سیاست‌نامه
شماره ۰۳۰۲۰۱
اردیبهشت ۱۴۰۳

بررسی حکمرانی امنیت سایبری صنعتی شبکه برق (مطالعه موردی: امریکا و هند)

عنوان گزارش: **بررسی حکمرانی امنیت سایبری صنعتی شبکه برق (مطالعه موردی: امریکا و هند)**

تهیه و تدوین: **معین احمدی، امیر محمدی‌دوست**

آدرس وب سایت: iranergi.com

تاریخ تهیه گزارش: **اردیبهشت ۱۴۰۳**

نشانی: تهران، خیابان شهید دکتر حبیب الله، تقاطع خیابان شهید سروش (یکم)، پلاک ۹۶، پژوهشکده مطالعات فناوری- ۰۲۱۶۶۵۰۰۰۶۵

فهرست مطالب

فهرست اشکال

خلاصه مدیریتی

انرژی الکتریکی پیش‌نیاز مهمی در پیشرفت حوزه‌های اقتصادی، اجتماعی و رفاهی در کلیه جوامع و کشورها محسوب می‌شود. به‌ویژه در کشورهای درحال‌توسعه یا کمتر توسعه‌یافته، در دسترس بودن برق با قابلیت اطمینان بالا همراه با قیمت‌های مناسب، نقش مهمی در توسعه اقتصادی و اجتماعی دارد. در صورت اختلال در کارکرد شبکه برق به دلیل وابستگی دیگر زیرساخت‌های حیاتی به آن (ازجمله: شبکه آب‌رسانی، شبکه گاز، بانکداری، ترافیک و حمل‌ونقل، زیرساخت ارتباطات)، پیامدهای سیاسی، اجتماعی و اقتصادی را در پی خواهد داشت.

از مهم‌ترین مسائل و چالش‌های مربوط به «مقاوم‌سازی شبکه برق در مقابل حملات سایبری»، چالش حکمرانی و نامتوازن بودن چینش نهادی است. تعدد و موازی کاری‌های سازمان‌های مقررات گذار این حوزه و برخی دیگر از بازیگران در این بخش، شرکت‌های برق را دچار سردرگمی کرده است. همچنین در ساختار سازمانیِ متولیان این حوزه، مسئولیت اختصاصی برای این موضوع به‌صورت دقیق مشخص نشده است. در خصوص شبکه IT اخیرا با مصوبه سازمان استخدامی و اداری مدیران IT به مدیران IT و امنیت سایبری تغییر یافته‌اند (بدون تغییر چارت زیرمجموعه). در خصوص شبکه صنعتی (OT) در ساختار سازمانی، تعیین مسئولیت و وظایف همچنان به صورت دقیق تعریف نشده است. لذا بررسی ساختار حمکرانی سایر کشورهای پیشرو در این زمینه می‌تواند راهگشا باشد. از این رو ابتدا تجربه دو کشور ایالات متحده امریکا و کشور هند بررسی شده و سپس در تطبیق با ساختار نظام حمکرانی امنیت سایبری صنعتی در داخل کشور پیشنهادهایی برای تکمیل ساختار سازمانی مسئولیت امنیت سایبری شبکه‌ی اداری (IT) و صنعتی (OT) در صنعت برق ارائه شده است.

توجه جدی کشور آمریکا به امنیت زیرساخت‌های حیاتی[1]آن کشور از سال ۲۰۰۱ و در پی حمله یازده سپتامبر جلب شد. قانون Patriot Act در سال ۲۰۰۱ در واکنش به حمله یازده سپتامبر و برای محافظت زیرساخت‌های این کشور در مقابل حملات تروریستی وضع گردید و به دنبال آن وزارت امنیت داخلی (DHS[2]) در سال ۲۰۰۲ با هدف حفاظت از زیرساخت‌های حیاتی داخلی[3]تاسیس شد. در دهه‌ی ابتدایی

---

[1] There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

[2] Department of Homeland Security

فعالیت این وزارت‌خانه و همچنین پیدایش حملات سایبری به زیر ساخت‌های حیاتی در امریکا مسئولیت حفاظت از زیرساخت‌های اساسی بر عهده وزارت امنیت داخلی گذاشته شد. پس از تجربه چندساله و عدم تحقق اهداف و برنامه‌ریزی‌ها، در حوزه‌هایی از جمله حوزه انرژی وزارت خانه مربوطه به عنوان دستیار وزارت امنیت داخلی به امن‌سازی حوزه‌های زیرمجموعه خود پرداختند. وزارت انرژی برای انجام وظیفه محوله خود دفتری را تحت عنوان "دفتر امنیت سایبری، امنیت انرژی و واکنش سریع[۴]" ایجاد کرد. علاوه بر تغییرات وزارت انرژی؛ دفتر امنیت سایبری در وزارت امنیت داخلی در سال ۲۰۱۸ به " سازمان امنیت سایبری و امنیت زیرساخت[۵]" ارتقا یافت که در ذیل آن اداره امنیت زیرساخت از اداره امنیت سایبری تفکیک شده است. در حال حاضر، سطوح نظام حکمرانی امنیت سایبری زیرساخت‌های اساسی در کشور امریکا را به بخش‌های زیر می توان تقسیم نمود:

- سیاست گذاری و برنامه ریزی
- مقررات گذاری و تنظیم‌گری و استاندارد
- نظام اشتراک گذاری تهدیدهای سایبری
- شرکت های عملیاتی

در کشور هند برخلاف کشور امریکا مساله امنیت سایبری زیرساخت‌های حیاتی سبقه‌ی طولانی ندارد. مرتبط‌ترین فعالیت‌ها در این خصوص به قانون فناوری اطلاعات[۶]مصوب سال ۲۰۰۰ بر می‌گردد و طبق آن از سال ۲۰۱۱ سازمان‌ها موظف به اجرای استاندارد ایزو ۲۷۰۰۱ در شبکه‌ی اداری سازمان خود می‌شوند. در سال ۲۰۱۳ سیاست ملی امنیت سایبری[۷]توسط وزارت الکترونیک و فناوری ارتباطات منتشر می‌شود. طبق بخش ۷۰ قانون فناوری اطلاعات مرکز ملی حفاظت از زیرساخت‌های حیاتی[۸] در ذیل سازمان ملی تحقیقات فنی (ذیل نخست وزیر هند) و تیم امداد اضطراری هند[۹] در وزارت الکترونیک و فناوری اطلاعات تشکیل می‌شوند. در سال ۲۰۲۱ مقررات امنیت سایبری در شبکه برق توسط سازمان مرکزی برق هند[۱۰]به عنوان نهاد مقررات‌گذار فنی بخش برق ابلاغ می‌شود که به موجب آن سازمان‌ها موظف به ایجاد

←

۳ زیرساخت‌های حیاتی در کشور امریکا طبق فرمان اجرایی رئیس جمهور (Presidential directive PDD-63) در سال ۱۹۹۸ تعیین شده اند. در سال ۲۰۰۳ پس از تشکیل وزارت امنیت داخلی لیست زیرساخت‌های حیاتی تکمیل گردید.

۴Office of Cybersecurity and Energy security and emergency response

۵Cybersecurity and Infrastructure Security Agency

۶Information Technology Act

۷National Cybersecurity policy

۸National Critical Information Infrastructure Protection centre (NCIIPC)

۹Computer Emergency response Teams (CERT-In)

۱۰Central Electricity Authority

اداره امنیت سایبری می‌شوند و این اداره نقطه تماس با سازمان‌های مقررات‌گذار حوزه امنیت سایبری اداری و صنعتی می‌شود.

