ها ایجاد نمی‌کند. حقوق بین‌الملل به همه دولت‌هـا حـق‌حاکمیـت برابر اعطا داشته‌است و فضای مجازی نیز اساسـا ایـن وضـعیت را تحـت‌تـأثیر قرارنمـی‌دهـد. درمقابل، اگر فضای مجازی به معنای توانایی کنتـرل جریـان‌هـای اطلاعـات بـرون‌مـرزی یـا به‌کارگرفتن اقتدار داخلی در درون مرزهای سرزمینی باشد با پیامـدهای قابـل‌تـوجهی بـرای حاکمیت دولت همراه خواهدبود.

مفهوم چندمعنایی حق‌حاکمیت بر فضای مجازی با تفکیک و به‌رسـمیت‌شـناختن حاکمیـت داخلی و بین‌المللی بر فضای سایبر در ادامه به پیدایش مفهوم حکمرانی فـضای مجـازی منجرشـد که میان دو اقتدار داخلی و بین‌المللی در نوسان است (Bozhkov,2020:1-2). مفهوم حکمرانـی فضای مجازی درواقع، بر استقلال واژه "حکمرانی" از "حکومت" به‌مثابـه یکـی از معیارهـای شناسایی و ویژگـی‌هـای انحـصاری دولـت تأکیـد دارد. از دیـدگاه جیمـز روزنـا[4] (1992:4)

---

[1]. Polysemic
[2]. David J. Betz
[3]. Tim Stevens
[4]. James Rosenau

حکومت به کنش‌هایی اشاره‌دارد که ازسوی یک اقتدار رسمی و اختیارات پلیس برای تضمین اجرای سیاست‌های به‌نحو مقتضی تدوین‌شده پشتیبانی می‌شود؛ درحالی‌که حکمرانی به فعالیت‌هایی ارجاع دارد که با اهداف مشترکی پشتیبانی‌می‌شوند که ممکن‌است از مناصب دستوری رسمی و قانونی صادر نشده‌باشد و برای فائق‌آمدن بر مقاومت یا دست‌یافتن به ایجاب نیازی به تکیه بر اختیارات پلیس نداشته‌باشند. به‌عبارت دیگر، حکمرانی پدیده‌ای فراتر از حکومت است که سازوکارهای غیررسمی و ترتیبات غیردولتی نیز علاوه بر نهادهای حکومتی دربرمی‌گیرد. در نگاه رابرت کیوهن[1] (2003: 133) نیز حکمرانی محاط بر حکومت است. وی حکمرانی را به‌مثابه "ساخت و پیاده‌سازی قواعد و اعمال قدرت در یک حوزه فعالیت خاص" توصیف می‌کند.

ایجاد و توسعه مفهوم حکمرانی دربرابر مفهوم حاکمیت نسبت مسقیمی با ورود بازیگران غیردولتی به اداره امور داخلی و بین‌المللی دارد. به همین جهت نیز ایده مشترک تمام تعاریف و انواع حکمرانی را می‌توان در عبارت "زمام‌داری بدون نقش فقط دولت" خلاصه کرد (قوچانی و حسین‌پور، ۱۳۹۶: ۵۴). از این چشم‌انداز، یک رژیم حکمرانی شامل مجموعه‌ای از ابزارها، موجودیت‌ها و نهادهای اجتماعی به‌طور مشترک پذیرفته‌شده همچون اصول صریح یا ضمنی، هنجارها، قواعد و روندهای تصمیم‌گیری است که با درجه‌های متفاوتی از رسمیت و به‌صورت نهادی بر رفتار و برهم‌کنش‌های بازیگران در یک قلمروی موضوعی و/یا جغرافیایی خاص تأثیرمی‌گذارد و در جهت هدایت مسایل و تنظیم فرایندهای آن گام‌برمی‌دارد (Hufty, 2011:405-409). دولت رسمی‌ترین و در عین حال به‌لحاظ بین‌المللی کوچک‌ترین رژیم حکمرانی جهانی به‌شمارمی‌آید زیرا گستره آن به مرزهای سیاسی یک کشور محدوداست.

سودمندی مفهوم گستره‌تر حکمرانی بر عبارت محدودتر حکومت به توانایی آن برای شمول راهبردی برهم‌کنش‌های میان موجودیت‌هایی بازمی‌گردد که در سلسله‌مراتب رسمی سامان نیافته‌اند. ایراد مفهوم حکمرانی نیز در این است که مشروعیت حکمرانی در غیاب حاکمیت اغلب ازسوی افراد تحت‌تأثیر با تردید مواجه‌می‌شود. با وجود این، فضای اجرایی روبه‌رشدی وجود دارد که کارویژه‌های حقوق و حکمرانی بین‌الملل را با اتخاذ شگردهای پیچیده‌ای همچون درهم آمیختن مؤلفه‌های خصوصی و عمومی، نهادهای داخلی و

[1]. Robert O. Keohane

بین‌المللی، حقوق سخت و نرم، اصول صریح و ضمنی و قواعد غیرالـزام‌آور و قـانونی بـه اجـرا درمی‌آورد (Krisch and Kingsbury,2006:3). در مقایسه با رویکردهـای سـنتی طرفـدار تمرکزگرایی و تلقی دولت‌ها به‌مثابه مراجع انحصاری اقتدار به‌نظر می‌رسد که موجودیت‌هایی از این دست نویدبخش ارزش افزوده بیشتر، اثربخشی شدیدتر، انعطاف‌پـذیری اضـافه، سـطح بالاتری از دقت و احتمالا جایگزینی دموکراتیک‌تـر بـرای ایجـاد و توسـعه حقـوق و مقـررات بین‌المللی هستند. همچنین تا آنجا که به موضوع حکمرانی فضای مجازی مربوط می‌شود این ترتیبـات غیررسـمی بـرای اطمینـان از وجـود انعطـاف‌پـذیری کـافی درجهـت پیـشرفت بدون‌محدودیت این فناوری نورسته ضروی به‌شمارمی‌آیند (Andjelkovic, 2006:14).

در هر صورت، ماهیت فضای سایر و تفاوت‌های ذاتی آن با فضای ژئوپلیتیـک بـه‌گونـه‌ای است که حتی ایجاد یک رژیم جهانی حکمرانی سایبری با مشارکت تمامی دولت‌هـای جهـان برای خط‌مشی‌گذاری و اداره جهانی فضای مجازی نیز دست‌کم در کوتاه‌مـدت قـادر بـه رفـع چالش‌های مـرتبط بـا حاکمیـت بـر قلمـروی سـایبری نخواهـدبود. قلمـروی اطلاعـاتی[1] در جغرافیای فضای سایبر همان نقشی را ایفامی‌کند که سرزمین (یا خاک) در فضای ژئوپلیتیک برعهده‌دارد (قادری و نصرتی، ۱۳۹۲: ۱۰۳). قلمروی اطلاعاتی به‌طور عمده شامل دامنه‌هـای فضای مجازی[2]، پایگاه داده‌ها[3]، میزبان‌های وب/شبکه[4] و کارسازهای فضای مجازی[5] می‌شـود که همه آنها دارای ماهیت دوگانه مجازی/واقعـی هـستند. بـه‌عبـارت بهتـر بـا اینکـه اجـزای قلمروی اطلاعاتی با کارویژه‌های مجازی تعریف و شناسایی می‌شوند، اما محـل اسـتقرار خـود این اجزا یا نهادهای متولی آنها در قلمروی سـرزمینی و حـوزه صـلاحیت دولـت اسـت. ایـن دوگانگی، چالش اصلی ایجاد یک رژیم "جهانی" حکمرانی فضای مجازی به‌شمارمی‌آید.

ریشه شکل‌گیری رژیم کنونی حکمرانی فضای مجازی به ایجاد "مرجع انتساب اعـداد در فضای مجازی" (آیانا)[6] در سال ۱۹۸۸ بازمی‌گردد که در ابتدا برپایه قرارداد میان وزارت دفـاع ایالات متحده[7] با "مؤسسه علوم اطلاعات"[1] دانشگاه کالیفرنیای جنوبی[2] اداره‌می‌شد و سـپس

---

1. Information Realm
2. Internet domains
3. Databases
4. Web/Network Hosting
5. Internet servers
6. Internet Assigned Numbers Authority (IANA)
7. United States Department of Defense (DoD)

نظارت بر آن برعهده آژانس "ارتباطات ملی مدیریت اطلاعات"[۳] زیرمجموعه وزارت بازرگانی ایالات متحده[۴] گذاشته‌شد (Weinberg, 2000:194-195). مهم‌ترین و حساس‌ترین کارویژه این نهاد، مدیریت سامانه نام دامنه (ساناد)[۵] و تدوین پروتکل‌های فضای مجازی است. ساناد یک نظام سلسه‌مراتبی نام‌گذاری برای وبگاه‌ها، رایانه‌ها، گوشی‌های هوشمند، کارسازها، میزبان‌ها یا هر منبع دیگری است که به شبکه فضای مجازی متصل هستند.

هر وبگاه، کارساز، میزبان، شبکه یا دستگاه متصل به فضای مجازی با مجموعه‌ای از اعداد باقاعده تحت عنوان "نشانی پروتکل فضای مجازی" (آی‌پی آدرس)[۶] مورد شناسایی قرارمی‌گیرد. به عنوان مثال، دامنه یک وبگاه (google.com) تنها یک نام کاربرپسند برای حل مشکل به‌خاطرسپردن آی‌پی آدرس آن (۱۷۲,۲۱۷,۱۰,۱۴) است[۷]. تبدیل یا ترجمه متقابل این اعداد و نام‌ها را ساناد برعهده‌دارد و بنابراین کنترل بر این سامانه به‌نوعی به‌معنای کنترل بر فضای مجازی است زیرا امکان تغییر جهت درخواست کاربران از طریق تغییر پروتکل‌ها وجود دارد.

با رشد فضای مجازی و گسترش آن در جهان، آژانس ارتباطات ملی مدیریت اطلاعات فرایندی را برای ایجاد یک سازمان جدید برای انجام کارویژه‌های آیانا آغاز کرد که پاسخ‌گوی انتقادهای جهانی مبنی بر سلطه حکومت ایالات متحده بر مدیریت ساناد نیز باشد. نتیجه این سیاست، تأسیس "شرکت فضای مجازی برای نام‌ها و اعداد واگذارشده" (آیکان)[۸] در سپتامبر ۱۹۹۸ بود که به‌مثابه یک نهاد حاکمرانی خصوصی چندذی‌نفعی و ناسودبر[۹] برپایه قوانین ایالت کالیفرنیا به ثبت رسید. انتقال کامل کارویژه‌های آیانا از وزارت بازرگانی ایالات متحده به آیکان تا سال ۲۰۱۶ به‌طول انجامید و در اول اکتبر آن سال آیکان و آیانا برپایه یک توافق‌نامه تاریخی میان وزارت بازرگانی ایالات متحده و آیکان به‌طور کامل از نظارت

---

1. Information Sciences Institute (ISI)
2. University of Southern California (USC)
3. National Telecommunications and Information Administration (NTIA)
4. U.S. Department of Commerce (DoC)
5. Domain Name System (DNS)
6. Internet Protocol Address (IP Address)
7. به‌طور معمول هرچه یک وبگاه پربازدیدتر باشد، گستره آی‌پی آدرس آن نیز بیشتر است. از این رو آی‌پی آدرس قیدشده در اینجا برای وبگاه گوگل تنها برای نمونه است.
8. Internet Corporation for Assigned Names and Numbers (ICANN)
9. Multistakeholder and Nonprofit

حکومت ایالات متحده خارج‌شدند (Radu, 2019:23-59). در هر صورت، با توجه به اینکه آیکان در حوزه صلاحت قانونی دولت ایالات متحده و ایالت کالیفرنیا قرار دارد (Rojszczak, 2020:40)، بسیاری از دولت‌ها خواهان تغییر حوزه قضایی این نهاد به‌منظور بررسی دعاوی بین‌المللی مربوط به آن برحسب نظام حقوقی بین‌المللی هستند (Gwynn, 2019: 212).

