سیاست‌های صنعتی و نقش دولت در صنایع امنیت سایبری

قربانعلی مهربانی [۱]

[۱] دکتری مدیریت راهبردی، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران
a.mehrabanii54@gmail.com

چکیده

موضوع امنیت سایبری و توسعه این صنعت، بیش از پیش موردتوجه است. توسعه بازار و محصولات حوزه امنیت، به گسترش این صنعت انجامیده است و در کشورهای مختلف، سیاست‌های صنعتی گوناگونی تدوین شده است. هدف تحقیق کنونی بررسی سیاست‌های صنعتی و نقش دولت در صنایع امنیت سایبری است. روش تحقیق از نوع کتابخانه‌ای و مروری است و با جستجوی کلیدواژه‌های مرتبط مثل امنیت سایبری، سیاست‌های صنعتی در پایگاه‌های نمایه‌ساز معتبر، ادبیات مربوطه استخراج گردید. نتایج نشان داد که سیاست‌های صنعتی در امنیت سایبری شامل ایجاد بازار، تسهیل بازار، اصلاح بازار، ممنوعیت بازار و جایگزینی بازار است. همچنین مداخله دولت در این صنعت می‌تواند به پیامدهای داخلی، شکست در طراحی و شکست در اجرا منجر شود. تحقیقات مختلف نشان داد که رویکرد کشورهای مختلف در توسعه صنعت امنیت سایبری متفاوت بوده و بسته به شرایط، دیدگاه ویژه‌ای به این صنعت و توسعه بازار و محصولات آن دارند.

کلمات کلیدی: امنیت سایبری، صنعت سایبری، سیاست‌های صنعتی، بازار امنیت سایبری، محصولات سایبری.

۱ مقدمه

در سال‌های اخیر با رشد و توسعه زیرساخت‌های سایبری کشور موضوع امنیت فضای سایبری بیش‌ازپیش موردتوجه قرارگرفته است. به بیان دیگر امنیت زیرساخت‌های حیاتی و اطلاعاتی می‌بایست متناسب با رشد و توسعه سایبر پایه شدن سازمان‌ها و نهادها و فرآیندهای متنوع اداره عمومی کشور صورت پذیرد. این مهم طی سال‌های اخیر همراه با تأسیس شورای‌عالی فضای مجازی توسط رهبر معظم انقلاب اسلامی همواره مورد تأکید قرارگرفته است، تدوین اسناد ملی و راهبردی متنوع در حوزه امنیت فضای سایبر از قبیل: سند راهبردی افتا، سند نظام مقابله، سند هویت معتبر و ... که همگی حاکی از ضرورت نگاه راهبردی جامع آینده‌نگر و پیش کنش‌گرایانه به مقوله امنیت فضای سایبر است. به‌گونه‌ای که در برنامه ششم توسعه حداقل ۱۵ درصد پروژه‌های ICT کشور به حوزه امنیت تخصیص‌یافته است.

مطالعه سیاست‌ها و برنامه‌های سایر کشورها در زمینه امنیت سایبری می‌تواند به شناخت بهتر این بازار بزرگ و اتخاذ تصمیمات بهینه خواهد شد.

۲ مبانی نظری

در میان انواع تحولات حاصل از به‌کارگیری فناوری‌های انقلاب صنعتی چهارم و پیامدهای مثبت آن [۱]، می‌توان گفت که در بعد دیگر، امنیت سایبری به عنوان یک تهدید امنیت ملی و منبع خطرات ژئوپلیتیکی در دو دهه گذشته مطرح شده است. به‌عنوان‌مثال، موارد نقض داده‌ها در طول زمان در حال افزایش بوده است، از سال ۲۰۰۵ تا ۲۰۱۸۱۲ بیش از سه برابر شده است و هزینه‌ای بین ۵۷ تا ۱۰۹ میلیارد دلار برای هر سال داشته است. بر اساس برخی از برآوردهای محافظه‌کارانه‌تر. برخی معتقدند که هزینه‌های اقتصادی و اجتماعی انواع مختلف جرایم سایبری می تواند به تریلیون‌ها دلار برسد، درحالی‌که پیش‌بینی می شود بازار جهانی امنیت سایبری تا سال ۲۰۲۷ به بیش از ۳۴۰ میلیارد دلار افزایش یابد. با ادامه گسترش اقتصاد دیجیتال، این خطرات همچنان به رشد خود ادامه خواهند داد و نیازمند شناسایی مناسب آنها برای ایجاد پاسخ‌های متقابل مناسب است [۲]. یافته‌های کلیدی از ادبیات تأکید می‌کند که اقدامات امنیت سایبری قوی اعتماد و وفاداری مشتری را افزایش می‌دهد، تمایز بازار را امکان‌پذیر می‌سازد، به طور یکپارچه با اهداف راهبردی کسب‌وکار ادغام می‌شود، نوآوری را تقویت می‌کند و انطباق با استانداردهای نظارتی را تضمین می‌کند. راهبردهایی مانند ارتباطات شفاف در مورد تلاش‌های امنیت سایبری، توسعه راه‌حل‌های امنیتی سفارشی، ادغام ارزیابی‌های ریسک امنیت سایبری در برنامه‌ریزی راهبُردی، و سرمایه‌گذاری در تحقیق و توسعه امنیت سایبری به‌عنوان ابزاری مؤثر برای استفاده از امنیت سایبری برای مزیت رقابتی برجسته می‌شوند [۳]. دولت‌ها در سراسر جهان به شکست‌های بازار در صنایع امنیت سایبری داخلی خود به روش‌های مختلف پاسخ داده‌اند. برای مثال، مقررات امنیت سایبری ایالات متحده در حال حاضر پراکنده است و قادر به ایجاد تغییرات معنادار نیست. باتوجه‌به مجموعه قوانین فدرال امنیت سایبری فدرال، شکاف حاکمیتی نامطلوب در امنیت سایبری ایالات متحده، و تلاش های بخش خصوصی برای توسعه بهترین شیوه‌های امنیت سایبری و هنجارهای صنعت بیانگر نیاز به بررسی‌های بیشتر در زمینه نقش دولت است. اجرای نوعی مشوق مالیاتی برای تقویت امنیت سایبری، به‌عنوان یک گزینه، می‌تواند برای بهبود بازار امنیت سایبری باشد [۴].در ادامه انواع سیاست‌های صنعتی و مداخلات دولت توضیح داده شده است.