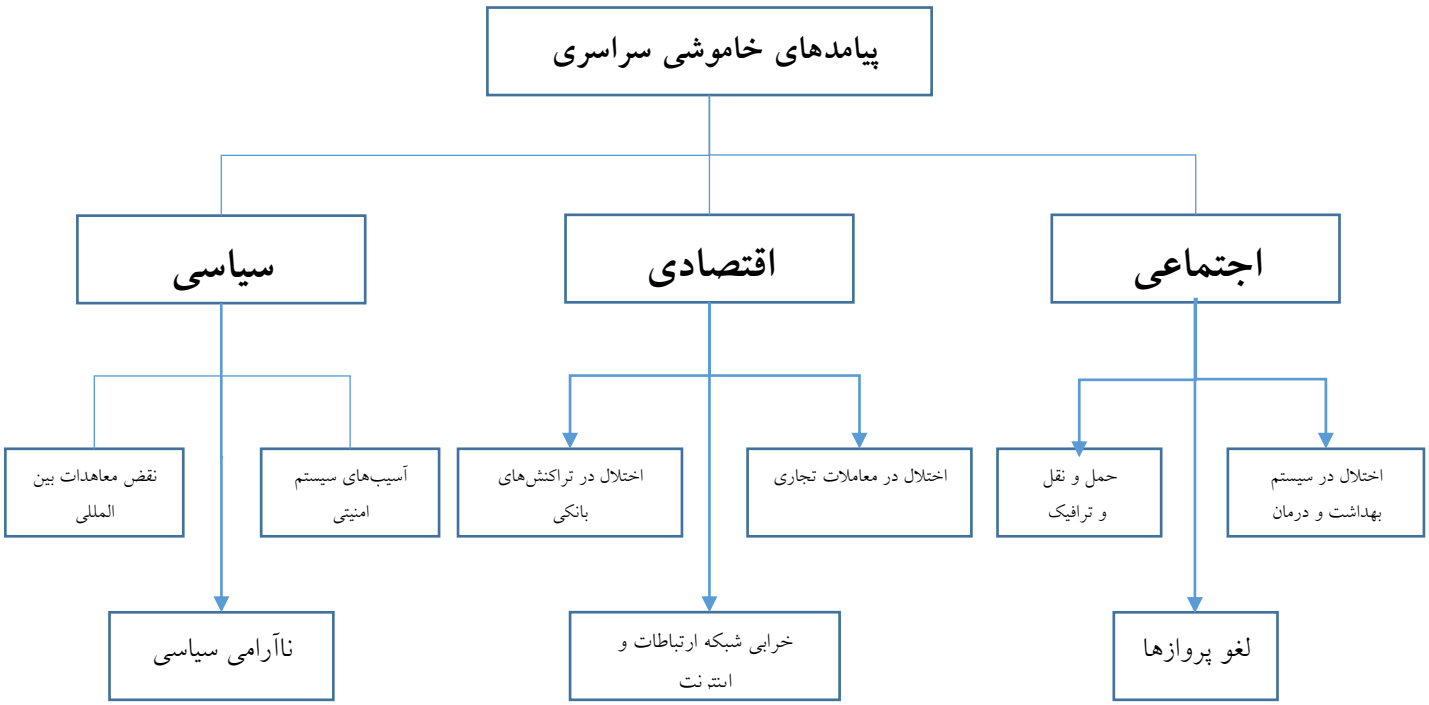
با توجه به بررسی تجربه نظام حکمرانی امنیت سایبری زیرساخت صنعتی برق در کشور امریکا و هند و همچنین وضعیت کنونی کشور در این خصوص جهت رفع نقایص ساختار موجود در کشور پیشنهادهای زیر قابل طرح است:

- در خصوص اصلاح چارت سازمانی پیشنهاد می‌شود که مسئولیت‌ها در حوزه IT و حوزه‌ی OT از یکدیگر مجزا گردند. حوزه شبکه اداری به دفاتر فناوری اطلاعات و حوزه صنعتی به دفاتر فنی مرتبط به هر بخش اختصاص یابد.
- پیشنهاد می‌شود نظام اشتراک‌گذاری تهدیدهای امنیت سایبری صنعتی با الگو از کشور امریکا ایجاد شود، این اتفاق سطح آمادگی زیرساخت‌ها در مقابل آسیب پذیری‌های سایبری را بالا می‌برد.
- آموزش‌های مرتبط با امنیت سایبری صنعتی با کمک دانشگاه‌ها و موسسات آموزشی و همچنین مراکز معتبر بین المللی برای برگزاری دوره‌های تخصصی این حوزه و تربیت نیروی متخصص یکی دیگر از نیازمندی‌های کشور است.
- زیرساخت‌های آزمایشگاهی برای ارزیابی آسیب پذیری‌های نرم افزاری و سخت افزاری تجهیزات صنعتی در کشور بایستی ایجاد گردد.
- زیست بوم توسعه فناوری‌های امنیت سایبری صنعتی با ایجاد محیط‌های آزمون (Test Beds) برای کمک به تنظیم‌گران این حوزه در زمینه مقررات‌گذاری و استانداردگذاری و همچنین ارزیابی عملکرد فناوری‌های مرتبط با این بخش که در محیط صنعتی واقعی بکاربرده خواهند شد، تکمیل گردد.
- پیشنهاد می‌شود موضوع توسعه فناوری‌های امنیت سایبری صنعتی با توجه به اهمیت زیرساخت-های حیاتی صنعتی در اولویت توسعه فناوری‌های کشور قرار گیرد.

مقدمه

انرژی الکتریکی پیش‌نیاز مهمی در پیشرفت حوزه‌های اقتصادی، اجتماعی و رفاهی در کلیه جوامع و کشورها محسوب می‌شود. به‌ویژه در کشورهای درحال‌توسعه یا کمتر توسعه‌یافته، در دسترس بودن برق باقابلیت اطمینان بالا همراه با قیمت‌های مناسب نقش مهمی در توسعه اقتصادی و اجتماعی دارد. در صورت اختلال در کارکرد شبکه برق به دلیل وابستگی دیگر زیرساخت‌های حیاتی به آن (ازجمله: شبکه آب‌رسانی، شبکه گاز، بانکداری، ترافیک و حمل‌ونقل، زیرساخت ارتباطات)، پیامدهای سیاسی، اجتماعی و اقتصادی را در پی خواهد داشت[۱].

یکی از مهم‌ترین و مخرب‌ترین نوع حملات که در سال‌های اخیر موردتوجه گروه‌ها و حتی کشورهای معاند حکومت‌ها قرارگرفته است، حملات سایبری به شبکه برق است. این حملات با توجه به اتصالات جهانی اینترنت، می‌تواند از بیرون مرزهای جغرافیایی و به‌گونه‌ای برنامه‌ریزی‌شده انجام شود و کشورها را به مرز استیصال برساند، به‌گونه‌ای که مقالات متعددی، با عنوان «براندازی حکومت‌ها با اخلال در شبکه برق»، مورد بررسی و توجه جدی قرار گرفته است. اتفاقاتی مانند حملات سایبری به نیروگاهی در اوکراین و اخلال در شبکه برق کشور ونزوئلا، نمونه‌هایی از این جریانات مخرب در گذشته بوده‌اند که بررسی‌ها نشان می‌دهند، اکنون به شکل هدفمندتر و برنامه‌ریزی‌شده‌تری دنبال می‌شود.



شکل ۱:پیامدهای خاموشی سراسری شبکه برق [۲]

در صورت موفقیت‌آمیز بودن حملات سایبری به شبکه برق، خاموشی سراسری شبکه برق را به همراه خواهد داشت. همان‌طور که در شکل ۱ پیداست اختلال در شبکه برق‌رسانی درصورتی‌که طولانی شود به دلیل وابستگی زیاد دیگر زیرساخت‌ها به یکدیگر علاوه بر تحمیل خسارت به شبکه برق، پیامدهایی را به همراه خواهد داشت. این پیامدها از اختلال در زندگی روزمره شهروندان شروع‌شده و در صورت استمرار به نارضایتی‌های عمومی در سطح شهر و کشور نیز خواهد رسید. با توجه به وابستگی زیرساخت‌ها به یکدیگر و شبکه برق، شبکه آب‌رسانی و گاز رسانی در ساعات ابتدایی قطع شدن برق دچار اختلال خواهند شد. اختلال در سیستم مدیریت ترافیک در شهرها، رفت‌وآمد را دچار مشکل خواهد کرد و همچنین حمل‌ونقل ریلی و هوایی نیز دچار اختلال خواهند شد. درصورتی‌که کشور تعهداتی برای صادرات برق داشته باشد قابلیت پایبندی به آن را نخواهد داشت و این موضوع منجر به نقض معاهدات بین‌المللی خواهد شد. بخش درمان و بیمارستان‌ها برای ساعات محدودی به سیستم برق اضطراری مجهز هستند. قطع برق این بخش‌ها خسارات جانی را برای مردم به دنبال خواهد داشت. شبکه ارتباطات و مخابرات نیز با قطعی برق به مدت محدودی توان سرویس‌دهی را دارا هستند و با اختلال در فعالیت‌های ارتباطی به فعالیت‌های بانکی، تجاری و صنعتی زیان اقتصادی قابل‌توجهی تحمیل می‌شود. استمرار این وضعیت منجر به نارضایتی عمومی در سطوح وسیعی خواهد شد. لذا در تمام کشورها کارکرد منظم و بدون ریسک و مخاطره شبکه برق در هرلحظه و شرایطی موردتوجه جدی بوده و برای حفظ تداوم آن تمهیداتی در ساختار حاکمیت اندیشیده شده است[۳].