علاوه بر این، اگرچه هیات‌مدیره آیکان در ظاهر چندذی‌نفعی است، اما گزینش اعضای آن در دو لایه عملا توسط دولت‌های غربی و در رأس آن ایالات متحده انجام‌می‌شود. هیات‌مدیره آیکان متشکل از ۲۲ عضو است که ۱۵ نفر از اعضا دارای حق رای و ۷ نفر شامل نماینده کمیته مشورتی حکومتی[1] (متشکل از نمایندگان دولت‌های عضو)، فاقد حق رای هستند. اعضای کمیته‌ها و کارگروه‌های اصلی که سهم بزرگی در تعیین هیات‌مدیره و تصمیم‌گیری‌های آیکان دارند نیز از سوی خود آیکان انتخاب می‌شوند. بنابراین، همانگونه که در یکی از مقاله‌های منتشرشده در وبگاه "مرکز ملی فضای مجازی" وابسته به "شورای عالی فضای مجازی" آمده‌است، «ادعای شکل‌گیری سیاست‌های آیکان توسط کارگروه‌ها و کمیته‌های پشتیبان در یک فرایند چندذینفعی مقرون به صحت نیست و ایالات متحده کماکان سیاست‌های خود را در عرصه حاکمیت فضای مجازی پیش‌می‌برد. با انتخاب، پذیرش و ارزیابی رجیستری‌ها و رجیسترارها توسط آیکان که یک شرکت آمریکایی است، دولت‌ها و اشخاصی که تحت تحریم‌های ایالات متحده هستند، نخواهند توانست در فرآیند حکمرانی فضای مجازی کوچکترین نقشی ایفاکنند. ظالمانه‌تر اینکه شرکت‌ها، اشخاص تحت تحریم و افراد مقیم کشورهای تحت تحریم نیز علاوه بر دولت‌ها مشمول تحریم آیکان خواهندبود. بخش خصوصی نیز به‌واسطه این تحریم‌ها در ساختار به‌ظاهر چندذی‌نفعی آیکان امکان اثرگذاری نخواهد داشت» (یوسف‌نژاد، ۱۳۹۷).

بحث پیرامون حاکمیت فضای مجازی با برگزاری اجلاس سران جامعه اطلاعاتی[2] ازسوی اتحادیه بین‌المللی مخابرات (آی‌تی‌یو)[3] وابسته به سازمان ملل در سال‌های ۲۰۰۳ و ۲۰۰۵ در ژنو و تونس به‌طور جدی پی‌گیری‌شد (ضیایی و شکیب‌نژاد، ۱۳۹۶: ۲۳۶). دولت‌های

---

[1]. Governmental Advisory Committee (GAC)
[2]. World Summit on the Information Society (WSIS)
[3]. International Telecommunication Union (ITU)

اروپایی و آمریکای شمالی در این دو اجلاس بر پشتیبانی از آیکان به‌مثابه مرجع حکمرانی فضای مجازی اصرارداشتند، اما روسیه، چین، ایران، برزیل، کوبا و بسیاری دیگر از دولت‌های نوظهور و درحال‌توسعه خواهان زمام‌داری اتحادیه بین‌المللی مخابرات بر فضای مجازی بودند (Cuihong, 2018:656). در هر صورت، اجلاس سران جامعه اطلاعاتی در سال ۲۰۰۳ با ایجاد گروه کاری حاکمیت فضای مجازی[1]، زمینه تشکیل مجمع حکمرانی فضای مجازی[2] را فراهم‌ساخت که نخستین نشست آن در سال ۲۰۰۶ در آتن برگزار شد (Kurbalija, 2016:6). فضای حاکم بر چهارهمین نشست این مجمع در برلین در نوامبر ۲۰۱۹ نیز بنا به گزارش مرکز ملی فضای مجازی حاکی از تقویت گفتمان حاکمیت ملی در فضای سایبر و تسری آن از روسیه، چین و ایران و کشورهای درحال توسعه به حوزه اروپا بود و اعمال حاکمیت ایالات متحده بر تمام سطوح و لایه‌های فضای مجازی ازسوی بسیاری از دولت‌ها مورد انتقاد قرارگرفت. در این نشست اغلب معماران فضای مجازی و وب، سخنرانان کلیدی، نمایندگان چین، روسیه، دولت‌های درحال توسعه، اروپا و سازمان‌های غیردولتی بین‌المللی علیه انحصار واشنگتن بر فضای سایبر و ضرورت رعایت چارچوب‌های حقوقی بین‌المللی موضع‌گرفتند (مکبری، ۱۳۹۸: ۱۶).

تلاش دولت‌های برای تأثیرگذاری بر رژیم حکمرانی فضای مجازی و اعاده حاکمیت خود بر فضای سایبر داخلی نسبت مستقیمی با نگرانی از تهدیدها علیه امنیت ملی از رهگذر سوءاستفاده دیگر بازیگران از ظرفیت‌های فضای سایبر دارد. کاربرد معمول عبارت "حکمرانی امنیت سایبری"[3] به‌جای حکمرانی سایبری نیز نشان از اهمیت موضوع امنیت در مفهوم‌سازی حکمرانی فضای مجازی دارد. کوفی عنان[4]، دبیرکل وقت سازمان ملل در تلاش برای ایجاد و توسعه همکاری‌های بین‌دولتی برای محدودکردن درگیری‌های سایبری در سال ۲۰۰۴ گروه متخصصان حکومتی سازمان ملل[5] راجع به پیشبرد رفتار مسئولانه دولت در فضای سایبر در زمینه امنیت بین‌الملل[6] را با ۲۵ عضو به‌منظور وضع قوانین امنیت سایبری

---

1. Working Group on Internet Governance (WGIG)
2. Internet Governance Forum (IGF)
3. Cyber Security (Cybersecurity) Governance
4. Kofi Atta Annan
5. United Nations Group of Governmental Experts (UN GGE)
6. on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security

منصوب‌کرد. مجمع عمومی سازمان ملل نیز در دسامبر ۲۰۱۸ با صدور قطعنامه‌ای گروه کاری باز[1] راجع به پیشرفت‌ها در حوزه فناوری اطلاعات و ارتباطات در زمینه امنیت بین‌الملل[2] را به‌موازات گروه متخصصان حکومتی برای دوره زمانی ۲۰۱۹-۲۰۲۱ تشکیل‌داد که مشارکت در آن برای همه دولت‌های علاقه‌مند ممکن‌است (Ruhl et al., 2020:4-7). چگونگی تدوین هنجارها و قواعد حاکم بر فضای سایبر و برقراری امنیت در آن بخش جدایی‌ناپذیر مفهوم‌سازی حکمرانی فضای مجازی به‌شمارمی‌آید. بنابراین تلاش این دو نهاد و دیگر موجودیت‌های بین‌المللی برای تنظیم مقررات امنیت سایبری در کنار قانون‌گذاری ملی دولت‌ها نشان از تقویت شیوه مختلط حکمرانی فضای مجازی دارد.

با اینکه چندپارگی لزوما سرنوشت حکمرانی سایبری نخواهد بود، اما برداشت‌ها از حق‌حاکمیت فضای مجازی میان دولت‌ها بسیار متفاوت است. این تفاوت نسبت مستقیمی با میزان نفوذ دولت‌ها بر رژیم کنونی حکمرانی فضای مجازی دارد. بدیهی است ایالات متحده که از رهگذر استقرار آیکان در خاک خود به حاکم بلامنازع مقولات فنی فضای مجازی تبدیل شده‌است، مخالف هرگونه تغییری در رژیم حکمرانی فضای مجازی باشد. در برابر، قدرت‌های نوظهوری همچون اعضای بریکس[3] (برزیل، روسی، هند، چین و آفریقای جنوبی) به‌درستی تلاش‌دارند تا سهم خود در توسعه نظام حقوقی حاکم بر فضای سایبر را هم‌راستا با افزایش نقش خود در اقتصاد سیاسی بین‌الملل ارتقابخشند.

از این مهم‌تر به‌رسمیت شناخته‌شدن حق‌حاکمیت دولت‌های نوظهور بر فضای سایبر داخلی و حکمرانی داده‌ها برای اطمینان از ثبات داخلی و حفظ اسرار فنی و مزایای تجاری آنها ضرورتی انکارناپذیر به‌شمار می‌آید. فدراسیون روسیه به‌مثابه کشوری نوظهور علاوه بر داشتن همه این انگیزه‌ها به جنگ سایبری غرب علیه مسکو و لزوم ایجاد بازدارندگی راهبردی در برابر آن نیز به‌شدت باور دارد. بنابراین، همان‌گونه که دیپلماسی و جنگ دو به دو ناسازگار نیستند، دیپلماسی سایبری روسیه نیز از چشم‌انداز مسکو بخشی از جنگ سایبری این کشور با غرب به‌ویژه ایالات متحده محسوب‌می‌شود.

---

1. Open-Ended Working Group (OEWG)
2. on Developments in the Field of ICTs in the Context of International Security
3. BRICS: Brazil, Russia, India, China, and South Africa

راهبرد سایبری روسیه

مباحث مربوط به حکمرانی سایبری تقریبا در همه آموزه‌های رسمی و اسناد بالادستی فدراسیون روسیه طی یک دهه گذشته به‌چشم‌می‌خورد. به‌عنوان مثال، فضای سایبر نقش برجسته‌ای در تدوین راهبردهای سیاسی، نظامی یا انرژی روسیه از ابتدای دهه دوم سده بیست‌ویکم داشته‌است. رهنامه‌های امنیت اطلاعات[1] روسیه نیز فراگیرترین و مستقیم‌ترین اسنادی هستند که دیدگاه‌ها و انتظارات رسمی مسکو در قبال حکمرانی فضای مجازی و امنیت در فضای سایبر را ارائه می‌دهند. نخستین رهنامه امنیت اطلاعات فدراسیون روسیه در سال ۲۰۰۰ پیش از تبدیل‌شدن حکمرانی فضای مجازی به موضوعی محوری در عرصه بین‌المللی تدوین شده‌بود. این رهنامه در سال ۲۰۱۶ همراه با تغییرات قابل‌توجه در ساختار، محتوا و حجم به‌روزرسانی شد.

سپهر اطلاعات در رهنامه امنیت اطلاعات ۲۰۰۰[2] به‌مثابه ترکیبی از"اطلاعات، زیرساخت اطلاعاتی، موجودیت‌های مشغول به گردآوری، تکوین، انتشار و به‌کارگیری اطلاعات و نظام حاکم بر مناسبات عمومی ناشی از این وضعیت" تعریف شده‌بود. این تعریف بسیار گسترده‌است و تمام جنبه‌های اطلاعات از خود این مفهوم گرفته تا زیرساخت و نظام‌های اطلاعاتی را پوشش‌می‌دهد. در این رهنامه برای امنیت اطلاعات کارویژه "پاسداری از منافع ملی فدراسیون روسیه در سپهر اطلاعات که از رهگذر منافع متوازن سرتاسری در سطح فرد، جامعه و دولت تعیین می‌شود" درنظر گرفته شده‌بود. معنای این توازن با رجوع به مفاد متعاقب این رهنامه بیشتر آشکار می‌شود به‌ویژه آنجا که اظهار داشته‌بود، «توسعه سیاسی و اجتماعی-اقتصادی کنونی در کشور تناقض‌های شدیدی را میان مقتضیات جامعه از باب گسترش تبادل آزاد اطلاعات و ضرورت حفظ محدودیت‌های تنظیم‌شده فردی در انتشار اطلاعات سبب شده‌است.»