۱.۲ سیاست‌های صنعتی دولت‌ها در صنایع امنیت سایبری

۱.۱.۲ ایجاد بازار

سیاست صنعتی برای ایجاد بازار شامل استفاده از سیاست‌های عمومی برای ایجاد بازارها از طریق ایجاد حقوق، انگیزه‌ها و فرصت‌هایی برای مبادله است که در غیر این صورت وجود نداشت [۵]. در بسیاری از کشورها، دولت‌ها با تبدیل‌شدن به مشتریان اصلی (و گاهی اوقات، اولیه) کالاها و خدمات مرتبط با امنیت سایبری، نقش مهمی در ایجاد بازارهای امنیت سایبری داخلی دارند. در چین، دولت تنها مشتری محصولات

امنیت سایبری است که توسط نهادهای حمایت‌شده دولتی ایجاد می‌شوند. در فرانسه، شاهد استفاده از فرآیندهای تدارکات هماهنگ با تمرکز بر ایجاد قابلیت‌های بومی هستیم – که به‌عنوان یک «راه‌حل مستقل» برای چالش‌های امنیت سایبری تصور می‌شود. این موارد در Loi de Programmation Militaire-LPM 2014-2019 (قانون برنامه‌ریزی نظامی [۱]) گنجانده شده است. این سیاست‌ها نشان‌دهنده سنت دیرینه دولت فرانسه در کمک‌های عمومی قابل‌توجه در توسعه بازار فناوری اطلاعات این کشور است. در ایالات متحده، دولت و ارتش مصرف‌کنندگان عمده (اگرچه نه‌تنها) کالاها و خدمات مرتبط با امنیت سایبری هستند و دارای بازوهای سرمایه‌گذاری خطرپذیر مرتبط با دولت هستند که به حفظ عرضه این خدمات از طریق تأمین سرمایه برای توسعه مستمر اختصاص‌داده‌شده‌اند [۶].

۲.۱.۲ تسهیل بازار

اقدامات تسهیل‌کننده بازار شامل سیاست‌هایی است که با کاهش هزینه‌های مبادله، افزایش انگیزه‌ها یا درونی‌سازی مزایا و هزینه‌ها، عملکرد بازارها را ارتقا یا بهبود می‌بخشد. در ایالات متحده، شتاب‌دهنده فناوری امنیت ملی (NSTXL) [۲] که برای تأمین بودجه اولیه برای فناوری‌هایی که توسط ارتش و جامعه اطلاعاتی به‌عنوان وعده‌دار تلقی می‌شوند، طراحی‌شده است، به‌عنوان نمونه‌ای از سازوکار تسهیل‌کننده بازار طراحی‌شده برای ارائه فناوری اطلاعات به بازار عمل می‌کند. سریع‌تر. «دستورالعمل‌های تدارکات نوآوری بومی [۳]» پکن به طور مشابه به دنبال تقویت بازار امنیت سایبری داخلی در چین با ایجاد انگیزه برای سازمان‌های دولتی برای تبدیل‌شدن به مشتریان اصلی شرکت‌های امنیت سایبری بومی بود[۷]. در فنلاند، گریفیث (۲۰۱۸) ارائه یک سیستم نظارت و هشدار را مشاهده کرد که اطلاعات کلیدی تهدید را برای استفاده توسط کسانی که به دنبال ایمن‌سازی سیستم‌های خود و همچنین سرمایه‌گذاری در تحقیق و توسعه هستند، ارائه می‌دهد [۸]. از سوی دیگر، ژاپن از سیاست مالیاتی خود از طریق «سیستم مالیاتی تقویت پایگاه اطلاعاتی [۴] » برای ارائه یارانه به شرکت‌های امنیت سایبری استفاده کرده است [۹].

۳.۱.۲ اصلاح بازار

سیاست صنعتی اصلاح‌کننده بازار از مقررات برای تغییر رفتار موضوع‌ها، اشیا، رسانه یا شرایط مبادله استفاده می‌کند تا نتایجی متفاوت از نتایجی که بازار در غیر این صورت ایجاد می‌کند ایجاد کند. در مورد ایالات متحده، تلاش‌ها برای تنظیم صنعت و مصرف‌کنندگان از طریق قانون به‌اشتراک‌گذاری اطلاعات امنیت سایبری (CISA) [۵] و قانون امنیت اطلاعات و حفاظت از اشتراک‌گذاری سایبری (CISPA) [۶] به‌عنوان نمونه‌هایی از این نوع رویکرد عمل می‌کنند. در فرانسه، نمونه‌هایی شامل طرح سایبری صنعتی و ایجاد اشتراک‌گذاری

[1] Military Programming Law
[2] National Security Technology Accelerator (NSTXL)
[3] Indigenous innovation procurement guidelines
[4] Information Base Strengthening Tax System
[5] Cybersecurity Information Sharing Act (CISA)
[6] Cybersecurity Intelligence and Sharing Protection Act (CISPA)

اطلاعات داوطلبانه (CERT-FR)[۷] است که سازوکار گزارش‌دهی و بهترین شیوه‌ها را در بین شرکت‌ها به اشتراک می‌گذارد، حمایت مالی دولت از تمرین‌های مدیریت بحران (Piranet) شامل بخش خصوصی، و طرح‌های صدور گواهینامه عمومی برای شرکت‌ها و افراد برای نشان‌دادن تخصص موضوع [۱۰]. سازوکارهای اصلاح بازار خود فنلاند شامل الزامات قانونی، قطعنامه‌های دولتی، پلتفرم‌های همکاری داوطلبانه، انجمن‌هایی برای ایجاد تفاهم مشترک، و مشارکت‌های عمومی و خصوصی است [۸]. در سطح اتحادیه اروپا، کمیسیون اروپا قوانین مربوط به حفظ داده‌ها و استانداردسازی دستورالعمل‌های امنیت سایبری را تدوین کرده است و مانند فرانسه، تلاش‌هایی را برای ایجاد یک طرح صدور گواهینامه برای شرکت‌های امنیت سایبری انجام داده است [۱۱].