تشریح مساله و راه‌حل‌های آن

علیرغم این‌که دانش امنیت سایبری در زمینه شبکه‌های IT نسبتا پیشرفت خوبی در کشور داشته است. در خصوص شبکه‌های صنعتی در دنیا موضوع جدیدی بوده و در کشور ایران عمق ندارد. از طرفی حملات به زیرساخت‌های حیاتی در سالیان اخیر بسیار گسترش یافته‌اند. متاسفانه، مساله ضعف امنیت سایبری در شبکه برق از سوی شرکت‌های بهره‌بردار شبکه، با تصور اشتباه اینکه شبکه صنعتی این شرکت‌ها از شبکه IT مجزا است، انکار می‌شده است. ولی به دلایل زیادی در سالیان گذشته این دو شبکه در نقاط زیادی به هم متصل شده‌اند و هر تهدیدی که متوجه شبکه IT شرکت‌های برق است، متوجه شبکه صنعتی آن‌ها نیز به دلیل اتصال این دو شبکه خواهد بود.

از دیگر مسائل و چالش‌های مربوط به «مقاوم‌سازی شبکه برق در قبال حملات سایبری»، «چالش حکمرانی» این بخش و نامتوازن بودن چینش نهادی است. تعدد و موازی کاری‌های سازمان‌های مقررات گذار این حوزه و برخی دیگر از بازیگران در این بخش، شرکت‌های برق را دچار سردرگمی کرده است.

بنابراین، بررسی ساختار حمکرانی سایر کشورهای پیشرو در این زمینه می‌تواند راهگشا باشد. از این رو ابتدا تجربه دو کشور ایالات متحده امریکا و کشور هند بررسی می‌شود و سپس با تطبیق با ساختار نظام حمکرانی امنیت سایبری صنعتی در داخل کشور پیشنهادهایی ارائه می‌شوند[٤].

تجربه‌ی ایالات متحده امریکا

توجه جدی کشور امریکا به امنیت زیرساخت‌های حیاتی[۱۱] آن کشور از سال ۲۰۰۱ و در پی حمله یازده سپتامبر جلب شد. قانون Patriot Act در سال ۲۰۰۱ در واکنش به حمله یازده سپتامبر و برای محافظت زیرساخت‌های این کشور در مقابل حملات تروریستی وضع گردید و به دنبال آن وزارت امنیت داخلی (DHS)[۱۲] در سال ۲۰۰۲ با هدف حفاظت از زیرساخت‌های حیاتی داخلی[۱۳] تاسیس شد. در دهه‌ی ابتدایی فعالیت این وزارت خانه و همچنین پیدایش حملات سایبری به زیر ساخت‌های حیاتی در امریکا مسئولیت حفاظت از زیرساخت‌های اساسی بر عهده وزارت امنیت داخلی گذاشته شد. دفتری در زیر مجموعه‌ی وزارت امنیت داخلی مسئولیت حفاظت از زیرساخت‌ها در مقابل حملات سایبری را عهده دار شد. در برخی بخش‌ها وزارت خانه‌های مرتبط وظیفه کمک به وزارت امنیت داخلی را عهده دار شدند. از آن‌جا که امنیت سایبری در بخش IT و OT با اهداف متفاوتی دنبال می‌شوند و از نظر زیرساختی دارای ابعاد فناورانه متفاوتی هستند و همچنین روند اجرای برنامه‌ها مطلوب نبودند در سال ۲۰۱۳ رئیس جمهور امریکا فرمانی[۱۴] صادر کرد و در آن بخشی از وزارت‌خانه‌ها به عنوان دستیار[۱۵] وزارت امنیت داخلی در حفاظت از امنیت سایبری زیرساخت‌های هر بخش مشخص شدند. وزارت انرژی به عنوان دستیار بخش انرژی و وزارت بهداشت برای زیرساخت پزشکی و همچنین وزارت دفاع برای بخش صنایع پایه انتخاب شدند.

---

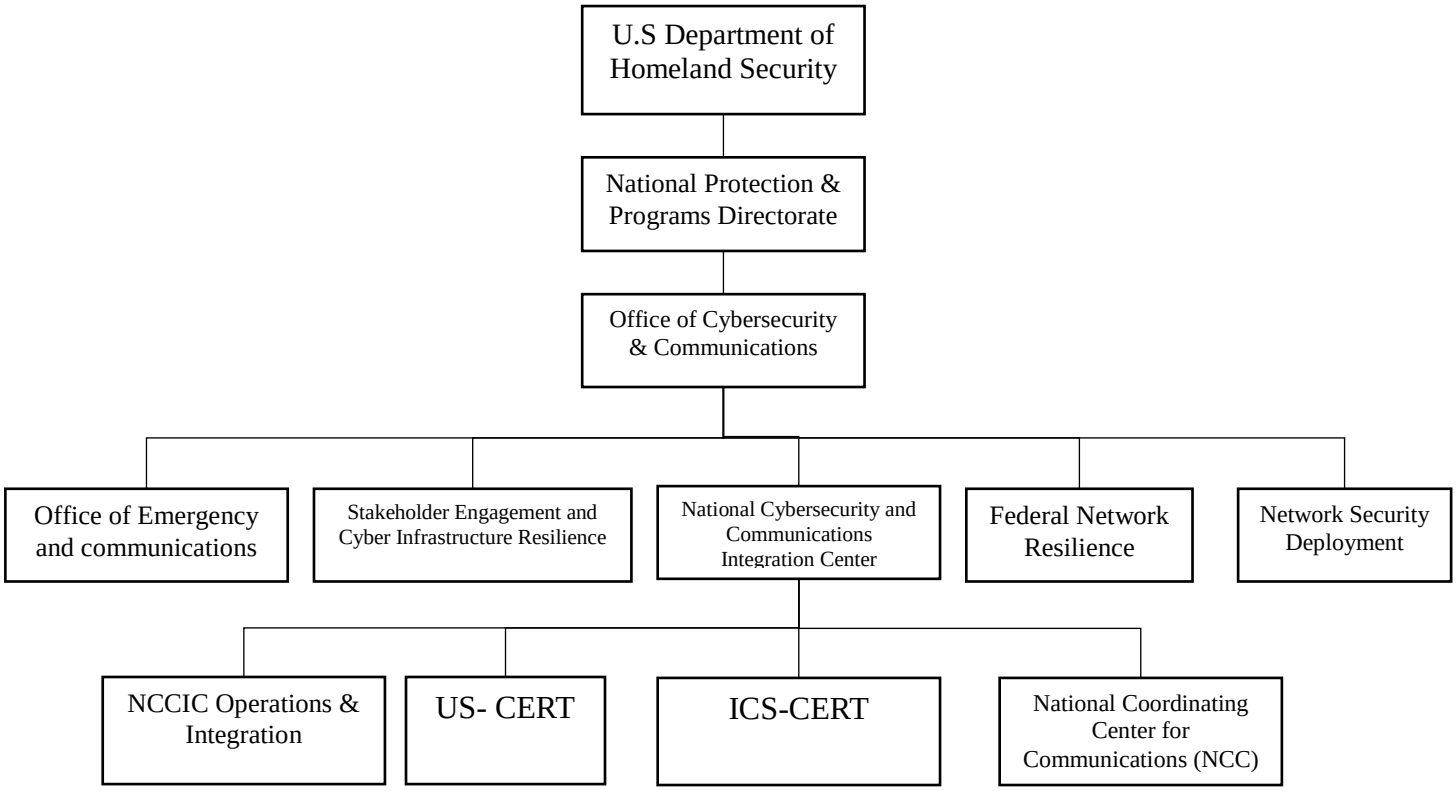
۱۱ There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

۱۲ Department of Homeland Security

۱۳ زیرساخت‌های حیاتی در کشور امریکا طبق فرمان اجرایی رئیس جمهور (Presidential directive PDD-63) در سال ۱۹۹۸ تعیین شده اند. در سال ۲۰۰۳ پس از تشکیل وزارت امنیت داخلی لیست زیرساخت‌های حیاتی تکمیل گردید.