رهنامه امنیت اطلاعات ۲۰۰۰ در رابطه با تهدیدهای ناشی از جنگ اطلاعاتی به فهرستی از تهدیدهای پیش روی حقوق اساسی و آزادی انسان و شهروندان اشاره‌دارد که شامل «استفاده غیرقانونی از ابزارهای ویژه نفوذ بر فرد، گروه و آگاهی عمومی» می‌شود.

---

[1]. The Information Security Doctrines

[2]. تمامی مطالب منتسب به رهنامه امنیت اطلاعات ۲۰۰۰ (2000 Information Security Doctrine) در این مقاله از متن اصلی این سند استخراج شده‌است: (ДИТ, 2000:1-14)

مبحث جنگ اطلاعاتی در این رهنامه همچنین اخلال در رسانه‌های روسی به‌واسطه سپهر اطلاعات ملی و افزایش وابستگی حوزه‌های معنوی، اقتصادی و سیاسی زندگی جمعی روسیه به موجودیت‌های اطلاعاتی بیگانه را نیز دربرمی‌گرفت. تهدیدها علیه سیاست‌های دولتی ازجمله انحصار بازار اطلاعات روسیه به‌دست موجودیت‌های داخلی و بیگانه و همچنین انسداد رسانه‌های دولتی روسیه به‌لحاظ داخلی و بین‌المللی نیز به‌طور مشابه در حوزه جنگ اطلاعاتی قرارمی‌گرفتند که نیازمند برنامه‌ریزی برای مقابله با آنها بود.

از آنجاکه فضای سایبر و موضوع حکمرانی فضای مجازی تنها با آغاز هزاره سوم میلادی راه خود را به‌طور جدی به مباحثه‌های سیاسی بین‌المللی بازکرد، پدیده جنگ سایبری توجهات کمی را در رهنامه امنیت اطلاعات ۲۰۰۰ به‌خود معطوف داشته‌بود. جنگ سایبری طی نیمه دوم دهه نخست از سده بیست‌ویکم به جریان اصلی مناظره‌ها در روسیه و میان روسیه و غرب تبدیل‌شد. با وجود این در رهنامه ۲۰۰۰ بدون اشاره به عبارت‌های فضای مجازی و فضای سایبر از نفوذ فنی و اطلاعاتی شامل حمله‌های الکترونیکی و رخنه از طریق شبکه‌های رایانه‌ای توسط دشمنان احتمالی به‌مثابه تهدیدهای بیرونی علیه سپهر دفاعی فدراسیون روسیه نام برده شده‌بود که این هشدار را می‌توان به لایه‌های اولیه و ساده جنگ سایبری تعبیرکرد. تهدیدهای خارجی در این رهنامه شامل فعالیت‌های «سیاسی، اقتصادی، نظامی، جاسوسی و اطلاعاتی موجودیت‌های بیگانه» و همچنین برخی کشورهای مشخص که به‌دنبال «غلبه و تجاوز به منافع روسیه در فضای اطلاعات جهانی و خلع‌ید از این کشور در بازارهای اطلاعاتی خارجی و داخلی» هستند نیز می‌شد.

«توسعه مفهوم جنگ اطلاعاتی نزد برخی دولت‌ها که زمینه را برای پیدایش ابزارهای حمله پرخطر علیه سپهر اطلاعاتی دیگر کشورهای جهان، ایجاد اختلال در عملکرد عادی سامانه‌های اطلاعاتی و ارتباطی آنها، نقض امنیت منابع اطلاعاتی و ایجاد دسترسی غیرمجاز به آنها» فراهم آورده‌است نیز در رهنامه امنیت اطلاعات ۲۰۰۰ در زمره منابع تهدیدهای بیرونی علیه امنیت اطلاعات فدراسیون روسیه دسته‌بندی شده‌بود. این رهنامه در ادامه به سرویس‌های اطلاعاتی خارجی به‌چشم عامل فعالیت‌های توطئه‌گرایانه و خرابکارانه با استفاده از روش‌های نفوذ اطلاعاتی و روان‌شناختی و بنابراین یک تهدید علیه سپهر دفاعی فدراسیون روسیه می‌نگریست.

برپایه این رهنامه، «عدم اطمینان از حقوق شهروندان در دسترسی به اطلاعات و دستکاری اطلاعات، واکنش‌های منفی را در میان مردم برخواهدانگیخت که ممکن است در برخی موارد به بی‌ثباتی اوضاع اجتماعی و سیاسی در جامعه منجر شود». به‌طور مشابه، هماهنگی ملی و ثبات اقتدار دولتی نیز در این رهنامه به‌عنوان چالش‌هایی در سپهر سیاست داخلی ذکر شده‌بود. این موارد تا آنجاکه به استفاده موجودیت‌ها و جریان‌های بیگانه از اطلاعات و دستکاری آنها برای جهت‌دهی افکار عمومی و گمراهی شهروندان مربوط می‌شود را می‌توان برای فهم بهتر زمینه‌ها و علل وقوع انقلاب‌های رنگی به کاربرد (Jonsson, 2019:97). رهنامه امنیت اطلاعات ۲۰۰۰ همچنین با تمرکز بر تهدیدها در سپهر معنوی و علیه آگاهی عمومی بر ابعاد اطلاعاتی-روان‌شناختی تأکیدداشت، چراکه این تهدیدها می‌توانند به بی‌ثباتی اجتماعی و سیاسی در روسیه منجرشوند. این رهنامه نسبت به تلاش‌های موجودیت‌ها و سرویس‌های اطلاعاتی بیگانه برای نفوذ معنوی و روان‌شناختی بر روسیه نیز هشدارمی‌داد.

در ادامه تلاش‌های مسکو برای تدوین چارچوب‌های مفهومی و کاری سپهر اطلاعات و سپس سایبری فدراسیون روسیه، وزارت دفاع این کشور در سال ۲۰۱۱ سند کوتاهی را درباره چشم‌انداز مفهومی راجع‌به فعالیت نیروهای مسلح فدراسیون روسیه در سپهر اطلاعات[1] منتشرنمود که تعریف روشنی از جنگ اطلاعات ارائه‌می‌داد، «جنگ اطلاعاتی- مقابله دو یا چند کشور در فضای اطلاعاتی برای آسیب‌رساندن به سامانه‌های اطلاعاتی، فرآیندها و منابعی که از اهمیت اساسی برخوردار هستند و دیگر ساختارها، تخریب سیستم‌های سیاسی، اقتصادی و اجتماعی و شستشوی مغزی گسترده مردم به‌منظور بی‌ثبات‌کردن جامعه و دولت و همچنین وادارکردن دولت به تصمیم‌گیری به‌نفع طرف مقابل» (Ajir and Vailliant, 2018:71). این تعریف پیش‌تر در موافقت‌نامه میان حکومت دولت‌های عضو سازمان همکاری شانگهای برای همکاری در حوزه تضمین امنیت اطلاعات بین‌المللی[2] نیز آمده‌بود (Von Heinegg, 2019:5).

---

[1]. Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space

[2]. Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of Ensuring International Information Security

شورای امنیت فدراسیون روسیه[1] نیز در ژوئیه ۲۰۱۳ سندی را تحت عنوان "اصول پایه برای خط‌مشی دولتی فدراسیون روسیه در زمینه امنیت اطلاعات بین‌المللی تا سال ۲۰۲۰"[2] به‌تصویب رساند. در این سند، استفاده از فناوری‌های اطلاعات و ارتباطات به‌مثابه «سلاح اطلاعاتی برای مقاصد نظامی و سیاسی متناقض با حقوق بین‌الملل و برای اقدام‌ها خصمانه و اعمال تجاوزکارانه باهدف بی‌اعتبار ساختن حاکمیت و تخطی از تمامیت ارضی دولت‌ها و تهدید ثبات راهبردی، امنیت و صلح بین‌المللی» عمده‌ترین تهدید برای امنیت اطلاعات بین‌المللی قلمداد شده‌بود. این سند همچنین شامل تهدید تروریسم و مداخله در امور داخلی با هدف دامن‌زدن به ناآرامی‌ها و خشونت‌ها می‌شد. سند مذکور در پاسخ به تهدیدهایی از این دست، خط‌مشی دولتی روسیه را ترسیم‌می‌کرد که شامل تمایل به کاهش استفاده از فناوری‌های اطلاعات و ارتباط برای این مقاصد می‌شد. این اصول پایه همچنین به‌دنبال راه‌هایی برای مقابله با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد افراط‌گرایان از جمله دخالت در امور داخلی دولت‌های مستقل بود (СБРФ, 2013). اگرچه این سند در سپهر نظامی از ژرفای نظری بالایی برخوردارنبود، اما مفهوم‌سازی فناوری‌های اطلاعات و ارتباطات به‌مثابه سلاح برای مقاصد سیاسی و نظامی و تمرکز عمیق بر مفهوم عدم مداخله در امور داخلی از رهگذر به‌کارگیری این‌گونه فناوری‌ها را می‌توان از دستاوردهای مهم آن برشمرد.

گام مهم بعدی مسکو در تکوین حکمرانی امنیت سایبری در دسامبر ۲۰۱۶ با انتشار دومین رهنامه امنیت اطلاعات فدراسیون روسیه برداشته شد. با وجود فاصله زمانی طولانی میان انتشار نسخه اول و دوم این رهنامه، پیوستگی محتوایی آنها در مقایسه با آموزه‌های نظامی یا سیاست خارجی این کشور بیشتر بوده‌است. البته پیوستگی نسبی رویکرد کرملین در قبال موضوع امنیت اطلاعات در مقایسه با سپهرهای نظامی و سیاست خارجی نافی تغییرات، تحولات و پیشرفت‌های رهنامه امنیت اطلاعات ۲۰۱۶[3] نسبت به نسخه پیشین نیست. کما اینکه حجم نسخه ۲۰۱۶ تنها یک سوم حجم نسخه ۲۰۰۰ است که نشان از حذف برخی مباحث منسوخ و تمرکز بر ارزش کیفی مطالب در برابر توضیحات کمی دارد.

---

1. Security Council of the Russian Federation
2. Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020
3. تمامی مطالب منتسب به رهنامه امنیت اطلاعات ۲۰۱۶ (2016 Information Security Doctrine) در این مقاله از متن اصلی این سند استخراج شده‌است: (ПР, 2016:5-12)

رهنامه جدید در سپهر اطلاعاتی-روان‌شناختی عنوان می‌دارد که فرصت‌های روبه‌رشد برای گردش اطلاعات فرامرزی به‌طور فزاینده‌ای هم برای دستیابی به مقاصد ژئوپلیتیک و سیاسی-نظامی مشروع بازیگران و هم در جهت اهداف تروریستی، افراطی‌گری، جنایی و سایر مقاصد غیرقانونی به‌زیان ثبات راهبردی و امنیتی بین‌المللی مورد استفاده قرار می‌گیرند. این سند اظهارمی‌دارد که «این میدان برای کاربرد خدمات ویژه دولت‌های منفرد درحال گسترش بوده که به‌معنای فراهم‌شدن نفوذ اطلاعاتی-روان‌شناختی است که بی‌ثبات‌سازی وضعیت‌های سیاسی و اجتماعی داخلی در مناطق گوناگون جهان و تضعیف حاکمیت و نقض تمامیت ارضی دیگر دولت‌ها را هدف قرارمی‌دهد». در برابر، آموزه‌های پدافند اطلاعاتی ذکرشده‌اند که شامل خنثی‌سازی اثرات روان‌شناختی و اطلاعاتی به‌ویژه در رابطه با تخریب بنیان‌های تاریخی و سنت‌های میهن‌پرستانه و نیز بهبود توانایی نیروهای مسلح برای هدایت و مقابله با جنگ اطلاعاتی می‌شوند. اولویت بعدی به خنثی‌کردن تأثیر اطلاعاتی بازمی‌گردد که با هدف فرسایش ارزش‌های اخلاقی و معنوی دیرپای روسیه انتشار داده‌می‌شوند.