۴.۱.۲ ممنوعیت بازار

سیاست صنعتی که رفتار خاص در یک بازار را منع می‌کند، شامل اقدامات دولتی است که تلاش می‌کند رفتارهای خاص را ممنوع کند. واپایش‌های صادرات و قوانین تدارکات شاید واضح‌ترین استفاده از ابزارهای بازدارنده بازار باشد که توانایی شرکت‌های امنیت سایبری داخلی را برای مشارکت در بازارهای بین‌المللی محدود می‌کند. به‌عنوان‌مثال، ایالات متحده واپایش صادرات را در قانون واپایش صادرات تسلیحات، مقررات شدآمد بین‌المللی اسلحه و مقررات اداره صادرات گنجانده است، درحالی‌که بریتانیا به‌عنوان بخشی از راهبُرد صادرات امنیت سایبری و راهبُرد امنیت سایبری ملی خود این کار را انجام می‌دهد. اتحادیه اروپا همچنین به پیشبرد برنامه‌های خود برای اعمال واپایش‌های صادراتی بر روی فناوری‌های مرتبط با نظارت سایبری ادامه می‌دهد که باعث ناراحتی BAE Systems و سایر شرکت‌های خصوصی در بخش سایبری می‌شود که باید با دولت مربوطه ارتباط برقرار کنند تا فروش فناوری مناسب را تعیین کنند و بالقوه ضرر کنند. مشتریان خارج از کشور به رقبای خارجی [۱۱].

۵.۱.۲ جایگزینی بازار

سیاست‌های جایگزین بازار شامل ایجاد بازارهایی از سوی دولت می‌شود که در آن بازار خصوصی وجود نداشت. در چین، ما شاهد سیاست‌هایی از بالابه‌پایین بوده‌ایم که شامل شناسایی «صنایع استراتژیک[۸]» و قهرمانان ملی مرتبط با آن‌ها می‌شود [۷]. با استفاده از رویکرد کمتر مستقیم، ژاپن سرمایه‌گذاری مستقیم را از سازمان‌های دولتی به شرکت‌ها از طریق ارائه مستقیم خدمات به‌عنوان خدمات عمومی به شرکت‌هایی مانند برنامه حذف ربات و مرکز پاک سایبری ارائه می‌دهد که دو نمونه از این رویکرد را ارائه می‌دهد که در آن دولت ژاپن مستقیماً ارائه می‌کند. خدمات به صنعت خصوصی [۹]. در ایالات متحده، In-Q-Tel یک سرمایه‌گذار متمرکز بر دولت که بر سرمایه‌گذاری‌های مربوط به فناوری‌های نظامی و اطلاعاتی متمرکز است، جایگزین شرکت‌های سرمایه‌گذاری خطرپذیر می‌شود، درحالی‌که برنامه‌های مختلف مرتبط با سرمایه انسانی به آموزش امنیت سایبری، ازجمله راهبُرد نیروی کار فدرال امنیت سایبری، یارانه می‌دهند. ابتکار ملی برای

[7] Cyber Plan and the creation of a voluntary information-sharing (CERT-FR)
[8] strategic industries

آموزش فضای سایبری، سایبر کورپس، و برنامه‌های کمک‌آموزشی و آموزشی امنیت سایبری [۶] (CETAP). فنلاند و بریتانیا همچنین برای رشد نیروی کار امنیت سایبری مربوطه خود از طریق ابتکارات مختلف، ازجمله برنامه‌های کارشناسی‌ارشد و برنامه‌های حرفه‌ای مانند مهارت‌های دیجیتال برای اقتصاد بریتانیا و آکادمی بازآموزی سایبری [۸][۱۲] تلاش می‌کنند. هر یک از این سیاست‌های صنعتی در سایه روابط دولت–جامعه ساخته‌شده‌اند که در آن سازمان‌های دولتی مختلف سیاست‌هایی را در چارچوب سیاست‌های بوروکراتیک، با ورودی‌ها و چالش‌های بازیگران اجتماعی ازجمله کارگران، مصرف‌کنندگان، گروه‌های ذی‌نفع و شرکت‌های فناوری اطلاعات ایجاد و اجرا می‌کنند. درواقع، هر یک از مقالات این شماره ویژه به این نتیجه می‌رسد که تنوع در انواع سیاست‌های صنعتی به‌کارگرفته‌شده توسط دولت‌های مختلف، تا حدی نشان‌دهنده روابط متمایز دولت–جامعه در هر کشور است.

۲.۲ اجرای سیاست‌های صنعتی دولت‌ها در صنایع امنیت سایبری

پس از تشریح شکست‌های بازار و تعدادی از پاسخ‌ها به این شکست‌های بازار در هر مورد، اکنون به طور خلاصه به اجرای این سیاست‌های صنعتی می‌پردازیم. درحالی‌که هنوز خیلی زود است که به طور قطعی نتیجه‌گیری کنیم که کدام سیاست‌ها مؤثر بوده و کدام نه ارزش دارد که عواقب مداخله در بخش فناوری اطلاعات را در نظر بگیریم [۶].

