دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)
یازدهمین کنفرانس فرماندهی و کنترل ایران
(۲۰ و ۲۱ آذرماه ۱۳۹۸)
انجمن علمی فرماندهی و کنترل ایران
(C4I)

اخلال در سیستم‌های فرماندهی و کنترل، مبنای چهارچوب نوین طراحی تهدیدات و بحران‌ها

محمّد علی شکوهیان‌راد

مدرّس مهمان دانشکده‌ی مهندسی پردیس فارابی دانشگاه تهران، کارشناس ارشد؛ cm@shokoohian.ir

چکیده

عمده‌ی تهدیدات و بحران‌هایی که بشر با آن مواجه است، طبیعی نیست و عامل آن انسان می‌باشد. از سوی دیگر بر اساس سیر تاریخی تهدیدات و بحران‌های بشری مشخص می‌شود که سطح اثرگذاری و پیچیدگی این قبیل بحران‌ها در هر دوره، ارتباط مستقیم با سطح پیشرفت دانش و تکنولوژی آن دوره دارد. از این رو دانش و تکنولوژی غالب در هر دوره، نقش چهارچوب طراحی و ایجاد تهدید و بحران را بر عهده دارد.

در عصر حاضر که به‌دلیل توسعه‌ی دانش سایبرنتیک، تصمیمات و رفتار پدیده‌های هوشمند از طریق کانالیزه کردن اطلاعات ورودی‌شان کنترل می‌شود، مفهوم «فرماندهی – کنترل» به‌عنوان یک مفهوم بنیادین پذیرفته شده است تا آنجا که بسیاری از طرح‌ریزی‌های راهبردی و طرح‌های علمی مبتنی بر فرماندهی - کنترل تعریف می‌شوند. بر همین اساس سیستم فرماندهی – کنترل که بر مفهوم فرماندهی – کنترل جامه‌ی عمل پوشانده، در تمامی زمینه‌ها و حوزه‌های نظامی، غیر نظامی، تأسیسات حساس و در یک کلام «زیرساخت‌های تمدنی» نقش جدی و بی‌بدیل یافته؛ به‌گونه‌ای که وقفه در عملکرد یک سیستم فرماندهی – کنترل به‌معنای وقفه در زیرساخت حساس تحت مدیریت آن است و وقفه در زیرساخت‌های تمدنی نیز به‌مثابه اخلال در حوزه‌های تمدنی است که می‌تواند عواقب جدی و بعضاً جبران‌ناپذیر در پی داشته باشد.

بدین سبب چهارچوب طراحی تهدید و بحران در حال تغییر است به‌طوری که «اخلال در سیستم‌های فرماندهی – کنترل» مبنای تهدیدات و بحران‌های نوین بشری می‌باشد. جامعیت چهارچوب نوین از این حیث است که سیستم‌های فرماندهی – کنترل را به ماشین‌های هوشمند مدیریتی نظیر اسکادا، PLC و ... محدود نمی‌کند بلکه پدیده‌های هوشمند زیستی را نیز از یک سلول گرفته تا انسان مورد مطالعه قرار داده و ضمن شناسایی سیستم فرماندهی – کنترل هر کدام، برای کنترل آن برنامه‌ریزی عملیاتی می‌نماید. چنین چهارچوب جامعی که از سیستم‌های فرماندهی – کنترل زیستی تا فرماندهی – کنترل‌های زیرساختی را در برگیرد، بی‌سابقه است.

لذا مشخص می‌شود که اولاً اخلال در سیستم‌های فرماندهی – کنترل، مبنای طرح‌ریزی تهدیدات و بحران‌های نوین است، ثانیاً بحران‌های نوین نسبت به بحران‌های سابق از چهار جنبه‌ی دقت، عمق اثرگذاری، کنترل‌پذیری از سوی عامل بحران و بازدارندگی قربانی بحران پیشرفت چشمگیری دارد و ثالثاً مدیریت این تغییر مهم و راهبردی نیازمند بازنگری، بروز رسانی و ارتقاء محتوای دانش مدیریت بحران در تناسب با چهارچوب نوین تهدید و بحران است تا بتوان همچنان بالاترین سطح پیش‌بینی و آمادگی در برابر تهدیدات و بحران‌های نوین را فراهم نمود.

کلمات کلیدی: اخلال در سیستم‌های فرماندهی و کنترل؛ چهارچوب نوین طراحی تهدید و بحران؛ بازنگری در دانش مدیریت بحران

۱. مقدمه

تهدیدات و بحران‌ها از جمله پدیده‌هایی هستند که همواره با بشر همراه بوده‌اند. مطالعات نشان می‌دهد که سطح وقوع تهدید و بحران در هر دوره، به میزان پیشرفت دانش و تکنولوژی آن دوره وابسته است. به‌عبارت دیگر ابعاد کیفی و کمّی دانش بشری بر نوع و کمیّت تهدیدات و بحران‌ها اثرگذار است. این مهم حتی در خصوص تهدیدات و بحران‌های زیست‌محیطی صادق است. برای نمونه بحران گرم شدن کره‌ی زمین ناشی از تکنولوژی‌هایی است که میزان گازهای گلخانه‌ای را بیش از ظرفیت زیست‌محیطی زمین انتشار داده‌اند. بر این اساس می‌توان اذعان داشت که ارتباط میان بحران‌ها و تهدیدات با میزان پیشرفت کیفی و کمّی دانش و تکنولوژی در آینده نیز استمرار خواهد یافت.

مفهوم تهدید و بحران که همان ایجاد خطر برای حیات فردی و جمعی انسان و محیط وی است، همواره در طول تاریخ ثابت بوده و آنچه تغییر نموده، خاستگاه تهدید و بحران و شیوه‌های وقوع آن علیه تمدن‌های بشری است. از تفاوت در کیفیت و کمیّت تهدیدات و بحران‌ها، سبک‌های مختلفی برای کنترل و مهار آنها حاصل شده که در مجموع دانش مدیریت بحران را تدوین و تقویت نموده‌اند.

مدیریت بحران؛ علاوه بر تأثیرپذیری از عقاید، باورها، فرهنگ (امیری، علوی‌وفا و صادقی، زمستان ۱۳۹۵) و سایر ویژگی‌های و ظرفیت‌های غالب یک ملت در هر عصر؛ تحت تأثیر شرایط جهانی نیز می‌باشد. به‌عبارت دیگر دانش مدیریت بحران در هر ملتی علاوه بر آنکه به مرور زمان تکامل می‌یابد، با رشد و ارتقاء تکنولوژی‌های بشری و آثار آن بر سایر مؤلفه‌های تمدنی دیگر کشورها نیز دست‌خوش تغییر و تحول می‌گردد.

در مطالعات صورت گرفته به‌منظور فهم روند تغییرات و فرایند پیچیده شدن تهدیدات و بحران‌هایی که بشر مسبب آنها است؛ این مهم حاصل شده که در هر عصر، کیفیت تهدید و بحران از قواعد و چهارچوب مشخصی پیروی می‌کند. لذا شناخت آن چهارچوب کلان -که خود تکیه بر سطح دانش و تکنولوژی آن عصر دارد- می‌تواند جنس و نحوه‌ی وقوع تهدیدات و بحران‌های احتمالی را پیش‌بینی نموده و برای مدیریت آنها از قبل به طرح‌ریزی راهبردی بپردازد.

فهم دقیق چهارچوب تهدید و بحران از منظر علمی و عملی و همچنین میزان وابستگی عاملان تهدید به آن، یکی از شروط اساسی جهت آینده‌شناسی و مدیریت بحران‌ها است. از سوی دیگر شرایط امروز جهان از حیث تکنولوژی‌های پیشرفته و طرح‌ریزی‌های راهبردی به‌گونه‌ای است که انتظار می‌رود در آینده‌ی نزدیک، چهارچوب تهدید و بحران تغییر نموده و بازطراحی شود. مبنای چهارچوب نوین تهدید و بحران در عصر جدید «اخلال در سیستم‌های فرماندهی – کنترل» است که تکیه بر دانش سایبرنتیک[1] و تکنولوژی‌های سایبری[2] دارد.

این مهم برای تمامی کشورها بالأخص جمهوری اسلامی ایران که در معرض تهدیدات و بحران‌های متنوع و عامدانه است از اهمیت ویژه برخوردار می‌باشد چرا که اگر برای شناخت و تسلط کامل بر چهارچوب جدید تهدید و بحران، مطالعات تخصصی انجام نشود در آینده دچار غافلگیری راهبردی خواهند شد.

در پژوهش حاضر تلاش بر این است تا چهارچوب تهدید و بحران مبتنی بر اخلال در سیستم‌های فرماندهی – کنترل تشریح شود. طبیعی است که این مهم، هم از منظر نظامی قابل تحلیل و بررسی است و هم از نگاه زیرساخت‌های حساس تمدنی که نظامی نیستند اما اخلال در آنها عملاً می‌تواند موجب وقوع تنش، تهدید و بحران در حوزه‌ی تمدنی و انسانی شود از اهمیت ویژه برخوردار است.

۲-۱. ضرورت پژوهش

وضعیت امروزی جهان به‌نحوی است که تکنولوژی در زمینه‌های مختلف، نقش تحول‌آفرین و چشمگیری داشته و بخش عمده‌ای از امور از طریق ماشین انجام می‌َشود. از این رو لازم است سیستم‌هایی جامع و واسط میان انسان و ابزارهای اجرایی قرار داشته باشند که توسط آن بتوان فرمان را صادر و کنترل لازم را اعمال نمود. فرماندهی از آن جنبه مورد نیاز است تا انسان بتواند کنترل وقایع و رویدادها را

[1] Cybernetics

[2] Cyber Technology

به‌دست گیرد.چنین وظیفه و امکانی توسط سیستم‌های فرماندهی – کنترل مهیا شده است.