۱۴ Presidential Policy Directive (PPD)/ PDD-21

۱۵ Sector-Specific Agencies (SSAs)



وزارت انرژی برای انجام وظیفه محوله خود دفتری را تحت عنوان "دفتر امنیت سایبری، امنیت انرژی و واکنش سریع[۱۴] ایجاد کرد[۵].

شکل ۲: چارت وزارت امنیت داخلی برای حملات سایبری قبل از تغییرات سال ۲۰۱۸[۶]

علاوه بر تغییرات وزارت انرژی؛ دفتر امنیت سایبری در وزارت امنیت داخلی در سال ۲۰۱۸ به " سازمان امنیت سایبری و امنیت زیرساخت[۱۵]" ارتقا یافت که در ذیل آن اداره امنیت زیرساخت از اداره امنیت سایبری تفکیک شده است. در حال حاضر، سطوح نظام حکمرانی امنیت سایبری زیرساخت‌های اساسی در کشور امریکا را به بخش‌های زیر می توان تقسیم نمود:

- سیاست‌گذاری و برنامه‌ریزی
- مقررات‌گذاری و تنظیم‌گری و استاندارد
- نظام اشتراک‌گذاری تهدیدهای سایبری
- شرکت‌های عملیاتی

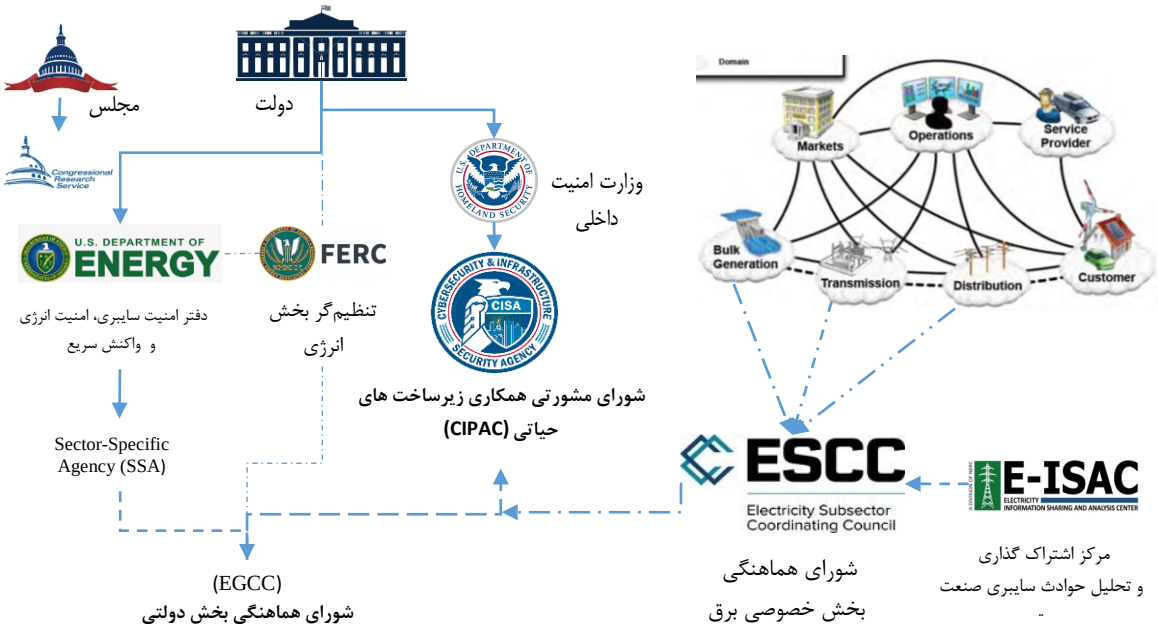
۱۴Office of Cybersecurity and Energy security and emergency response

۱۵Cybersecurity and Infrastructure Security Agency

در ادامه به توضیح هر یک از این سطوح پرداخته می‌شود.

سیاست گذاری و برنامه‌ریزی

مسئولیت سیاست‌گذاری و برنامه‌ریزی کلان در حوزه‌ی امنیت سایبری زیرساخت‌های اساسی بر عهده وزارت امنیت داخلی امریکا است. سازمان امنیت سایبری و امنیت زیرساخت از طریق شورای مشورتی که در ذیل خود تشکیل داده، از طریق دو شورای هماهنگی بخش دولتی و شورای هماهنگی بخش خصوصی نظرات مشورتی ذی‌نفعان حوزه را دریافت می‌کند. از وزارت انرژی دفتر امنیت سایبری، امنیت انرژی و واکنش سریع و تنظیم گر فدرال بخش انرژی ایفای نقش می‌کنند (شکل ۳).