۱.۲.۲ پیامدهای داخلی مداخله

با استفاده از مفهوم شکست بازار، مطالعات موردی اثرات مقررات بر بخش امنیت سایبری در کشورهای مختلف را در نظر می‌گیرند. به طور خاص، نگران معیارهایی هستیم که توسط دولت‌ها برای ایجاد و تصویب خط‌مشی عمومی استفاده می‌شود، شکست‌های بالقوه طراحی سیاست صنعتی، و چالش‌های مرتبط با اجرای سیاست صنعتی. در بخش زیر، معیارهایی را در نظر می‌گیریم که نویسندگان از طریق آن‌ها پیامدهای سیاست صنعتی را ارزیابی می‌کنند. باتوجه‌به اینکه سیاست صنعتی نشان‌دهنده یک فرآیند ذاتی سیاسی است که در آن بازیگران برنده و بازنده می‌شوند، لازم است معیارهایی برای سیاست‌های صنعتی موفق در بخش امنیت سایبری در نظر گرفته شود. ارزیابی کارایی سیاست صنعتی لزوماً مستلزم درنظرگرفتن هزینه‌های انطباق از سوی بازیگران اقتصادی و هزینه اجرای آن برای بازیگران دولتی است. درنهایت، هر یک از موارد، اثرات سیاست‌های صنعتی بر ثبات اقتصادی و رشد کلی اقتصادی را در نظر می‌گیرد. کشورهایی که به دنبال رشد بخش امنیت سایبری هستند، با چالش اعمال سیاست‌های صنعتی که مانع رشد اقتصاد گسترده‌تر از طریق مقررات و استانداردهای سخت‌گیرانه امنیت سایبری نمی‌شوند که داده‌ها و فعالیت‌های اینترنتی را ایمن‌تر می‌کنند، مواجه هستند [۶].

۲.۲.۲ شکست‌های طراحی

پس از تشریح معیارهایی که از طریق آن‌ها می‌توان سیاست‌های صنعتی را ارزیابی کرد، اکنون به بحث در مورد شکست‌های طراحی مرتبط با سیاست صنعتی می‌پردازیم [۵]. دلایل مختلفی برای شکست طراحی وجود

دارد. اول، دامنه شکست بازار ممکن است به‌درستی ارزیابی نشود. به‌عنوان‌مثال، در بازار امنیت سایبری ایالات متحده، نیازهای سرمایه انسانی بازار به‌قدری قابل‌توجه است که سیاست‌های موجود طراحی‌شده برای رفع کمبود ناکافی است. دوم، این سیاست ممکن است عواقب پیش‌بینی‌نشده یا عوارض جانبی ناخواسته داشته باشد. سوم، ممکن است یک اشتباه محاسباتی در پیش‌بینی هزینه‌ها و منافع یک سیاست صنعتی رخ دهد. درواقع، توزیع‌های متفاوتی از هزینه‌ها و منافع سیاست‌های صنعتی در میان انواع مختلف بازیگران اقتصادی وجود دارد.

علاوه بر این، هزینه‌های انطباق و هزینه‌های اجرایی باید در نظر گرفته شود و درنهایت، شکست در طراحی یک پاسخ نظارتی کافی به شکست بازار ممکن است حیاتی باشد. چندین نمونه وجود دارد که در این دسته آخر قرار می‌گیرند. رژیم‌های اشتراک‌گذاری اطلاعاتی که شرکت‌ها تمایلی به امضای آن‌ها ندارند، و اغلب علیه آن لابی می‌کنند، به‌عنوان نمونه‌ای از چالش‌های طراحی پیش روی تنظیم‌کننده‌های دولتی عمل می‌کنند، زیرا الزامات ایجاد یک پاسخ مشترک به حملات سایبری خاص از شرکتی به شرکت دیگر را در برمی‌گیرند، درحالی‌که فری‌رایدینگ را به حداقل می‌رسانند و به‌اشتراک‌گذاری اطلاعات اختصاصی در سراسر کشورها، این منجر به تنوع قابل‌توجهی در ماهیت الزام‌آور یا غیرالزام‌آور این رژیم‌ها شده است. همان‌طور که تحلیل اشاره می‌کند، به‌رغم تلاش‌های نظارتی برای رسیدگی به آن، اشتراک‌گذاری اطلاعات در ژاپن و ایالات متحده همچنان یکی از مشکلات اصلی امنیت سایبری است [۶].

۳.۲.۲ شکست در اجرا

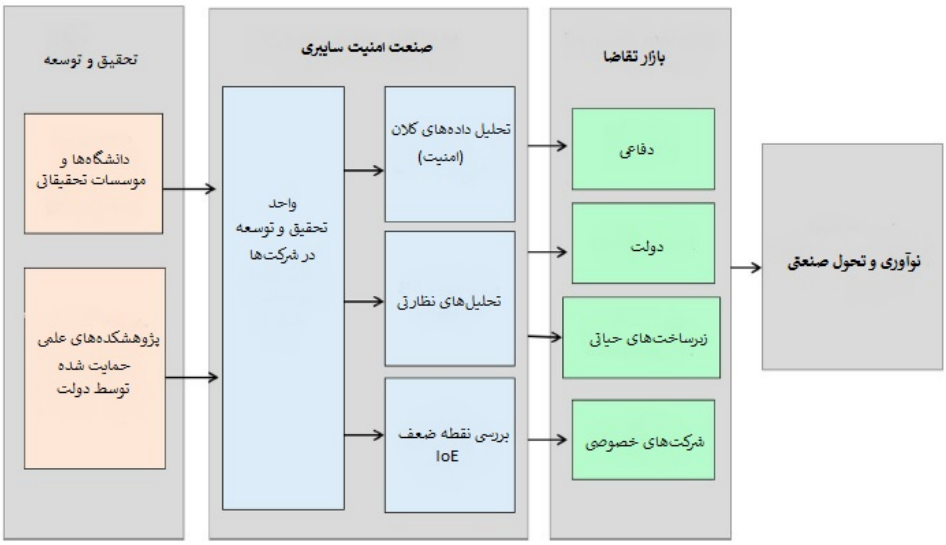
اجرای سیاست صنعتی از دو فرآیند ناشی می‌شود. در این بخش، انتخاب عمومی یک خط‌مشی خاص و متعاقباً چالش‌های پیش روی مجری را بررسی می‌کنیم. هریس و کارمن (۱۹۸۴) در تجزیه‌وتحلیل خود از مداخله به انواع شکست‌های قانونی بالقوه اشاره می‌کنند: شکست‌های انتخاباتی، شکست‌های بوروکراتیک، شکست‌های قانونی و شکست‌های قضایی. هر یک از این شکست‌ها شامل ناتوانی بخشی از جامعه در حمایت از سیاست‌های صنعتی است که شکست بازار را برطرف می‌کند[۵].