از سوی دیگر حیات تمدن‌ها به زیرساخت‌های حساس[3] وابسته است و هر بخش از آمایش جامعه با این زیرساخت‌ها عجین شده. در عصر حاضر مدیریت بر زیرساخت‌های حساس توسط سیستم‌های فرماندهی – کنترل صورت می‌پذیرد که علی‌رغم کاربردهای مختلف و گوناگون، از حیث دانش سایبرنتیک و منطق فنّی بر اساس اصول یکسان طراحی شده‌اند. از این رو سیستم‌های فرماندهی – کنترل برای اعمال قدرت و مدیریت بر زیرساخت‌ها و سامانه‌های مختلف با کاربردهای متفاوت به‌کارگیری می‌شوند. لذا اگر مدیریت این سیستم‌ها در اختیار افراد غیرمجاز و کشورهای متخاصم قرار گیرد، می‌تواند تبعات بسیار سهمگین و جبران‌ناپذیری را برای کشور در پی داشته و عمیق‌ترین و گسترده‌ترین تهدیدات و بحران‌ها را علیه امنیت ملی سبب شود.

در حوزه‌ی نظامی اگر سیستم‌های فرماندهی – کنترل مختل شوند بخش عمده‌ای از امور لجستیکی، آمادی، ارتباطی، تجهیزاتی و تسلیحاتی،جریان اطلاعات، اشراف اطلاعاتی، زنجیره‌ی فرمان، هماهنگی‌های عرضی، اقدامات به هنگام و ... غیر فعال شده یا حدأقل با تأخیر، افزایش سختی و کاهش چشمگیر کیفیت انجام می‌شوند. بنابر این اخلال در سیستم‌های فرماندهی – کنترل عملاً به‌معنای اخلال در عملکرد تمامی بخش‌های یک ارتش است که به ناتوانی آن منجر خواهد شد.

در حوزه‌ی غیر نظامی نیز عموم زیرساخت‌های تمدنی مانند بخش‌های انرژی، پولی و مالی و ... که نقش حیاتی در استمرار مدیریت جامعه توسط حاکمیت دارند، به سیستم‌های فرماندهی – کنترل وابسته هستند و متخصصان به‌واسطه‌ی چنین سیستم‌هایی می‌توانند طرح‌ریزی‌های عملیاتی را به اجرا در آورند.

از سوی دیگر سیستم‌های فرماندهی – کنترل، محدود به سیستم‌های ماشینی نیست بلکه در دانش نوین، برای سیستم‌های فرماندهی – کنترل طبیعی نیز امکان برنامه‌ریزی و به‌تبع اخلال وجود دارد. مهم‌ترین نمونه‌ی سیستم فرماندهی – کنترل طبیعی که با عنوان سیستم‌های بیوسایبر[4] شناخته می‌شود **انسان** است که فرایند درک ذهنی و پردازش اطلاعاتی وی، همانند سیستم‌های هوشمند ماشینی است زیرا فرماندهی – کنترل ماشین از فرماندهی – کنترل انسان الگو پذیرفته است و دانش هوش مصنوعی[5] روند مطالعات تکمیلی آن را دنبال می‌نماید.

لذا وقوع هرگونه اخلال در سیستم‌های فرماندهی – کنترل، از یک فرد گرفته تا یک کشور به منزله‌ی وقوع نوعی از تهدید و بحران است که از حیث کیفی و کمّی با بحران‌های ادوار گذشته قابل قیاس نیست، به‌ویژه اگر در کوتاه مدت رفع نشود و استمرار یابد. از این رو تمرکز پژوهشی و آینده‌شناسانه بر چهارچوب نوین تهدیدات و بحران‌ها که بر اساس اخلال در سیستم‌های فرماندهی – کنترل شکل گرفته، یکی از ضروری‌ترین و اُولی‌ترین مسائل در حوزه‌ی مدیریت بحران است.

۳-۱. سؤالات پژوهش

سؤالات پژوهش عبارت است از:

۱. سیستم‌های فرماندهی – کنترل در طرح‌ریزی تهدیدات و بحران‌های نوین از چه نقش و جایگاه برخوردار است؟
۲. تفاوت نظری و عملی میان تهدیدات و بحران‌های سابق با بحران‌هایی که ابتناء بر اخلال در سیستم فرماندهی – کنترل دارند چگونه است؟
۳. به استناد طرح‌ریزی تهدیدات و بحران‌ها بر اساس اخلال در سیستم‌های فرماندهی – کنترل، آیا دانش مدیریت بحران نیازمند بازنگری و بروز رسانی است؟

۴-۱. فرضیه‌های پژوهش

فرضیه‌های پژوهش عبارت است از:

۱. مبنای تهدیدات و بحران‌های نوین، اخلال در سیستم‌های فرماندهی – کنترل است؛

[3] Critical Infrastructure
[4] Biocyber system
[5] Artificial Intelligence

۲. محتوای فعلی دانش مدیریت بحران برای آمادگی و مقابله با بحران‌های نوین کافی نیست و باید بازنگری و بروز رسانی شود.

۱-۵. اهداف پژوهش

اهداف پژوهش حاضر عبارت است از:

۱. چهارچوب نوین تهدید و بحران که ابتناء بر اخلال در سیستم فرماندهی – کنترل دارد، تبیین شود؛
۲. نمودار احصاء تهدیدات و بحران‌های نوین که هم به‌منظور بحران‌زایی و هم مدیریت بحران‌های رخ داده کاربرد دارد، ارائه گردد؛
۳. بنابر چهارچوب نوین تهدید و بحران، تغییرات ضروری محتوایی در دانش مدیریت بحران مشخص گردد؛

۱-۶. روش پژوهش

از آنجا که پژوهش حاضر از حیث هدف پژوهش اولاً به‌دنبال تبیین رابطه‌ی چهارچوب نوین تهدید و بحران با اخلال در سیستم فرماندهی – کنترل است و تلاش دارد ارتباط مستقیم این دو گزاره را اثبات نماید و ثانیاً بر این اساس، تغییرات ضروری در دانش مدیریت بحران و نمودار احصاء تهدیدات و بحران‌های نوین را ارائه کند؛ پژوهشی کیفی و نظری بوده و در زمره‌ی پژوهش‌های بنیادی قابل دسته‌بندی و ارزیابی است.

۱-۷. پیشینه‌ی پژوهش

بر اساس جست‌وجوهای صورت گرفته در پایگاه‌های معتبر علمی فارسی و انگلیسی زبان، اثری یافت نشد که در قالب پژوهش بنیادی، کلیات و چهارچوب نوین تهدیدات و بحران‌ها را در تمامی زمینه‌ها اعم از زیرساختی و زیستی مبتنی بر اخلال در سیستم فرماندهی – کنترل بررسی کرده و بر اساس آن الگوی احصاء تهدید و بحران را ارائه نموده باشد. بنابر این پژوهش حاضر از این حیث دارای نوآوری است.

اما بررسی آثار علمی که به‌صورت کاربردی، تهدیدات و بحران‌های معینی را مطالعه کرده و اثبات نموده‌اند کنترل پدیده‌های هوشمند از طریق سیستم‌های سایبرنتیک نوعی جدید از بحران‌ها را پدید آورده؛ حاکی از رشد تدریجی ادبیات این حوزه میان پژوهشگران بوده و امید است در آینده‌ی نزدیک پژوهش‌های بنیادی نیز به انجام رسد.

تام برگهاردت در اثری با نام «پیش درآمدی برای جنگ افزایش حملات سایبری با از سرگیری تهدیدهای نظامی و اشنگتن علیه ایران» (ترجمه‌ی محمود سبزواری، ماهنامه‌ی سیاحت غرب، دی ۱۳۹۰) به بررسی تهدیدات و بحران‌های ناشی از حمله به فرماندهی – کنترل زیرساخت‌های حساس پرداخته است. وی اذعان داشته: یکی از حوزه‌هایی که بر خلاف همه‌ی ادعاهای دولت‌مردان آمریکایی، سال‌ها است این کشور در آن فعال است، ساخت و گسترش تسلیحات سایبری است که عمدتاً زیرساخت‌های غیر نظامی کشورهای مورد نظر را هدف قرار می‌دهند... این مهم را ژنرال کیت الکساندر فرمانده فرماندهی سایبری آمریکا چنین ابراز داشته «دولت آمریکا در حال کار روی سیستمی است که در انجام حملات به ISPها کمک می‌کند.» (همان، ص ۵۰) وی نتیجه می‌گیرد «قدرت‌های بین‌الملل [به‌منظور بحران‌افرینی] مسیر سایبری را بر پرتاب موشک‌های ویرانگر و حملات بمب‌افکن‌ها علیه تأسیسات و زیرساخت‌های غیرنظامی مقدم می‌دارند» (همان، ص ۵۳).

در حوزه‌ی کنترل پدیده‌های هوشمند زیستی مانند انسان و ایجاد بحران از این طریق نیز نتایج مشابهی در پژوهش‌های موردی حاصل شده است.

ایوب محمدی به یاری همکارانش در پژوهشی با عنوان «نقش شبکه‌های اجتماعی مجازی در ایجاد بحران‌های اجتماعی» (فصلنامه‌ی دانش انتظامی، بهار ۱۳۹۶) اثبات کرده سیستم‌های سایبری در ایجاد بحران‌های اجتماعی نقش مستقیم و قابل توجهی دارند و به موازات توسعه‌ی آنها، در ایجاد بحران‌های اجتماعی و گسترش شرایط بحرانی در جامعه نقش بیشتری خواهند داشت.