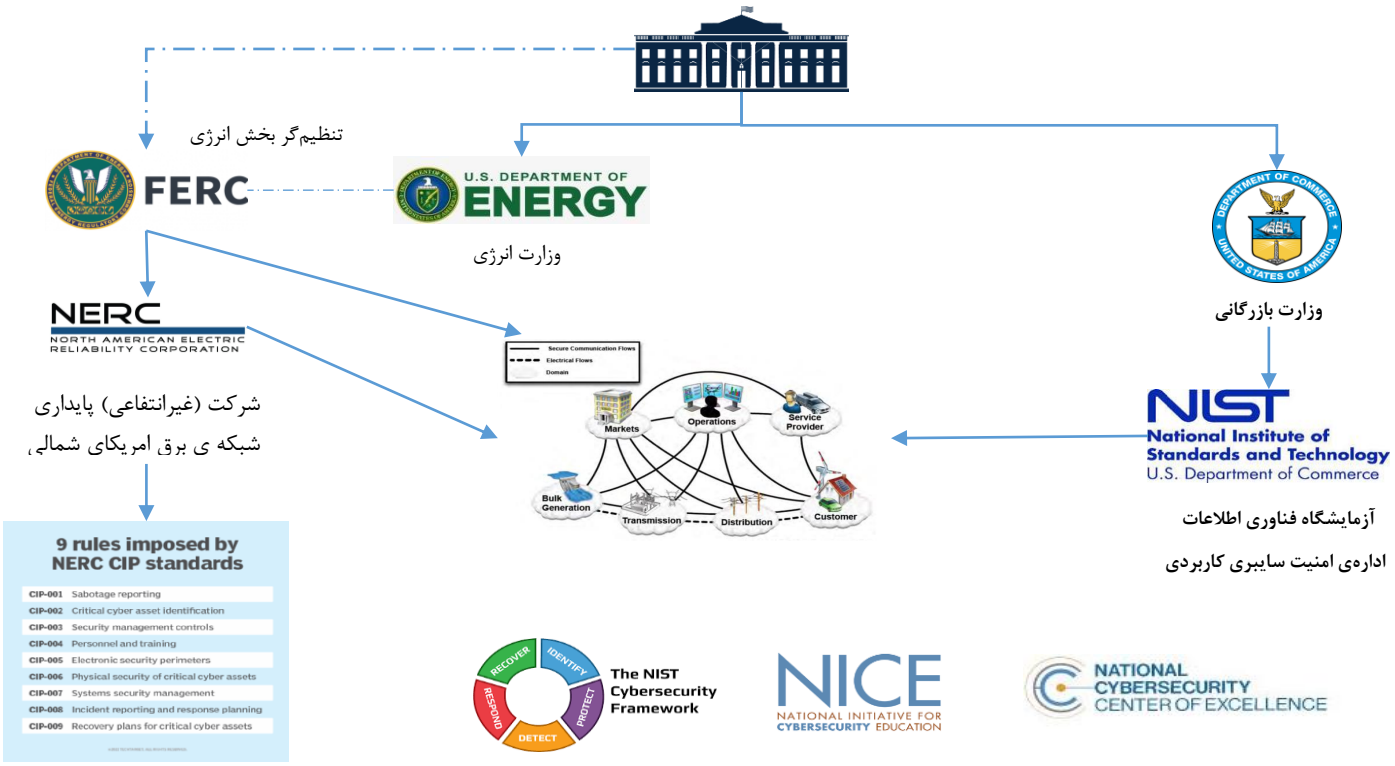


شکل ۳: چارچوب نهادی سیاست گذاری و برنامه ریزی بخش امنیت سایبری OT صنعت

مقررات‌گذاری و تنظیم‌گری و استاندارد

در خصوص تنظیم‌گری فنی حوزه برق شرکت غیر انتفاعی پایداری شبکه‌ی برق امریکای شمالی که ذیل تنظیم گر اقتصادی بخش انرژی فعالیت می‌کند. موارد مرتبط با امنیت سایبری شبکه برق نیز در دستورالعمل‌های این شرکت دیده شده است. در کنار این شرکت سازمان استاندارد و فناوری نیز دستورالعمل‌هایی بصورت کلی در همه‌ی زمینه‌های امنیت سایبری و همچنین بخش صنعتی تهیه می‌کند.

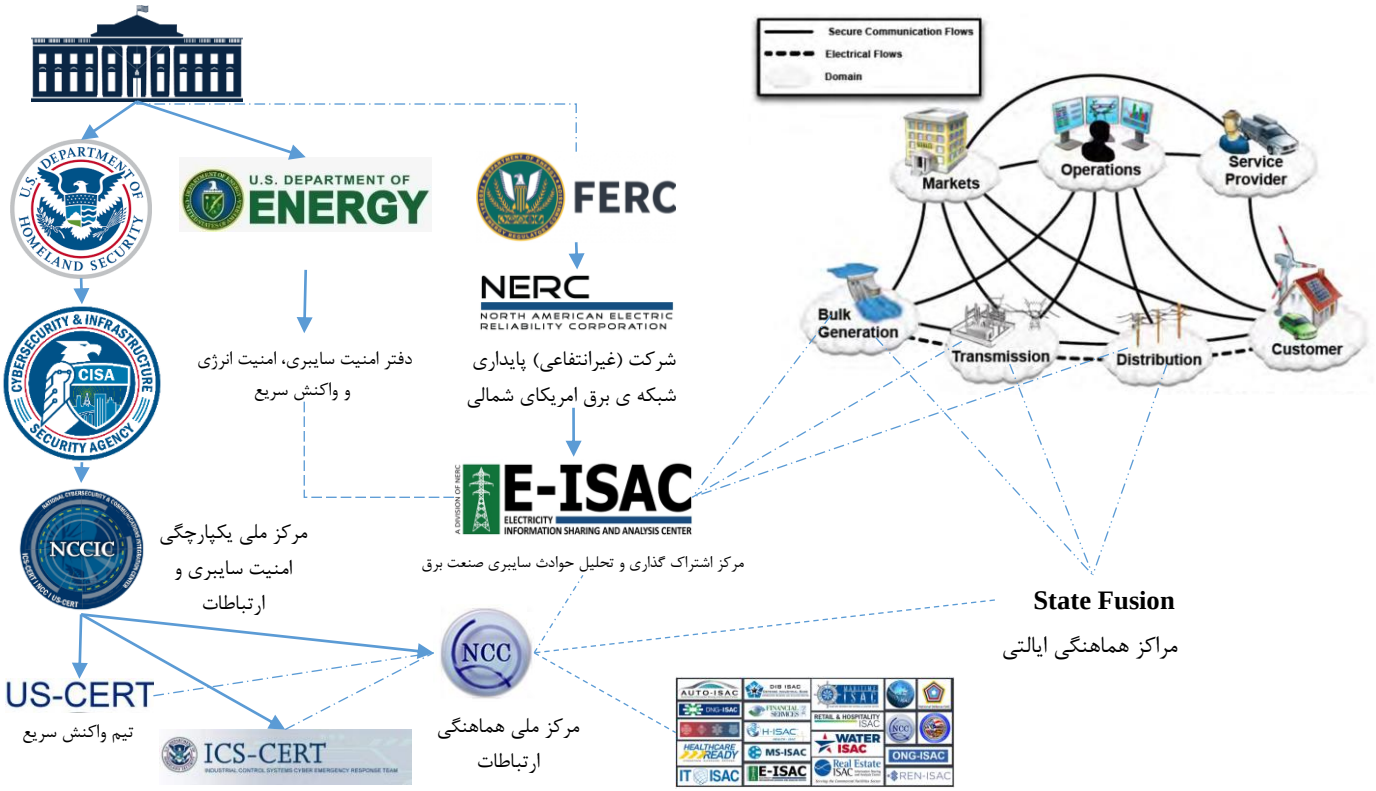
بخش آزمایشگاهی نیز در ذیل وزارت انرژی و از طریق ۱۷ آزمایشگاه ملی و همچنین آزمایشگاه‌های سازمان استاندارد پوشش داده می‌شود.



شکل ٤: تظام تنظیم گری و استاندارد حوزه امنیت سایبری صنعتی[٥]

نظام اشتراک‌گذاری تهدیدهای سایبری

در کشور امریکا در شانزده حوزه زیرساخت حیاتی، مراکزی تحت عنوان اشتراک‌گذاری و تحلیل حوادث سایبری تشکیل شده‌اند. این مراکز با بخش خصوصی و سازمان‌های حاکمیتی ارتباط داشته و به تحلیل حوادث سایبری و اشتراک تجربه حاصل از آن با سایر ذی نفعان آن بخش می‌پردازند. مراکز تحلیل حوادث سایبری از طریق مرکز ملی هماهنگی ارتباطات و توسط مرکز ملی یکپارچگی امنیت سایبری و ارتباطات که ذیل سازمان امنیت سایبری و زیرساخت تعریف شده است هماهنگ می‌شوند. همچنین ایالت‌های مختلف از طریق مراکز هماهنگی ایالتی با مرکز ملی هماهنگی ارتباطات در تماس هستند. بخش برق نیز مرکز اشتراک‌گذاری تهدیدهای سایبری صنعت برق را در ذیل شرکت غیر انتفاعی پایداری شبکه برق امریکای شمالی در اختیار دارد.



شکل ۵: نظام اشتراک گذاری تهدیدهای سایبری[۵]

سیاست‌گذاری علم و فناوری در زمینه امنیت سایبری صنعتی

در زمینه‌ی سیاست‌گذاری علم و فناوری در کشور امریکا شورای ملی علم و فناوری وجود دارد که در ذیل آن کمیته‌های تجاری‌سازی علم و فناوری، محیط زیست، امنیت ملی و داخلی، علوم بنیادی، آموزش‌های بین رشته‌ای، فناوری و دو کمیته خاص هوش مصنوعی و کمیته مشترک در خصوص زیست بوم پژوهش تشکیل شده‌اند. موضوع امنیت سایبری صنعتی در دو کمیته فناوری و امنیت ملی و داخلی پیگیری می‌شود که در آن از وزارت انرژی، دفتر امنیت سایبری، امنیت انرژی و واکنش سریع عضویت دارد. پروژه‌های فناورانه مرتبط با امنیت سایبری شبکه‌های صنعتی انرژی از طریق این دفتر امنیت سایبری وزارت انرژی و عاملیت آزمایشگاه‌های ملی و موسسه تحقیقات صنعت برق امریکا اجرایی می‌شوند.

