حکمرانی در عرصه پنجم

CYBERSPACE

گذار به دیپلماسی سایبری

عباس قنبری باغستان
عبدالحسین گلاندخری

حکمرانی در عرصهٔ پنجم: گذار به دیپلماسی سایبری

حکمرانی در عرصهٔ پنجم: گذار به دیپلماسی سایبری

عباس قنبری باغستان
عبدالحسین کلانتری

بهار ۱۴۰۰

سر شناسه	:	قنبری باغستان، عباس، ۱۳۵۷ -
عنوان و نام پدیدآور	:	حکمرانی در عرصه پنجم: گذار به دیپلماسی سایبری / نویسندگان عباس قنبری باغستان، عبدالحسین کلانتری
مشخصات نشر	:	تهران : پژوهشگاه فضای مجازی ، ۱۴۰۰
مشخصات ظاهری	:	۴۵۶ ص. : جدول. ؛ ۱۴×۲۱س م
شابک	:	۹۷۸-۶۲۲-۹۷۷۰۰-۶-۱
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	کتابنامه
یادداشت	:	نمایه.
موضوع	:	فضای مجازی — جنبه های سیاسی
موضوع	:	Cyberspace -- Political aspects
موضوع	:	فضای مجازی — تدابیر ایمنی — سیاست دولت
موضوع	:	Cyberspace -- Security measures -- Government policy
موضوع	:	همکاری های بین المللی -- تدابیر ایمنی-- فضای مجازی
موضوع	:	International cooperation --Cyberspace -- Security measures
شناسه افزوده	:	کلانتری، عبدالحسین، ۱۳۵۶ -
شناسه افزوده	:	پژوهشگاه فضای مجازی
رده بندی کنگره	:	HM۸۵۱
رده بندی دیویی	:	۳۰۳/۴۸۳۴
شماره کتابشناسی ملی	:	۷۶۶۹۴۲۶
اطلاعات رکود کتابشناسی	:	فیپا

حکمرانی در عرصهٔ پنجم: گذار به دیپلماسی سایبری

نویسندگان: عباس قنبری باغستان (عضو هیئت علمی دانشگاه تهران)

و عبدالحسین کلانتری (عضو هیئت علمی دانشگاه تهران)

ویراستاران: فخرالسادات حیدری و راهله میلانی

صفحه‌آرا: سعیده رجبلو

چاپ نخست: ۱۴۰۰

شمارگان: ۱۰۰۰ نسخه

ویرایش، آماده‌سازی و صفحه‌آرایی متن: مژگان مهدوی

لیتوگرافی، چاپ و صحافی: چاپ بلوط

این کتاب با همکاری مرکز ملی فضای مجازی، دانشکدهٔ روابط بین‌الملل وزارت امور خارجه و ادارهٔ هماهنگی امور پژوهشی و نشر وزارت امور خارجه به چاپ رسیده است.

فهرست

پیش‌گفتار

عرصهٔ سایبری جدی‌ترین مسئله و چالش حکمرانی در ابعاد ملی، منطقه‌ای و بین‌المللی است و درست همانند دوران گذارهای حساس تاریخی، همچون تسخیر فضا، ساخت بمب هسته‌ای، جهانی‌سازی و ...، تمامی معادلات در نظم مستقر بین‌الملل را به چالش کشیده است. عرصهٔ سایبری پدیده‌ای چندوجهی است که به دلیل ماهیت پیچیده و شبکه‌ای، خصلت مرکزگریزی و کنترل‌ناپذیری و نیز ظهور بازیگران قدرتمند غیررسمی و بعضاً ناشناخته در آن، مستلزم نگاه حاکمیتی و فراتر رفتن از رویکردهای تک‌بُعدی و کلاسیک است.

در مطالعهٔ اسناد و متون سایبری و نیز تجارب کشورهای مختلف در مواجهه با چالش‌های سایبری، کشورهای مختلف بعضاً سه فاز متفاوت را تجربه کرده‌اند: ۱. فاز دفاعی، ۲. فاز تهاجمی و ۳. فاز دیپلماسی سایبری. عمدهٔ کشورهای جهان در سطوح مختلف، فازهای اول و دوم را تجربه کرده‌اند، با این حال تعداد قلیلی از کشورها توانسته‌اند با تبدیل این عرصه به فرصت، وارد فاز «دیپلماسی سایبری» به معنای استفاده از پتانسیل عرصهٔ سایبری برای ظرفیت‌سازی و اعتمادسازی با هدف پیشبرد اهداف و منافع ملی خود در عرصه‌های منطقه‌ای و بین‌المللی بشوند.

در بین کشورهایی که وارد فاز دیپلماسی سایبری شده‌اند، دو رویکرد عمده قابل شناسایی است: ۱. رویکرد غربی با محوریت آمریکا: ایالات متحده آمریکا اولین کشوری است که دیپلماسی سایبری خود را تدوین و به

عنوان سند ملی اعلام نمود. به دنبال آن بسیاری از کشورهای غربی، از جمله کشورهای اروپایی و نیز استرالیا و نیوزلند به پیروی از این کشور اسناد سایبری ملی خود را تدوین کردند و به تصویب رساندند. ۲. رویکرد شرقی با محوریت کشورهای روسیه و چین که به لحاظ اصول و مبانی تا حد بسیار زیادی در مقابل کشورهای غربی قرار دارد. این رویکرد عمدتاً از سوی کشورهای عضو سازمان همکاری شانگهای دنبال می‌شود. در این بین، برخی از کشورها همچون ژاپن از یک سو به دلیل نزدیکی ایدئولوژیک با کشورهای غربی و از سوی دیگر به دلیل واقع شدن در منطقهٔ شرق آسیا و در مجاورت کشورهایی همچون روسیه و چین، سعی کرده‌اند بر اساس منافع ملی خود رویکرد بینابینی را دنبال کنند.

فراتر از سطوح ملی، در عرصهٔ منطقه‌ای و بین‌المللی نیز موضوع دیپلماسی سایبری از اهمیت خاصی برخوردار بوده است. سازمان ملل متحد و به طور مشخص «گروه کارشناسان دولتی این سازمان» از اوایل سال ۲۰۰۰ میلادی با هدف پیگیری این موضوع تشکیل شده و تا کنون چندین نشست با حضور اکثریت اعضای این سازمان برگزار کرده و اسناد و خروجی‌های آن، در قالب اسناد رسمی، به مجمع عمومی سازمان ملل یا شورای امنیت این سازمان ارجاع شده است. اتحادیهٔ اروپا، سازمان ناتو، سازمان همکاری شانگهای، گروه هفت، گروه بیست، اتحادیهٔ کشورهای جنوب شرق آسیا (آسه‌آن) و ... از دیگر نهادها و سازمان‌های بین‌المللی هستند که در چارچوب منافع کشورهای عضو به این موضوع پرداخته‌اند.

با توجه به چندوجهی و چندذی‌نفعی بودن عرصهٔ سایبری، نکتهٔ حائز اهمیت ظهور بازیگران نوظهور در قالب سازمان‌ها و کمپانی‌های بزرگ آی‌تی و نیز نهادها و سازمان‌های مدنی است که غالباً در انواع دیپلماسی‌های کلاسیک جایگاه چندانی نداشتند. این بازیگران که به ویژه

نمایندگان بخش خصوصی محسوب می‌شوند، به دلیل تضاد منافع با دولت‌ها و منابع رسمی دارای اولویت‌های متفاوتی هستند و به همین دلیل نیز دایرهٔ اثرگذاری و بازیگری دولت‌ها در این عرصه را محدود و بیش از گذشته تنگ کرده‌اند. پلتفرم‌ها و غول‌های آی‌تی همچون گوگل، مایکروسافت، اپل و ... از جمله مهم‌ترین بازیگران قدرتمند عرصهٔ سایبری هستند که دایرهٔ اثرگذاری و قدرت بازیگری آن‌ها بعضاً از مجموع بسیاری از کشورهای کوچک و بزرگ بیشتر می‌باشد.

مطالعهٔ مبانی و اصول دیپلماسی سایبری کشورهایی که دارای اسناد رسمی دیپلماسی سایبری هستند، و نیز برآیند ارزیابی بیش از ۸۰ سند بین‌المللی و منطقه‌ای که در ارتباط با دیپلماسی سایبری تدوین و تصویب شده‌اند، نشان می‌دهد که مدیریت و هدایت این عرصه به سبک و سیاق دیپلماسی‌های کلاسیک امکان‌پذیر نیست. مواجهه با چالش‌های این حوزه و نیز مقابله با بازیگران ناشناسی که عمدتاً از طریق سازماندهی حملات تهاجمی همچون حمله به زیرساخت‌ها، جاسوسی سایبری، سرقت اطلاعات و ... ظهور و بروز می‌یابند، مستلزم حضور کانون‌های قدرتمند نهادی از جمله «استراتژیست‌های سایبری» و «ژنرال‌های سایبری» در کنار «دیپلمات‌های سایبری» است تا بتوانند با هم‌افزایی منابع قدرت داخلی، به بهترین نحو ممکن اهداف و سیاست‌های منطقه‌ای و بین‌المللی مطلوب در این عرصه را پیش ببرند.

در ایران، مرکز ملی فضای مجازی به عنوان نهاد سیاست‌گذار در عرصهٔ سایبری و وزارت امورخارجه به عنوان دستگاه متولی سیاست خارجی کشور دو نهاد اصلی و تأثیرگذار در تدوین، تبیین و پیش‌بینی مسائل، چالش‌ها و فرصت‌های عرصهٔ سایبری و به تبع آن تدوین سیاست‌ها و برنامه‌های اصلی کشور در دو سطح ملی و بین‌المللی محسوب می‌شوند. با توجه به موقعیت ژئوپولیتیک و منحصربه‌فرد کشور از یک سو، و نیز گستردگی دامنهٔ تهدیدات

و فشارهایی که ناحیهٔ سایبری در شرایط نوین بین‌المللی بر کشور وارد می‌شود از سوی دیگر، همکاری، هم‌اندیشی و در نهایت رویکرد بین‌سازمانی با هدف هم‌افزایی منابع دانش و قدرت بیش از پیش ضرورت می‌یابد.

با این نگاه، کتاب *حکمرانی در عرصهٔ پنجم: گذار به دیپلماسی سایبری* به عنوان یکی از طرح‌های مطالعاتی در زمینهٔ دیپلماسی سایبری در ۱۰ فصل تدوین یافته و هم‌اکنون به صورت مشترک از سوی انتشارات پژوهشگاه فضای مجازی، دانشکدهٔ روابط بین‌الملل وزارت امور خارجه و ادارهٔ هماهنگی امور پژوهشی و نشر وزارت امور خارجه در اختیار محققان، پژوهشگران و علاقه‌مندان مسائل دیپلماسی سایبری قرار گرفته است.