احمد اکبری نیز در پژوهشی با عنوان نقش شبکه های اجتماعی در ایجاد و مهار بحران ها (فصلنامه‌ی ره‌آورد نور، تابستان ۱۳۸۹) ضمن بررسی نقش سیستم‌های سایبرنتیک در ایجاد بحران‌های مدنی، به نتایج مهمی دست یافته که عبارتند از:

- سیستم‌های سایبرنتیک وابسته به سازمان‌ها و نهادهای امنیتی و اطلاعاتی کشورها است. لذا در راستای اهداف امنیتی از آنها استفاده می‌شود.

- همانگونه که این سیستم‌ها در ایجاد بحران‌ها نقش مؤثری دارند، در جلوگیری از بحران و اطلاع‌رسانی صحیح، سریع و تبدیل ناهنجاری‌ها به هنجار و ایجاد فضای سالم و مثبت نیز می‌تواند مؤثر باشد، مشروط بر آنکه به خوبی و درستی از آن استفاده گردد.

۲. چهارچوب نظری پژوهش

جهان امروز از حیث مواجهه و مدیریت تهدید و بحران در شرایطی است که شاهد تغییر چهارچوب تهدیدات و بحران‌های بشری می‌باشد. مطالعه‌ی روند طرح‌ریزی، اقدامات و کنش‌های بین‌المللی این حوزه حاکی از آن است که چهارچوب تهدید و بحران در شرف یک تغییر مهم است و شواهد اولیه‌ی آن نیز عیان گشته. به‌عبارت دیگر قدرت‌های جهانی دریافته‌اند که باید به‌منظور کسب مزیت راهبردی نسبت به رقبا، چهارچوب تهدیدات و بحران‌ها را به‌گونه‌ای نوین طراحی نمایند.

سابق بر این عمده‌ی تهدیدات و بحران‌هایی که بشر مسبب آنها بود، ساختار و موجودیت قربانی را هدف قرار می‌داد. برای مثال می‌توان در حوزه‌ی بیولوژی و محیط‌زیست به مواردی همچون انتشار عوامل بیماری‌زا، آلوده‌سازی منابع حیاتی نظیر آب و استفاده از تسلیحات زیست‌محیطی و اتمسفری مانند هارپ[6] اشاره نمود یا در زمینه‌ی ایجاد بحران از طریق زیرساخت‌های تمدنی مواردی مانند خرابکاری صنعتی، تخریب و انهدام را ذکر کرد که کلیات پیکره‌ی زیرساخت را مورد حمله قرار می‌دادند.

این نوع تهدیدات دچار چهار اشکال مهم هستند:

یکم) عدم دقت لازم در تعیین اهداف: بدین معنا که تمام تهدید و بحران به آن بخش یا افراد که مد نظر عاملان بود، سرایت نمی‌کرد و همواره میزانی از خطا رخ می‌داد. برای مثال در ایجاد بحران زیست‌محیطی از طریق شیوع یک عامل بیماری‌زا، همواره بخشی از جامعه‌ی هدف از ابتلا مصون می‌ماند و به‌جای آن بخش دیگری از افراد که هدف نبودند مبتلا می‌گشتند.

دوم) عدم وجود عمق لازم در اثرگذاری بر اهداف: عبارت است از اختلاف میان میزان نتایج مدنظر عامل بحران با نتایجی که در عمل رخ داده است. در مثال فوق اگر عامل بیماری‌زا در جامعه‌ی هدف به‌منظور افزایش مرگ و میر انتشار یابد، عموماً بخشی از اهداف که مبتلا شده‌اند، نهایتاً به بیماری‌های شدید دچار شده و زنده می‌مانند.

سوم) کنترل‌پذیری پایین توسط عامل بحران: لازم است که عامل بحران بتواند بحران ایجاد شده را کنترل نماید تا به جوامع غیر هدف از جمله‌ی جامعه‌ی خود و متحدانش سرایت نکند اما در انواع تهدیدات و بحران‌هایی که بر چهارچوب سابق ابتناء دارند، میزان کنترل‌پذیری تهدید پایین و فرایند اعمال کنترل بر آن سخت است. برای نمونه در هنگام شیوع یک عامل بیماری‌زا، زمانی که عامل در محیط زیست انتشار یافت و دامنه‌ی ابتلا موسع شد، به‌واقع کنترل آن برای ممانعت از گسترش بیشتر بسیار سخت و گاهی غیرممکن است، از این رو سایر جوامع از جمله جامعه‌ی عامل بحران را نیز تهدید می‌نماید.

ویروس ابولا[7] مثالی از این نوع تهدیدات است که علی‌رغم انتشار توسط آمریکا در مناطقی از قاره‌ی آفریقا، پس از مدتی مشخص گردید که بعضی از شهروندان آمریکا نیز به آن مبتلا شده‌اند (MG, 2015).

چهارم) پایین بودن سطح بازدارندگی: عموماً تهدیدات و بحران‌های عمدی بدین منظور است که قربانی، یک سری از فعالیت‌ها و اقدامات خود را که بر خلاف منافع عامل بحران است، متوقف نماید. به‌عبارت دیگر این دست از بحران‌ها به‌منظور بازدارندگی در زمینه‌ای خاص ایجاد می‌شوند اما آنگونه که مورد انتظار عامل بحران است، بازدارندگی حاصل نمی‌شد.

مطالعه‌ی تهدیدات و بحران‌هایی که ساختار سیستم قربانی را هدف قرار می‌دادند بیانگر آن است که به تدریج در چند سال اخیر، اثرگذاری آنها نسبت به دهه‌ی گذشته کاهش یافته و اثرگذاری مد نظر را ندارند. برای مثال ایجاد آشوب‌های مدنی علیه یک حکومت از طریق تحریک مردم همان کشور، نوعی از بحران‌آفرینی است که سابق بر این بارها نتیجه‌ی مدنظر طراحان رسیده است که انقلاب‌های مخملی در کشورهای مختلف نمونه‌ای از آن است. اما این شیوه در سال‌های گذشته به نتایج قبلی دست نیافته است،

[6] HAARP: High Frequency Active Auroral Research Program

[7] Ebola Virus

از جمله آشوب‌های ایران در دی ۱۳۹۶ یا آشوب‌های مهر ماه ۱۳۹۸ در عراق (خبرگزاری آنا، مهر ۱۳۹۸) که اهداف متولیان را تأمین نکرد.

از سوی دیگر مدیریت زیرساخت‌های حساس و حیاتی (اعم از نظامی و غیرنظامی) تمامی کشورهای جهان در چند سال اخیر وابستگی بیشتری به سیستم‌های سایبرنتیک و فرماندهی – کنترل پیدا نموده که علی‌رغم وجود مزایا و نقاط قوت، آسیب‌پذیری‌های ذاتی نیز به‌همراه دارد. بنابر این عاملان تهدید و بحران به‌دنبال چهارچوبی نوین جهت ایجاد تهدید و بحران هستند تا حصول اهداف را از طریق نابودی یا اخلال در سیستم‌های فرماندهی – کنترل محقق سازند.

بعلاوه اینکه با توجه به هزینه‌ها، پیامدهای ناخواسته و غیرقابل کنترل بحران‌ها و تهدیدات بشری مانند بیماری‌های بیولوژیک، تسلیحات هسته‌ای و ... که بر اساس چهارچوب سابق تهدید و بحران مرسوم بود، تقریباً قابل پذیرش نیست که جهان امروز به سمت نسخه‌ای از چهارچوب تهدید و بحران حرکت کند که تأکید بر شیوع بحران‌های غیرقابل کنترل و گسترده دارد؛ بلکه انتظار بر این است که چهارچوب نوین به‌صورت هدفمند و موردی اثرگذار بوده و حتی‌المقدور قابل کنترل باشد. بنابر این، چهارچوب نوین تهدید و بحران مبتنی بر اخلال در سیستم‌های فرماندهی – کنترل مطرح شده است.

۱-۲. اخلال در فرماندهی – کنترل، مبنای چهارچوب نوین تهدید و بحران

دانش سایبرنتیک، بسیاری از حوزه‌های نظری و عملی را تحت تأثیر قرار داده که چهارچوب طراحی تهدید و بحران از آن جمله است. سایبرنتیک، دانش کنترل پدیده‌های هوشمند است که از طریق اشراف و احاطه بر جریان اطلاعات ورودی آنها، به کنترل اهداف مد نظر می‌پردازد. فرض اصلی در دانش سایبرنتیک چنین است که اگر به یک پدیده‌ی هوشمند (شامل انسان یا اشیاء) اطلاعات ورودی به‌صورت هدفمند و کانالیزه داده شود، در نهایت مبتنی بر آن اطلاعات به باور، تصمیم و اقدامی می‌رسد که از ابتدا مد نظر کنترل‌کننده است (شکوهیان‌راد، ۱۳۹۷). در واقع سایبرنتیک برای کنترل یک پدیده‌ی هوشمند، به‌جای تحت تأثیر قرار دادن ساختار و فیزیک آن، بر مدیریت سیستم فرماندهی – کنترل تمرکز می‌نماید.