آشکارترین نوآوری رهنامه جدید به‌لحاظ داخلی را شاید بتوان به فراخوان آن برای توسعه "سامانه ملی مدیریت بخش فضای مجازی روسیه[1]" نسبت‌داد. در این رهنامه همچنین بر «محافظت از حاکمیت فدراسیون روسیه در فضای اطلاعاتی ازطریق سیاست‌های ملی و مستقل برای تعقیب منافع ملی خود در سپهر اطلاعات» تأکید شده است. با وجود این، اصلی‌ترین و بیشترین تضمین‌های امنیت اطلاعات در رهنامه امنیت اطلاعات ۲۰۱۶ را باید در تلاش‌های این کشور در حوزه بین‌المللی و مشارکت راهبردی با دیگر دولت‌ها جستجوکرد. این رهنامه در برابر دو تضمین داخلی پیش‌گفته به سه تضمین بین‌المللی اشاره‌دارد:

- «شرکت در استقرار یک سامانه امنیت اطلاعات بین‌المللی که به‌طور مؤثر قادر به مقابله با استفاده از فناوری‌های اطلاعاتی برای اهداف نظامی و سیاسی ناقض قوانین بین‌المللی یا برای اهداف تروریستی، افراطی، جنایی یا دیگر موارد غیرقانونی باشد؛

- ایجاد سازوکارهای قانونی بین‌المللی بالحاظ ماهیت خاص فناوری‌های اطلاعات و به‌منظور جلوگیری و حل اختلافات بین دولت‌ها در سپهر اطلاعات؛ و

[1]. National System of the Russian Internet Segment Management

- ارتقاء جایگاه فدراسیون روسیه در سازمان‌های بین‌المللی در دفاع از همکاری سودمند متقابل و منصفانه با تمام طرف‌های ذی‌نفع در سپهر اطلاعات».

رهنامه ۲۰۱۶ بسیاری از اصول ۲۰۰۰ را با تأکید جدی‌تر بر تهدیدهای ناشی از حوزه اطلاعاتی-روان‌شناختی و تأثیر آن بر ارزش‌ها و ثبات اجتماعی و دولتی حفظ کرده‌است. بیشترین تفاوت میان این دو نسخه نیز به ضرورت همکاری‌های بین‌المللی برای دستیابی به تضمین‌های معتبر برای محافظت از امنیت اطلاعات در سپهر سایبر بازمی‌گردد. در حقیقت، ماهیت گریزپذیر فضای مجازی و جریان آزاد اطلاعات بر فراز مرزها راهی به‌جز همکاری و مشارکت میان دولت‌ها برای تضمین امنیت فضای سایبر باقی نگذاشته‌است. انگیزه اصلی تلاش‌های دیپلماتیک روسیه در زمینه حکمرانی فضای مجازی را نیز ضرورت‌های مقابله بین‌المللی چندجانبه با آثار مخرب جنگ سایبری در سپهر اطلاعات تشکیل‌می‌دهد.

تلاش‌های دیپلماتیک روسیه در سپهر سایبر

روسیه یکی از پیشگامان بحث در زمینه تأثیر فناوری‌های اطلاعات و ارتباطات بر ثبات بین‌المللی و امنیت داخلی دولت‌ها به‌شمارمی‌آید. ابتکارهای این کشور در زمینه حکمرانی جهانی فضای مجازی تا حد زیادی به جلوگیری از درگیری و شروع رقابت تسلیحاتی سایبری میان دولت‌ها معطوف‌است. روسیه نخستین کشوری بود که سپهر سایبری را به اصل حقوقی عدم مداخله در امور داخلی دولت‌ها پیوندزد و آن‌را در دستورکار سیاسی بین‌المللی قرارداد.

مسکو در ۲۳ سپتامبر ۱۹۹۸ یعنی دو سال پیش از انتشار رهنامه امنیت اطلاعات در سال ۲۰۰۰، پیش‌نویس قطعنامه "تحولات در حوزه اطلاعات و ارتباطات در زمینه امنیت بین‌الملل[1]" را با هدف ارتقا امنیت سایبری در جهان برای تصویب در مجمع عمومی سازمان ملل در اختیار کمیته اول این مجمع قرارداد. دستورکار کمیته اول مجمع عمومی تحت عنوان "خلع سلاح و امنیت بین‌المللی"[2] به موضوع‌های بنیادین مرتبط با صلح و امنیت بین‌الملل شامل رژیم امنیت بین‌المللی و خلع سلاح اختصاص دارد. از این رو، اقدام روسیه در ارائه پیش‌نویس این قطعنامه را می‌توان به فهم این کشور از فضای اطلاعات و سایبر

[1]. Developments in the Field of Information and Telecommunications in the Context of International Security

[2]. Disarmament and International Security (First Committee)

به‌مثابه سلاح و تلاش دیپلماتیک مسکو برای جلوگیری از سوءاستفاده دولت‌ها از ظرفیت‌های فناوری اطلاعات و ارتباطات برای مداخله در امور داخلی دولت‌های دیگر نسبت‌داد.

قطعنامه پیشنهادی روسیه پس از بررسی و تأیید ازسوی کمیته اول در ۴ دسامبر ۱۹۹۸ از سوی مجمع عمومی بدون رأی‌گیری در قالب قطعنامه ۷۰/۵۳ به‌تصویب رسید. در این سند ابراز نگرانی شده‌بود که ابزارها و فناوری‌های جدید به‌طور بالقوه می‌توانند برای مقاصد متناقض با اهداف تداوم ثبات و امنیت بین‌المللی و برخلاف امنیت دولت‌ها مورد استفاده قرارگیرند. قطعنامه مذکور همچنین بر جلوگیری از سوءاستفاده از فناوری‌ها و منابع اطلاعاتی برای مقاصد جنایتکارانه یا تروریستی تأکیدداشت (UN,1998). ایگور ایوانوف[1]، وزیر خارجه وقت روسیه در اظهارات خود در نشست تصویب این قطعنامه از این نیز فراتر رفت و خواستار رسیدگی به تهدیدهای بزرگتری شامل نظامی‌سازی فضای سایبر و تأثیرات مخرب سلاح‌های سایبر شده‌بود. روسیه در سال ۱۹۹۹ نیز قطعنامه مشابهی را ارائه داد، اما دو نکته حائز اهمیت از دیدگاه مسکو در آن گنجانده شده‌بود؛ نخست اینکه ممکن است از فضای سایبر برای اهداف نظامی سوءاستفاده شود و دوم اینکه جامعه جهانی باید اصولی در مورد چگونگی کاهش چنین مخاطراتی ارائه‌دهد (UN,1999). این قطعنامه‌ها تا دسامبر ۲۰۰۴ هر ساله با اندکی تغییر و پیشرفت با اجماع از سوی کمیته اول و سپس مجمع عمومی صادر می‌شد. تا اینکه ایالات متحده در دسامبر ۲۰۰۵ خواستار رأی‌گیری برای آن شد و تنها دولتی بود که به آن رأی منفی داد (UNODA, 2005).

اگرچه قطعنامه "تحولات در حوزه اطلاعات و ارتباطات در زمینه امنیت بین‌الملل" در سال ۲۰۰۵ بار دیگر در کمیته اول و مجمع عمومی به‌تصویب رسید، اما شکست اجماع و رأی منفی دولتی که فضای مجازی در آن زاده شده بود، ضربه سنگینی به فرایند شکل‌گیری هنجارهای سایبری در سازمان ملل وارد ساخت. دلیل رأی منفی واشنگتن به پیش‌نویس روسیه را باید در تلاش‌های مسکو طی اجلاس سران جامعه اطلاعاتی در ژنو (۲۰۰۳) و تونس (۲۰۰۵) برای جایگزین‌ساختن اتحادیه بین‌المللی مخابرات با آیکان در فرایند حکمرانی فضای مجازی و همراهی بخش بزرگی از جامعه بین‌الملل با این ایده جستجوکرد. در هر صورت، قطعنامه "تحولات در حوزه اطلاعات و ارتباطات در زمینه امنیت بین‌الملل" تا

[1]. Igor Ivanov

سال ۲۰۰۵ تنها ازسوی روسیه پیشنهاد و پشتیبانی می‌شد، اما این اقدام واشنگتن باعث شد تا پشتیبانان[1] این قطعنامه از سال ۲۰۰۶ به‌تدریج افزایش‌یابند.

این قطعنامه به‌مدت سه سال با موافقت همه رأی‌دهندگان به‌جز ایالات متحده به‌تصویب رسید تا اینکه در سال ۲۰۰۹ با آغاز دوران ریاست‌جمهوری باراک اوباما این قطعنامه بار دیگر با اجماع پذیرفته‌شد و در سال ۲۰۱۰ ایالات متحده یک گام نیز جلوتر نهاد و به جمع پشتیبانان قطعنامه پیوست. واشنگتن بین سال‌های ۲۰۱۱ تا ۲۰۱۴ به عدم‌مخالفت با این قطعنامه اکتفا کرد و از فهرست پشتیبانان آن کنارکشید. در سال ۲۰۱۵ ایالات متحده بار دیگر به‌منظور تلاش برای تعدیل مفاد این قطعنامه، رویکرد پشتیبانی را درپیش گرفت (سلطانی، ۱۳۹۶: ۱۹۰). در سال ۲۰۱۶ و در آخرین سال حضور اوباما در کاخ سفید، اگرچه ایالات متحده در جمع پشتیبانان این قطعنامه قرارنگرفت، اما به آن رأی موافق‌داد. با این همه، اصرار اوکراین در دادن رأی ممتنع، مانع از رسیدن به اجماع شد (UNODA, 2016).

این قطعنامه در سال ۲۰۱۷ به‌رغم تصویب در کمیته اول در مجمع عمومی به‌دلیل شدت گرفتن دوباره تضادها پس از آغاز دوران ریاست‌جمهوری دونالد پرامپ میان روسیه و دیگر دولت‌های درحال توسعه و نوظهور با ایالات متحده و هم‌پیمانانش در زمینه حکمرانی سایبری به رأی گذاشته نشد. در برابر، تصمیم گرفته‌شد از سال آینده قطعنامه پیشنهادی گروه دوم نیز هم‌زمان به رای گذاشته‌شود. بر این پایه در سال‌های ۲۰۱۸ و ۲۰۱۹ قطعنامه "رفتار مسئولانه دولت در فضای سایبر در زمینه امنیت بین‌الملل"[2] نیز در کنار قطعنامه سنتی روسیه (به‌رغم رای منفی متقابل دولت‌های روسیه و ایالات متحده و برخی هم‌پیمانان آنها) به‌تصویب مجمع عمومی رسید (UN, 2019:5-6).

دیپلماسی سایبری روسیه در سازمان ملل از سال ۲۰۰۴ به‌دنبال تشکیل "گروه متخصصان حکومتی سازمان ملل راجع به پیشبرد رفتار مسئولانه دولت در فضای سایبر در زمینه امنیت بین‌الملل" ازسوی عنان چهره تازه‌ای به‌خود گرفت. ۲۵ دولت عضو این گروه هر دوسال یک‌بار ازسوی مجمع عمومی انتخاب می‌شوند و به‌طور سنتی، پنج کرسی آن به اعضای دائم شورای امنیت اختصاص‌یافته و ۲۰ جایگاه دیگر برپایه گروه‌بندی‌های جغرافیایی

---

1. Sponsors
2. Advancing Responsible State Behaviour in Cyberspace in the Context of International Scurity

توزیع می‌شود. این گروه از سال ۲۰۰۴ تا به امروز به‌جز در سال‌های ۲۰۰۶-۲۰۰۸ برپایه قطعنامه‌های جداگانه مجمع عمومی طی شش دوره تشکیل شده‌است که ریاست دو دور نخست آن برعهده روسیه بوده‌است (GIP, 2020).