به‌عنوان مثال، در چین، مدل‌های تدارکات و مجوز پکن منجر به میزان قابل‌توجهی از فساد و آسیب‌پذیری دولت در برابر حملات سایبری شده است و همین امر امنیت سایبری را که دولت چین در تلاش برای تقویت آن است، تنزل داده است. درعین‌حال، برنامه‌های سرمایه انسانی که توسط دولت حمایت می‌شوند، نتوانسته‌اند به‌اندازه‌ای که انتظار می‌رفت، کارگران آموزش‌دیده در زمینه امنیت سایبری تولید کنند [۷]. مقررات ایجادشده توسط دولت چین نیز مبهم بوده و ورود شرکت‌های جدید به بخش امنیت سایبری را پیچیده کرده است. در فرانسه، تلاش‌های دولت برای تنظیم و تقویت صنعت امنیت سایبری با مقاومت انجمن‌های تجاری مواجه شده است، زیرا بسیاری با ایجاد یک رژیم گواهی‌نامه که شرکت‌ها را بر اساس عملکردشان در برابر معیارهای امنیت سایبری رتبه‌بندی می‌کند مخالف هستند [۱۰]. در سطح اتحادیه اروپا، هماهنگی بین اتحادیه اروپا و کشورهای عضو آن باتوجه‌به خطرات آربیتراژ نظارتی – که در آن کسب‌وکارها راحت‌ترین محیط نظارتی را دنبال می‌کنند، یک مشکل مداوم برای اجرای سیاست سایبری است.

۴.۲.۲ روابط دولت و جامعه

با تشریح شکست‌های بازار، سیاست‌های صنعتی ایجادشده برای رسیدگی به آن‌ها، و چالش‌های مرتبط با اجرا، اکنون به روابط دولت – جامعه[۹] می‌پردازیم که ایجاد آن‌ها را چارچوب می‌دهد. ادبیات اقتصاد سیاسی در مورد سیاست صنعتی انواع توضیحات غنی از نیروهایی را ارائه می‌دهد که باعث ایجاد تنوع در انتخاب‌های سیاست صنعتی دولت‌ها می‌شود[۶]. به‌عنوان‌مثال، تای مینگ چونگ در تحلیل خود از چین اشاره می‌کند که پکن از مدل سرمایه‌داری عمدی تحت رهبری دولت استفاده می‌کند [۷]. از سوی دیگر، بن بارتلت خاطرنشان می‌کند که ژاپن توسعه بازار امنیت سایبری تحت رهبری بخش خصوصی را ترویج می‌کند [۹]. حتی در میان دولت‌های سرمایه‌داری غربی، در مقالات این شماره مشهود است که در نحوه پیگیری و اجرای سیاست‌هایی که کشورها منعکس‌کننده نوع رژیم، سیاست بوروکراتیک، ژئوپلیتیک و موقعیت آن‌ها در نردبان توسعه است، تفاوت زیادی وجود دارد [۶].

شکل ۱، مدل نهایی اکوسیستم و نقش مداخله‌گر دولت در بازار امنیت سایبری را نشان می‌دهد.



شکل ۱: توسعه صنعت امنیت سایبری: برنامه‌های اقدام دولت

بازیگران دولتی شامل شاخه‌های مختلف دولت، ارتش و انواع سازمان‌ها یا وزارتخانه‌ها هستند. رابطه بین آن‌ها بسته به سازمان خاص ساختار دولتی ممکن است کم‌وبیش پراکنده باشد؛ بنابراین ما ممکن است کم‌وبیش سیاست بوروکراتیک را در کشورهای مختلف ببینیم. علاوه بر خروجی‌های سیاست (در این مورد، سیاست صنعتی) که از تعامل میان این بازیگران پدید می‌آید، دولت‌ها نیز با فشار سیستمی در قالب رقابت اقتصادی و امنیتی جهانی مواجه هستند. بازیگران اجتماعی شامل نیروی کار، سازمان‌های

[9] State-society relations

غیردولتی، شرکت‌ها، مصرف‌کنندگان و سایر بازیگران ازاین‌قبیل هستند. بازهم، رابطه این بازیگران بسته به قوانین، مقررات و هنجارهای خاص متفاوت است. به‌عنوان‌مثال، در آلمان، نیروی کار نقش بسیار فعال‌تری در هیئت‌مدیره شرکت‌ها نسبت به ایالات متحده دارد [۶]. جدول ۱، تقسیم‌کار وظایف امنیت سایبری در وزارتخانه‌های دولتی را نشان می‌دهد [۱۳].

جدول ۱: تقسیم‌کار وظایف امنیت سایبری در وزارتخانه‌های دولتی

وزارت	وظایف اصلی امنیت سایبری
وزارت امور اقتصادی	– ایجاد مرکزی برای به اشتراک‌گذاری و تجزیه‌وتحلیل اطلاعات (ISAC) در زیرساخت‌های حیاتی منابع آبی و تأمین انرژی – حمایت از صنعت امنیت سایبری و پرورش استعدادهای برتر
وزارت علوم و فناوری	ایجاد ISAC برای زیرساخت‌های حیاتی پارک‌های علم و فناوری ارائه یارانه به دانشگاه‌ها به‌منظور پرورش استعدادها و تحقیق در مورد فناوری‌های پیشرفته امنیت سایبری
وزارت بهداشت و رفاه	ایجاد ISAC به‌منظور تأمین زیرساخت‌های حیاتی بهداشت عمومی
وزارت کشور	افزایش ظرفیت‌های پزشکی قانونی دیجیتال در جرائم با فناوری پیشرفته
وزارت آموزش‌وپرورش	بهبود امنیت سایبری اتصال شبکه دانشگاهی تایوان و مؤسسات دانشگاهی و تحقیقاتی
وزارت حمل‌ونقل و ارتباطات	ایجاد ISAC به‌منظور زیرساخت‌های حیاتی حمل‌ونقل
کمیسیون ارتباطات ملی	تقویت حفاظت از شبکه ارتباطی پایه ملی و اجرای تحقیقات در مورد امنیت اطلاعات اینترنت اشیاء
وزارت دفاع ملی	ایجاد نیروی الکترونیکی ارتباطات اطلاعاتی به‌منظور محافظت از دامنه دیجیتال در تایوان و تقویت صنعت امنیت سایبری ایجاد توافق‌نامه چندجانبه امنیت سایبری به‌منظور افزایش همکاری‌های چندملیتی