بر این اساس، چهارچوب نوین تهدید و بحران به‌گونه‌ای است که به‌جای هدف قرار دادن ساختار و پیکره‌ی قربانی، بخش پردازش و تصمیم‌گیری آن را مختل می‌سازد. با ورود دانش سایبرنتیک به مباحث تهدید و بحران، نوع تهدیدات و بحران‌های جدید نیز بر اخلال در سیستم فرماندهی – کنترل پدیده‌های هوشمند (اعم از انسان و سیستم‌های مدیریت زیرساخت‌های حساس) تمرکز یافته است.

بر خلاف تهدیدات و بحران‌های مبتنی بر چهارچوب سابق، در تهدیدات و بحران‌های نوین چهار اشکالی که قبلاً تشریح شد تا حد چشمگیری مرتفع شده است. به‌عبارت دیگر تهدیدات و بحران‌های نوین دقیق هستند زیرا هدف قرار دادن فرماندهی – کنترل، قابلیت برنامه‌ریزی دارد و می‌تواند به‌گونه‌ای باشد که عیناً اهداف از پیش تعیین شده قربانی شوند، نه غیر از آن. همچنین عمق تهدید و بحران عموماً معادل سطحی است که از ابتدا مد نظر عامل بحران بوده است زیرا سیستم فرماندهی – کنترل به سطوح و فرایندهای مختلف پدیده‌ی هوشمند دسترسی دارد و آنها را کنترل می‌نماید، لذا برای ایجاد اختلال در هر بخش از پدیده‌ی هوشمند، کافی است کنترل‌گر آن در بخش فرماندهی – کنترل مختل گردد. از سوی دیگر امکان کنترل بحران برای عامل بحران وجود دارد زیرا می‌توان بحران را به‌گونه‌ای طراحی کرد که دقیقاً بر بخش فرماندهی – کنترل همان سیستمی که مد نظر است، اثرگذار باشد، نه سایر سیستم‌ها. و نهایتاً بازدارنده است زیرا با ایجاد خلل در سیستم فرماندهی – کنترل قربانی، حداقل برای مدتی امکان تصمیم‌گیری و اقدام متقابل از قربانی سلب شده و در بهترین حالت می‌تواند به احیای خود بپردازد.

سلاح سایبری استاکس‌نت[8]، یک نمونه‌ی گویا از تهدید و بحران علیه سیستم‌های هوشمند است که ضمن هدف قرار دادن بخش فرماندهی – کنترل قربانی، هر چهار ویژگی فوق را دارا است. یعنی دقیق است زیرا از مجموعه‌ی تأسیسات هسته‌ای نطنز، طبق خواسته‌ی عاملان فقط سیستم مدیریت سانتری‌فیوژها را تحت حمله قرار داد؛ عمیق است

[8] Stuxnet Cyber Weapon

زیرا هدف از آن، تخریب بخشی از سانتری‌فیوژها بود که به‌وقوع پیوست؛ قابلیت کنترل دارد زیرا علی‌رغم انتشار در بخش‌های مختلفی از جغرافیای جهان، فقط بر سیستم هسته‌ای نطنز اثر گذاشت (به‌دلیل آنکه در ساختار کد استاکس‌نت تعریف شده بود که فقط به سری مشخصی از کنترل‌گرهای زیمنس که مورد استفاده‌ی ایران بود حمله کند و اگر یافت نشد، در سیستم غیر فعال باقی بماند) و نهایتاً بازدارنده‌تر از تهدیدات و بحران‌های سنتی است زیرا نوع خرابی که در سیستم ایجاد می‌کرد برای مدتی مبهم بود و کشف آن نیازمند دانش و تخصص بالا و صرف زمان نسبتاً طولانی بود.

همین مطلب درخصوص جوامع انسانی نیز صادق است. قبلاً بیان شد که دانش سایبرنتیک، توانایی کنترل سیستم فرماندهی – کنترل موجودات هوشمند مانند انسان را نیز دارد. مطالعات سابق بیانگر آن است اهمیت شبکه‌های اجتماعی و به‌طور عام فضای سایبر[9] را نمی‌توان تنها منحصر در استقبال روزافزون کاربران از این شبکه ها و جا گذاشتن رقبا در رتبه های جهانی توسط آنها دانست، بلکه باید از زاویه‌های دیگر همچون استفاده از شبکه‌های اجتماعی برای رساندن پیام و القای تفکرات به کاربران و تبدیل حوادث عادی به یک بحران در کنار جذابیت‌ها و همچنین اثرات شگرفی که این تکنولوژی‌های اطلاعاتی بر جوامع می‌گذارد، جستجو نمود (محمدی و همکاران، ۱۳۹۶). سیستم‌های سایبرنتیک می‌توانند بحران‌هایی نظیر اعتراضات مدنی را سازماندهی کرده و در اطلاع‌رسانی روند رویدادها نقش‌آفرینی کنند (حاذق نیکرو، ۱۳۹۱).

هر چند تهدیدات و بحران‌های مبتنی بر فرماندهی – کنترل که تاکنون از سوی قدرت‌های جهان اشاعه یافته‌اند عموماً با هدف اثرگذاری دقیق و عمیق بر اهداف مد نظر طراحی شده‌اند اما در عین حال هیچ‌کدام خطر فراگیری جهانی را به‌صورت عملیاتی نداشته‌اند. برای مثال سلاح سایبری استاکس‌نت توسط آمریکا و رژیم صهیونیستی به‌منظور فلج‌سازی سیستم اتمی ایران از طریق اخلال در سیستم فرماندهی – کنترل زیمنس که در نیروگاه نطنز وظیفه‌ی کنترل سانتری‌فیوژها را بر عهده داشت طراحی و اجرا شد اما خطر بازطراحی و استفاده‌ی مجدد از آن به میزان تهدیدات بیولوژیک و اتمی نبود. به‌همین نسبت ایجاد تهدید و بحران در جوامع هدف از طریق سیستم‌های سایبرنتیک مانند شبکه‌های اجتماعی، علی‌رغم آنکه حتی ممکن است به براندازی یک دولت یا حکومت منتج شود، خطر بازگشت‌پذیری به سمت عامل تهدید و بحران را ندارد.

۲-۲. منطق چهارچوب نوین تهدید و بحران

چگونگی طراحی و اجرای تهدیدات و بحران‌ها بر اساس اخلال در سیستم فرماندهی – کنترل، از منطق پایه در دانش سایبرنتیک حاصل شده است. بر اساس دیدگاه سایبرنتیک، هر سیستم فرماندهی – کنترل مبتنی بر چهار رکن است که عبارتند از اطلاعات، ارتباطات، محاسبات و کنترل (فولادی، ۱۳۹۴). ماهیت هر رکن نحوه‌ی ارتباط چهار رکن مذکور در جدول زیر بیان شده است (همان):

جدول ۱: ارکان سیستم فرماندهی – کنترل در دانش سایبرنتیک

«ارکان سیستم فرماندهی - کنترل»			
اطلاعات محتوا	ارتباطات انتقال محتوا	محاسبات پردازش و ذخیره‌سازی محتوا	کنترل اشراف و نظارت کامل بر محتوا

از آنجا که تمام ارکان فوق در سیستم فرماندهی – کنترل نقش مستقیم و بی‌بدیل دارند، اگر هر کدام از آنها دچار اشکال گردند عملکرد سیستم فرماندهی – کنترل مختل خواهد شد که مبنای شکل‌گیری تهدیدات و بحران‌های نوین است. به‌عبارت دیگر بر اساس آنکه اختلال در کدام یک از ارکان چهارگانه‌ی سیستم‌های فرماندهی – کنترل ایجاد شود، نوع تهدید و بحران قابل احصا است. مطالعات موردی نیز گواهی بر این ادعا است که پس از بیان و تشریح تهدیدات و بحران‌های حاصل از اخلال در هر رکن، نمونه‌هایی از آنها نیز بیان خواهد شد.

کلیات تهدیدات و بحران‌های نوین از طریق حذف، توقف، تحریف، ایجاد تأخیر در اجرا یا جابجایی اولویت در فرایندها و دستورات هر کدام از ارکان چهارگانه حاصل می‌شود (شکوهیان‌راد، تهدیدات سایبری علیه سیستم‌های فرماندهی – کنترل، ۱۳۹۷).

[9] Cyber Space

الف) تهدیدات و بحران‌های حاصل از اخلال در رکن اطلاعات

رکن اطلاعات در سیستم‌های فرماندهی – کنترل، منشأ صدور فرمان بوده و اراده‌ای است برای انجام اقدامات مشخص. لذا مهم‌ترین تهدیدی که علیه آن امکان وقوع دارد، عبارت است از **حذف اطلاعات، توقف اطلاعات، تحریف اطلاعات، ایجاد تأخیر در صدور اطلاعات** و **جابجایی اولویت اطلاعات**. هر کدام از موارد فوق در هر مدل از سیستم‌های فرماندهی کنترل نظامی و غیرنظامی رخ دهد مستقیماً بر عملکرد زیرساخت‌های حساس و منابعی که تحت مدیریت سیستم فرماندهی – کنترل هستند، اثر می‌گذارد.

مشخص است که یک سیستم فرماندهی – کنترل بر اساس اطلاعات برنامه‌ریزی شده عمل می‌کند. برای مثال اگر اطلاعات برنامه‌ریزی شده در خصوص نحوه‌ی توزیع انرژی در اوج مصرف از سیستم‌های فرماندهی – کنترل یک نیروگاه برق حذف گردد، عملاً سیستم اولویت توزیع را در زمان اوج مصرف از دست داده و ممکن است انرژی اماکن حساس و اضطراری را به سایر نقاط غیر حساس انتقال دهد یا تمام مشترکان را با اولویت یکسان در نظر گیرد که می‌تواند موجب بروز عواقب منفی برای اماکن حساس (نظیر مراکز درمانی، حمل و نقل، انتظامی و ...) شود.