عمده هدف دیپلماسی سایبری روسیه در واپسین سال‌های سده بیستم و نخستین سال‌های سده بیست‌ویکم به جلوگیری از نظامی‌سازی فضای سایبر معطوف‌بود؛ اما دستیابی به این هدف به‌دنبال توسعه ظرفیت‌های نظامی قدرت‌های بزرگ ازجمله روسیه در فضای سایبر به‌تدریج غیرواقع‌بینانه جلوه‌کرد و مسکو امیدواربود که تلاش‌های گروه متخصصان حکومتی سازمان ملل راجع به فضای سایبر به پذیرش برخی انواع قواعد حاکم بر رفتار دولت‌ها در فضای سایبر منجرشود. نخستین دستاورد قابل‌توجه این گروه در سال ۲۰۱۳ با ایجاد اجماع بر سر پیش‌نویس گزارشی نهایی با هدف ترویج محیط فناوری اطلاعات و ارتباطات مسالمت‌آمیز، امن، باز و قابل‌دسترس حاصل‌شد (Chernenko, 2018:45). در گزارش نهایی این گروه که ۷ ژوئن ۲۰۱۳ منتشرشد بر سه دسته راه‌کارهای "همکاری‌جویانه" منجر به افزایش ثبات و امنیت شامل هنجارها، قواعد و اصول رفتار مسئولانه دولت‌ها، راه‌کارهای "داوطلبانه" برای افزایش شفافیت، اطمینان و اعتماد میان دولت‌ها و راه‌کارهای "ظرفیت‌سازی" تأکید شده‌بود. این گزارش برای نخستین‌بار تصریح‌می‌داشت، حقوق بین‌الملل و به‌ویژه منشور سازمان ملل در فضای سایبر قابل‌اجرا است و هم‌زمان بر اعمال حق‌حاکمیت دولت و هنجارها و اصول بین‌المللی منبعث از حق‌حاکمیت بر رفتار و کنش‌های دولت در سپهر سایبر و صلاحیت آنها بر زیرساخت فناوری اطلاعات و ارتباطات در قلمرو خود تأکیدداشت. گزارش مذکور همچنین مجموعه توصیه‌هایی برای راهکارهای ظرفیت‌سازی و اعتمادسازی داوطلبانه پیش روی دولت‌ها قرارمی‌داد (UNDL, 2013: 2-8).

گروه متخصصان حکومتی سازمان ملل راجع به فضای سایبر در دومین گزارش خود که ژوئن ۲۰۱۵ منتشرشد ضمن تأکید بر هنجارهای اختیاری و داوطلبانه رفتار مسئولانه دولت در فضای مجازی و تأثیر آن بر کاهش مخاطرات مربوط به ثبات، امنیت و صلح بین‌المللی به این نکته اشاره‌کردند که هنجارها به‌دنبال محدودساختن یا منع‌کردن کنش‌های دولتی غیرمتناقض با حقوق بین‌الملل نیست. این گزارش از جنبه هنجاری توصیه می‌کند که یک دولت نباید کنش‌های سایبری متناقض با تعهدات خود تحت حقوق بین‌الملل که عامدانه به زیرساخت‌های حیاتی آسیب می‌رساند یا به‌گونه‌ای استفاده و بهره‌برداری از زیرساخت‌های

حیاتی برای ارائه خدمات عمومی را معیوب‌می‌سازد، انجام‌دهد یا آگاهانه پشتیبانی نماید (UNDL, 2015:7-8). با اینکه گزارش ۲۰۱۵ گروه متخصصان حکومتی سازمان ملل کاربردی‌ترین و شفاف‌ترین مجموعه اقدام‌ها و راهکارهایی بوده‌است که تا به‌امروز ازسوی نهادهای بین‌المللی تدوین و ارائه شده‌است، اما این راهکارها تنها جنبه توصیه‌آمیز دارند و پیاده‌سازی آنها به ظرفیت و تمایل دولت‌ها بستگی‌دارد (Meyer, 2020:353).

مسکو نقش برجسته‌ای در تدوین این گزارش و گنجاندن برخی توصیه‌های هنجاری در آن داشت و امیدوار بود که محتوای این گزارش شالوده‌ای برای شناسایی بین‌المللی قواعد رفتاری دولت‌ها در فضای سایبر فراهم‌آورد. از این رو، دیپلمات‌های روسی تلاش‌کردند این پیشنهادها را در گزارش سال ۲۰۱۷ گروه متخصصان حکومتی سازمان ملل راجع به فضای سایبر به‌سمت تنظیم یه کنوانسیون جهانی جهت‌دهند. اما همان‌گونه که پیشتر نیز گفته‌شد، حضور دونالد ترامپ در کاخ سفید برخلاف برخی پیش‌بینی‌های اولیه با تنش‌های بی‌سابقه میان واشنگتن و مسکو همراه‌شد و سپهر سایبر یکی از محورها و حتی به‌نوعی یکی از دلایل این تنش به‌شمارمی‌آید.

روسیه در کنار دیپلماسی سایبری چندجانبه در چارچوب سازمان ملل از همکاری دوجانبه با دیگر دولت‌ها برای ارتقای امنیت سایبری نیز استقبال می‌کند و از ظرفیت‌های نهادهای منطقه‌ای در ترویج حکمرانی جهانی فضای مجازی غافل‌نیست. روسیه به‌همراه سه عضو دیگر سازمان همکاری شانگهای[1] شامل چین، تاجیکستان و ازبکستان در سپتامبر ۲۰۱۱ پیش‌نویس نظام‌نامه بین‌المللی مدیریت امنیت اطلاعات[2] را به سازمان ملل پیشنهاد داد که در شصت‌وششمین جلسه مجمع عمومی این سازمان به‌مثابه سندی رسمی برای رسیدن به اجماع بر سر هنجارهای بین‌المللی در سپهر سایبری پذیرفته‌شد. روسیه در همان ماه پیش‌نویس کنوانسیون بین‌المللی امنیت اطلاعات[3] را نیز در اختیار سازمان ملل قرارداد (Christou, 2016:59). هر دو سند بازتاب‌دهنده توسعه تفکر سیاست خارجی روسیه در ارتباط با قلمروی سایبر هستند.

---

[1]. Shanghai Cooperation Organisation (SCO)
[2]. International Code of Conduct for Information Security
[3]. Convention on International Information Security

کشورهای غربی در آن مقطع زمانی برای اشاره به چالش‌های امنیتی فضای مجازی تنها از واژه "امنیت سایبری" استفاده می‌کردند که نیاز به حمایت نرم‌افزاری و سخت‌افزاری و همچنین محافظت از اطلاعات کاربران دربرابر بازیگران مخرب را گوشزدمی‌کند، اما روسیه درحال ترویج واژه "امنیت اطلاعات بین‌المللی"[1] بود. این مفهوم نه‌تنها امنیت سایبری را دربرمی‌گیرد، بلکه بر جلوگیری از سوءاستفاده از فناوری‌های اطلاعات و ارتباطات برای اهداف سیاسی و نظامی نیز تمرکزدارد. هم پیش‌نویس نظام‌نامه بین‌المللی مدیریت امنیت اطلاعات و هم پیش‌نویس کنوانسیون بین‌المللی امنیت اطلاعات که توسط روسیه تألیف شده‌است بر اهمیت حق‌حاکمیت دولت بر فضای سایبر تأکیددارند. پیش‌نویس کنوانسیون همچنین از دولت‌ها می‌خواهد که جنگ اطلاعاتی را به‌مثابه جنایت علیه صلح و امنیت بین‌الملل به‌رسمیت بشناسند و از به‌کارگیری فناوری‌های اطلاعات و ارتباط برای مداخله در امور داخلی دیگر دولت‌ها پرهیزکنند (MFA, 2011). برخی از تهدیدهای سایبری اصلی ذکرشده در این سند شامل کنش‌هایی با هدف تضعیف سیستم سیاسی، اقتصادی و اجتماعی یک دولت و راه‌انداختن کارزارهای روان‌شناختی علیه جمعیت یک کشور با هدف بی‌ثبات‌سازی جامعه می‌شود. همچنین چگونگی پیش‌گیری از مناقشه‌ها و جرایم سایبری و نیز سوءاستفاده شبکه‌های تروریستی از فضای مجازی در این سند به‌تفصیل مورد بحث قرار گرفته‌است، اما دلیل اصلی روسیه برای تهیه این پیش‌نویس را باید در تلاش‌های دیپلماتیک این کشور برای ترویج هنجار عدم مداخله در امور داخلی دولت‌ها در سپهر سایبر جستجو کرد (Chernenko, 2018:46).

تلاش‌های دیپلماتیک روسیه همچنین به پشتیبانی اعضای سازمان پیمان امنیت دسته‌جمعی[2] از ابتکارهای مسکو در رابطه با ارتقای حکمرانی جهانی فضای مجازی و حق‌حاکمیت دولت‌ها بر فضای مجازی منجرشد. اعضای سازمان پیمان امنیت دسته‌جمعی در نشست سال ۲۰۱۴ ضمن محکوم‌کردن جنگ اطلاعاتی حریفان غربی علیه کشورهای پساکمونیستی بر لزوم مشارکت با یکدیگر برای مقابله با تهدیدهای سایبری غرب تأکید کردند (De Haas, 2016:399). دیپلماسی سایبری روسیه در قبال گروه بریکس نیز کاملا موفقیت‌آمیزبود و اعضای این گروه در سال ۲۰۱۵ با پیشنهاد روسیه مبنی بر تشکیل گروه

---

[1]. International Information Security
[2]. Collective Security Treaty Organization (CSTO)

کاری بریکس راجع به امنیت استفاده از فناوری‌های اطلاعات و ارتباطات[1] موافقت کردند (BRICS, 2015:71). مسکو همچنین در ژوئن ۲۰۱۳ نخستین توافق‌نامه سایبری دوجانبه را با هدف ایجاد اطمینان و تقویت اعتماد با واشنگتن به امضارساند که بر جنبه‌های فنی همکاری تمرکزداشت (Libicki, 2019:42). روسیه امیدواربود که این توافق‌نامه گامی اولیه در مسیر رسیدن به یک پیمان بسیار گسترده‌تر با ایالات متحده برای اجتناب از درگیری سایبری میان دو کشور باشد (Chernenko, 2018:47)، اما رویدادهای متعاقب به‌ویژه بحران ۲۰۱۴ اوکراین و افشاسازی‌های ادوارد اسنودن[2] -پیمان‌کار سابق آژانس امنیت ملی ایالات متحده[3]- درخصوص جاسوسی ایالات متحده از شهروندان و مقام‌های رسمی دولت‌های گوناگون مانع از تحقق آن شد.