مبنای تدوین این کتاب، مطالعهٔ موردی است و به طور خاص مبانی، اصول و راهبردهای دیپلماسی سایبری چند کشور مهم از جمله آمریکا، روسیه، چین، اتحادیهٔ اروپا و مالزی در آن ارزیابی شده است. در کنار مطالعات موردی، بیش از ۸۰ سند منطقه‌ای و بین‌المللی در این حوزه نیز مورد مطالعه قرار گرفته و پس از احصاء اصول اصلی آن‌ها، مهم‌ترین بازیگران این عرصه در سطوح ملی، منطقه‌ای و بین‌المللی، و نیز بازیگران بخش خصوصی معرفی و رویکرد آن‌ها به مقوله سایبری تبیین شده است. همچنین با توجه به اهمیت ظهور بازیگران غیردولتی، یک فصل به طور کامل به ارزیابی و مطالعهٔ این بازیگران پرداخته و به طور خاص گافام، به عنوان بزرگ‌ترین پلتفرم‌های آی‌تی، در چارچوب دیپلماسی شرکتی ارزیابی و تحلیل شده است.

ویژگی متمایز این کتاب، بررسی تطبیقی تمامی مطالعات موردی و نیز رویکردهای مهم منطقه‌ای و بین‌المللی به دیپلماسی سایبری در فصل پایانی می‌باشد. بر مبنای این مقایسهٔ تطبیقی، در نهایت یک الگوی عملیاتی با محوریت ۲۴ مقولهٔ مهم سایبری برای تدوین سند دیپلماسی سایبری در ایران پیشنهاد شده است.

این کتاب در اصل فتح بابی در خصوص مسائل مرتبط با دیپلماسی سایبری کشور در این عرصهٔ چالشی و در عین حال روبه‌توسعه می‌باشد و امید است علاقه‌مندان به این حوزه با مطالعه و نقد این کتاب فضای دیالکتیکی و گفتمانی مناسبی را برای پیشبرد مباحث مربوطه در این حوزه فراهم سازند.

عبدالحسین کلانتری؛ مرکز ملی فضای مجازی
محمدحسن شیخ‌الاسلامی؛ دانشکدهٔ روابط بین‌الملل

مقدمه

زمین، دریا، هوا و فضا؛ و اکنون فضای سایبری، به عنوان عرصهٔ پنجم، حوزه‌ای کاملاً جدید برای بسط قدرت و نفوذ در تعاملات منطقه‌ای و بین‌المللی کشورهاست. به این اعتبار، سازوکار و مکانیسم فعالیت در این عرصه که عموماً «دیپلماسی سایبری» نامیده می‌شود، متأخرترین نوع دیپلماسی در ادبیات روابط بین‌الملل است که عمر آن به کمتر از یک دهه می‌رسد.

اهمیت مقولهٔ «فضای سایبری» در گسترهٔ روابط بین‌الملل به حدی است که برخی از محققان، اهمیت ظهور آن را با اختراع «بمب اتم» مقایسه کرده و تأکید داشته‌اند که عرصهٔ سایبری به همان اندازه مستلزم تکاپوی جدی و بی‌شمارِ دیپلماسی و دیپلمات‌هاست تا بتوان از پیامدها و آسیب‌های ملی، منطقه‌ایِ و بین‌المللیِ به مراتب بیشتر، وسیع‌تر و خطرناک‌ترِ آن (در مقایسه با بمب‌های هسته‌ای) اجتناب کرد. با توجه به نوظهور بودنِ و نیز اهمیت روزافزون آن، با قاطعیت می‌توان گفت که دیپلماسی سایبری در سطوح مختلف ملی، منطقه‌ای و بین‌المللی در صدر توجهات سیاسی ـ حاکمیتی قرار داشته و (گرایش به پرداختن به آن) به عنوان مؤلفهٔ اصلی تعیین‌کنندهٔ قدرت و نفوذ در قرن ۲۱، بیش از پیش افزایش یافته است.

در مطالعه‌ای که در کتب، متون علمی و نیز اسناد ملی و منطقه‌ای کشورهای خارجی صورت گرفت، در مجموع بیش از هشتاد سند یا

اعلامیهٔ تبیین‌کنندهٔ دیپلماسی سایبری کشورها، استراتژی‌های ملی، دوجانبه و چندجانبه و بین‌المللی اتخاذشده در ارتباط با دیپلماسی سایبری و رویکردهای جهانی به این مقوله شناسایی شده است. اگر بنا به اقتضای اشرافیت راهبردی و فنّاورانهٔ کشورهای غربی از پیشگامی آن‌ها در این حوزه صرف‌نظر کنیم، برخی تلاش‌ها و ابتکارات دیپلماتیک در ارتباط با دیپلماسی سایبری به کشورهای حوزهٔ خلیج فارس، آسیای میانه و حتی کشورهای آفریقایی نیز کشیده شده است که نشان از درجه و اهمیت این موضوع در بازیگری منطقه‌ای و بین‌المللی هر یک از کشورها دارد. با توجه به اهمیت این اقدامات و ابتکارات، برخی از مهم‌ترین آن‌ها در این کتاب به صورت «مطالعهٔ جامع اقدامات و سازوکارهای جهانی دیپلماسی سایبری» در فصل ۲ و برخی دیگر نیز به صورت مطالعهٔ موردی (فصول ۴ ــ ۹) در این کتاب مورد مطالعه و ارزیابی قرار گرفته‌اند.

با این حال و به رغم موضوعیت فراوان آن، به مقولهٔ دیپلماسی سایبری در ایران کمتر توجه شده است. در عرصهٔ نظری، هنوز کتابی جامع و مانع در این حوزه که مبیّن مبانی، اصول و مؤلفه‌های دیپلماسی سایبری باشد، وجود ندارد. در عرصهٔ عمل، در حالی که رویکردهای جدید بر گذار به مرحلهٔ شناسایی و ردیابی فعالیت‌های سایبری و نیز اتخاذ استراتژی‌های نفوذ در قلمروهای به دقت طراحی‌شدهٔ سایبری در اقصی نقاط جهان تأکید دارد، عمدهٔ اقدامات و ابتکارات سایبری کشور با رویکرد «دفاعی» تنظیم و سامان یافته که بر اساس شواهد تاریخی، رویکرد بسیار ابتدایی و اولیهٔ تمامی کشورها به مقولهٔ فضای سایبری بوده است. در برخی نظریه‌پردازی‌های پراکندهٔ دیگر نیز مقولهٔ دیپلماسی سایبری با برخی مفاهیم مشابه همچون دیپلماسی دیجیتال، دیپلماسی الکترونیکی، دیپلماسی عمومی و... خلط معنایی پیدا کرده و یا حتی کرانه‌های

آن به حضور چند مقام ارشد کشور در شبکه‌های اجتماعی جهانی، همچون توییتر و اینستاگرام، تقلیل یافته است.

به لحاظ مفهومی، دیپلماسی سایبری را به معنای عامِ آن می‌توان در دو سطح بررسی کرد: نخست، ادامه و تداوم دیپلماسی سنتی در فضا و بستر جدید است که فضای سایبری نامیده می‌شود. به این اعتبار، تمامی فعالیت‌های دیپلماتیک را، که سابقاً به صورت سنتی جاری و ساری بوده است، می‌توان از این طریق و در بستر فضای سایبری نیز دنبال کرد. دوم، که بیشتر و مهم‌تر جلوه یافته، به معنای مدیریت تضادها و اختلافات منطقه‌ای و بین‌المللی مرتبط با فضای سایبری از طریق گفت‌وگو و مذاکره، استفاده از قابلیت‌ها و توانمندی‌های سایبری برای «دفاع» از منافع ملی و در سطح ایدئال آن، پیشبرد منافع ملی از طریق ظرفیت‌سازی سایبری، اعتمادسازی سایبری و اتخاذ استراتژی‌های مؤثر با هدف نفوذ در حوزه‌های قدرت و ثروت در عرصهٔ جهانی است. به این اعتبار، دیپلماسی سایبری از سیاست‌گذاریِ ملی در حوزهٔ فضای سایبری تمایز یافته و از سطح پیشین (تداوم و گسترش دیپلماسی سنتی در فضای سایبری) نیز فراتر می‌رود. سطح دوم از تعریف فوق، در واقع نقطهٔ ایدئال و مطلوبِ دیپلماسی سایبری است که باید به دنبال آن بود.

با توجه به این مقدمه و تعریفی که در بالا در دو سطح از دیپلماسی سایبری ارائه شده، این کتاب تلاشی است در زمینهٔ ۱. مطالعهٔ اصول و مبانی دیپلماسی سایبری برخی کشورهای پیشرو در حوزهٔ سایبری، و ۲. ارائهٔ یک چارچوب مفهومی از مؤلفه‌ها و مقولات مرتبط با دیپلماسی سایبری با هدف پیشنهاد یک الگوی عملی از دیپلماسی سایبری در ایران.

بر اساس این اهداف، کتاب حاضر در مجموع دارای ده فصل است:

۱. دیپلماسی سایبری؛ مسائل، چالش‌ها و رسالت: این فصل ترجمهٔ مقاله‌ای است که به درخواست نویسندهٔ اصلی آن، هلی تییرما کلار،[1] به عنوان مقدمه‌ای بر موضوع دیپلماسی سایبری ترجمه و تلخیص شده است. نویسندهٔ مقاله یکی از پیشگامان مفهوم‌پردازی در حوزهٔ دیپلماسی سایبری است. هلی تییرما کلار از ۲۰۱۳، در اتحادیهٔ اروپا به عنوان دیپلماتی برجسته درگیر موضوعاتِ حوزهٔ سایبری بوده و هم‌اکنون نیز در کسوت سفیر ارشد حوزهٔ سایبری، در وزارت امور خارجهٔ کشور استونی مشغول به فعالیت است. مقالهٔ وی حاوی یکی از جامع‌ترین مفهوم‌پردازی‌های صورت‌گرفته دربارهٔ دیپلماسی سایبری است که تا کنون به رشتهٔ تحریر درآمده است. این مقاله صورت‌بندی کاملی از مسائل، چالش‌ها و دستورالعمل‌های موضوعات سایبری در عرصهٔ بین‌الملل را ارائه می‌دهد.