حال اگر جریان اطلاعات متوقف شود، به این معنا است که سیستم از اقدامات مقتضی مطلع است اما آنها را اجرا نمی‌کند. برای مثال، سیستم فرماندهی – کنترل یک سد آبی از باز شدن دریچه‌های اضطراری در زمان افزایش میزان آب پشت سد مطلع است اما اطلاعات لازم جهت اجرای آن را به سیستم‌های اپراتور دریچه‌های اضطراری منتقل نمی‌کند. از حیث فنّی به این «انقطاع فرمان»[10] گفته می‌شود.

در تحریف دستورات که سهمگین‌ترین نوع تهدید علیه رکن اطلاعات است، اقدامات و واکنش‌های سیستم فرماندهی – کنترل به‌علت تحریف اطلاعات و فرامین سیستم، تغییر می‌یابد. برای مثال ممکن است اطلاعات یک سیستم رادار شناساگر هوایی چنین تحریف شود که در صورت رصد و شناسایی هواپیماهای خودی، به سمت آنها شلیک کند و در مقابل اگر هواپیمای غیر خودی را شناسایی نمود، به اپراتور سیستم اعلام هشدار نکند. یعنی دقیقاً برخلاف روالی که رادار شناساگر برای آن استقرار یافته است.

ایجاد تأخیر در اجرای اطلاعات و جابجایی اولویت‌های صدور آنها، نمونه‌هایی از تحریف دستورات هستند که به‌دلیل مهم بودن به‌صورت جداگانه بیان شده‌اند.

موارد فوق برای هر سیستم فرماندهی – کنترل امکان وقوع دارد که در نتیجه، وظایف آن سیستم را به مشکلاتی مشابه آنچه بیان شد دچار می‌نماید. هک سد نیویورک در سال ۲۰۱۶ (Thompson, 2016)، قطع شبکه‌ی برق شهر کی‌یِف[11] (پایتخت اوکراین) در ۲۳ دسامبر ۲۰۱۵ (Zetter, 2016) و خاموش کردن هواپیماهای EC-130s و AC-130s آمریکا در حال پرواز توسط روسیه در جنگ سوریه (Clark, 2018)، نمونه‌هایی از بحران‌آفرینی علیه فرماندهی – کنترل از طریق اخلال در رکن اطلاعات است.

ب) تهدیدات و بحران‌های حاصل از اخلال در رکن ارتباطات

رکن ارتباطات در اصل موظف به انتقال صحیح و مجاز اطلاعات در زیربخش‌های سیستم فرماندهی – کنترل است. این جابجایی می‌تواند درون سیستم، میان چند سیستم یا بین سیستم و اپراتور انسانی آن باشد. در هر صورت در تمامی حالات، رکن ارتباطات است که وظیفه‌ی خود را باید به درستی انجام دهد تا انتقال اطلاعات به‌طور کامل و صحیح صورت پذیرد.

مشابه رکن اطلاعات، برای رکن ارتباطات نیز تهدیدات حذف، توقف، تحریف، ایجاد تأخیر در اجرا و جابجایی اولویت مطرح است. عموماً آثار نهایی اختلال در ارتباطات به‌گونه‌ای است که کارکرد اطلاعات را به چالش می‌کشد. لذا در سیستم‌های فرماندهی – کنترل مبتنی بر معماری C4ISR، دو مؤلفه‌ی فرماندهی[12] و اینتلیجنس[13] دچار مشکل خواهد شد. حذف ارتباطات منجر به سکوت خبری

[10] Command Intrerupt
[11] Kiev
[12] Command
[13] Intelligence

کلیه‌ی بخش‌های سیستم می‌شود. توقف ارتباطات نیز نتیجه‌ای مشابه خواهد داشت. تحریف در ارتباطات از دو جنبه قابل بروز است:

۱- تحریف در اطلاعاتی که باید انتقال یابد
۲- تحریف در گیرنده یا فرستنده‌ی اطلاعات

بروز حالت اول باعث فریب سیستم فرماندهی – کنترل از حیث دریافت دستور یا اشراف اطلاعاتی آن خواهد شد که در نتیجه منجر به تصمیم‌گیری و واکنش اشتباه در مواقع مقتضی می‌گردد. اگر حالت دوم رخ دهد، اصل اطلاعات صحیح است اما گیرنده یا فرستنده‌ی آن مجاز نمی‌باشد. لذا منجر به شنود، جاسوسی و دسترسی عوامل غیرمجاز به اطلاعات خواهد شد.

ایجاد تأخیر در ارتباطات و همچنین تغییر اولویت‌های جابجایی و انتقال اطلاعات نیز آثار منفی بر رکن فرماندهی و اشراف اطلاعاتی سیستم خواهند داشت. از سوی دیگر یک ویژگی منحصر به‌فرد برای رکن ارتباطات وجود دارد که در دیگر ارکان فرماندهی - کنترل نیست. هر تهدید و بحران علیه یک سیستم فرماندهی – کنترل باید با دسترسی به رکن ارتباطات، عملیات خود را آغاز نماید در غیر این‌صورت امکان تحقق آن وجود ندارد. به‌عبارت دیگر چه تهدید علیه رکن اطلاعات باشد، چه کنترل و چه رکن محاسبات، گذرگاه آن برای اقدام رکن ارتباطات سیستم است. از این رو در منطق مدیریت بحران جهت مقابله با بحران‌های نوین که اتکا بر اخلال در سیستم فرماندهی – کنترل دارند؛ حفاظت از زیرساخت‌های حساس و تأمین امنیت ارتباطات تا حد چشمگیری از وقوع تهدیدات و بحران‌ها پیشگیری می‌نماید. همچنین تمامی مدل‌های حملات سایبری شامل جنگ الکترونیک، جنگ شبکه‌ای، تسلیحات خودمختار و ... با استفاده از درگاه و گذرگاه ارتباطی بر قربانی اثر می‌گذارند، در غیر این‌صورت امکان وقوع نخواهند داشت. لذا اکثر توان پدافندی در برابر تهدیدات و بحران‌ها در تمامی سیستم‌های فرماندهی – کنترل بر امنیت ارتباطات سیستم تمرکز دارد.

حمله به زیرساخت‌های مخابراتی کشور در ۱۷ فروردین ۱۳۹۷ (اطلاعیه وزارت ارتباطات درباره حمله سایبری، ۱۳۹۷) و اقدام به شنود و استراق سمع اطلاعات و برقراری ارتباطات غیرمجاز از طریق شبکه‌ی برق (Stockton, 2018) نمونه‌هایی از تهدیدات و بحران‌های شکل گرفته علیه سیستم فرماندهی – کنترل بر اساس اخلال در رکن ارتباطات آن است.

پ) تهدیدات و بحران‌های حاصل از اخلال در رکن محاسبات

رکن محاسبات در سیستم فرماندهی - کنترل موظف به تحلیل، پردازش و ذخیره‌سازی اطلاعات است؛ خواه اطلاعات شامل دیتا، اینفورمیشن یا اینتلیجنس باشد، خواه اساساً متادیتا یا داده‌های ارتباطی را شامل شود. در کل هر آنچه که جنبه‌ی اطلاعاتی داشته باشد برای تحلیل، تبدیل و ذخیره‌سازی به رکن محاسبات نیازمند است.

رکن محاسبات از منظر فنّی، واسط دیگر ارکان سیستم فرماندهی - کنترل است، زیرا هر رخدادی در سه رکن اطلاعات، ارتباطات و کنترل، برای تشخیص و سپس صدور دستور مقتضی به محاسبات وابسته است. برای مثال اگر در پروتکل‌های حفاظتی یک شبکه‌ی اطلاعاتی حساس چنین تعریف شده باشد که در صورت شناسایی هرگونه نفوذ غیر مجاز به اطلاعات جاری در شبکه اعلام سکوت رادیویی شود؛ وظیفه‌ی تشخیص نفوذ، اعلام دستور مقتضی با آن و همچنین ثبت زمان و اطلاعات این کنش و واکنش در تاریخچه‌ی وقایع سیستم، بر عهده‌ی رکن محاسبات است. لذا با ایجاد اختلال در عملکرد محاسبات سیستم فرماندهی – کنترل می‌توان عملاً سیستم را ناکارآمد نمود.

یکی از جنبه‌های منحصر به‌فرد رکن محاسبات این است که قابلیت برنامه‌ریزی دارد. از این رو در صورت دسترسی به آن، وضعیت تهدیدات حذف، توقف، تحریف، تأخیر در اجرا و جابجایی اولویت؛ نسبت به سایر ارکان فرماندهی – کنترل پیچیده‌تر خواهد شد. زیرا اگر مثلاً در رکن ارتباطات، بحران مبتنی بر حذف صرفاً از انتقال اطلاعات جلوگیری می‌کند و می‌توان با صرف کمی زمان مجدد شبکه‌ی ارتباطی را برقرار نمود، در رکن محاسبات چنین تهدیدی منجر به حذف مبانی محاسباتی سیستم فرماندهی – کنترل شده و شاید اصلاح آن چند روز فرصت نیاز داشته باشد، ضمن آنکه باید آثار جانبی آن را یافته و رفع نمود.

حمله سایبری به سیستم فرماندهی – کنترل پدافند هوایی سوریه که منتج به شلیک اشتباه موشک به اهداف نامعلوم

شده است (Bussoletti, 2018) نمونه‌ای از ایجاد تهدید و بحران علیه سیستم فرماندهی – کنترل از طریق اخلال در رکن محاسبات است، به‌گونه‌ای که سامانه در تحلیل و تعیین اهداف دچار اشتباه محاسباتی شده است.