سؤال کلیدی که از شکل ۲ برمی‌آید، موضوع همگرایی یا واگرایی در سیاست صنعتی است. آیا فشارهای بین‌المللی سامان‌مند، باتوجه‌به اهمیت منحصربه‌فرد امنیت سایبری، همه کشورها را به دنبال سیاست‌های مشابه در طول زمان سوق خواهد داد؟ یا اینکه تنوع ملی عامل اصلی توضیحی است که به ایجاد اختلاف در سیاست امنیت سایبری ادامه خواهد داد؟ ازنظر اندیشیدن به سیاست صنعتی با توجه به بخش امنیت ملی، لیندا وایس استدلال می‌کند که ژئوپلیتیک و درک تهدید منجر به یک حرکت از بالابه‌پایین شده است.

ازنظر اندیشیدن به سیاست صنعتی دررابطه‌با بخش امنیت ملی، لیندا وایس[10] استدلال می‌کند که ژئوپلیتیک و ادراک تهدید منجر به رابطه‌ای از بالابه‌پایین بین «دولت امنیت ملی» و شرکت‌های تجاری شاغل در بخش فناوری شده است [۱۴]. به عقیده او، این رابطه، به‌طورکلی، پایه‌های بخش تجاری با فناوری پیشرفته و نوآوری‌های تکنولوژیکی را که به‌رغم «ضد دولت‌گرایی[11]» در بین شرکت‌ها و افراد به کار می‌بریم، توضیح می‌دهد. مشارکت خصوصی که امروزه وجود دارد. وایس استدلال می‌کند که این محیط نهادی خاص «دولت

[10] Linda Weiss
[11] anti-statism

امنیت ملی[۱۲]» تفاوت مشاهده‌شده بین ایالات متحده و سایر دموکراسی‌های پیشرفته را توضیح می‌دهد. آگاروال و ردی (۲۰۱۸) در بررسی خود از ایالات متحده به روابط مختلف شرکت و دولت اشاره می‌کنند که نمونه‌ای از پیوندهای نزدیک بین آژانس‌های اطلاعاتی، شرکت‌های دفاعی تثبیت‌شده و سیلیکون‌ولی است [۶]. گریفیث (۲۰۱۸) نیز بازار امنیت سایبری در فنلاند را در پس‌زمینه نگرانی‌های ژئوپلیتیک گسترده‌تر بررسی می‌کند [۸].

در مقابل، فرد بلاک و متیو کلر (۲۰۰۹) پیشنهاد می‌کنند که منطق مداخله دولت برای تقویت نوآوری، فعالیت دولت را «عادی[۱۳]» می‌کند و به گسترش «وضعیت توسعه پنهان» که کارکردهای سیاست صنعتی قابل‌توجهی را بر عهده می‌گیرد، کمک می‌کند [۱۵]. همچنین پیشنهاد می‌کند که نقش دولت را می‌توان به چهار وظیفه متمایز اما همپوشانی تقسیم کرد – منابع هدفمند، باز کردن پنجره‌ها، دلالی و تسهیل. همان‌طور که وایس ادعا می‌کند، اقتصاد کسب‌وکار به‌عنوان منحصربه‌فرد ایالات‌متحده است، بلوک پیشنهاد می‌کند که نشان‌دهنده همگرایی در سیاست‌گذاری صنعتی در مرز فناوری در میان دموکراسی‌های پیشرفته است.