۲. مطالعهٔ جامع اقدامات و سازوکارهای جهانی دیپلماسی سایبری: در این فصل، مطالعهٔ نسبتاً جامعی دربارهٔ بیش از هشتاد اقدام و سازوکار ملی، منطقه‌ای، بین‌المللی و جهانی که تا کنون در ارتباط با دیپلماسی سایبری به سرانجام رسیده، صورت گرفته است. این فصل از این جهت حائز اهمیت است که در وهلهٔ اول مهم‌ترین بازیگران عرصهٔ دیپلماسی سایبری را در سطوح مختلف (کشورها، سازمان‌های بین‌المللی، مذاکرات دوجانبه، چندجانبه، بخش خصوصی و شرکت‌های فناوری و ...) شناسایی کرده و بر اساس آن می‌توان مهم‌ترین ابتکارات صورت‌گرفته، میزان پیشرفت کشورها، رویکردهای منطقه‌ای و بین‌المللی و نیز مهم‌ترین سازوکارهایی را که در سطح جهان در ارتباط با اقدامات مرتبط با دیپلماسی سایبری تعریف و نهایی شده، به صورت تطبیقی با یکدیگر مقایسه کرد. حضور فعال برخی

1. Heli Tiirmaa-Klaar

کشورها در مناطق مختلف (چه در پلتفرم سازمان‌های منطقه‌ای و بین‌المللی و چه در قالب مذاکرات دوجانبه) در سازوکارهای تعریف‌شدهٔ منطقه‌ای و بین‌المللی حائز اهمیت است.

۳. گذار ژاپن به دیپلماسی سایبری (۲۰۱۸): این فصل مطالعهٔ موردی اقدامات ژاپن دربارهٔ دیپلماسی سایبری، رویکرد اصلی این کشور به این مقوله و اقدامات منطقه‌ای و بین‌المللی این کشور در ارتباط با فضای سایبری است. به لحاظ اصول و مبانی، اگرچه دیپلماسی سایبری ژاپن در سطح بین‌الملل شباهت‌ها و قرابت‌های زیادی با دموکراسی‌های غربی همچون آمریکا و اتحادیهٔ اروپا دارد، اما در سطح داخلی، درست همانند چین و روسیه، مهم‌ترین دغدغهٔ این کشور موضوع «امنیت داخلی» است، به خصوص اینکه اقتصاد این کشور تماماً به زیرساخت‌های اقتصاد دیجیتال وابسته است. شاید بر همین اساس نیز ژاپن در استراتژی‌های عملیاتی برای پیشبرد دیپلماسی سایبری خود، اولویت بیشتری برای همسایگان پیرامونی خود به خصوص در آسیا و اقیانوسیه قائل است. از این رو مطالعهٔ کشور ژاپن، که تلاش می‌کند همسو با اصول و مبانی دموکراسی‌های غربی دغدغه‌ها و چالش‌های شرقی (همچون روسیه و چین) را نیز مدیریت کند، می‌تواند حائز اهمیت باشد.

۴. ظهور و افول دیپلماسی سایبری آمریکا، بازگشت به رویکرد امنیتی ـ تهاجمی: این فصل به مطالعهٔ تاریخچهٔ دیپلماسی سایبری در آمریکا، به عنوان کشوری که در حوزهٔ سایبری به لحاظ فنی از سایر کشورها جلوتر است، بر اساس اسناد تدوین‌شده در دو دههٔ اخیر می‌پردازد. نکتهٔ اصلی و قابل توجه در این مطالعه، افول دیپلماسی سایبری آمریکا از سیاست‌های آرمان‌گرایانهٔ تاریخی و بازگشت این کشور به رویکرد امنیتی ـ نظامی در ارتباط با فضای سایبری به

خصوص پس از انتخاب دونالد ترامپ به ریاست‌جمهوری در ۲۰۱۶ است. با توجه به رویکرد تجاری ـ نظامیِ دولت ترامپ، به نظر می‌رسد دولت فعلی حاکم بر این کشور از بعضی از مهم‌ترین اصول و مؤلفه‌های بنیادینی همچون «حقوق بشر» و «آزادی بیان» و ...، که در دیپلماسی کلاسیک بین‌الملل خود مدعی آن‌ها بود، افول کرده و در چارچوب دیپلماسی سایبری جدید، بیشتر به دنبال تضمین «امنیت سایبری» خود (جلوگیری از حملات سایبری یا جاسوسی سایبری) و نیز کسب بیشترین منافع تجاری و اقتصادی در تمامی استراتژی‌های تعاملی دوجانبه و چندجانبه در عرصهٔ منطقه‌ای و جهانی است. در این فصل، همچنین به مهم‌ترین چالش‌های پیش روی آمریکا در عرصهٔ دیپلماسی سایبری، یعنی چالش مخالفت‌ها با «جریان آزاد و فرامرزی داده‌ها» که در قالب جنبش‌هایی همچون تقاضا برای محلی‌سازی داده‌ها، تدوین استانداردهای ملی امنیت اطلاعات، ارائهٔ الگوهای جایگزین از حکمرانی اینترنت و حکمرانی سایبری و ... از سوی کشورهایی همچون هندوستان، چین، روسیه و حتی اتحادیهٔ اروپا دنبال می‌شود، پرداخته شده است.

۵. چین و گذار به دیپلماسی سایبری مدبرانه: این فصل مطالعهٔ موردی کشور چین به عنوان یک قدرت بزرگ جهانی، در ارتباط با دیپلماسی سایبری است که می‌توان آن را در قالب یک استراتژی سه‌وجهی دنبال کرد: ۱. تهاجمی؛ از طریق نفوذ در زیرساخت‌های اطلاعاتی و ارتباطی کشورهای رقیب، به خصوص آمریکا و اروپا، ۲. تجاری ـ اقتصادی؛ از طریق سرمایه‌گذاری گسترده در زیرساخت‌های کشورها و مناطق هدف به خصوص اروپا، آفریقا، خاورمیانه، آسیای میانه و آمریکای لاتین،۳. استانداردسازی؛ از طریق مشارکت جدی در تعریف پروتکل‌ها و استانداردهای فناوری در نرم‌افزار، سخت‌افزار و شبکه‌های مدرن. گذار

چین از یک موضع تدافعی در ارتباط با دیپلماسی سایبری به یک سیاست مدبرانه با هدف مقابله با نفوذ و اشرافیت راهبردی آمریکا در حوزهٔ سایبری، تثبیت اصل «حاکمیت ملی» در حکمرانی فضای سایبری، صورت‌بندی تهدیدات سایبری، پیشبرد اهداف سایبری از طریق سرمایه‌گذاری‌های تجاری هنگفت منطقه‌ای و بین‌المللی، پیشبرد صلح سایبری از طریق اتخاذ استراتژی‌های تعامل چندجانبه (با سازمان ملل[1]، اتحادیهٔ اروپا و سازمان همکاری شانگهای) و نیز استراتژی تعامل دوجانبه با آمریکا، روسیه و انگلستان از جمله مهم‌ترین محورهایی است که در این فصل به آن پرداخته شده است. الگوی عملیاتی پیاده‌سازی دیپلماسی سایبری در ساختار حاکمیتی این کشور و نقش شرکت‌های فناوری چینی به خصوص هوآوی و زدتی‌ای، در پیشبرد اهداف دیپلماسی سایبری چین نیز در جای خود قابل تأمل است.

۶. دیپلماسی سایبری روسیه، حاکمیت ملی و امنیت اطلاعات: روسیه، همانند چین، به عنوان اصلی‌ترین رقیب آمریکا در عرصهٔ دیپلماسی سایبری، از اهمیت قابل‌توجهی برخوردار است. موضوع مقابلهٔ تاریخی و ایدئولوژیک این کشور با دموکراسی‌های غربی که امروزه به عرصهٔ سایبری نیز کشیده شده، بر اهمیت رویکرد سایبری روسیه می‌افزاید. در این فصل، به طور کلی رویکرد روسیه با تأکید بر دو مؤلفهٔ «حاکمیت ملی» و «امنیت اطلاعات»، که آشکارا مؤلفه‌ها و مبانی اصلی دیپلماسی سایبری غربی را زیر سؤال می‌برد، بررسی شده است. علاوه بر این، استراتژی‌هایی که روسیه برای پیشبرد دیپلماسی سایبری در عرصهٔ جهانی و منطقه‌ای، به خصوص از طریق مکانیسم سازمان ملل، سازمان همکاری شانگهای و ...

1. United Nation Group of Governmental Experts (UNGGE)

در پیش گرفته، همراه با چالش‌های آن نیز با جزئیات بحث و بررسی می‌شود. نکتهٔ قابل تأمل‌تر در ارتباط با دیپلماسی سایبری روسیه این است که روند روزافزون تهدیدات سایبری به طور خودکار برداشت بسیاری از کشورها را، حتی کشورهای غربی، به مبانی فکری روسیه در ارتباط با ماهیت چالش‌های فضای سایبری نزدیک ساخته است.

۷. دیپلماسی سایبری اتحادیهٔ اروپا، از تاب‌آوری سایبری تا بستهٔ دیپلماسی سایبری: این فصل رویکرد کلان اتحادیهٔ اروپا را به دیپلماسی سایبری ارزیابی می‌کند. اگرچه سیاست‌های اتحادیهٔ اروپا در سطح کلان در ارتباط با دیپلماسی سایبری تا حدودی همسو با آمریکاست، اما در مقایسه با آمریکا، کمتر تهاجمی و بیشتر دفاعی و همراه با تلاش برای حل مسائل سایبری از طریق مذاکرات سیاسی است. به طور مثال، بستهٔ دیپلماسی سایبری، که در سال ۲۰۱۷ به تصویب رسید، به عنوان یکی از ابتکارات اتحادیهٔ اروپا، بر اساس محور صلح‌طلبی طیف نسبتاً جامعی از اقدامات سایبری مشترک با هدف پیشبرد اهداف سیاسی این اتحادیه ارائه می‌دهد. با این حال، همان طور که در این فصل به آن پرداخته شده، این بسته نیز در عمل به دلیل دشواری مکانیزم‌های تصمیم‌گیری اشتراکی و دیگر چالش‌هایی که با آن مواجه است، بیشتر شبیه یک مانیفست سیاسی است تا یک برنامهٔ جامع عملیاتی. این فصل در نهایت با ارائهٔ چشم‌اندازی از آیندهٔ بستهٔ دیپلماسی سایبری اتحادیهٔ اروپا و نیز استراتژی‌هایی که به صورت چندجانبه، دوجانبه و نیز از طریق درگیر ساختن تمامی ذی‌نفعان غیردولتی از سوی این اتحادیه در پیش گرفته شده، پایان می‌یابد.