ت) تهدیدات و بحران‌های حاصل از اخلال در رکن کنترل

رکن کنترل، ضمانتی است برای اطمینان از عملکرد سایر ارکان و وظایف محوله به سیستم فرماندهی - کنترل. از این رو مهم‌ترین تهدید علیه کنترل، تحریف آن است که به اپراتور سیستم، بازخورد اشتباه باز می‌گرداند. در این صورت آنچه اتفاق می‌افتد، فریب کاربرِ سیستم فرماندهی – کنترل است. اما دیگر تهدیدات شامل حذف کنترل، توقف کنترل، ایجاد تأخیر در فرایند کنترل و جابجایی اولویت‌های کنترلی نیز برای رکن کنترل قابل وقوع است. حذف کنترل، سیستم فرماندهی - کنترل را یک‌طرفه می‌نماید به‌گونه‌ای که صرفاً اطلاعات و دستورات به سیستم می‌رسد اما فرایند کنترلی جهت بازگشت بازخورد و همچنین ممانعت از بروز خطا فعال نیست. توقف کنترل نیز آثار و نتایجی مشابه با حذف آن در پی خواهد داشت. ایجاد تأخیر در فرایندهای کنترلی می‌تواند منجر به بروز اشتباهات سیستمی یا عدم تشخیص دسترسی و تغییرات غیرمجاز در بخش‌های مختلف سیستم فرماندهی – کنترل شود. جابجایی اولویت‌های کنترلی باعث می‌َشود تا در بعضی مواقع، سیستم کنترلی حتی بر خلاف مأموریت سیستم فرماندهی - کنترل، فرایند کنترل را اجرا نماید. شدت این امر وابسته به نوع جابجایی دستورات کنترلی است.

تسلیحات سایبری استاکس‌نت و فلیم[۱۴] (Khalifa) و انفجارات خطوط لوله‌ی انتقال نفت و گاز ایران در مرداد و شهریور ۱۳۸۹ (Coughlin, 2010) نمونه‌هایی از اقدام بحران‌زا علیه سیستم فرماندهی – کنترل از طریق اخلال در رکن کنترل هستند.

چهارچوب ایجاد تهدید و بحران مبتنی بر اخلال در سیستم‌های فرماندهی - کنترل اولاً نسبت به تهدیدات و بحران‌های سابق نظیر سلاح هسته‌ای، هزینه‌های بسیار کمتری را به سازنده‌ی آن تحمیل می‌نماید و ثانیاً به‌دلیل تضعیف زنجیره‌ی فرماندهی، کاهش هماهنگی و انسجام قوای قربانی که ناشی از اخلال در سیستم‌های فرماندهی – کنترل وی است، احتمال ورود به تهدیدات دو طرفه مانند جنگ را کاهش می‌دهد، از این رو قدرت بازدارندگی را به‌نفع عامل تهدید افزایش می‌دهد.

ژنرال پائول ناکاسون[۱۵] فرمانده‌ی جدید آژانس امنیت ملی[۱۶] و فرماندهی سایبری[۱۷] آمریکا ضمن بیان اظهاراتی مهم در خصوص تهدیدات و بحران‌های فرماندهی – کنترل، راهبرد آمریکا در قبال سیستم‌های فرماندهی – کنترل در منازعات آینده را چنین شرح می‌دهد:

> *حملات سایبری علیه شبکه‌های زیرساختی، یک آسیب‌پذیری بحرانی در پدافند کشور است که تهدیداتی علیه امنیت آمریکا ایجاد می‌نماید. ما با یک محیط پُر تهدید، چالش‌برانگیز و بی‌ثبات مواجه هستیم و تهدیدات سایبری علیه امنیت ملی و زیرساخت‌های حیاتی در صدر فهرست تهدیدات قرار دارد.*
>
> *حال اگر نتوانیم تمام امنیت خود را از طریق پدافند به‌دست آوریم، برای حملات سایبری به زیرساخت‌های حساس کشورهای خارجی آماده می‌شویم. هدف ما این است که توانایی تعطیل کردن یا ایجاد خرابکاری در زیرساخت‌های حساس کشورهای خارجی را تقویت کنیم و این موضوع را به‌عنوان بخشی از راهبرد بازدارندگی ایالات متحده اعلام نماییم* (Nakasone, 2018)

اظهارات ژنرال ناکاسون نیز تأیید دیگری بر این ادعا است که چهارچوب نوین طراحی تهدید و بحران اولاً افزایش بازدارندگی نسبت به مدل تهدیدات و بحران‌های سابق را دنبال می‌کند و ثانیاً در نگاه مدیریت بحران قدرت‌های جهان جایگاه ویژه‌ای یافته به‌طوری که به راهبردهای آتی آنها جهت می‌دهد. لذا انتظار بر این است که قدرت‌های جهان، اولاً مبنای مدیریت تهدیدات و بحران‌های ملّی، منطقه‌ای و جهانی را بر مفهوم فرماندهی – کنترل مستقر

[14] Flame
[15] Lt. Gen. Paul Nakasone
[16] NSA: National Security Agency
[17] US Cyber Command

نمایند و ثانیاً جهت تحمیل اراده‌ی خود بر سایر کشورهای هدف، سیستم‌های فرماندهی – کنترل آنها هدف قرار دهند.

۱-۳. تأثیرات چهارچوب تهدید و بحران مبتنی بر اخلال در سیستم‌های فرماندهی – کنترل بر دانش مدیریت بحران

اکنون که چهارچوب نوین تهدید و بحران مطرح شده، لازم است تا آثار آن بر دانش مدیریت بحران بررسی شود تا بتوان بر اساس آن به تدوین طرح و برنامه‌ی عملیاتی پرداخت.

به‌طور کل مدیریت بحران، فرایند پیش‌بینی و پیشگیری از وقوع بحران، مقابله در زمان وقوع بحران و بازسازی و بازیابی پس از وقوع بحران است (صیوری، ۱۳۹۶). بر این اساس چرخه‌ی مدیریت بحران به‌صورت زیر تعریف می‌شود:

نمودار ۱: چرخه‌ی مدیریت بحران در دانش مدیریت بحران

چهارچوب تهدید و بحران مبتنی بر اخلال در سیستم فرماندهی – کنترل، محتوای هر چهار گام چرخه‌ی دانش مدیریت بحران را متحول می‌سازد که باید به‌طور موردی بررسی گردد.

الف) گام پیشگیری و کاهش

در حوزه‌ی پیشگیری و کاهش تهدید و بحران، اصل بر این است که علت بالقوه‌ی وقوع بحران حذف گردد. از آنجا که مبنای وقوع تهدید و بحران در عصر جدید اخلال در سیستم فرماندهی – کنترل است، به لحاظ منطقی دو راهکار قابل پیشنهاد است:

۱. حذف سیستم‌های فرماندهی – کنترل از دایره‌ی مدیریت زیرساخت‌های حساس نظامی و غیرنظامی

هر چند استفاده از سیستم‌های فرمانده – کنترل موجب افزایش دقت، کارایی و سهولت در مدیریت زیرساخت‌های حساس می‌شود اما در بعضی از موارد، طراز امنیت زیرساخت از سایر ویژگی‌ها مهم‌تر است. اگر در چنین مواقعی، نوع زیرساخت حساس به‌گونه‌ای باشد که امکان کنترل و مدیریت کامل بر آن بدون حضور یک سیستم فرماندهی – کنترل پیچیده میسر شود؛ منطق حکم می‌کند از سیستم‌هایی که روال غیر سیستمی استفاده شود تا خطر بروز تهدید و بحران از طریق سیستم فرماندهی – کنترل مرتفع گردد.

هر چند این راه در برخی از مواقع مؤثر و موفق است اما قطعاً به‌عنوان یک راهبرد جامع قابل پذیرش نیست.

۲. ارتقاء کیفی و کمّی دستورات و برنامه‌های امن‌سازی و حفاظت از سیستم‌های فرماندهی – کنترل

افزایش سطح امنیت و حفاظت از سیستم‌های فرماندهی – کنترل می‌تواند منتج به افزایش توان پیشگیری در برابر وقوع تهدید و بحران گردد.

از حیث فنّی، دسترسی غیر مجاز به سیستم‌های فرماندهی – کنترل صرفاً از طریق نفوذ به رکن ارتباطات سیستم میسر است، خواه به‌صورت حضور فیزیکی در محل باشد یا از طریق دسترسی از راه دور فراهم شود. لذا افزایش سطح تدابیر حراست فیزیکی محیط از یک سو و مسدودسازی هرگونه امکان ارتباط از راه‌دور از سوی دیگر، به میزان چشمگیری به افزایش امنیت سیستم‌های فرماندهی – کنترل و پیشگیری از وقوع بحران در این حوزه می‌انجامد.

به‌منظور افزایش امنیت ارتباطات از راه دور نیز از آنجا که از حیث فنّی، هرگونه ارتباطات بر اساس یک پروتکل تعریف شده است، بازنگری در کدهای پروتکل و تعریف روال‌های اختصاصی می‌تواند امنیت را تأمین نماید. برای مثال اگر

ارتباط میان اپراتور و سیستم فرماندهی – کنترل یک زیرساخت حساس از طریق پروتکل TCP/IP باشد، با سفارشی‌سازی آن و تعریف روال امنیتی جدید و منحصر به‌فرد، می‌توان امنیت ارتباطات را به‌طور ویژه افزایش داد.