۵.۲.۲ پیامدهای بین‌المللی مداخله

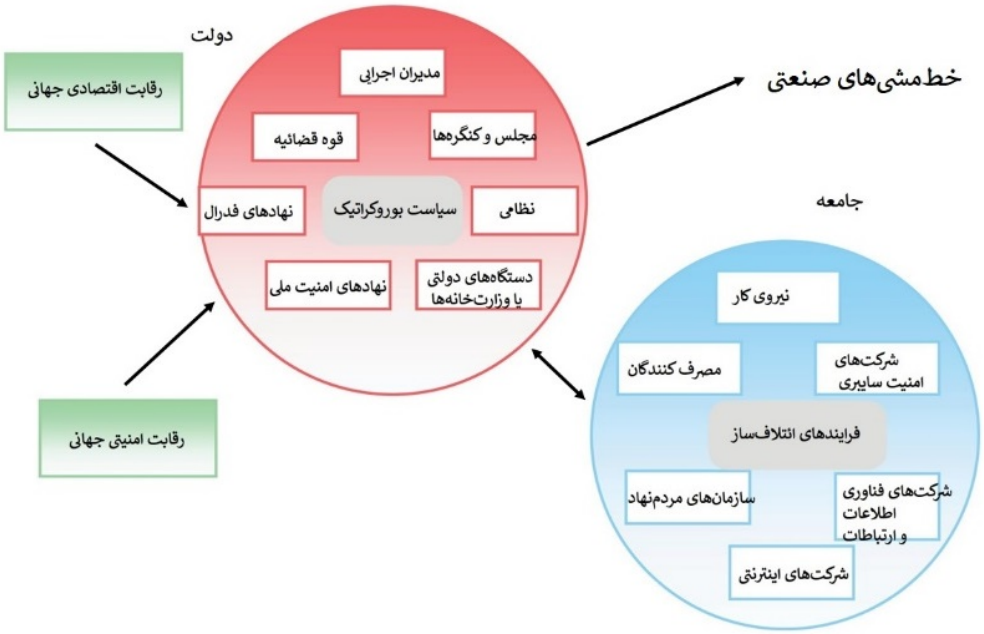
ازآنجایی‌که کشورها سیاست‌های صنعتی در امنیت سایبری را دنبال می‌کنند، تضاد بین شرکت‌ها و دولت‌ها بر سر دسترسی به بازارها تقریباً اجتناب‌ناپذیر است. درواقع، سیاست‌های امنیت سایبری را می‌توان به‌عنوان نمونه‌ای عالی از مسائل «پشت مرز» – برخلاف تعرفه‌ها و سهمیه‌ها، در نظر گرفت. موانع اقداماتی هستند که اساساً بخشی از دستگاه نظارتی دولت‌ها هستند. باتوجه‌به تفاوت شدید در نحوه برخورد دولت‌ها با چنین مسائلی و همچنین ساختارهای سیاسی متفاوت آن‌ها، احتمال همگرایی هنوز نامشخص است. گات تا حدودی در مدیریت برخی درگیری‌های پشت مرزی موفق بود، مانند صنعت هواپیماسازی شامل بوئینگ و ایرباس، اما حل‌وفصل اختلافات در این بخش نه آسان بوده و نه حتی به طور دائمی حل‌وفصل شده است. در مقابل، سازمان تجارت جهانی برای رسیدگی به بسیاری از این مسائل با مشکلاتی مواجه شده است، همان‌طور که دور طولانی‌مدت دوحه که در سال ۲۰۰۱ آغاز شد و در دسامبر ۲۰۱۵ از هم پاشید، گواه آن است. TPP (Trans Pacific Partnership) و TTIP (Transatlantic Trade and Investment Partnership) [۱۶]. بااین‌حال، ازآنجایی‌که این مگا–FTAها در ایالات‌متحده و اتحادیه اروپا به‌شدت موردبحث قرارگرفته است، به‌هیچ‌وجه یک نتیجه قطعی نیست که این توافقات هرگز اجرایی شوند. درواقع، ایالات‌متحده از TPP خارج‌شده است و سایر کشورها با ایجاد توافقنامه جامع و مترقی برای مشارکت ترانس پاسیفیک (CPTPP) پیش رفته‌اند. ترتیبات جایگزین برای مقابله با چنین مسائلی از طریق توافق‌نامه‌های بخشی؛ مانند موافقت‌نامه فناوری اطلاعات (ITA)، موافقت‌نامه پایه مخابرات (توسعه‌یافته در اواخر دهه ۱۹۹۰) و ITA II که در سال ۲۰۱۵ به امضا رسید، ایجادشده است؛ بنابراین، حداقل در اصول، یک راه بالقوه برای همکاری بر سر مدیریت سیاست‌های صنعتی امنیت سایبری در سطح بین‌المللی وجود دارد.

اگر همکاری در بخش امنیت سایبری ظهور کند، چگونه خواهد بود؟ یکی از راه‌های مفهوم‌سازی این است

[12] national security state
[13] normalizes

که به این فکر کنیم که چگونه کشورها تلاش می‌کنند تا با اثرات خارجی سیاست‌های داخلی کنار بیایند، چه دولت‌ها یا شرکت محور باشند. این‌ها شامل محدودیت‌های داخلی مرتبط با صنعت یا توافق‌نامه‌های دوجانبه است که ممکن است با حذف شرکت‌ها از بازارها یا آسیب‌دیدگی توسط سیاست‌های صنعتی خارجی، درگیری ایجاد کند. این ممکن است منجر به درخواست برای ایجاد اصول و هنجارهای بین‌المللی (فراترژیم[۱۴]) یا رویه‌های قانونی (رژیم بین‌المللی[۱۵]) برای پرداختن به اثرات خارجی سیاست‌های صنعتی در امنیت سایبری شود.

تاکنون، تلاش‌ها برای ایجاد تعامل و مشارکت بین‌المللی با محوریت امنیت سایبری تا حد زیادی شکست‌خورده است. موانع بر سر راه شرکت‌های خارجی همچنین مانع از جریان‌های دانش شده و پتانسیل شرکت‌ها برای یادگیری از شرکت‌های باتجربه‌تر در خارج از کشور را متوقف کرده است، درحالی‌که دستیابی به مزیت نسبی در این بخش را نیز محدود کرده است. به‌عنوان‌مثال، در ایالات‌متحده، قوانین تدارکات دولتی که خرید از شرکت‌های خارجی (به‌ویژه شرکت‌های چینی) را محدود می‌کند، تنش‌ها را بین پکن و واشنگتن در بحبوحه اختلاف‌نظرهای گسترده‌تر پیرامون شرایط مربوط به جریان‌های تجاری، کسری‌ها و موانع تعرفه افزایش داده است [۶].



شکل ۲: تبیین تنوع در تعامل دولت و جامعه در سیاست‌گذاری

جدول ۲ به‌طور خلاصه، سیاست صنعتی امنیت سایبری را در تایوان نشان می‌دهد [۱۳].