۸. دیپلماسی سایبری مالزی: این فصل به مطالعهٔ کشور مالزی، به عنوان یک کشور اسلامیِ نسبتاً پیشرفته، در ارتباط با مقولهٔ دیپلماسی سایبری

می‌پردازد. اگرچه این کشور به لحاظ زیرساخت، رویکرد و حتی نقشی که در این حوزه دارد، قابل مقایسه با سایر کشورهایی که در این کتاب مورد مطالعه قرار گرفته‌اند نیست، با این حال تاریخچهٔ توسعهٔ فناوری (به خصوص استفاده از فناوری اطلاعات و ارتباطات در حکمرانی ملی و نیز کسب رتبهٔ عالی در دولت الکترونیک) و نیز پرداختن زودهنگام به مقولهٔ سایبری در سیاست‌گذاری و برنامه‌ریزی‌های مختلف که سابقهٔ آن به دههٔ ۱۹۹۰ می‌رسد، حائز اهمیت است. اگر از چالش‌های داخلی مالزی، از جمله دشواری برقراری توازن استراتژیک بین ملاحظات حکمرانی ملی با تأکید بر چندقومی و چندنژادی بودن این کشور و الزامات همراهی آن با جریانات غالب حکمرانی بین‌المللی در عرصهٔ سایبری، صرف‌نظر کنیم؛ نقشی که مالزی در دهه‌های اخیر به عنوان یک کشور اسلامیِ پیشرفته در معادلات منطقه‌ای و بین‌المللی ایفا کرده، به خصوص از منظر همسویی با جامعهٔ جهانی، مورد توجه خاص بسیاری از کشورها واقع شده است.

۹. گافام و دیپلماسی شرکتی: گافام نام یک کشور یا واحد سیاسی با مختصات حکمرانی همراه با قلمرو مشخص و مرزهای جغرافیایی معیّن نیست. بلکه پنج پلتفرم (گوگل، اپل، فیس‌بوک، آمازون و مایکروسافت) پیشتاز در عرصهٔ سایبری هستند که به لحاظ سیاسی به پادشاهان آنلاین، به لحاظ ثروت به امپراتوری‌های تجاری و به لحاظ فناوری به غول‌های آی‌تی مشهور شده‌اند. در واقع ترکیب «ثروت» و «فناوری» در دستان این پلتفرم‌ها، به گافام قدرت بازیگری و اثرگذاری بسیار زیادی در عرصهٔ سیاست و نیز روابط بین‌الملل داده که در هیچ سپهر سیاسی نمی‌توان آن‌ها را نادیده گرفت. در این فصل، گافام در چارچوب مفهوم پلتفرم، دیپلماسی شرکتی، عوامل قدرت‌افزای آن‌ها در حکمرانی شبکه‌ای و نیز چالش‌هایی

که از این ناحیه متوجه دیپلماسی به معنای کلاسیک آن شده، واکاوی شده است. ارزش تجاری گافام در سه ماههٔ اول سال ۲۰۲۰ به بیش از پنج هزار میلیارد دلار (پنج تریلیون دلار) رسید و برای فهم نقش و جایگاه آن‌ها در دنیای سیاست مدرن می‌توان به استعارهٔ «کودکان نابخرد» شرود براون[1] سناتور آمریکایی، اشاره کرد که در اعتراض به عملکرد این پلتفرم‌ها گفت دنیا همانند یک خانه است و این پلتفرم‌ها همچون کودکان نابخرد بارها همه آن را به آتش زده‌اند. با توجه به اهمیت این پلتفرم‌ها و حضور آن‌ها به عنوان بازیگر مستقل در بسیاری از منازعات سیاسی داخلی و خارجی، امروزه بسیاری از کشورها فارغ از تعاملات سیاسی کلاسیک، باب تعامل دیپلماتیک سایبری با این پلتفرم‌ها گشوده‌اند که از جمله می‌توان به انتصاب اولین سفیر در گوگل از سوی کشور دانمارک اشاره کرد.

۱۰. گذار به دیپلماسی سایبری، چارچوب مفهومی و پیشنهاد الگوی عملی دیپلماسی سایبری در ایران: این فصل در مجموع جمع‌بندی تمامی فصل‌های تدوین‌شده در این کتاب است. این فصل افزون بر مقدمهٔ آن، مطالعهٔ سیر تاریخی ظهور مفاهیم مشابه با دیپلماسی سایبری، و مرزبندی و تمایز معنایی و مفهومی که بین آن‌ها صورت پذیرفته، از دو حیث حائز اهمیت است: ۱. جمع‌بندی‌ای را که از گرایش‌های مختلف ملی، منطقه‌ای و جهانی به مقولهٔ دیپلماسی سایبری به دست آمده در قالب دو رویکرد کلان همراه با مبانی و اصول اصلی آن‌ها، که به طور هم‌زمان از سوی دو جبههٔ متفاوت (یکی به رهبری آمریکا در غرب و دیگری به رهبری چین و روسیه در شرق) در سطح جهان دنبال می‌شود، به معرض نمایش می‌گذارد. ۲. مهم‌ترین مقولات یا مفاهیمِ دیپلماسی سایبری را، که از طریق مطالعات

1. Sherrod Brown

موردی و نیز تکنیک هم‌افزایی فکری در جلسات بحث متمرکز احصا شده، در قالب «جدول مقولات سایبری» ارائه و با تعریف دقیق آن‌ها در قالب یک الگو برای تدوین به صورت عملیاتی در ایران پیشنهاد می‌دهد.

با مطالعهٔ عمیق فصول این کتاب می‌توان دریافت که علاوه بر اصول، مبانی و مؤلفه‌های دیپلماسی سایبری در هر یک از این کشورها، صف‌بندی جهانی در ارتباط با دیپلماسی سایبری، رویکرد کشورها به این مقوله و استراتژی‌هایی که گاهی از سوی هر یک از کشورها، چه به صورت دوجانبه یا چندجانبه و یا بین‌المللی، اتخاذ شده نیز روشن و مبرهن است.

با وجود این، در صف‌بندی فعلی از نظام حاکم بر فضای سایبری جهانی، نکته‌ای قابل تأمل دربارهٔ دیپلماسی سایبری وجود دارد و آن اینکه تنها، کشورهایی در این زمینه موفق بوده‌اند که توانسته‌اند دربارهٔ اصول و مؤلفه‌های حاکم بر این نظم، «استانداردسازی» کرده و در قالب دیپلماسی سایبری، این استانداردها را در روابط بین‌الملل به جوامع مختلف تحمیل کنند. در واقع می‌توان گفت تنها ایالات متحده آمریکاست که توانسته استانداردِ مورد نظر خود در این زمینه را به نظام جهانی (جامعهٔ جهانی) تحمیل کند به طوری که بر اساس بررسی‌های انجام‌شده، حداقل ۲۵ کشور جهان که عمدتاً غربی و از کشورهای اروپایی‌اند، عیناً از استراتژی دیپلماسی سایبری این کشور اقتباس کرده و دنباله‌رو آن هستند. در سطوحی پایین‌تر، روسیه و چین نیز تلاش‌هایی در این زمینه کرده‌اند، هرچند هنوز در مراحل اولیه قرار دارند و با چالش‌های اساسی از سوی رقبای غربی خود مواجه‌اند. صرف‌نظر از آمریکا و روسیه و چین، عمدهٔ کشورها (حتی کشورهایی در سطح انگلستان، آلمان، فرانسه و اتحادیهٔ اروپا) عمدتاً در ابعاد امنیت سایبری با تأکید بر ملاحظات داخلی متوقف

مانده و نتوانسته‌اند به راهبردهای دیپلماتیک بـا تأکیـد بـر عرصـهٔ سیاسـت خارجی دست یابند. به عبارت دیگر، به جرئت می‌توان گفت که بـه غیـر از آمریکا و تا حدودی روسیه و چین، عمدهٔ کشورها اغلب در ابعاد داخلـی و امنیتی سایبری متوقف مانده و اگر کمی فراتر رفته‌اند، یا دنباله‌روی کرده‌انـد و یا صرفاً به بیان لزوم دیپلماسی در این حوزهٔ جدید بسنده کرده‌اند.

با توجه به ملاحظهٔ فوق، ادعای اصلی کتاب این است که با توجه به تبـدیل شدن فضای سایبری به منشأ اصلی نبرد و مناقشه بـین کشـورها و قـدرت‌هـای بزرگ در عرصهٔ جهانی، نظام حکمرانی کشور باید هر چه سریع‌تر از لایـه‌هـای دفاعی ـ امنیتی فضای سایبری فراتر رفته و به پشتوانهٔ قابلیت‌هـا و ظرفیـت‌هـای سایبری که تا کنون به دست آورده، در ارتباط با مقولات و مؤلفه‌های دیپلماسـی سایبری (جدول مقولات ارائـه‌شـده در فصـل دهـم) استانداردسـازی کنـد. بـه عبارت روشن‌تر، نظام حکمرانی باید به یـک تعریـف، جمـع‌بنـدی و سیاسـت واحد در ارتباط با هر یک از مقولات حوزهٔ سایبری برسد تا بتواند بـه صـورت منسجم و یکپارچه در قالب الگـویی عملـی[1] و صـاحب‌گفتمـان (و در جایگـاه مدعی) برای پیشبرد منافع ملی کشور در این حـوزه وارد تعامـل اسـتراتژیک بـا طرف‌های خارجی در عرصهٔ منطقه‌ای و بین‌المللی بشود. در غیر ایـن صـورت، همواره باید در چارچوب و استانداردهای دیپلماسی سایبری کشـورهای پیشـرو بازیگری کند و بپذیرد که همواره در موضـع دفـاعی قـرار داشـته و نسـبت بـه مطالبات آن‌ها ــ به خصوص آنچه به طور مشخص می‌توان برنامهٔ هدایت‌شـدهٔ ایران‌هراسی سایبری نامید ــ پاسخگو باشد.

در پایان و به مناسبت چاپ این کتاب بر خود لازم مـی‌دانـیم از تمـامی

---

۱. این الگوی عملی که از آن به عنوان دیپلماسی سایبری یاد می‌شود، بـه تفصـیل در فصل دهم به همراه مقولات پیشنهادی برای تصمیم‌گیـری و سیاسـت‌گـذاری بررسـی می‌گردد.

افرادی که به روش‌های مختلف در به سرانجام رسیدن این مجموعه ما را یاری کرده‌اند، به خصوص دبیر محترم شورای‌عالی و رئیس مرکز ملی فضای مجازی، ریاست محترم دانشکدهٔ روابط بین‌الملل، کارشناسان پژوهشگاه فضای مجازی و همکاران هیئت‌علمی دانشکدهٔ روابط بین‌الملل وزارت امور خارجه، قدردانی نماییم.