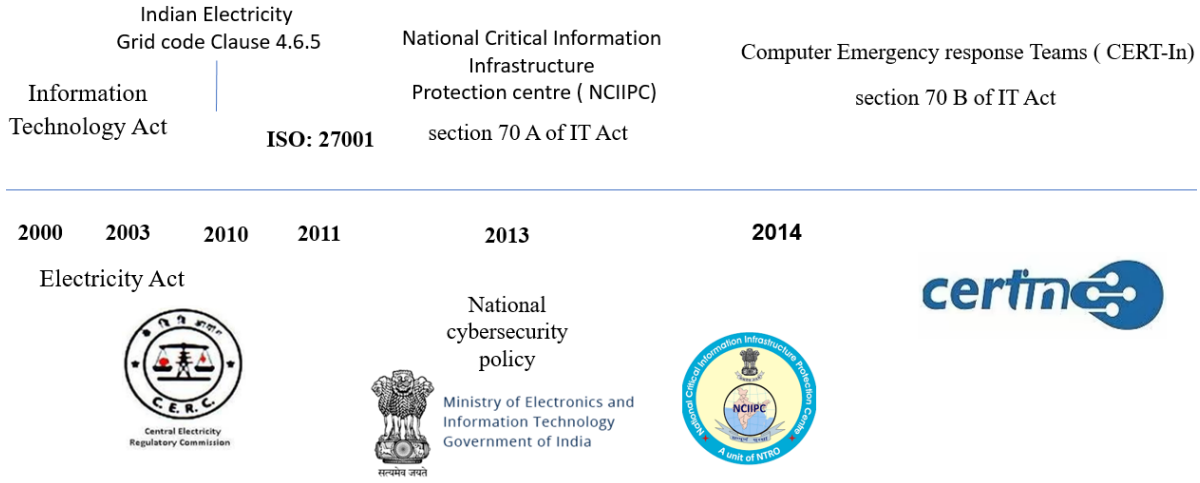
شکل ٦: جایگاه امنیت سایبری صنعتی در نظام سیاست‌گذاری علم و فناوری امریکا[۵]

شرکت‌های بهره‌بردار و عملیاتی

حدود هشتاد درصد از شرکت‌های برق در کشور ایالات متحده امریکا خصوصی هستند و بر اساس مقرراتی که شرکت غیر انتفاعی پایداری شبکه برق امریکای شمالی وضع می‌کند، فعالیت می‌کنند. در شرکت‌ها، مدیر امنیت سایبری[۱۸]مسئولیت تامین امنیت سایبری را بر عهده دارد.

تجربه کشور هند

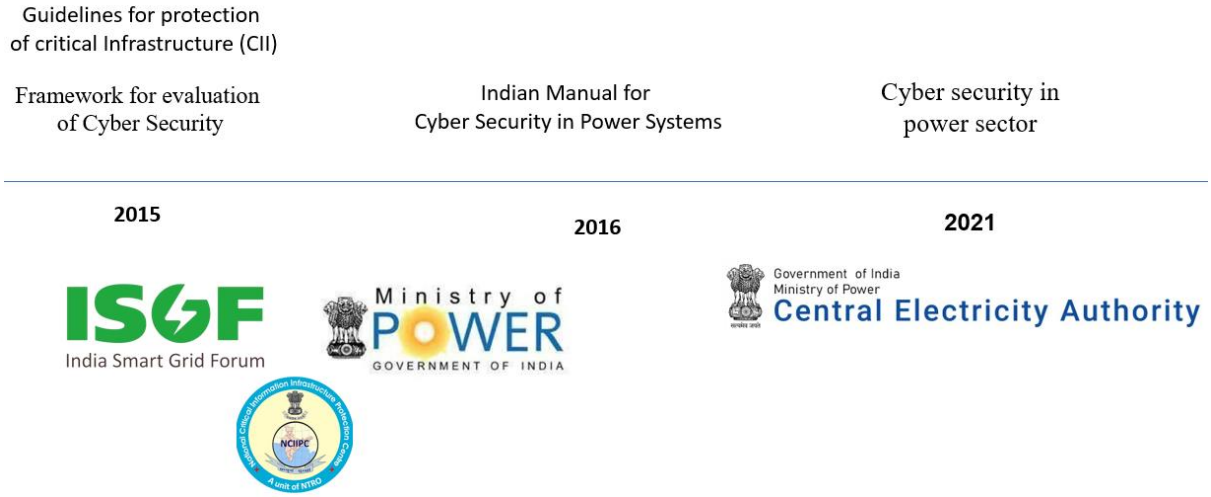
در کشور هند برخلاف کشور امریکا مساله امنیت سایبری زیرساخت‌های حیاتی سبقه‌ی طولانی ندارد. مرتبط‌ترین فعالیت‌ها در این خصوص به قانون فناوری اطلاعات[۱۹]مصوب سال ۲۰۰۰ بر می‌گردد و طبق آن از سال ۲۰۱۱ سازمان‌ها موظف به اجرای استاندارد ایزو ۲۷۰۰۱ در شبکه‌ی اداری سازمان خود می-شوند. در سال ۲۰۱۳ سیاست ملی امنیت سایبری[۲۰]توسط وزارت الکترونیک و فناوری ارتباطات منتشر می‌شود. طبق بخش ۷۰ قانون فناوری اطلاعات مرکز ملی حفاظت از زیرساخت‌های حیاتی[۲۱] در ذیل سازمان ملی تحقیقات فنی (ذیل نخست وزیر هند) و تیم امداد اضطراری هند[۲۲]در وزارت الکترونیک و فناوری اطلاعات تشکیل می‌شوند (شکل۷ و ۸)[۷].



شکل ۷: قوانین و مقررات کشور هند در حوزه امنیت سایبری صنعت در گذر زمان

منبع: یافته های پژوهش

۱۸ chief information security officer (CISO)
۱۹ Information Technology Act
۲۰ National Cybersecurity policy
۲۱ National Critical Information Infrastructure Protection centre (NCIIPC)
۲۲ Computer Emergency response Teams (CERT-In)