[14] meta-regime
[15] international regime

جدول ۲: سیاست صنعتی امنیت سایبری تایوان

نوع بازار	منطق دولت	ابزارهای خط‌مشی پیشنهادی	راهبرد	چالش‌های مداخله دولت
بازار دولت	۱. هدف سیاست ملی ۲. تهدید شرکت‌های بزرگ بین‌المللی	۱. دستور مقررات جدید ۲. قراردادهای متمرکز برای خرید دولتی نرم‌افزار امنیت سایبری و خدمات ابری	افزایش تقاضای داخلی	۱. ناکارآمدی در یافتن بهترین راه‌حل‌ها ۲. حمایت بیش‌ازحد از شرکت‌های داخلی
بازار شرکت‌های خصوصی	۱. عوامل خارجی فناوری ۲. اقتصادهای مقیاس پویا (فقدان VCs و بازار سرمایه)	۱. اعتبار مالیاتی برای سرمایه‌گذاری تحقیق و توسعه در امنیت سایبری، با هدف قرار دادن شرکت‌های فناوری اطلاعات و هایSME موجود ۲. ارائه کمک‌های مالی یا یارانه‌های تحقیق و توسعه	تشویق تحقیق و توسعه	۱. شکست دولت ۲. اثر ازدحام ۳. هیچ انگیزه‌ای برای رقابتی بودن شرکت محلی ایجاد نمی‌کند
بازار CIIP	خارجی بودن	۱. دستور مقررات جدید ۲. کمک به شرکت زیرساخت‌های حیاتی برای ارتقاء سیستم‌های حفاظت از امنیت سایبری ۳. ارائه انگیزه مالی برای تحقیق و توسعه و ارتقاء فناوری	ایجاد تقاضای بازار جدید	رفتار راهبردی در اطاعت از مقررات
بازار دفاعی	۱. اهداف امنیت ملی ۲. عدم قطعیت در روابط بین‌المللی	۱. راه‌اندازی فرماندهی اطلاعات، ارتباطات و جنگ الکترونیک در سال ۲۰۱۷ ۲. افزایش انشعاب فناوری‌های نظامی و اکتشافات تحقیقاتی	امنیت ملی	۱. ناتوانی در دستیابی به اقتصاد مقیاس ۲. یک سوراخ تاریک در بودجه دولت
بازار بررسی ایمنی اپلیکیشن موبایل	اطلاعات ناقص	۱. ایجاد نهادهای شخص ثالث برای بررسی ایمنی برنامه‌های تلفن همراه	بازار جاویژه (نیچ مارکت)	رفتار استراتژیک در گرفتن بررسی ایمنی

۳ نتیجه‌گیری

سیاست‌های صنعتی، برای بلوغ و رشد هر صنعتی الزامی است؛ اما نوع رابطه دولت با صنعت و میزان مداخله دولت در صنایع، می‌تواند بازار را تحت‌تأثیر قرار دهد. هدف تحقیق کنونی، بررسی مطالعات گذشته است. با بررسی تحقیقات مختلف دریافتیم که دولت‌ها بزرگترین مشتریان محصولات امنیت سایبری هستند و اکثر دولت‌ها به صنعت امنیت سایبری توجه ویژه دارند. به همین دلیل، سیاست‌های بازار امنیت سایبری را مداخله‌گری کرده و سعی می‌کنند با تدوین برنامه‌های ویژه، آن را بهبود بخشند. رویکرد کشورهای مختلف نسبت به صنعت امنیت سایبری متفاوت است و با درنظرگرفتن شرایط هر کشور، ممکن است نسبت به بازار امنیت سایبری، سیاست‌های ویژه‌ای اتخاذ کنند. تصمیماتی که اتخاذ می‌شد، می‌تواند به بهبود شرایط بازار و یا اصلاح آن منجر شود و یا در نهایت به شکست و تغییراتی در بازار بینجامد.

تحقیقات حوزه صنعت و بازار امنیت سایبری بسیار محدود هستند، بنابراین پیشنهاد می‌شود با انجام تحقیقات تطبیقی و کیفی، عناصر و ارکان تصمیم‌گیری‌های دولت و میزان مداخله آن در صنعت امنیت سایبری شناسایی و تبیین شود. همچنین، شرایط فعلی بازار امنیت سایبری جهانی با ایران مقایسه و چالش‌ها و موانع آن شناسایی و راهکارهایی ارائه گرد.

مراجع

[1] Tavakolirad, R; Zargaran Khouzani, F. Successful Organizational Digital Transformation Model. 6th International Conference on Interdisciplinary Studies in Management and Engineering 2023.

[2] Shackelford SJ, Boustead A, Makridis C. Defining" Reasonable" Cybersecurity: Lessons from the States. Yale JL and Tech.. 2023;25:86.

[3] Mmango N, Gundu T. Cybersecurity as a Competitive Advantage for Entrepreneurs. InAnnual Conference of South African Institute of Computer Scientists and Information Technologists 2024 Jul 8 (pp. 374-387). Cham: Springer Nature Switzerland.

[4] Hiller J, Kisska-Schulze K, Shackelford S. Cybersecurity carrots and sticks. American Business Law Journal. 2024 Mar;61(1):5-29.

[5] Harris RG, Carman JM. Public regulation of marketing activity: Part II: Regulatory responses to market failures. Journal of Macromarketing. 1984 Jun;4(1):41-52.

[6] Aggarwal VK, Reddie AW. Comparative industrial policy and cybersecurity: the US case. Journal of Cyber Policy. 2018 Sep 2;3(3):445-66.

[7] Cheung TM. The rise of China as a cybersecurity industrial power: Balancing national security, geopolitical, and development priorities. Journal of Cyber Policy. 2018 Sep 2;3(3):306-26.

[8] Griffith MK. A comprehensive security approach: Bolstering Finnish cybersecurity capacity. Journal of Cyber Policy. 2018 Sep 2;3(3):407-29.

[9] Bartlett B. Government as facilitator: how Japan is building its cybersecurity market. Journal of Cyber Policy. 2018 Sep 2;3(3):327-43.

[10] D'elia D. Industrial policy: the holy grail of French cybersecurity strategy?. Journal of Cyber Policy. 2018 Sep 2;3(3):385-406.

[11] Timmers P. The European Union's cybersecurity industrial policy. Journal of Cyber Policy. 2018 Sep 2;3(3):363-84.

[12] Carr M, Tanczer LM. UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions. Journal of Cyber Policy. 2018 Sep 2;3(3):430-44.

[13] Huang, H., and Li, T. S. (2018). A centralised cybersecurity strategy for Taiwan. Journal of Cyber Policy, 3(3), 344-362.

[14] Weiss, M., and Jankauskas, V. (2019). Securing cyberspace: How states design governance arrangements. Governance, 32(2), 259–275. https://doi.org/10.1111/gove.12368

[15] Block F, Keller MR. Where do innovations come from? Transformations in the US economy, 1970–2006. Socio-Economic Review. 2009 Jul 1;7(3):459-83.

[16] Azmeh S, Foster C. The TPP and the digital trade agenda: Digital industrial policy and Silicon Valley's influence on new trade agreements. Working Paper Series; 2016.