همچنین با توجه به قلّت منابع نظری داخلی و خارجی در این زمینه، آشکارا مفروض است که این مجموعه صرفاً فتح بابی در زمینهٔ دیپلماسی سایبری است و لذا مشتاقانه منتظر دریافت نظریات، پیشنهادات و نقد و بررسی‌های مشفقانه و کارشناسانهٔ تمامی کنشگران این عرصه هستیم.

فصل نخست

دیپلماسی سایبری: مسائل، چالش‌ها و اهداف[1]

درآمد

بسیاری از کارشناسان روابط بین‌الملل و دیپلمات‌های حرفه‌ای با موضوع جدیدی به نام مسائل سایبری بین‌المللی یا دیپلماسی سایبری مواجه‌اند. این امر شامل سیاست فناوری اطلاعات و ارتباطات، امنیت سایبری بین‌المللی، گفت‌وشنودهای دوجانبهٔ سایبری، سیاست توسعه، مسائل اینترنتی، حقوق بشر در عصر سایبری، موضوعات تجارت و مالکیت معنوی و بسیاری از مسائل سیاسی دیگر است. این در حالی است که ابعاد و عناصر و مؤلفه‌های دیپلماسی سایبری همواره در حال تغییر بوده و به سرعت نیز در حال توسعه است.

این موضوع در ارتباط با فعالیت‌های دیپلمات‌ها، مسیر کاملاً جدید و تازه‌ای را پیش روی روابط بین دولت‌ها قرار داده است که طیف گسترده‌ای از ابزارهای سیاست خارجی را در بر می‌گیرد و نیز بسیاری از ذی‌نفعان داخلی و خارجی را شامل می‌شود. بنابراین، وظایف هماهنگ‌سازی

---

۱. نویسندهٔ اصلی این مقاله هلی تییرما کلار، اولین دیپلمات امنیت سایبری اتحادیهٔ اروپا و سفیر ارشد حوزهٔ سایبری در وزارت امور خارجهٔ کشور استونی، است. این مقاله به درخواست ایشان به عنوان مقدمه‌ای بر بحث «دیپلماسی سایبری» عیناً ترجمه شده است.

جدیدی برای وزارت‌های امور خارجه مطرح می‌شود که نیازمند دانش جامعی در زمینهٔ فناوری اطلاعات، امنیت رایانه و شبکه، حکمرانی اینترنت، امنیت بین‌المللی، جرایم سایبری، هوش سایبری و غیره است. حال آنکه همواره آکادمی‌های دیپلماتیک یا مدارس امور بین‌الملل به تمام این مباحث نمی‌پردازند. همچنین دیپلمات‌ها باید به سرعت بر اصول و مؤلفه‌های فضای سایبری اشراف یابند، زیرا این فضا به سرعت در حال تغییر و تحول است. این امر در حال حاضر اهمیت ویژه‌ای دارد، به این دلیل که دولت‌ها همواره مقامات ارشدی را به هدایت این روابط بین‌المللی تازه روی‌کارآمده منصوب می‌کنند. در آینده، در اختیار داشتن نسل جدیدی از دیپلمات‌های توانمند و آموزش‌دیده به منظور پیشبرد برنامه‌های بین‌المللی سایبری بسیار حائز اهمیت خواهد بود. در اینجا، به شفاف‌سازی دربارهٔ چالش‌ها و الزامات اصلی این حوزهٔ سیاسی، که به احتمال زیاد دیپلمات‌های آینده در طول فعالیت شغلی خود با آن مواجه خواهند شد، می‌پردازیم.

چنانچه از دست‌اندرکاران این حوزه دربارهٔ ماهیت دیپلماسی سایبری سؤال شود، به احتمال زیاد دیدگاه‌های متفاوتی ارائه خواهند داد. عده‌ای ادعا می‌کنند که عمدتاً آزادیِ بیان از طریق اینترنت است، برخی دیگر اظهار خواهند داشت که باید علیه جرایم سایبری مبارزهٔ جهانی صورت گیرد، حال آنکه برخی دیگر معتقدند که می‌بایست به قوانین جنگ سایبری بپردازیم. حقیقت امر آن است که یک دیپلمات سایبری موفق باید به طور هم‌زمان به بسیاری از موضوعات موازی اشراف داشته باشد، زیرا در موقعیت‌های مختلف کاری، باید با آگاهی از جنبه‌ها و ابعاد مختلف سیاست خارجی تصمیم‌گیری کنند.

از آنجا که در مراحل بسیار اولیهٔ شکل‌گیری سیاست خارجی سایبری به

سر می‌بریم، تنها تعداد محدودی از وزارت‌های امور خارجه دارای یک دفتر سایبری ویژه هستند. در اغلب وزارتخانه‌ها، حتی در صورتی که واحد سایبری ویژه‌ای در آن‌ها تأسیس نشده باشد، به مباحث سایبری در کنار امور روزمرهٔ دیگر، از جمله حقوق بشر، امنیت بین‌المللی، تهدیدات فراملّی و سایر موارد توجه می‌شود. چنانچه دولت‌ها تمایل داشته باشند تمام جنبه‌های حوزهٔ سایبری را تحت پوشش قرار دهند، در اختیار داشتن گروهی از دیپلمات‌های سایبری الزامی است. دارا بودن یک دفتر تخصصی با دانش کافی در زمینهٔ مسائل سایبری یک مزیت محسوب می‌شود، حال آنکه وجود هماهنگی افقی[1] کافی بین دیپلمات‌هایی که در موضوعات خاص و ژئوپلیتیک متبحرند، در حوزهٔ مسائل سایبری نیز حائز اهمیت است. یک ساختار هماهنگی سایبری افقی ایدئال باید شامل حقوق بشر، امنیت بین‌المللی، تجزیه و تحلیل اطلاعات، مسائل مربوط به تهدید جهانی و دیپلمات‌های جغرافیایی و چندجانبه[2] در وزارتخانه‌های امور خارجه باشد.

اولویت‌بندی مسائل مختلف سایبری بین‌المللی کار چندان آسانی نیست. عنصر اصلی سیاست خارجی همواره حمایت از حقوق و آزادی‌های اولیه بوده است و شروع از این نقطه منطقی به نظر می‌رسد. در دموکراسی‌های لیبرال، ترویج فعالیت‌های بین‌المللی یکی از اصلی‌ترین عناصر سیاست خارجی است که به صورت اینترنتی یا غیراینترنتی به دفاع از حقوق بشر کمک می‌کند. تنش ذاتی بین آزادی اینترنتی و الزامات امنیت سایبری موجب شده است که بسیاری از دولت‌ها، از جمله دولت‌های لیبرال دموکرات، دربارهٔ چگونگی استفاده از فناوری اینترنت به منظور به حداکثر رساندن میزان تأثیرگذاری بر رفاه جمعی، همراه با کمترین موارد

1. Horizontal Coordination
2. Geographical and Multilateral Diplomats

نقض حقوق اساسی، تصمیمات دشواری اتخاذ کنند. روند افزایشی سانسور و نظارت گسترده بر اینترنت مستلزم اقدام جمعی برای محکوم کردن رژیم‌های سرکوبگرِ آزادی بیان در رسانه‌های جدید است.

دیپلمات‌ها باید همواره در محافظت از اینترنت کوشاتر باشند. اینترنت آزاد و باز به‌خودی‌خود پدیدهٔ بخصوصی نیست و از ابتدای راه، توجه بسیاری از دست‌اندرکاران را به خود جلب کرده است. شبکهٔ جهانی وب به عنوان سکویی برای ارتباطات، در جوامع مختلف روی کار آمد و به یک زیرساخت مهم و اساسی در سراسر جهان تبدیل گشت که نحوهٔ ارتباط با افراد دیگر و تفکر و انجام امور و فرایندها را تغییر داد. تأثیر اینترنت به عنوان یک فناوری آزادی‌بخش، برای بسیاری از گروه‌های اجتماعی غیرممتاز و دورافتاده و کم‌سواد بسیار چشمگیر است و باید به شکل فعلی آن حفظ شود. اینترنت به دلیل نوآوری و همکاری داوطلبانهٔ نشئت‌گرفته از بخش خصوصی، بین گروه‌های غیردولتی و بخش مدنی بسیار موفقیت‌آمیز عمل کرده است. شرط اصلی تداوم این گونه نوآوری‌ها حفظ تأثیر نوآوری بخش خصوصی و محرک‌های جامعهٔ مدنی در الگوی فعلی حکمرانی اینترنت است. این موضوع نیز باید در سیاست خارجی در نظر گرفته شود.

دیپلمات‌ها هم‌زمان با ترویج اینترنت آزاد و حقوق بشر به صورت اینترنتی، باید به جامعه‌ای بپردازند که به اجرای قانون اهمیت زیادی می‌دهد و به افزایش سریع جرایم سایبری واقف است. مسئلهٔ حائز اهمیت دیگری که می‌تواند نگران‌کننده‌تر نیز باشد، جاسوسی سایبری مخفیانه با اهداف صنعتی است. تمامی این جوانب باید در طراحی گفتمان‌های سایبری و سیاست‌های سایبری بین‌المللی در نظر گرفته شوند؛ برای مثال، یک کشور نمی‌تواند در حوزهٔ امنیت سایبری با شرکای خارجی خود، که به نفوذ مخفیانه به رایانه‌ها و سرقت اسرار تجاری شهرت دارند، مشارکت کند.

همچنین دیپلمات‌ها باید در برنامه‌های اجرایی و عملیاتی خود، کشورهایی که از این ابزار برای سرکوبی آزادی بیان یا دستگیری وبلاگ‌نویسان ضد دولت بهره می‌جویند را مدنظر قرار دهند.

در پایان، تمام دیپلمات‌ها باید به خوبی با قوانین جنگ و درگیری در عرصهٔ جدید سایبری آشنایی داشته باشند. سرمنشأ نگرانی‌های امنیتی بین‌المللی در فضای سایبری این حقیقت است که کشورها همواره در حال تعیین قوانین و هنجارهای رفتاری در فضای سایبری هستند. نخستین چالش سایبری در حوزهٔ امنیت بین‌المللی، دستیابی به درک مشترکی از پارامترهای رفتاری دولت است. برخی طرح‌ها در دستیابی به این هدف همواره نقش مؤثری داشته‌اند، از جمله گزارش‌های گروه متخصصان دولتی سازمان ملل متحد در سال ۲۰۱۰ و ۲۰۱۳ یا کنفرانس جهانی فضای سایبری که از سال ۲۰۱۱ در لندن راه‌اندازی شد. در سازمان امنیت و همکاری اروپا[1] به منظور دستیابی به توافق در حوزهٔ اقدامات اعتمادسازِ مربوط به امنیت سایبری، فعالیت‌هایی در حال انجام است. جامعهٔ علمیِ دراین‌باره داده‌های ارزشمندی را، همچون راهنمای تالین، دربارهٔ کاربرد قوانین بشردوستانهٔ بین‌المللی[2] در جنگ سایبری ارائه کرده است. نخستین گام‌ها در تعیین هنجارها در دورهٔ غرب وحشی[3] فضای سایبری باید در مباحث سیاست‌های امنیتی بین‌المللی گنجانده شود. فعالیت‌های خطیری در راستای توافق دربارهٔ جزئیات نحوهٔ پیاده‌سازی اقدامات اعتمادسازی یا قوانین بشردوستانهٔ بین‌المللی در فضای سایبری صورت گرفته است؛ بنابراین بستر مناسبی برای توسعهٔ این فعالیت‌ها وجود دارد.