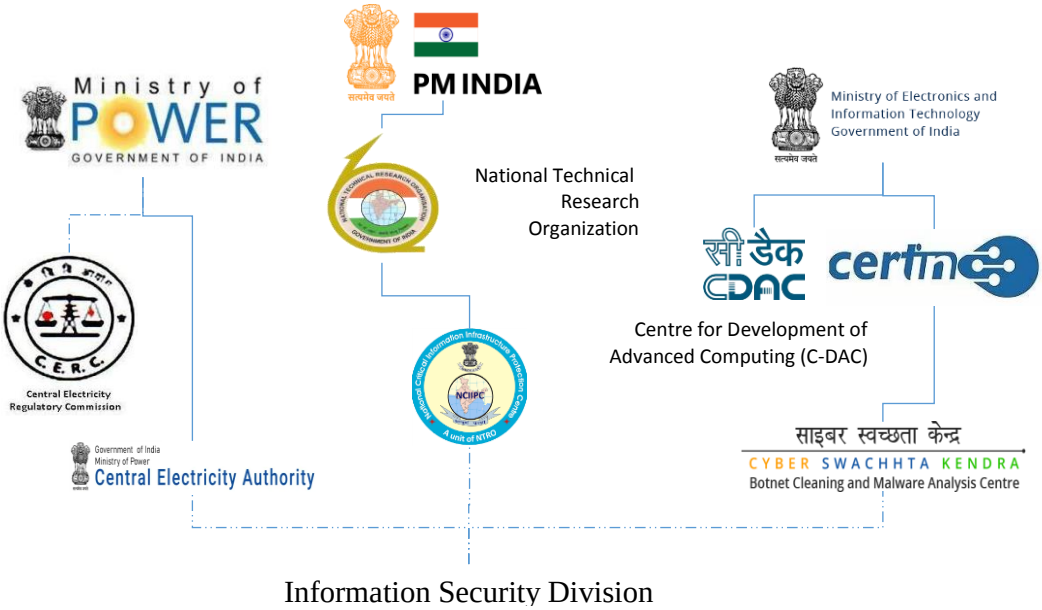


شکل ۸: قوانین و مقررات کشور هند در حوزه امنیت سایبری صنعت برق

منبع: یافته های پژوهش

اولین دستورالعمل‌ها توسط مرکز حفاظت از زیرساخت‌های حیاتی در سال‌های ۲۰۱۵ و ۲۰۱۶ منتشر می‌شود. در حوزه صنعت برق قانون برق در سال ۲۰۰۳ تصویب شده است. بخش چهارم از مقررات بخش برق که در سال ۲۰۱۰ توسط تنظیم‌گر بخش برق هند ابلاغ شده است، به موضوع امنیت سایبری اشاره دارد. سازمان مرکزی برق هند[۲۳]نیز به عنوان مقررات‌گذار فنی بخش برق در سال ۲۰۱۵ الزامات مرتبط با امنیت سایبری سیستم‌های کنترل در بخش برق را تدوین می‌کند. همچنین در سال ۲۰۲۱ مقررات امنیت سایبری در شبکه برق توسط این نهاد ابلاغ می‌شود که به موجب آن سازمان‌ها موظف به ایجاد اداره امنیت سایبری می‌شوند و این اداره نقطه تماس با سازمان‌های مقررات‌گذار حوزه امنیت سایبری اداری و صنعتی می‌شود (شکل۹)[۸] . دو نهاد مرکز ملی آموزش قدرت [۲۴]و مرکز تحقیقات برق[۲۵]در وزارت نیرو و مرکز توسعه و محاسبات پیشرفته کامپیوتری[۲۶]در ذیل وزارت الکترونیک و فناوری اطلاعات خدمات تست و آزمایشگاه را ارئه می‌دهند.

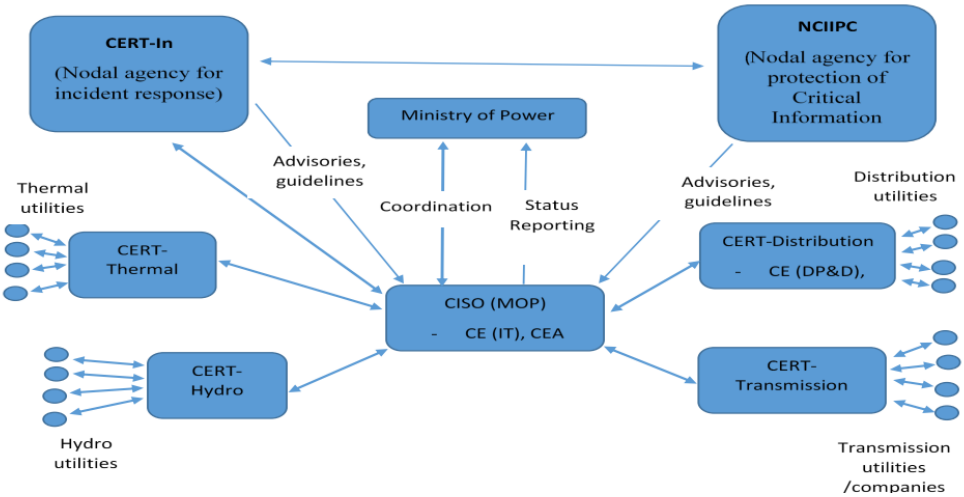
۲۳ Central Electricity Authority
۲۴ National Power Training Institute (NPTI)
۲۵ Central Power Research Institute (CPRI)
۲۶ Centre for Development of Advanced Computing (C-DAC)



شکل ۹: سازمان های کلیدی در نظام حمکرانی امنیت سایبری زیرساخت های اساسی کشور هند

منبع: یافته های پژوهش

همچنین شش مرکز امداد اضطراری در بخش‌های نیروگاه‌های حرارتی، نیروگاه‌های برق‌آبی، شبکه انتقال، شبکه توزیع، بهره‌برداری شبکه و بخش انرژی‌های تجدید پذیر شکل گرفته که این بخش‌ها همزمان تهدیدهای سایبری را نیز به اشتراک می‌گذارند. در برخی بخش‌ها تیم امداد اضطراری در ذیل اداره امنیت سایبری ایجاد شده است. شکل ۱۰ ارتباط بین این نهادها و نهادهای سیاست‌گذار و مقررات گذار را نشان می‌دهد.

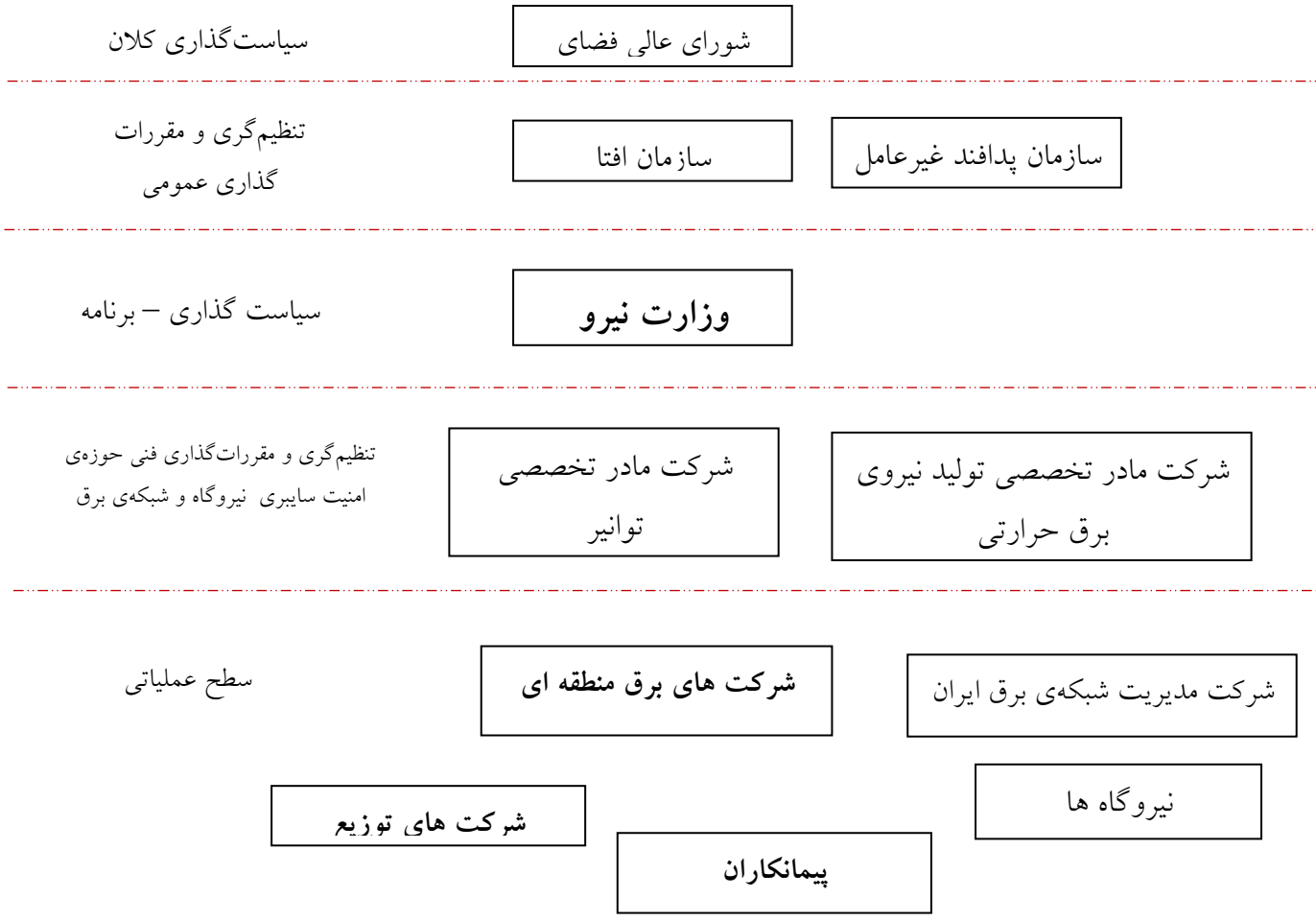


شکل ۱۰: ارتباط بین نهادهای ذی نفع در نظام امنیت سایبری شبکه برق هند[۹]