اهداف دیپلماسی سایبری روسیه

به‌طور خلاصه، دیپلماسی سایبری روسیه دو انگیزه اصلی را دنبال‌می‌کند که انگیزه نخست به‌طور مستقیم به سپهر سایبر بازنمی‌گردد. در وهله نخست، مسکو انتظاردارد که تلاش‌های دیپلماتیک روسیه به‌مثابه یک بازیگر پیشرو در سپهر سایبر بر پرستیژ و احترام این کشور نه‌تنها در منطقه، بلکه به‌طور بالقوه در سطح جهانی بیافزاید. در حقیقت این همان موقعیتی است که روسیه با فروپاشی اتحاد جماهیر شوروی در ابتدای دهه ۹۰ میلادی از دست‌داد و مشتاقانه خواهان بازپس‌گیری آن است (Kurowska, 2019:4). با این همه، تلاش‌های دیپلماتیک روسیه در سپهر سایبر، اگرچه بر ظرفیت این کشور برای تأثیرگذاری بر نظم جهانی لیبرال می‌افزاید، اما تبدیل این آرزو به تثبیت نقش روسیه در مدیریت جهانی به‌سادگی ممکن‌نیست. تحقق این هدف، پیامدهای حائزاهمیتی برای نظم بین‌الملل به‌همراه خواهدداشت و بنابراین رویکرد کشورهای غربی در قبال دیپلماسی سایبری روسیه احتمالا بسیار پایین‌تر از انتظارات مسکو برای رفتاری است که احساس‌می‌کند شایسته آن است.

انگیزه دوم مسکو از تعقیب دیپلماسی سایبری به‌طورمستقیم سپهر سایبر را هدف قرار داده‌است و ایجاد شرایط برای ترویج جهانی ابتکارعمل روسیه در جهت تدوین و پذیرش

---

1. BRICS Working Group on Security in the Use of ICTs
2. Edward Snowden
3. US National Security Agency

کنوانسیون امنیت اطلاعات بین‌المللی ازسوی دولت‌های عضو سازمان ملل را دنبال‌می‌کند. تدوین قانون خاص[1] برای قلمروی سایبر ممکن‌است هنوز به معنای واقعی کلمه واقع‌بینانه نباشد، اما روسیه در تلاش است تا زمینه را برای آن فراهم‌سازد (Kurowska, 2019:4). دیپلماسی سایبری روسیه به‌دنبال ایجاد انسجام میان دولت‌های هم‌فکری است که به وضعیت کنونی حکمرانی فضای مجازی اعتراض‌دارند و قوانین موجود در سپهر سایبر را ناعادلانه می‌پندارند. تلاش‌های دیپلماتیک روسیه در این مسیر به تدوین پیمان‌های سایبری بین‌المللی معطوف‌است که به‌طور خاص برای این سپهر وضع شده‌باشند نه اینکه در اصل برای قلمروی واقعی تهیه‌شده و سپس به فضای سایبر امتداد یافته‌باشند.

پیمان‌های سایبری بین‌المللی از دیدگاه مسکو همچنین به‌مثابه ابزاری برای مهار نظم بین‌المللی لیبرال تلقی می‌شوند زیرا طبق درک روسیه و دولت‌های همفکر قراراست تحت اصول عدم مداخله در امور داخلی دیگر دولت‌ها و احترام به حق‌حاکمیت آنها تدوین شوند (Moynihan, 2019:2-9). مسکو به‌خوبی از چگونگی شکل‌گیری هنجارهای بین‌المللی برپایه رویه قدرت‌های بزرگ آگاه‌است و با تلاش‌های دیپلماتیک خود قصددارد که اجازه‌ندهد نظم بین‌المللی سایبری نیز همچون بسیاری دیگر از اجزای نظم بین‌المللی لیبرال به‌صورت قاعده‌محور حول عملکردها و خواسته‌های ایالات متحده و دیگر دولت‌های غربی تنظیم شود.

از این چشم‌انداز، نظم قانون‌محور بین‌المللی[2] به‌ویژه از این جنبه حائزاهمیت است که به‌جای پیروی از نظم بین‌المللی قاعده‌محور[3] به‌مثابه جایگزین آن فهم می‌شود (Kurowska, 2019:5). ایده نظم بین‌المللی قاعده‌محور در سپهر سایبر ازسوی دیپلماسی روسیه به‌مثابه تلاشی برای غصب‌کردن فرآیند تصمیم‌گیری جمعی در مورد مسایل کلیدی ازطریق جایگزین‌ساختن سازوکارها و ابزارهای قانونی بین‌المللی موردتوافق در سطح جهانی با اشکال محدود قاعده‌سازی -همچون آیکان- به‌شدت مورد حمله قرار گرفته‌است. دیپلماسی سایبری روسیه بر اجماع یا دست‌کم کسب موافقت حداکثری دولت‌ها برای ایجاد قوانین سایبری بین‌المللی اصراردارد و قواعد کنونی حاکم بر فضای مجازی را آغشته به خواسته‌ها و گرایش‌های سیاسی ایالات متحده و دیگر دولت‌های غربی می‌داند.

---

1. Lex Specialis
2. International Law-based Order
3. Rules-based International Order

در هر صورت، دفاع روسیه از پیمان سایبری بین‌المللی به‌جز عرصه سیاسی به‌لحاظ فنی و حقوقی نیز با چالش‌هایی مواجه‌است. حقوق بین‌الملل در فضای سایبر قابل‌اعمال است، اما حتی کارشناسان حقوقی نیز به‌دلیل پیچیدگی‌های فنی سپهر سایبر از چگونگی آن مطمئن‌نیستند. به‌عنوان نمونه، معنای عبارت "رفتار مسئولانه دولت در فضای سایبر"[1] در تفسیر روسیه شفاف‌نیست. همچنین به‌نظرمی‌رسد که حقوق دادرسی بین‌المللی به‌مثابه مجموعه اصول و هنجارهای حاکم بر اعمال حقوق و تعهدات تابعان حقوق بین‌الملل با مقررات روابط بین‌الملل در زمینه فناوری اطلاعات و ارتباطات از بسیاری جهات سازگاری‌ندارد.

علاوه بر این، استفاده از عرف بین‌المللی و اصول کلی حقوقی در سپهر سایبر با توجه به فقدان درک مشترک از برخی مفاد مقررات حقوقی مانند استفاده از برخی فناوری‌های اطلاعات و ارتباطات به‌مثابه ابزار جنگی غیرقابل اطمینان است. در نهایت اینکه به‌رغم ادعای بی‌طرفی و بی‌غرضی حقوق بین‌الملل، قوانین بین‌المللی بیش از نقد و محدودسازی قدرت سیاسی در خدمت رشد آن بوده‌اند و بنابراین ابتکارعمل روسیه برای ایجاد شرایط منجر به مذاکره در مورد پیمان سایبری بین‌المللی باید روند نقد و احتمالا محدودساختن قدرت دولت‌های لیبرال غربی و مهمتر از همه ایالات متحده را در دستورکار خود داشته‌باشد.

با وجود چالش‌هایی از این دست، مسکو به احتمال زیاد اهداف سایبری خود را در سطح بین‌المللی در چارچوب سازمان ملل و در سطح منطقه‌ای ازطریق نهادهایی همچون سازمان همکاری شانگهای، سازمان پیمان امنیت دسته‌جمعی و گروه بریکس و نیز برهم‌کنش‌های دوجانبه با دولت‌های همفکر ادامه خواهدداد. علاوه بر این، دیپلماسی سایبری روسیه از جلب نظر دولت‌های غیرهمفکر به‌منظور دستیابی به اجماع جهانی یا حداکثری بر سر تدوین قوانین سایبری بین‌المللی نیز غافل نبوده‌است.

از آنجاکه مسکو بیشترین تهدید سایبری را از جانب واشنگتن احساس‌می‌کند، عادی‌سازی مناسبات سایبری با ایالات متحده یکی از اهداف رهبران روسیه به‌ویژه پوتین در سپهر فناوری اطلاعات و ارتباطات به‌شمارمی‌آید. به‌همین جهت حتی پس از منتفی‌شدن توافق‌نامه ژوئن ۲۰۱۳، مسکو در سال ۲۰۱۷ به سبک "موافقت‌نامه حوادث دریایی ایالات

[1]. Responsible State Behaviour in Cyberspace

متحده-شوروی"[1] در سال ۱۹۷۲ به واشنگتن پیشنهاد امضای پیمان دوجانبه پیش‌گیری از فعالیت‌های نظامی خطرناک در فضای سایبر را داد. پاسخ ایالات متحده به این پیشنهاد تاکنون با سردرگمی همراه بوده‌است. واشنگتن در ابتدا موافقت خود را برای رایزنی در این‌باره اعلام‌داشت و شروع دور نخست مذاکرات برای پایان فوریه ۲۰۱۸ در ژنو تعیین‌شد، اما کاخ سفید به‌ناگاه تنها یک روز پیش از موعد ملاقات آن‌را به‌تعویق انداخت (Chernenko, 2018:47-48). یکی از دلایل این موضع تردیدآمیز را می‌توان به جریان‌داشتن تحقیقات مربوط به مداخله احتمالی روسیه در انتخابات ریاست‌جمهوری ۲۰۱۶ ایالات متحده در این کشور نسبت‌داد.

روسیه هم‌زمان با تقویت مناسبات دوجانبه با دولت‌های همفکر و تلاش برای دستیابی به پیمان منع متقابل توسل به جنگ سایبری با ایالات متحده مشتاق به پی‌گیری رایزنی‌ها برای انعقاد موافقت‌نامه‌های دوجانبه احتمالی در فضای سایبر با آلمان، فرانسه، ژاپن و کره جنوبی نیز بوده‌است. دولت‌هایی که مسکو در گام نخست خواهان رسیدن به تفاهم دوجانبه با آنها در سپهر سایبر است طی یک سند داخلی شورای امنیت فدراسیون روسیه مشخص‌شده‌اند که همگی نیز عضو سازمان همکاری و توسعه اقتصادی[2] (متعهد به اصول دموکراسی و اقتصاد آزاد) به‌شمارمی‌آیند، اما تا به امروز هیچ مذاکره‌ای در این‌خصوص صورت نپذیرفته‌است. تنها اینکه به‌جز واشنگتن، برلین نیز نشست برنامه‌ریزی‌شده مارس ۲۰۱۸ برای رایزنی و رسیدن به تفاهم سایبری با مسکو را با ادعای دخالت کرملین در یک حمله سایبری علیه وزارت امور خارجه آلمان به‌رغم انکار مقام‌های رسمی روسیه لغو کرده‌بود (Achten, 2018). تلاش‌های دیپلماتیک روسیه برای امضای موافقت‌نامه‌های سایبری با کشورهای عضو سازمان همکاری و توسعه اقتصادی، اگرچه تا به امروز به‌ثمر ننشسته‌است، اما دست‌کم ماهیت بازدارنده اقدام‌های سایبری روسیه را برجسته‌می‌سازد.

سیستم بازدارندگی راهبردی روسیه یک سازوکار پدافندی است که برای فعالیت مداوم در زمان صلح طراحی شده‌است. این مفهوم در راهبرد امنیت ملی روسیه[3] که در سال ۲۰۰۹ منتشرشد تحت عنوان "ایجاد و پیاده‌سازی یک سیستم پیچیده به‌هم‌پیوسته از

---

[1]. U.S.–Soviet Incidents at Sea Agreement
[2]. Organisation for Economic Co-operation and Development (OECD)
[3]. Russian National Security Strategy (NSS)

اقدام‌های سیاسی، نظامی، اقتصادی، اطلاع‌رسانی و دیگر تدابیر با هدف پیش‌گیری یا کاهش تهدید اقدام‌های ویران‌گر ازجانب یک دولت یا ائتلافی از دولت‌های مهاجم" تعریف شده است (ПР, 2009). بنابراین، ایده بازدارندگی راهبردی روسیه مجموعه‌ای از ترفندها (از جمله جنگ سایبری) را دربرمی‌گیرد که باهم عمل‌می‌کنند و می‌توانند ذیل عنوان جنگ ترکیبی[1] مورد بررسی قرارگیرند، هرچند روس‌ها عبارت "جنگ از نوع جدید"[2] را ترجیح‌می‌دهند (Thornton and Miron, 2019:258).