---

1. Organization for Security and Co-operation in Europe (OSCE)
2. International Humanitarian Law (IHL)
3. Wild West

یکی از مهم‌ترین اهداف سیاست‌گذاران ملی و بین‌المللی فضای سایبری همواره باید گنجاندن مسائل سایبری در حوزه‌های سیاست‌های موجود، از جمله امنیت داخلی، حفاظت از زیرساخت‌های اساسی، امنیت بین‌المللی و سیاست‌های حقوق بشر باشد. با توجه به تعدد عوامل داخلی و بین‌المللی در این حوزه ممکن است درک و مشارکت در تصمیم‌گیری دربارهٔ سیاست‌های سایبری برای دیپلمات‌ها بسیار چالش‌برانگیز باشد. در این مقاله ابتدا به شرح امنیت سایبری، که امروزه دولت‌ها با آن مواجه‌اند، پرداخته خواهد شد. سپس، پنج حوزهٔ اصلی فعالیت که سیاست‌های بین‌المللی می‌توانند در آنجا در زمینهٔ پاسخگویی به تهدیدات سایبری روزافزون مؤثر واقع شوند مطرح می‌گردد. هدف دیگر این مطالعه اشاره به اهمیت جریان مداوم سیاست‌های سایبری و چگونگی غلبه بر تمایل طبیعی انفکاک پروژه‌های سایبری کشورهاست. برای دستیابی به یک سیاست خارجی موفق در حوزهٔ سایبری، دیپلمات‌ها باید از هماهنگی سایبری ساختاریافته و ملی برخوردار باشند.

چالش‌های سیاست‌گذاری در عرصهٔ سایبری

پس از آنکه ویلیام هرشل[1] نور مادون قرمز را در سال ۱۸۰۰ کشف کرد، اکتشاف امواج الکترومغناطیسی پیشرفت روندهای فناورانه را تسهیل ساخت. توسعهٔ فیبر نوری برای ارتباطات از راه دور و فناوری رایانه‌ای، آغازگر عصر جدیدی بود که اکنون آن را انقلاب فناوری اطلاعات و ارتباطات[2] می‌نامیم. در حال حاضر، در عصری به سر می‌بریم که شاهد تغییر بزرگی در الگوی نگرش به انقلاب فناوری اطلاعات و ارتباطات و مدیریت فناوری در آینده است. در حالی که ابتدا، انقلاب فناوری اطلاعات و ارتباطات به عنوان

1. William Herschel
2. ICT Revolution

حرکتی مثبت و سودمند برای رشد اقتصادی در نظر گرفته می‌شد، در دههٔ ۱۹۹۰ با گسترش بدافزارها به عنوان یک تهدید و چالش جهانی برای صنایع و دولت‌ها، این تغییر الگو صورت گرفت. ممکن است در کتاب‌های تاریخی آینده از دههٔ ۲۰۰۰ ــ ۲۰۱۰ به عنوان یک نقطهٔ عطف تاریخی[1] یاد شود؛ هنگامی که بشر شاهد حملات سایبری حمایتگرانه برای پیشرفت‌های نظامی بود و از ابزارهای سایبری برای نخستین‌بار به منظور ایجاد اختلال و نابودی زیرساخت‌های فیزیکی بهره‌برداری شد.

در سال‌های ابتدایی فناوری اطلاعات و ارتباطات و اینترنت، این حقیقت که این پشتیبانی فنی نوین ممکن است به یک زیرساخت اساسی برای تمام اقتصادها و جوامع تبدیل شود قابل پیش‌بینی نبود. نقاط عطف بخصوصی دربارهٔ چگونگی توسعهٔ اینترنت و فناوری اطلاعات و ارتباطات به یک بستر مهم جهانی در پی معرفی نظام نام‌گذاری دامنه[2] و تجاری‌سازی اینترنت، انفجار محصولات نرم‌افزاری، رشد اقتصاد اینترنتی و سایر رویدادها وجود دارد که تمام این موارد نمایانگر وابستگی روزافزون به فناوری اطلاعات و ارتباطات است. توسعهٔ فناوری اطلاعات و ارتباطات در بخش خصوصی به سوی حمایت از استمرار مشاغل، تضمین دسترسی سریع به اطلاعات و اتصال پرسرعت سوق داده شده بود. با آنکه شرکت‌ها و دولت‌ها در حال توسعهٔ نظام‌های اطلاعاتی پیچیده‌ای بودند، غالباً در ابتدای امر به مسئلهٔ امنیت نمی‌پرداختند. اکنون متخصصان امنیت فناوری اطلاعات و ارتباطات بر این باورند که به دلیل پیچیدگی ساختار فناوری اطلاعات و ارتباطات در اکثر سازمان‌ها، دستیابی به امنیت صددرصد در هر یک از این نظام‌ها غیرممکن است. امروزه بهترین اقدام ممکن، شناسایی سریع بازدیدکنندگان ناخواسته در

---

1. Breaking Point
2. Domain Name System (DNS)

شبکه‌های رایانه‌ای است، زیرا همواره احتمال شکستن کدها و دسترسی غیرمجاز به هر یک از رایانه‌ها وجود دارد. متخصصان معتقدند که پیشگیری و دفاع تا حد زیادی با شکست مواجه شده و اکنون تمرکز اصلی متخصصان امنیت رایانه‌ای ردیابی و تفحص است. با وجود آنکه می‌بایست با پیشرفت‌های جدید فناوری به راه‌حل این مسئله دست یافت و این موضوع را در نشست‌های رمزنگاری و ریاضیات دانشگاهی بررسی کرد، سیاست‌گذاران همواره در شرایط فعلی فعالیت می‌کنند. حال آنکه سطح پایین امنیت فناوری اطلاعات و ارتباطات از ویژگی‌های فزایندهٔ این دامنهٔ ساخت بشر است.

با این حال، این تحولات رخ داده است و هرگز قادر نیستیم به زمان الواح سنگی، طومارهای کاغذی و ماشین‌های تحریر بازگردیم. کماکان کفهٔ رشد اقتصادی نشئت‌گرفته از فضای سایبری سنگین‌تر از کفهٔ نگرانی‌های امنیتی است و سیاست‌های امنیت سایبری به عنوان مسائل و دغدغه‌های اصلی رهبران ارشد ملی یا صنعتی محسوب نشده‌اند. میزان آگاهی عوام نیز از فضای سایبری و میزان وابستگی ما به آن و سیاست‌های داخلیِ به‌کارگرفته‌شده به منظور حفاظت از امنیت نظام‌های اطلاعاتی مهم بسیار ناچیز است.

اینترنت تنها جزء تشکیل‌دهندهٔ فضای سایبری نیست، بلکه از فناوری‌های مختلف، رایانه‌ها، تلفن‌ها، دستگاه‌ها، کابل‌های فیبر نوری، روترها[1]، نرم‌افزارها و ... تشکیل شده است که همگی در چرخهٔ توسعه‌ای ثابت و پرسرعت قرار دارند. دنیای فناوری توانسته است امکان اتصالات پرسرعت و روش‌های نوین دسترسی به اطلاعات و فرصت‌های شغلی زیادی را فراهم کند. فناوری اطلاعات و ارتباطات تمامی خدمات مهم و اساسی جوامع و اقتصاد، از جمله انرژی، ارتباط از راه دور، تأمین آب یا سیستم‌های کنترل هوا را تسهیل

1. Routers

می‌کند. امروزه تقریباً تمام خدمات ضروری به سیستم‌های اطلاعاتی وابسته‌اند و فناوری اطلاعات در همهٔ امور نفوذ یافته است. حتی بایگانی اسناد قرون وسطایی و همچنین پرونده‌های پزشکی و سایر اطلاعات شخصی حساس نیز در عصر حاضر دیجیتالی شده‌اند.

سیاست‌گذاران عمومی، با توجه به پیچیدگی مسائل فناوری، همواره در مرحلهٔ اولیهٔ شناخت نحوهٔ هدایت سیاست‌های امنیت سایبری ملی، محافظت از اسرار صنعتی یا دولتی و کمک به مقامات قانونی در مبارزه با جرایم سایبری به سر می‌برند. از آنجا که اکثریت قریب به اتفاق دارایی‌های مهم سایبری به بخش خصوصی تعلق دارد، هر گونه سیاست سایبری ملی موفقیت‌آمیز باید شامل همکاری تنگاتنگ دولتی ـ خصوصی و هماهنگی افقی بین بخش‌های صنعتی و ادارات دولتی باشد. حال آنکه هماهنگی سیاست سایبری ملی باید شامل مسائل سیاست خارجی و مسائل امنیتی نیز باشد. از آنجایی که سیاست‌های سایبری ملی همواره در حال شکل‌گیری است و دولت‌ها کماکان در جست‌وجوی یک قهرمان ملی برای هدایت فعالیت‌های سایبری هستند، سیاست خارجی به دشواری می‌تواند خود را در این زمینهٔ دشوار تثبیت کند. با توجه به فضای بین‌المللی حاکم که در آن تمامی اعلامیه‌های امنیت سایبری می‌بایست دربارهٔ حقوق بشر و سیاست‌های خارجی دیگر باشد، دیپلمات‌ها باید جزئی از محافل سیاست‌گذاری سایبری کشورها به شمار آیند. به طور کلی، دیپلمات‌ها باید محرک‌های مؤثری در سیاست سایبری باشند که دلایل آن در ادامه توضیح داده خواهد شد.

به احتمال زیاد، هر متخصص سیاست خارجی هنگام مواجهه با سیاست‌گذاران ملی با این بحث روبه‌رو می‌شود که هر حوزهٔ بخصوصی به شاخه‌ای از دانش تخصصی نیاز دارد که دیپلمات‌ها از آن بهره‌مند نیستند.