طراحی و تعریف الگوریتم‌های رمزنگاری بومی و روش‌های تأیید دسترسی بیومتریک اپراتورها نیز می‌تواند به بسته شدن ارتباطات غیرمجاز کمک شایانی نماید.

همچنین نباید میان واحد تأمین انرژی سیستم فرماندهی – کنترل با فضای بیرون، راهی برای ارتباط از راه دور تعریف شده باشد، زیرا می‌توان از طریق شبکه‌ی انرژی به سیستم فرماندهی – کنترل و زیرساخت حساس متصل به آن اقدام به بحران‌آفرینی نمود.

ب) گام آمادگی

در گام آمادگی نیاز به تقویت دانش، تخصص و تکنولوژی‌های سایبرنتیک است زیرا اساس سیستم‌های فرماندهی – کنترل ابتناء بر این دانش دارد.

بدین منظور مطالعه و شناخت تسلیحات سایبری، روش‌های اقدام در محیط سایبر جهت خرابکاری و اشراف فنّی بر ساز و کار نمونه‌های ایجاد تهدید و بحران علیه سیستم‌های فرماندهی – کنترل در سایر کشورهای جهان، ضرورت دارد و اجتناب‌ناپذیر است. حال بر اساس اطلاعات حاصل، با انجام **رزمایش‌های پدافندی** برای تمامی زیرساخت‌های نظامی و غیرنظامی و همچنین طراحی و **اجرای بازی جنگ** مدیریت بحران مبتنی بر چهارچوب نوین می‌توان سطح آمادگی ذهنی و عملیاتی تمامی نیروها را در سطوح مختلف افزایش داد تا برای شرایط بحران واقعی آماده‌تر باشند. لازم است موارد فوق به‌صورت مستمر ادامه یابد تا اصل آمادگی نیروها همواره در سطح قابل قبول باشد.

شایان ذکر است محتوای فعلی که در حوزه‌ی آموزش مدیریت بحران در سطوح مختلف سازمان مورد استفاده است، توانمندی لازم برای آمادگی و مقابله با بحران‌های نوین را ندارد و نیاز است در متون تخصصی به‌طور مفصل به‌روز رسانی شود.

پ) گام مقابله

گام مقابله از حیث زمانی، برهه‌ای را در بر می‌گیرد که بحران آغاز شده و زمان اقدامات پیشگیرانه و تلاش برای آمادگی به‌پایان رسیده است. ویژگی گام مقابله آن است که به‌دلیل شدت و سرعت بالای وقوع تهدید و بحران، فرض بر این است که هیچ فرصتی برای فکر و آموزش نیست و تمام توان عملیاتی در این زمان، ماحصل فعالیت‌ها و برنامه‌ریزی‌هایی است که در دو گام قبل انجام شده است.

مقابله با تهدیدات و بحران‌های سیستم‌های فرماندهی – کنترل ریشه در شناخت کامل نظری و فنّی نسبت به دانش سایبرنتیک دارد. به‌طور کل می‌توان:

۱. برای هر زیرساخت حیاتی، می‌توان علاوه بر مدیریت آن از طریق سیستم‌های فرماندهی – کنترل، بستر مدیریت غیر سیستمی را نیز تعبیه نمود تا در زمان اخلال در سیستم فرماندهی – کنترل، با سوییچ نحوه‌ی مدیریت به حالت غیر سیستمی، خطرات اخلال در سیستم به زیرساخت انتقال نیابد.
۲. مبتنی بر اصل فریب، یک سیستم فرماندهی – کنترل با شرایط نسبتاً واقعی تعریف کرد که عاملان نفوذ تصور نمایند به سیستم فرماندهی – کنترل اصلی دست یافته‌اند اما پشت‌پرده سیستم دیگری برای مدیریت زیرساخت حساس استفاده شود و صرفاً بخشی از اطلاعات آن به‌صورت دستی به سیستم فرماندهی – کنترل فریب تزریق شود. با این تاکتیک می‌توان ضمن حفظ سیستم‌های اصلی از دسترسی غیر مجاز، اولاً از وقوع بحران جلوگیری کرد ثانیاً با رصد اقداماتی که عاملان بحران انجام می‌دهند به نیات اصلی و شیوه‌های اقدام آنها دست یافت.

ت) گام بازسازی

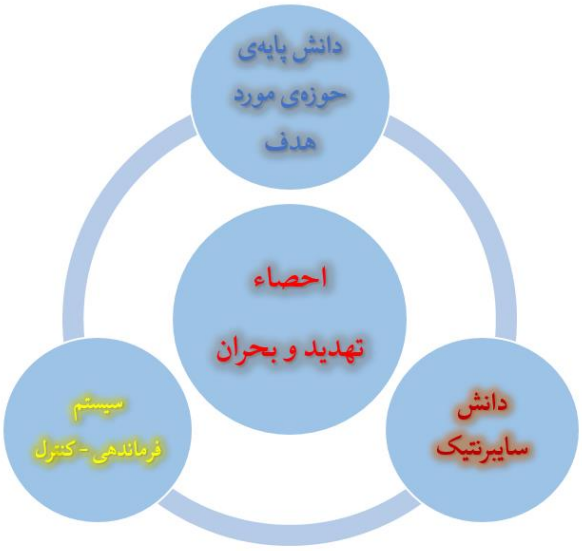
در گام بازسازی که وقوع بحران به پایان رسیده و تهدید جاری مرتفع شده است، عموماً خسارات ناشی از بحران ترمیم می‌شود اما در چهارچوب نوین تهدید و بحران، این اقدام کافی نیست زیرا عامل بحران به منطق مدیریت بحران ما دست یافته و قطعاً با استفاده از آن، بحران دقیق‌تر و

عمیق‌تری را در آینده رقم خواهد زد. از این رو لازم است پس از وقوع هر تهدید و بحران مبتنی بر فرماندهی – کنترل، چهار اقدام انجام شود:

۱. چینش منطقی و ارتباطی سیستم‌های فرماندهی – کنترل نسبت به زیرساخت‌های حساس تا حد امکان تغییر یابد. این امر باعث می‌شود عامل بحران در هنگام اقدام جهت بحران آتی تصور کند با مسیری کاملاً متفاوت مواجه است.
۲. راهبردها، تاکتیک‌ها و تکنیک‌های مدیریت بحران ارتقاء یابد به‌گونه‌ای که از منظر عامل بحران، راهبردی کاملاً جدید طلقی شود. این اقدام موجب غافلگیری برای عامل بحران در بخشی یا تمامی مسیر ایجاد بحران جدید خواهد شد که تبعاً توان عملیاتی وی را کاهش خواهد داد.
۳. چینش بازیگران مؤثر در مدیریت بحران تغییر یابد. بدین معنا که سازمان‌ها و نهادهای متولی اعم از دولتی و خصوصی و همچنین بعضی از افراد حقیقی تغییر یابد. برای مثال اگر سه زیرساخت حساس الف، ب و پ وجود دارد، می‌توان نیروهای هر زیرساخت را به زیرساختی دیگر منتقل نمود. قطعاً تغییر بازیگران از جنبه‌ی حقوقی و حقیقی به تغییر نگاه، روند و روش‌ها منتج می‌شود که می‌تواند بخشی از تغییر منطقی و راهبردی که اشاره شد را به انجام رساند.
٤. آسیب‌های درونی شناخته شود تا در بحران‌های آتی موجب بروز تهدیدات جدید علیه سیستم‌های فرماندهی – کنترل و زیرساخت‌های حساس نشود.

۳. یافته‌ها و نتیجه‌گیری

بر اساس آنچه در پژوهش حاضر تبیین و تشریح شد، روش کلان احصاء تهدید و بحران در عصر حاضر در حوزه‌های مختلف، مبتنی بر نمودار زیر است:



نمودار ۲: نمودار مفهومی احصاء تهدید و بحران بر اساس چهارچوب نوین

نمودار فوق بدین معنا است که هم برای طراحی و ایجاد تهدیدات و بحران‌های نوین و هم به‌منظور مقابله با آنها در مدیریت بحران، بر اساس سه عامل که شامل «منطق و دانش سایبرنتیک»، «سیستم فرماندهی – کنترل» و «دانش پایه‌ی حوزه‌ی مورد هدف» می‌باشند، اقدام شده و بحران متناظر آن احصاء می‌گردد.

همانطور که چهارچوب نظری پژوهش بیان شد، اساس شکل‌گیری تهدیدات و بحران‌های نوین از منطق و دانش سایبرنتیک نشأت پذیرفته است. از سوی دیگر سیستم‌های فرماندهی – کنترل امروزی، حاصل نگاه سایبرنتیک در بُعد مدیریت پدیده‌های هوشمند است. همچنین محرز است که گستردگی و اثرگذاری دانش و تکنولوژی‌های سایبرنتیک در تمامی عرصه‌ها چشمگیر بوده و موجب تحول در اکثر زمینه‌های نظری و عملی شده است، از این رو تقریباً در تمامی حوزه‌ها می‌توان با اتکا به منطق سایبرنتیک و سیستم‌های فرماندهی – کنترل، تغییرات مد نظر را ایجاد نمود.

حال اگر تغییرات مد نظر منفی بوده و در راستای بحران‌آفرینی باشد، می‌تواند مبنای طراحی تهدیدات و بحران‌های نوین علیه تمامی حوزه‌ها گردد. به‌همان نسبت که می‌تواند از جنبه‌ی مثبت موجبات پیشرفت و ارتقاء در حوزه‌های گوناگون را فراهم آورد.