روسیه با تکیه بر مؤلفه‌های جنگ ترکیبی توانسته‌است بدون توسل به جنگ آشکار به بخشی از اهداف راهبردی خود در برابر قدرت‌های غربی دست‌یابد. با این همه، راهبرد بازدارندگی سایبری روسیه را باید در کنار تلاش‌های دیپلماتیک این کشور برای دست‌یابی به تفاهم سایبری با دولت‌های غربی مورد ملاحظه قرارداد. در حقیقت، بازدارندگی و حتی جنگ سایبری روسیه مکمل دیپلماسی سایبری این کشور است که به‌طور عمده در شرایط فقدان اثربخشی کوشش‌های دیپلماتیک مسکو مورد استفاده قرارمی‌گیرند.

مسکو به‌خوبی از برتری نیروهای نظامی متعارف ناتو نسبت به روسیه آگاه‌است و بنابراین از جنگاوری جنبشی[3] (جنگ سنتی) در برابر قدرت‌های غربی پرهیزدارد. در مقابل، ارتش روسیه رویکرد غیرمستقیم[4] را علیه اعضای ناتو به‌کار گرفته‌است که جنگ سایبری و بازدارندگی سایبری بخش مهمی از آن‌را تشکیل‌می‌دهد. در این میان، یکی از کارویژه فرعی دیپلماسی سایبری روسیه، متقاعدساختن دولت‌های غربی برای انعقاد توافق‌نامه‌های سایبری با مسکو به‌منظور پرهیز از به‌کارگیری متقابل سلاح سایبری علیه یکدیگر است.

به‌عبارت بهتر، روسیه در سپهر سایبر برپایه این توصیه پیش‌می‌رود که اگر نمی‌توان با پدیده‌ای مقابله کرد، پس بهتر است با آن همراه‌شد و از آن استفاده‌کرد. از این چشم‌انداز، به‌کارگیری سلاح سایبری روسیه در برابر قدرت‌های غربی تنها در صورتی متوقف خواهدشد که دولت‌های غربی ضمن پاسخ به تلاش‌های دیپلماتیک روسیه در سپهر سایبر و انعقاد موافقت‌نامه‌های سایبری دوجانبه یا یک پیمان سایبری بین‌المللی به مداخله در امور داخلی این کشور پایان‌دهند.

---

1. Hybrid Warfare
2. New-type Warfare
3. Kinetic Warfare
4. Indirect Approach

نتیجه‌گیری

دیپلماسی سایبری روسیه تا به امروز سه مرحله از توسعه را پشت سر گذاشته‌است. آغاز این پدیده را می‌توان به اواخر دهه ۹۰ میلادی ارجاع داد، هنگامی‌که مسکو سعی‌کرد با ارائه پیش‌نویس "قطعنامه تحولات در حوزه اطلاعات و ارتباطات در زمینه امنیت بین‌الملل" به مجمع عمومی سازمان ملل، تصویری مثبت از روسیه به‌مثابه بخشی مهم از سیستم جامعه جهانی به‌نمایش‌بگذارد. هدف دیپلماسی سایبری روسیه در آن زمان به جلوگیری از نظامی‌سازی فضای سایبر معطوف‌بود. با توسعه ابعاد جنگ سایبری و اطلاعات، تلاش‌های دیپلماتیک روسیه در سپهر سایبر نیز از ابتدای دهه دوم سده بیست‌ویکم به مرحله متقاعدسازی دولت‌ها برای پذیرش برخی انواع قواعد حاکم بر رفتار دولت‌ها در فضای سایبر واردشد. سومین مرحله از توسعه دیپلماسی سایبری روسیه نیز به تلاش مسکو برای انعقاد موافقت‌نامه‌های دوجانبه با برخی دولت‌های عضو سازمان همکاری و توسعه اقتصادی با هدف منع متقابل توسل به جنگ در سپهر سایبر بازمی‌گردد.

تدقیق در تاریخچه تلاش‌های دیپلماتیک روسیه در سپهر سایبر نشان‌می‌دهد که دیپلماسی سایبری نزد رهبران روسیه به‌مثابه روشی برای تجدید قدرت پیشین و اعاده نقش جهانی مسکو تلقی‌می‌شود. علاوه بر این، روسیه از دیپلماسی سایبری به‌منظور غلبه بر تهدیدهای امنیتی ذاتی فضای سایبر نیز بهره‌می‌برد. در واقع، هرچند حمایت از منابع اطلاعاتی یکی از اولویت‌های اصلی امنیت ملی دولت‌ها از جمله فدراسیون روسیه به‌شمارمی‌آید، اما ماهیت فرامرزی فضای مجازی به‌گونه‌ای است که غلبه بر تهدیدهای فضای سایبر تنها توسط نهادهای داخلی یک دولت ممکن‌نیست.

توانایی دولت‌های منفرد برای کنترل تولید و مصرف اطلاعات در سپهر سایبر بسیار محدوداست. بنابراین، لزوم استقرار یک زیرساخت اطلاعاتی جهانی پایا و قابل‌اعتماد انکارناپذیراست. همچنین بدیهی است که هنجارهای بین‌المللی قانونی امنیت سایبری باید پیامد تلاش‌های چندملیتی و چندذینفعی باشند تا ازسوی جامعه جهانی مورد پذیرش قرارگیرند. کما اینکه منافع دولت‌ها و بازیگران گوناگون (از جمله افراد غیردولتی) نیز باید در آن مورد توجه قرارگیرد.

مذاکرات مربوط به تدوین یک پیمان سایبری بین‌المللی از ابتدای سده بیست‌ویکم در سازمان ملل شکل‌گرفت که فدراسیون روسیه و ایالات متحده به‌تدریج دو موضع متفاوت و

تقریبا ناسازگار را در قبال آن اتخاذکردند. ایالات متحده به‌مثابه خاستگاه فضای مجازی و محل استقرار آیکان مدافع وضع موجود است و حق‌حاکمیت ملی دولت‌ها بر فضای سایبر را به‌لحاظ فنی ممکن و به‌لحاظ سیاسی پسندیده نمی‌داند. شرایط کنونی را می‌توان معادل سلطه سرزمینی و حقوقی واشنگتن بر حکمرانی فضای مجازی دانست، زیرا آیکان که امروزه به حاکم بلامنازع مقولات فنی فضای مجازی -و به‌عبارتی کلید فضای سایبر- تبدیل شده‌است در حوزه صلاحیت قضایی ایالت کالیفرنیا و دولت ایالات متحده قراردارد. وضعیت موجود اگرچه مطلوب اروپا نیست، اما از آنجاکه دولت‌های اروپایی جایگزین بهتری برای آن سراغ‌ندارند با آن کنارآمده‌اند.

در مقابل، روسیه نیز همچون بسیاری از قدرت‌های نوظهور و درحال توسعه جهان آشکارا مخالفت خود را با وضعیت کنونی حکمرانی فضای مجازی ابراز داشته‌است و بر ویژگی چندذینفعی حکمرانی فضای مجازی تأکیددارد. تحت اکوسیستم حکمرانی فضای مجازی چندذینفعی، هیچ نهاد، ذینفع یا کنش‌گری به‌تنهایی دارای نقش منحصربه‌فرد فنی یا حقوقی در مدیریت فضای سایبر نیست، بلکه حکمرانی فضای مجازی به‌صورت جهانی و به‌شیوه مشارکتی صورت‌می‌پذیرد.

هدف غایی تلاش‌های دیپلماتیک روسیه در فضای سایبر را تبدیل "حکمرانی فضای مجازی تحت نفوذ ایالات متحده" به "حکمرانی جهانی فضای مجازی" تشکیل‌می‌دهد. برای این منظور، روسیه ابتکارهای متعددی را همچون ارائه پیش‌نویس‌های "قطعنامه تحولات در حوزه اطلاعات و ارتباطات در زمینه امنیت بین‌الملل"، "نظام‌نامه بین‌المللی مدیریت امنیت اطلاعات" و "کنوانسیون بین‌المللی امنیت اطلاعات" و مشارکت با اعضای سازمان پیمان امنیت دسته‌جمعی در ترویج حکمرانی جهانی فضای مجازی و تشکیل "گروه کاری بریکس راجع به امنیت استفاده از فناوری‌های اطلاعات و ارتباطات" را درپیش گرفته‌است. علاوه بر این، مسکو نقش برجسته‌ای در مدیریت "گروه متخصصان حکومتی سازمان ملل راجع به فضای سایبر" و تدوین گزارش‌های این گروه و گنجاندن برخی توصیه‌های هنجاری در آنها با هدف شناسایی بین‌المللی قواعد رفتاری دولت‌ها در فضای سایبر داشته‌است.

اولویت تلاش‌های دیپلماتیک مسکو در سپهر سایبر طی هر یک از مراحل سه‌گانه توسعه دیپلماسی سایبری این کشور متفاوت بوده‌است. در آخرین مرحله از این توسعه، اولویت دیپلمات‌های روسیه به متقاعدسازی اعضای قدرت‌مند سازمان همکاری و توسعه

اقتصادی برای انعقاد موافقت‌نامه‌های دوجانبه با این کشور در فضای سایبر معطوف بوده‌است. در حقیقت، از آنجاکه رسیدن به یک پیمان سایبری بین‌المللی فراگیر زمان‌بر خواهدبود، کوشش‌های دیپلماتیک روسیه به‌سمت تنظیم توافق‌نامه‌های دوجانبه با دولت‌های غربی با هدف منع متقابل استفاده نظامی از فناوری‌های اطلاعات و ارتباطات علیه یکدیگر تمایل پیدا کرده‌است.

انگیزه‌های دیپلماسی سایبری مسکو علاوه بر ارتقای پرستیژ روسیه به‌مثابه کشوری پیشرو در عرصه مدیریت جهانی به فراهم‌سازی زمینه‌های تدوین قوانین خاص برای سپهر سایبر به‌ویژه ایجاد و پذیرش کنوانسیون امنیت اطلاعات بین‌المللی ازسوی دولت‌های عضو سازمان ملل بازمی‌گردد. در واقع، انگیزه تلاش‌های دیپلماتیک روسیه را ترویج جهانی ابتکارعمل این کشور با هدف جایگزین‌ساختن نظم قانون‌محور بین‌المللی با نظم بین‌المللی قاعده‌محور در سپهر سایبر تشکیل‌می‌دهد. قواعد کنونی حاکم بر فضای مجازی از چشم‌انداز روسیه آغشته به خواسته‌ها و گرایش‌های سیاسی ایالات متحده و دیگر دولت‌های غربی است و بنابراین، دیپلماسی سایبری روسیه بر اجماع یا دست‌کم کسب موافقت حداکثری دولت‌ها برای ایجاد قوانین سایبری بین‌المللی اصراردارد.

در نهایت، برپایه یافته‌های مقاله می‌توان، ریشه دیپلماسی سایبری روسیه را به فهم این کشور از قلمروی سایبر به‌مثابه ابزار جدید سلطه غرب نسبت داد. هدف غایی مسکو از تلاش‌های دیپلماتیک در سپهر سایبر را نیز رفع تصدی‌گری نهادهای بین‌المللی تحت‌نفوذ واشنگتن، بروکسل و ناتو بر فضای سایبر (به‌ویژه آیکان) با ایجاد حکمرانی جهانی فضای مجازی تشکیل‌می‌دهد. با این توصیف، فرضیه آغازین مقاله را می‌توان صادق دانست.

منابع و مآخذ

- جعفری، افشین (۱۳۹۸)، «حاکمیت بر فضای سایبر از منظر حقوق بین‌الملل و نظام حقوقی جمهوری اسلامی ایران»، فصلنامه *رهیافت انقلاب اسلامی*، ۱۳(۴۹)، ۱۰۹-۱۳۲.