وضعیت کنونی کشور ایران

نقاط قوت و ضعف ساختار موجود در ایران

از نقاط قوت نظام حکمرانی موجود برای امنیت سایبری زیرساخت‌های حیاتی در کشور وجود نهادهای سیاست‌گذار (شورا و مرکز ملی فضای مجازی) و مقررات گذار عمومی حوزه امنیت سایبری (دو نهاد مقررات گذار مرکز راهبردی افتا و پدافند غیر عامل)، کمیته‌ها و کارگروه‌های امنیت سایبری در سطح وزارت نیرو، شرکت‌های مادر تخصصی و همچنین شرکت‌های عملیاتی و همچنین مشخص بودن مقام پاسخگو در قبال حملات سایبری (بالاترین مقام هر دستگاه) هستند. از نقاط ضعف و چالش‌هایی که کشور آن مواجه هست، می‌توان به عدم مشخص بودن مسئولیت امنیت سایبری شبکه‌ی صنعتی در چارت سازمانی شرکت‌ها، موازی کاری نهادهای تنظیم‌گر عمومی که شرکت‌ها را با چالش مواجه کرده است و عدم شفاف بودن بودجه امنیت سایبری و همچنین عدم بلوغ دانش حوزه‌ی امنیت سایبری صنعتی را اشاره کرد (شکل۱۱). در خصوص زیست بوم توسعه فناوری این بخش، آزمایشگاه‌ها و محیط‌های آزمون مورد نیاز برای مقررات و استانداردگذاری و همچنین تست سایبری تجهیزات و همچنین سنجیدن عملکرد فناوری-های نوین، تکمیل نشده‌اند. همچنین آموزش‌های مورد نیاز برای متخصصین در دانشگاه‌ها و محیط‌های صنعتی به اندازه نیاز کشور توسعه پیدا نکرده است.



شکل ۱۱: سطوح مختلف حکمرانی امنیت سایبری در حوزه صنعت برق

منبع: یافته‌های پژوهش

پیشنهادهای سیاستی:

با توجه به بررسی تجربه نظام حکمرانی امنیت سایبری زیرساخت صنعتی برق در کشور امریکا و هند و همچنین وضعیت کنونی کشور در این خصوص جهت رفع نقایص ساختار موجود در کشور پیشنهادهای زیر قابل طرح است:

- در خصوص اصلاح چارت سازمانی پیشنهاد می شود که مسئولیت‌ها در حوزه IT و حوزه-ی OT از یکدیگر مجزا گردند. حوزه شبکه اداری به دفاتر فناوری اطلاعات و حوزه صنعتی به دفاتر فنی مرتبط به هر بخش اختصاص یابد.
- پیشنهاد می‌شود نظام اشتراک‌گذاری تهدیدهای امنیت سایبری صنعتی با الگو از کشور امریکا ایجاد شود، این اتفاق سطح آمادگی زیرساخت‌ها در مقابل آسیب پذیری‌های سایبری را بالا می‌برد.
- آموزش‌های مرتبط با امنیت سایبری صنعتی با کمک دانشگاه‌ها و موسسات آموزشی و همچنین مراکز معتبر بین المللی برای برگزاری دوره‌های تخصصی این حوزه و تربیت نیروی متخصص یکی دیگر از نیازمندی‌های کشور است.
- زیرساخت‌های آزمایشگاهی برای ارزیابی آسیب پذیری‌های نرم افزاری و سخت افزاری تجهیزات صنعتی در کشور بایستی ایجاد گردد.
- زیست بوم توسعه فناوری‌های امنیت سایبری صنعتی با ایجاد محیط‌های آزمون (Test Beds) برای کمک به تنظیم‌گران این حوزه در زمینه مقررات‌گذاری و استانداردگذاری و همچنین ارزیابی عملکرد فناوری‌های مرتبط با این بخش که در محیط صنعتی واقعی بکاربرده خواهند شد، تکمیل گردد.
- پیشنهاد می‌شود موضوع توسعه فناوری‌های امنیت سایبری صنعتی با توجه به اهمیت زیرساخت‌های حیاتی صنعتی در اولویت توسعه فناوری‌های کشور قرار گیرد.

مراجع

[1] Soltan, S.; Mazauric, D.; Zussman, G. Cascading failures in power grids: Analysis and algorithms. In Proceedings of the 5th International Conference on Future Energy Systems, Cambridge, UK, 11–13 June 2014; pp. 195–206. [Google Scholar]

[2] Haes Alhelou, H.; Hamedani-Golshan, M.E.; Njenda, T.C.; Siano, P. A Survey on Power System Blackout and Cascading Events: Research Motivations and Challenges. Energies 2019, 12, 682. https://doi.org/10.3390/en12040682

[3] General (ret.) Michael Hayden, Curt Hébert and Susan Tierney, Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat, Bipartisan Policy Center, 2014.

[4] Keith Stouffer (NIST), Suzanne Lightman (NIST), Guide to Industrial Control Systems (ICS) Security, Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC), 2015, http://dx.doi.org/10.6028/NIST.SP.800-82r2

[5] Ballou, T. M.; Allen, Joseph A.; and Francis, Kyle, "U.S. Energy Sector Cybersecurity: Hands-Off Approach or Effective Partnership?" (2016). *Psychology Faculty Publications*. 170. https://digitalcommons.unomaha.edu/psychfacpub/170

[6] William K.Tirrell," United States Cyber security Strategy, Policy, and Organization: Poorly Postured to cope with a Post-9/11 Security Environment? ", Master's Thesis, U.S. Army Command and General Staff College

[7] P. K. Jha, F. Teotia and A. K. Saxena, "Cyber Security in the Indian Electricity Distribution System: A Review," *2023 5th International Conference on Energy, Power and Environment: Towards Flexible Green Energy Technologies (ICEPE)*, Shillong, India, 2023, pp. 1-6, doi: 10.1109/ICEPE57949.2023.10201598

[8] Transmission, Grid Operation, RE and Distribution for ensuring cyber security in Indian. Power Sector, 2021.

https://cea.nic.in/wpcontent/uploads/notification/2021/10/Guidelines_on_Cyber_Security_in_Power_Sector_2021-2.pdf

[9] CYBER SECURITY IN POWER SYSTEM, 2017. https://erpc.gov.in/wp-content/uploads/2018/03/ERPC_Cyber-Security-in-Power-system_presentation.pdf

[۱۰] تاسیس شورا و مرکز ملی فضای مجازی، https://majazi.ir/general_content/76438%D9%85%D8%B9%D8%B1%D9%81%DB%8C%D9%85%D8%B1%DA%A9%D8%B2%D9%85%D9%84%DB%8C%D9%81%D8%B6%D8%A7%DB%8C%D9%85%D8%AC%D8%A7%D8%B2%DB%8C.html?t=%D9%85%D8%AD%D8%AA%D9%88%D8%A7%DB%8C-%D8%B9%D9%85%D9%88%D9%85%DB%8C

اندیشکده حکمرانی انرژی و منابع ایران

وابسته به پژوهشکده مطالعات فناوری ریاست‌جمهوری، به عنوان یک کانون تفکر تخصصی در حوزه انرژی و منابع در کشور، به منظور ارتقای سطح کیفیت تصمیم‌سازی و اثرگذاری بر فرآیند تصمیم‌گیری در زمینه تدوین سیاست‌های بخش انرژی و منابع تاسیس شده است. این اندیشکده با رویکرد مسئله محوری ضمن تشخیص موضوعات کلیدی بخش انرژی و منابع، آسیب‌شناسی آنها را در دستورکار خود قرار داده و درنهایت به تصمیم‌گیران این عرصه راهکارهای سیاستی را پیشنهاد می‌دهد.

با توجه به اهمیت بخش انرژی در کشور و ضرورت ارائه راهبردهای تجویزی و عملیاتی برای توسعه این بخش، اندیشکده حکمرانی انرژی و منابع ایران قالبی با عنوان «سیاست‌نامه» طراحی کرده است. «سیاست‌نامه» نوشتاری است که پس از بیان یکی از مسائل بخش انرژی در کشور به ارائه‌ی راهبردها و راهکاری سیاستی جهت اصلاح آن مسأله می‌پردازد و امید دارد گامی اثربخش جهت اعتلای نظام جمهوری اسلامی ایران بردارد.