برای مثال اگر هدف، محروم‌سازی ساکنان یک کلان‌شهر از منابع آبی باشد، به‌جای آنکه همانند روش‌های سابق اقدام به آلوده‌سازی آب شود یا به‌صورت فیزیکی از طریق نیروهای نظامی، منابع تأمین آب شهری تصرف یا منهدم گردد؛ با اخلال در سیستم‌های فرماندهی – کنترل که وظیفه‌ی مدیریت زیرساخت‌های تأمین آب شهری را بر عهده دارند هدف مذکور حاصل می‌گردد.

به همین طریق می‌توان برای مسدودسازی یه معبر شهری مهم، به‌جای تخریب یا مسدود سازی فیزیکی آن از طریق اطلاعات ترافیکی، سیستم‌های فرماندهی – کنترل ترافیکی شامل چراغ‌های راهنما را به‌گونه‌ای تنظیم کرد که به‌جای هدایت ترافیک موجب گره‌خوردگی آن شود.

به همین نسبت می‌توان برای تسلط بر یک کشور، به‌جای تهدید و بحران فیزیکی، نظامی، تحریم اقتصادی و ... جریان اطلاعات را در کشور هدف به‌گونه‌ای مدیریت نمود که آحاد افراد در موضوعات مختلف، آنگونه که مد نظر کنترل‌کننده است فکر کنند. در نتیجه اقدامی را انجام خواهند داد که از ابتدا مطلوب عامل بحران بوده است. در این مثال، خود انسان‌ها به‌عنوان پدیده‌های هوشمند شناخته می‌شوند و سیستم فرماندهی – کنترلی که قصد اخلال در آن وجود دارد، نظام پردازشی و تحلیلی افراد است. از این رو مشخص می‌شود منظور از سیستم‌های فرماندهی – کنترل، صرفاً ماشین‌های دیجیتال و هوشمندی که زیرساخت‌ها را کنترل می‌کنند نیست. در این نگاه حتی سلول‌های زنده نیز از طریق اخلال در سیستم فرماندهی – کنترل (هسته‌ی سلول) امکان فریب دارند که باعث می‌شود با صدور دستور اشتباه، حیات سلول را به مخاطره و نابودی کشاند. بسیاری از تهدیدات و بحران‌های بیولوژیک که در دسته‌ی بحران‌های نوظهور و نوپدید زیستی جای می‌گیرند، بر مبانی اخلال در سیستم فرماندهی – کنترل طراحی و اجرا شده‌اند که مخدرهای صوتی[18] و بیو رزونانس[19] از آن جمله هستند.

تمامی نمونه‌های فوق حاکی از آن است که منطق طراحی تهدید و بحران تغییر نموده و چهارچوبی نوین را رقم زده که تهدیدات و بحران‌های نوین، ابتناء بر آن دارند و آن چهارچوب «اخلال در سیستم‌های فرماندهی و کنترل» است.

حال بر این اساس در پاسخ به پرسش‌های پژوهش باید اذعان داشت اولاً سیستم‌های فرماندهی – کنترل، مبنا و پایه‌ی اصلی طراحی و اجرای تهدیدات و بحران‌های نوین را شکل می‌دهند، لذا هرگونه غفلت از این مهم موجب غافلگیری راهبردی در برابر تهدیدات و بحران‌های نوین است. ثانیاً تهدیدات مبتنی بر این چهارچوب نوین، از دقت، اثرگذاری، امکان کنترل و بازدارندگی بیشتری نسبت به نوع تهدیدات و بحران‌های سابق برخوردارند که آمادگی و مقابله با آنها را پیچیده‌تر می‌نماید. ثالثاً نیاز است برای حفظ کیفیت و کارآمدی در برابر بحران‌های نوین، مبانی نظری و عملی دانش مدیریت بحران، منطبق و در تناسب با منطق سایبرنتیک و سیستم فرماندهی – کنترل مورد بازنگری، بروز رسانی و ارتقاء قرار گیرد تا بتواند به بهترین شکل چهار گام مدیریت بحران را تبیین، تدوین و تنظیم نماید.

مراجع

۴-۱. منابع فارسی

۱- امیری، ا.، علوی‌وفا، ح.، و صادقی، م. (زمستان ۱۳۹۵). ***بررسی نقش فرهنگ دینی در مدیریت بحرانهای سیاسی (مطالعه موردی فتنه ۸۸)***. *مدیریت بحران و وضعیت‌های اضطراری*، ص ۱۱۱ الی ۱۴۲.

۲- محمدی، ایوب؛ یاوری، امیرحسین؛ جوانمرد، محمد. (بهار ۱۳۹۶). ***نقش شبکه‌های اجتماعی مجازی در ایجاد بحران‌های اجتماعی***. فصلنامه‌ی دانش انتظامی، ص ۱ الی ۲۴.

۳- شکوهیان‌راد، م. (۱۳۹۷). ***تهدیدات سایبری علیه سیستم‌های فرماندهی – کنترل***. تهران: اندیشگاه علم و صنعت (به‌سفارش ستاد کل نیروهای مسلح جمهوری اسلامی ایران).

[18] Digital Drugs

[19] Bioresonance

۴- تام برگهاردت، ترجمه سبزواری، م. (دی ۱۳۹۰). ***پیش درآمدی برای جنگ افزایش حملات سایبری با از سرگیری تهدیدهای نظامی و اشنگتن علیه ایران***. ماهنامه‌ی سیاحت غرب، شماره‌ی ۱۰۱، ص ۴۹ الی ۶۰.

۵- اکبری، ا. (تابستان ۱۳۸۹). ***نقش شبکه های اجتماعی در ایجاد و مهار بحران ها***. فصلنامه‌ی ره‌آورد نور. ص ۳۲ الی ۳۹

۶- شکوهیان‌راد، م. (۱۳۹۷). ***نظریه‌ی جنگ در عصر سیستم‌های فرماندهی - کنترل***. تهران: انتشارات مؤسسه‌ی آموزشی - پژوهشی شهید سپهبد صیاد شیرازی.

۷- صیوری، م. (۱۳۹۶). ***بحران و مدیریت بحران***. بازیابی از دانشگاه علوم پزشکی تبریز:

https://amouzesh.tbzmed.ac.ir/Uploads/User/44/آموزش٪۲۰ضمن٪۲۰خدمت٪۲۰بسته/بحران٪۲۰و٪۲۰مدیریت٪۲۰بحران.pdf

۸- فولادی، ک. (۱۳۹۴). ***طرح دکترینال امنیت فضای سایبر***. تهران: ستاد کل نیروهای مسلح جمهوری اسلامی ایران.

۹- حاذق نیکرو، ح، ۱۳۹۱، ***اهمیت فضای مجازی در نگاه فرماندهان و افسران جنگ نرم جبهه‌ی استکبار***. بازیابی شده مورخ ۱۳۹۴/۶/۲۵:

http://www.bultannews.com/fa/news/78343 /

۱۰- *اطلاعیه وزارت ارتباطات درباره حمله سایبری*. (۱۳۹۷، فروردین ۱۸). بازیابی از مشرق‌نیوز:

https://www.mashreghnews.ir/news/844597/اطلاعیه-وزارت-ارتباطات-درباره-حمله-سایبری

۱۱- *پروژه «تابستان داغ» این‌بار در بغداد/ چرا آشوب‌های عراق با اغتشاشات دی ماه ۹۶ ایران شباهت دارد؟*. (۱۳۹۸، مهر ۱۴). بازیابی از خبرگزاری آنا:

https://ana.ir/fa/news/19/429018/پروژه-تابستان-داغ-این‌بار-در-بغداد-چرا-آشوب‌های-عراق-با-اغتشاشات-دی-ماه-۹۶-ایران-شباهت-دارد

۲-۴. منابع انگلیسی

1- Bussoletti, F. (2018, April 18). *Syria has probably undergone a cyber attack as well as an offensive with missiles*. Retrieved from Difesa & Sicurezza:

https://www.difesaesicurezza.com/en/defence-and-security/syria-has-probably-undergone-a-cyber-attack-as-well-as-an-offensive-with-missiles/

2- CLARK, C. (2018, April 24). *Russia Widens EW War, 'Disabling' EC-130s OR AC-130s In Syria*. Retrieved from Breaking Defense:

https://breakingdefense.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/

3- Coughlin, C. (2010, AUGUST 20). *Who's blowing up Iran's gas pipelines?* Retrieved from Activist Post:

https://www.activistpost.com/2010/08/whos-blowing-up-irans-gas-pipelines.html

4- Khalifa, E. (n.d.). *Military Cyber Threats: Transformations in Unconventional Security Threats*. Retrieved from Academia: https://www.academia.edu/10137546/Military_Cyber_Threats_Transformations_in_Unconventional_Security_Threats

5- MG, M. (2015). Ebola Virus Disease: A Perspective for the United States. *The American Journal of Medicine*, Abstract.

6- Nakasone, P. (2018, April 11). *Military Set for Cyber Attacks on Foreign Infrastructure*. Retrieved from Belfer Center:

https://www.belfercenter.org/publication/military-set-cyber-attacks-foreign-infrastructure

7- STOCKTON, N. (2018, 7 26). *Much of the US Electric Grid Could Go the Way of the Landline Phone*. Retrieved from Wired:

https://www.wired.com/story/electric-grid-rising-costs-renewables/

8- THOMPSON, M. (2016, March 24). *Iranian Cyber Attack on New York Dam Shows Future of War*. Retrieved from Time:

https://time.com/4270728/iran-cyber-attack-dam-fbi/

9- ZETTER, K. (2016). *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*. Retrieved from Wired:

https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/