- سلطانی، نصراله (۱۳۹۶)، «راهبردهای بین‌المللی روسیه در حوزه امنیت اطلاعات»، فصلنامه *مطالعات سیاست خارجی تهران*، ۲(۴)، ۱۸۷-۲۰۹.

- ضیایی، سیدیاسر و شکیب‌نژاد، احسان (۱۳۹۶)، «قانونگذاری در فضای سایبر: رویکرد حقوق بین‌الملل و حقوق ایران»، مجله *حقوقی بین‌المللی*، ۳۴(۵۷)، ۲۲۷ -۲۴۹.

- قادری حاجت، مصطفی و نصرتی، حمیدرضا (۱۳۹۲)، «فضای سایبر؛ چالش‌های حاکمیت و امنیت پایدار»، پژوهشنامه *جغرافیای انتظامی*، ۱(۲)، ۹۳-۱۱۸.

- قوچانی خراسانی، محمدمهدی و حسین‌پور، داود (۱۳۹۶)، «حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری»، فصلنامه *فرایند مدیریت و توسعه*، ۳۰(۱)، ۵۱-۸۰.

- مکبری، سیدامیرحسین (۱۳۹۸)، «چهاردهمین نشست سالانه مجمع حکمرانی فضای مجازی سازمان ملل»، *مرکز ملی فضای مجازی*، گزارش شماره ۲۸، بهمن‌ماه، قابل دسترسی در:
http://csri.majazi.ir//parameters/majazi/modules/cdk/upload/content/elib/100/15821082075779dih4chaq4lv3d7u1sjdqmfb04.pdf
تاریخ دسترسی: ۱۹ اسفند ۱۳۹۸.

- یوسف‌نژاد، هلیا (۱۳۹۷)، «بررسی نقش آیکان در شبکه حکمرانی فضای مجازی»، *مرکز ملی فضای مجازی*، ۱۰ دی‌ماه، قابل دسترسی در:
http://www.majazi.ir/article/85397
تاریخ دسترسی: ۲۳ اسفند ۱۳۹۸.

- Achten, N. (2018), "Germany's Position on International Law in Cyberspace", *The Lawfare Institute*, October, Available at: https://www.lawfareblog.com/germanys-position-international-law-cyberspace, Accessed on: 12 March 2020.

- Ajir, M and Vailliant, B. (2018), "Russian Information Warfare: Implications for Deterrence Theory", *Strategic Studies Quarterly*, 12(3): 70-89.

- Andjelkovic, M. (2006), *Internet Governance: In the Footsteps of Global Administrative Law*, A Dissertation Submitted to the University of Kent Law School, September, Brussels, Available at: https://www.iisd.org/pdf/2006/infosoc_int_gov_law.pdf, Accessed on: 25 March 2020.

−Betz, D. J. and Stevens, T. (2011.), *Cyberspace and the State: Toward a Strategy for Cyber-Power*, Abingdon: Routledge, Available at: https://pdfs.semanticscholar.org/9dee/e3336e875b5d625664f79a4575fec9ba9fb5.pdf, Accessed on: 12 March 2020.
−Bozhkov, N. (2020), "China's Cyber Diplomacy: A Primer", *Digital Dialogue*, March, Available at: https://eucyberdirect.eu/wp-content/uploads/2020/03/bozhkov-digital-dialogue-final.pdf, Accessed on: 29 March 2020.
−*BRICS* (2015), "The BRICS Handover Report: 2015-2016", Available at: http://en.brics2015.ru/load/885248, Accessed on: 15 March 2020.
−Chernenko, E. (2018), "Russia's Cyber Diplomacy", in N. Popescu and S. Secrieru (Eds.), *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, Paris: EU Institute for Security Studies.
−Christou, G. (2016), *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, New York: Palgrave Macmillan.
−Cuihong, C. (2018), "China and Global Cyber Governance: Main Principles and Debates", *Asian Perspective*, 42(4): 647–662, doi: 10.1353/apr.2018.0029.
−de Haas, M. (2016), "War Games of the Shanghai Cooperation Organization and the Collective Security Treaty Organization: Drills on the Move!", *The Journal of Slavic Military Studies*, 29(3): 378-406, doi: 10.1080/13518046.2016.1200383.
−GIP (2020), "The UN Group of Governmental Experts (GGE)", *GIP Digital Watch*, Available at: https://dig.watch/processes/un-gge, Accessed on: 26 March 2020.
−Gwynn, M. A. (2019), "Structural Power and International Regimes", *Journal of Political Power*, 12(2): 200-223, doi: 10.1080/2158379X.2019.1618486.
−Hufty, M. (2011), "Investigating Policy Processes: The Governance Analytical Framework (GAF)", In U. M. Wiesmann and H. Hurni (Eds.), *Research for sustainable development 6* (pp. 403-424), Bern: Geographica Bernensia, doi: 10.7892/boris.68343
−Jonsson, O. (2019), *The Russian Understanding of War: Blurring the Lines between War and Peace*, Washington, DC : Georgetown University Press.
−Keohane, R. O. (2003), "Global Governance and Democratic Accountability", in D. Held and M. Koenig-Archibugi (Eds.), *Taming Globalization: Frontiers of Governance* (pp. 103-158), Cambridge: Polity Press.
−Krasner, S. D. (2001), "Abiding Sovereignty", *International Political Science Review*, 22(3): 229-251, doi: 10.1177/0192512101223002.
−Krisch, N. and Kingsbury, B. (2006), "Introduction: Global Governance and Global Administrative Law in the International Legal Order", *European Journal of International Law*, 17(1): 1–13, doi: 10.1093/ejil/chi170.

−Kurbalija, J. (2016), *An Introduction to Internet Governance*, Malta: Diplo Foundation.
−Kurowska, X. (2019), "What Does Russia Want in Cyber Diplomacy? A Primer", *EU Cyber Direct*, December, Available at: https://eucyberdirect.eu/wp-content/uploads/2019/12/13-kurowska_rif-final.pdf, Accessed on: 26 March 2020.
−Libicki, M. C. (2019), "Norms and Normalization", In C. J. Connolly (Ed.), *The Cyber Defense Review* (pp. 41-52), New York: Army Cyber Institute.
−Meyer, P. (2020), "Norms of Responsible State Behaviour in Cyberspace", in M. Christen, B. Gordijn and M. Loi (Eds.), *The Ethics of Cybersecurity* (pp. 347-360), Cham: Springer, doi: 10.1007/978-3-030-29053-5_18.
−MFA (2011), "Convention on International Information Security", *The Ministry of Foreign Affairs of the Russian Federation*, 22 September, Available at: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666, Accessed on: 27 March 2020.
−Moynihan, H. (2019), "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention", *International Law Programme*, December, Available at: https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf, Accessed on: 27 March 2020.
−Radu, R. (2019), *Negotiating Internet Governance*, New York: Oxford University Press.
−Rojszczak, M. (2020), "Does Global Scope Guarantee Effectiveness? Searching for a New Legal Standard For Privacy Protection in Cyberspace", *Information & Communications Technology Law*, 29(1): 22-44, doi: 10.1080/13600834.2020.1705033.
−Rosenau, J. N. (1992), "Governance, Order, and Change in World Politics", In , J. N. Rosenau and E-O Czempiel (Eds.), *Governance Without Government: Order and Change in World Politics* (pp. 1-29), Cambridge: CUP, doi: 10.1017/cbo9780511521775.003.
−Ruhl, C., Hollis, D., Wyatt Hoffman, W. and Maurer, T. (2020), "Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads", *Carnegie Endowment for International Peace*, February, Available at: https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf, Accessed on: 29 March 2020.
−Satola, D. (2007), "Legal Aspects of Internet Governance Reform", *Information Polity*, 12(1-2): 49-62, doi: 10.3233/ip-2007-0109.

−Thornton, R. and Miron, M. (2019), "Deterring Russian Cyber Warfare: Thepractical, Legal and Ethical Constraints Faced by the United Kingdom", *Journal of Cyber Policy*, 4(2): 257-274, doi: 10.1080/23738871.2019.1640757
−UN (1998), "Resolution Adopted by the General Assembly: Developments in the Field of Information and Telecommunications in the Context of International Security", *United Nations*, 4 January 1999, Available at: https://undocs.org/pdf?symbol=en/a/res/53/70, Accessed on: 1 April 2020.
−UN (1999), "Resolution Adopted by the General Assembly: Developments in the Field of Information and Telecommunications in the Context of International Security", *United Nations*, 23 December, Available at: https://undocs.org/pdf?symbol=en/a/res/54/49, Accessed on: 1 April 2020.
−UN (2019), "Seventy-fourth Session", *United Nations*, 12 December, Available at: https://undocs.org/en/A/74/PV.46, Accessed on: 2 April 2020.
−UNDL (2013), "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", *United Nations Digital Library*, 24 June, Available at: https://digitallibrary.un.org/record/753055, Accessed on: 27 March 2020.
−UNDL (2015), "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", *United Nations Digital Library*, 22 July, Available at: https://digitallibrary.un.org/record/799853, Accessed on: 27 March 2020.
−UNODA (2005), "Item 86: Developments in the Field of Information and Telecommunications in the Context of International Security", *United Nations Office for Disarmament Affairs*, Available at: https://gafc-vote.un.org/UNODA/vote.nsf/91a5e1195dc97a630525656f005b8adf/c76a01775 9286486852570a1004a46b7?OpenDocument, Accessed on: 25 March 2020.
−UNODA (2016), "Item 93: Developments in the Field of Information and Telecommunications in the Context of International Security", *United Nations Office for Disarmament Affairs*, Available at: https://gafc-vote.un.org/UNODA/vote.nsf/91a5e1195dc97a630525656f005b8adf/05a1a2097 e5191708525808f0070c6f6?OpenDocument, Accessed on: 2 Ap25 March 2020.
−Von Heinegg, W. H. (2019), "International Law and International Information Security: A Response to Krutskikh and Streltsov", *The Tallinn Papers*, No. 9, Available at: https://ccdcoe.org/uploads/2018/10/TP_09_2015.pdf, Accessed on: 26 March 2020.
−Weinberg, J. (2000), "ICANN and the Problem of Legitimacy", Duke Law Journal, 50(1): 187-260, doi: 10.2307/1373114
−Zeng, J., Stevens, T. and Chen, Y. (2017), "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'", *Politics & Policy*, 45(3): 432-464, doi: 10.1111/polp.12202.

−ДИТ (2000), "Доктрина Информационной Безопасности Российской Федерации", *Департамент Информационных Технологий и Твязи Тамарской Тбласти*, 9 Сентября, Можно Купить в: https://dit.samregion.ru/external/dit/docs/prikaz_prezidenta_rf_ot_09_sentyabrya_2000_pr-1895_doktrina_informatsionnoj_bezopasnosti_rossijskoj_.pdf, Дата доступа: 24 Март 2020 г.

−ПР (2009), "Стратегия национальной безопасности Российской Федерации до 2020 года", *Президент России*, 13 Мая, Можно Купить в: http://kremlin.ru/supplement/424, Дата доступа: 28 март 2020 г.

−ПР (2016), "Об утверждении Доктрины информационной безопасности Российской Федерации", *Президент России*, 5 Ддекабря, Можно купить в: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf, Дата Доступа: 24 Март 2020 г.

−СБРФ (2013), "Основы Государственной Политики Российской Федерации в Области Международной Информационной Безопасности на Период до 2020 года", *Совет Безопасности Российской Федерации*, 24 июля, Можно Купить в: http://www.scrf.gov.ru/security/information/document114, Дата доступа: 27 Март 2020 г.