بنابراین، متخصصان هر حوزه باید تصمیمات لازم را أخذ کنند. این امر ممکن است در مباحث سایبری نیز صادق باشد که در آن همواره کنترل و ادارهٔ این حوزه از سیاست بر عهدهٔ جامعهٔ فنی ملی و وزارتخانه‌های مربوط است. به منظور تسهیل امور برای دیپلمات‌های فعال در این زمینه می‌توان این گونه استدلال کرد که چون عرصهٔ سایبری یک عرصهٔ مهم جهانی برای سایر فعالیت‌های بشری است، سیاست‌های جامع مربوط به مسائل سایبری به مشارکت متخصصان روابط بین‌المللی نیاز دارد. با توجه به اینکه مهندسان هسته‌ای در مذاکرات منع گسترش سلاح‌های هسته‌ای[1] نمایندهٔ دولت نیستند، کارشناسان فناوری نیز نباید به مسئلهٔ دیپلماسی سایبری بپردازند. همانند سیاست‌های سایبری داخلی، که طی آن مسائل سایبری باید در مدیریت بحران و محافظت از خدمات بحرانی مدنظر قرار گیرند، لازم است بنیان‌گذاران سیاست خارجی و دست‌اندرکاران امنیت ملی نیز مسائل سایبری را بیاموزند و آن‌ها را در فعالیت‌های معمول خود به کار گیرند.

به منظور قابل درک ساختن و شفاف‌سازی هر چه بیشتر عرصهٔ سایبری برای سیاست‌گذاران، برنامه‌ریزی سیاست‌های سایبری با در نظر گرفتن پیامدهای اختلال یا تخریب زیرساخت‌های سایبری یا ضرر اقتصادی ناشی از جرایم و جاسوسی سایبری مؤثر خواهد بود. پیشگیری و کاهش میزان خسارات و کاهش خطرات نظام‌مند در عرصهٔ سایبری مستلزم دخالت بنیان‌گذاران سیاست خارجی است. اساسی‌ترین نگرانی دیپلمات‌ها باید جلوگیری از عواقب احتمالی اختلال یا تخریب زیرساخت‌های اطلاعاتی در سطح جهانی و منطقه‌ای باشد. می‌توان انتظار داشت که تمامی عوامل مسئول بین‌المللی به دنبال جلوگیری از وقایع فاجعه‌بار عرصهٔ سایبری

1. Non-Proliferation Negotiations

باشند. با وجود این، از لحاظ نظری، برخی حملات سایبری ممکن است صدمات و آسیب‌هایی برابر با حملات جنبشی[1] به بار آورند. سازمان‌دهی درگیری منطقه‌ای و حملهٔ سیل‌آسا به همراه حملهٔ سایبری نقطه‌ای[2] یا حملهٔ فیزیکی به زیرساخت‌های اطلاعاتی، با هدف متضرر ساختن کشوری دیگر از لحاظ اقتصادی به دلایل سیاسی، قابل تصور است. چنانچه نظام مالی نیز به زیرساخت‌های اطلاعاتیِ حمله‌شده وابسته باشد، ممکن است موجب اختلالی جدی در خدمات مالی یک منطقه نیز بشود.

کشورهایی که از قابلیت دفاع سایبری متوسطی برخوردارند، نگرانی‌های بیشتری را تجربه می‌کنند، زیرا این رویکرد دوگانه سبب افزایش جرم و جنایت و نظامی‌سازی هر چه بیشتر حوزهٔ مربوط می‌شود. عدم تقارن کلی این حوزه، آسیب‌پذیری‌های غیرقابل‌قبولی برای سیستم‌های مهم اطلاعاتی خصوصی و عمومی ایجاد می‌کند. همچنین در درگیری‌های آینده ممکن است طی مبارزات نظامی یا در شرایطی دیگر، علیه زیرساخت‌های مهم یک کشور حملاتی سایبری صورت بگیرد. حملات سایبری‌ای که در جریان درگیری‌های مسلحانهٔ بین‌المللی اتفاق می‌افتند تحت نظارت حقوق بشردوستانهٔ بین‌المللی خواهند بود. در این شرایط، به منظور جلوگیری از تحت تأثیر قرار گرفتن افراد غیرنظامی، یافتن روش‌های مناسب یا محاسبهٔ تأثیرات ثانویهٔ کشورها باید از مقررات مربوط پیروی کنند. در واقع، عرصهٔ سایبری مباحث تازه‌ای را دربارهٔ نحوهٔ اعمال حقوق بشردوستانهٔ بین‌المللی ایجاد کرده است. بسیاری از وکلا بر این باورند که در زمینهٔ نظام‌مندسازی جنبه‌های بشردوستانهٔ یک درگیری، که موجب اختلال و آزار و اذیت افراد

---

1. Kinetic Attacks

۲. Surgical's Cyber Attack، حمله به هدفی مشخص است به طوری که هیچ گونه خسارتی به ساختارهای دیگر وارد نشود.

غیرنظامی در پی حملات سایبری شده، اما درگیری مسلحانه محسوب نمی‌شود، شکافی در حقوق بین‌المللی وجود دارد.

مسئلهٔ حل‌نشدهٔ دیگری نیز رویدادهای سایبری را، هم در زمان جنگ و هم در زمان صلح، پیچیده‌تر می‌کند. حتی در صورت موافقت کشورها با برخی هنجارها و قوانین، سهولت نسبی بهره‌برداری از بازیگران پراکسی[۱] می‌تواند آن‌ها را به انتخاب ابزار سایبری ترغیب کند. تا زمانی که کشورها در زمینهٔ نظارت بر جریان داده‌ها یا مبارزه با جرایم سایبری ضعیف عمل بکنند، چالش همچنان باقی است. به منظور کاهش تعداد پناهگاه‌های امن سایبری[۲] باید به صورت دسته‌جمعی وارد عمل شد.

طراحی سازوکارهای بین‌المللی برای روابط بین کشورها در زمینهٔ مسائل عرصهٔ سایبری عملاً به عهدهٔ عوامل سیاست خارجی خواهد بود. نخستین حرکت دیپلمات‌ها کاهش احتمال سوءتفاهم، سوء تفسیر و عدم اعتماد در روابط سایبری است. دیپلمات‌ها باید همراه با اجتماعات سایبری داخلی با هدف جلوگیری یا کاهش اختلالات سایبری بکوشند.

مسئلهٔ مهم سیاست امنیت ملی حمایت از زیرساخت‌های اساسی غیرنظامی است که احتمال دارد در درگیری‌های آینده بیشترین آسیب را متحمل شوند. در شرایطی که حدود ۸۰ ـ ۹۰ درصد زیرساخت‌های سایبری مهم متعلق به بخش خصوصی است، دولت‌ها باید در نظام‌های تاب‌آوری سایبری ملی[۳] سرمایه‌گذاری کنند. مشارکت‌های عمومی ـ خصوصی و چارچوب‌های مدیریت بحران در زمینهٔ امنیت سایبری باید به

---

۱. Proxy Actors، گروه‌ها و اشخاصی که به نیابت از یک کشور، علیه دولت‌ها اقدامات سایبری مخرب انجام می‌دهند.

2. Cyber Safe Heavens

3. National Cyber Resilience Systems

عنوان پاسخی به چشم‌انداز تهدیدهای تازه توسعه یابند. بخش خصوصی، برخی سازوکارهای مدیریت بحران سایبری را معرفی کرده است که تا کنون موفقیت‌آمیز بوده‌اند و دولت‌هایی که در آن‌ها بخش خصوصی نقش اصلی را به عهده دارد، نباید دخالت زیادی داشته باشند. جامعهٔ سیاست خارجی نیز می‌تواند در زمینهٔ اعتمادسازی بین ملت‌ها، ایجاد کانال‌های ارتباطی، و نشاندن احزاب مختلف بر سر میزهای مذاکره ایفای نقش کند؛ به ویژه جامعهٔ دیپلماتیک باید حساسیت بیشتری به حمایت از زیرساخت‌های مهم غیرنظامی در سراسر جهان داشته باشد. به منظور ایجاد پایگاه گسترده‌ای از قابلیت‌های سایبری غیرنظامی، وجود مکانیسم‌های پیشگیرانه و مدیریت بحران کارآمد، که ارکان یک نظام سایبری ملی را تشکیل می‌دهند، ضروری است. اغلب کشورهای پیشرفتهٔ سایبری پیشاپیش متوجه شده‌اند که تلاش‌های سنتی نظامی در درگیری‌های مدرن، که در آن فعالیت‌های گستردهٔ سایبری نقش اصلی را بازی می‌کنند، کافی نیستند. در مقابل، کشورهایی به دنبال سازوکارهای جدید مدیریت بحران‌های غیرنظامی و روش‌هایی برای سازمان‌دهی عوامل غیردولتی هستند که ممکن است نقش بنیادینی در درگیری‌های سایبری آینده داشته باشند.

عواقب ناشی از فعالیت‌های مخرب سایبری بیشتر از همه متوجه عوامل اقتصادی (شرکت‌ها و صنایع بخش‌های مختلف) است. فواید مالی، مجرمان سایبریِ صنعت بانکداری را به منظور تشکیل مراکز بازنشر اطلاعات امنیت سایبری و سرمایه‌گذاری بیشتر در جنبه‌های اعتباری، برای تأمین هزینه‌های جرایم سایبری، تجهیز کرده است. امروزه بسیاری از بخش‌های دیگر هم نفوذها و حملات مداومی را تجربه می‌کنند، زیرا جرایم سازمان‌یافته نیز به عرصهٔ سایبری راه یافته است. در صورتی که عوامل تحت حمایت دولت، که

دارای منابع اطلاعاتی قابل توجهی هستند، دربارهٔ شرکت‌های فعال در حوزهٔ خدمات‌رسانی تفحص کنند به کمک‌های بیشترِ دولت نیازمندند. به منظور تسهیل جرایم سنتی از ابزارهای سایبری به طور فزاینده‌ای استفاده می‌شود. اکثر شرکت‌های بزرگ در زمینهٔ حمایت سایبری سرمایه‌گذاری‌های گسترده‌ای انجام می‌دهند و خطر بروز جرایم سایبری را پذیرفته‌اند. حال آنکه شرکت‌های معدودی آمادگی افشای خسارات واقعی ناشی از حملات سایبری را دارند. این امر در طولانی‌مدت اثر بومرنگی یا بازگشتی دارد، زیرا در دسترس نبودن اطلاعات معتبر دربارهٔ جرایم سایبری مانع از واکنش سهامداران و سیاست‌گذاران عمومی در مواجهه با این تهدیدات روزافزون می‌شود.

کارشناسان قانونی از نظام سرمایه‌گذاری ناکافی در این حوزه که مبارزه با جرایم سایبری سازمان‌یافته را دشوارتر می‌کند شکایت دارند. از آنجا که «بو کشیدن» یا «لمس کردن» جرایم سایبری که در شبکه‌های رایانه‌ای صورت می‌گیرند دشوار است، مقامات دولتی از تأیید و واکنش به این تهدید جدید عقب مانده‌اند. در بیشتر کشورها، مسئولان اجرای قانون برای ردیابی جرایم سایبری روزافزون سخت در تلاش‌اند. شرکت‌های کوچک‌تر بیشترین خسارت را متحمل می‌شوند، زیرا از منابع کافی برای به‌روزرسانی سامانه‌های دفاع سایبری خود برخوردار نیستند. جنایتکاران با افزایش درآمدهای حاصل از جرایم سایبری جهانی سازمان‌یافته‌تر می‌شوند و ضرر اقتصادی ناشی از آن در طولانی‌مدت تهدیدی جدی برای دولت‌ها خواهد بود. دولت‌ها برای مبارزه با جرایم سایبری که تهدیدی برای امنیت داخلی و ملی و اقتصادی همهٔ کشورها محسوب می‌شوند، نیازمند قابلیت‌های خطیر ملی هستند.

هیچ یک از سازوکارهای ملی دولت‌ها در صورت بروز بحران سایبری گسترده یا در مبارزه با جرایم سایبری سازمان‌یافتهٔ بین‌المللی به تنهایی کافی

نیست. پرداختن به این نوع جرایم سایبری چالشی است که به وضوح به سطح نگران‌کننده‌ای رسیده است و باید جامعهٔ سیاست خارجی به آن توجه کند. به منظور اطمینان یافتن از وجود یک چارچوب قانونی مطلوب برای رسیدگی به جرایم سایبری در خارج از جهانِ توسعه‌یافته باید ارتقای کنوانسیون جرایم سایبری شورای اروپا[1] در فعالیت‌های دیپلماتیک گنجانده شود.

جاسوسی سایبری با اهداف اقتصادی، چالش دیگری را برای دولت‌ها از جمله دیپلمات‌ها به وجود آورده است. انتقال خاموش مالکیت معنوی ممکن است این خطر را در قالب جرایم سایبری ساده متوجه رونق اقتصادی کند. این امر به وضوح زمینهٔ دیگری است که در آن دخالت دیپلماتیک برای تأیید رفتار دولت که موجب تعیین هنجارهای عرصهٔ سایبری می‌شود ضرورت دارد. یقیناً درگیری‌های سایبری و دیگر موضوعات تهدیدآمیز بیشتر متوجه دیپلمات‌هایی است که در زمینهٔ رسیدگی به مسائل سیاستِ امنیتی آموزش دیده‌اند. بنابراین، دیپلمات‌ها نیز باید حمایت از مالکیت معنوی به صورت آنلاین و برخی دیگر از مسائل اقتصادی مرتبط با عرصهٔ سایبری را به خوبی بشناسند. کارشناسان حوزهٔ تجارت به طور فزاینده‌ای با موانع ناعادلانه‌ای در بازار مواجه هستند که برخی کشورها با تعیین استانداردهای محصولات حوزهٔ فناوری اطلاعات و ارتباطات در زمینهٔ امنیت ملی سبب ایجاد آن شده‌اند. این استانداردها برای جلوگیری از دسترسی بازار به تولیدکنندگان خارجی اعمال می‌شوند. در اینجا نیز اطلاع‌رسانی به دیپلمات‌ها از طریق مذاکرات تجاری مربوطه ضرورت دارد.

تحولات سایبری فعلی، عرصهٔ ناشناختهٔ دیگری را برای دیپلمات‌ها مطرح می‌سازند که همان حکمرانی اینترنت است. این حوزهٔ پیچیدهٔ

---

1. Council of Europe (CoE)

نوآوری‌ها و انجمن‌ها عمدتاً متعلق به فناوران است. اما توجه جامعهٔ سیاست خارجی باید هر چه بیشتر به این حوزه معطوف گردد، زیرا چندین کشور الگوی چندذی‌نفعی فعلی حکمرانی اینترنت را تحت فشار قرار داده‌اند. اختلافات دربارهٔ حاکمیت ملی رو به افزایش است و دیپلمات‌ها باید در حل‌وفصل این اختلاف در مجامع بین‌المللی نقش بسزایی داشته باشند.

دیپلمات‌ها همچنین باید به روندهای آتی تحولات سایبری توجه داشته باشند. آمادگی سایبری دولت‌ها در آینده به موضوع اصلی تصمیمات تجاری بدل خواهد شد. قابلیت‌های سایبری قدرتمند ملی عامل بازدارندهٔ مهمی برای مجرمان سایبری خواهد بود و ارائهٔ بسترهای امن به ایجاد یک فضای تجاری مناسب‌تر کمک خواهد کرد. بخش خصوصی ممکن است به دنبال آمادگی ملی امنیت سایبری در زمینهٔ راهبردهای سرمایه‌گذاری آتی باشد. کشورهایی که شاخص سایبری ضعیفی دارند مناسب نخواهند بود. به نوعی، امنیت سایبری می‌تواند به بخشی از سیاست اقتصادی خارجی برای جذب سرمایه و استعداد تبدیل شود. اگرچه دست‌اندرکاران خصوصی باید بیشتر اقداماتِ تاب‌آوری را انجام دهند، اما دولت‌ها بایستی توانایی شایان خود را در واکنش به تهدیدات سایبری نظام‌مند تضمین کنند. توسعهٔ ساختارهای هشدار و مشاورهٔ زودهنگام بین‌المللی و منطقه‌ای در زمینهٔ امنیت سایبری مسئلهٔ درازمدت دیگری است که دولت‌ها با آن روبه‌رو خواهند شد. این امر بدون دخالت جوامع دیپلماتیک سراسر جهان میسر نمی‌شود.

در حال حاضر، تعداد کشورهایی که در آن‌ها هماهنگی سایبری ملی کارآمد بوده است و قادر به ارائهٔ نظر یکپارچه و متحدانهٔ خود در تمامی مجامع بین‌المللی‌اند، بسیار محدود است. چالش‌های معمولی که تمامی دیپلمات‌ها با آن روبه‌رو هستند عبارت‌اند از: چالش ساختاری هماهنگی

سیاست ملی ضعیف، عدم همکاری و ارتباط[1] نهادی سیاست سایبری، سردرگمی و ابهام میان‌بخشی در خصوص رهبری ملی، آژانس‌های قدرتمند داخلی که نظریات سیاست خارجی را مردود شمرده‌اند و مدنظر قرار نمی‌دهند و همچنین نبود ژنرال‌های سایبری که قادر به تفسیر و شفاف‌سازی اصطلاحات فنی برای دیپلمات‌ها هستند. چنانچه دولت دارای راهبرد، سایبری ملی نداشته نباشد و هیچ گونه هماهنگی سایبری ساختاری در آن وجود نداشته نباشد، ارائهٔ گزینه‌های سیاسی آگاهانه برای جامعهٔ سیاسی بسیار دشوار خواهد بود. تدوین یک راهبرد ملی امنیت سایبری و ایجاد چارچوبی برای هماهنگی سایبری که بخش‌های اصلی دولت بتوانند در آن ایفای نقش کنند، فرایندی ضروری برای تمامی ملت‌هاست.

دیپلمات‌ها باید به طور منظم نظریات خود را با سیاست‌گذاران ملی حوزهٔ سایبری، واحدهای جنایی با فناوری پیشرفته، وکلا، آژانس‌های محافظت از زیرساخت‌های اطلاعاتی اساسی، مسئولان پاسخگویی به حوادث سایبری ملی و تحلیلگران اطلاعاتی هماهنگ سازند تا به یک دیدگاه کلی و درک درست از این حوزهٔ درحال‌توسعه دست یابند. همچنین این افراد، جدا از جزئیات عملکرد، به منظور شناسایی و تشخیص استدلال‌های سطحی ارائه‌شدهٔ سایر کشورها در مجامع بین‌المللی باید از نحوهٔ عملکرد فناوری آگاهی پیدا کنند، و نیز باید از روند تنظیم مقررات سایبری ملی و توسعهٔ تهدیدات سایبری در سطح جهان اطلاع داشته باشند. دیپلمات‌های سایبری نیز مانند دیپلمات‌های هسته‌ای باید آثار ابزارهای سایبری مخرب و نحوهٔ استفاده از زیرساخت‌های اساسی را برای فلج کردن و از کار انداختن کشورها در درگیری‌های پیش رو به خوبی بشناسند. کمال مطلوب آن است که جامعهٔ سیاست خارجی بتواند

---

1. Silfication

سالانه در بخشی از فعالیت‌های سایبری ملی مشارکت داشته باشد و از روش‌های حملات سایبری گستردهٔ بین‌المللی آگاهی پیدا کند.

از آنجا که در حال حاضر در جهانی به سر می‌بریم که در آن سیاست‌های سایبری همواره در حال رشدند و اکثریت کشورها تا به حال نتوانسته‌اند به یک راهبرد سایبری ملی جامع دست یابند، ممکن است از نظر جامعهٔ سیاست خارجی، به استحکام رسیدن در این عرصه دشوار باشد. حال آنکه برای آیندهٔ فضای سایبری آزاد و بدون حاشیه، فعالیت هر چه بیشتر دیپلمات‌ها در این زمینه ضرورت دارد. مدت‌زمان مدیدی است که جامعهٔ فنی هدایت تحولات بین‌المللی این حوزه را به عهده دارد. اکنون زمان آن فرارسیده است که هر دو سیاست‌های سایبری داخلی و بین‌المللی را در بستر راهبردی روابط بین‌الملل، تحولات اقتصادی بین‌المللی و امنیت ملی قرار دهیم. بدین منظور به تصمیم‌گیرندگان ارشد ملی، دیپلمات‌ها، وکلا و سایر جوامع غیرفنی نیازمندیم تا هر چه سریع‌تر در این زمینهٔ سیاسی جدید به آگاهی دست یابند و مشارکت در مباحث سایبری را در عرصهٔ جهانی از سر گیرند.

دستور کار فعلی روابط سایبری بین‌المللی

با توجه به آنچه در بالا به آن اشاره شده و نیز چشم‌اندازی که از تحولات مربوط به دنیای سایبری وجود دارد، پنج محور ذیل را می‌توان به عنوان مهم‌ترین دستور کار دیپلماسی سایبری، با تأکید بر نقشی که دیپلمات‌ها باید در آن ایفا کنند، پیشنهاد داد:

- **امنیت بین‌المللی و اعتمادسازی در عرصهٔ سایبری**

اعتماد و اطمینان مقوله‌های کمیابی در عرصهٔ سایبری هستند. در این حوزه